

El nuevo escenario informático

Uno de los cambios más sorprendentes del mundo de hoy es la rapidez de las comunicaciones. Modernos sistemas permiten que el flujo de conocimientos sea independiente del lugar físico donde nos encontremos. En ese sentido, ya no sorprende la transferencia de información en tiempo real o instantáneo y debido a que el conocimiento es poder; para adquirirlo, las empresas se han unido en grandes redes internacionales para transferir datos, sonidos e imágenes, y realizar el comercio en forma electrónica, con objeto de ser más eficientes. No obstante, al unirse en forma pública se han vuelto vulnerables, pues cada sistema de computadoras involucrado en la red es un blanco potencial y apetecible para obtener información.

El escenario electrónico actual en el cual las organizaciones enlazan sus redes internas a la Internet, crece a razón de más de un 10% mensual. Al unir una red a la Internet se tiene acceso también a las redes de otras organizaciones. De la misma forma en que accedemos a la oficina del frente de nuestra empresa, se puede recibir información de un servidor en Australia, conectarnos a una supercomputadora en Washington o revisar la literatura disponible desde Alemania. Del universo de varias decenas de millones de computadoras interconectadas, no es difícil pensar que pueda haber más de una persona con perversas intenciones respecto de una organización. Por ello, es fundamental tener protegida adecuadamente la red.

Con mayor frecuencia se encuentran noticias sobre la violación de redes de importantes organizaciones por criminales informáticos desconocidos. A pesar de que la prensa ha destacado que tales intrusiones son solamente obra de adolescentes con propósitos de entretenerse o de jugar, ya no se trata de un incidente aislado de una desafortunada institución. De manera permanente se reciben reportes de los ataques a redes informáticas, los que se han vuelto cada vez más siniestros: los archivos son alterados subrepticamente, las computadoras se vuelven inoperativas, se ha copiado información confidencial sin autorización, se ha reemplazado el software para agregar “puertas traseras” de entrada y miles de contraseñas han sido capturadas a usuarios inocentes; por mencionar algunas cuestiones.

Los administradores de sistemas requieren horas y a veces días enteros para volver a cargar o configurar nuevamente sistemas comprometidos, con el objeto de recuperar la confianza en la integridad de éstos. No hay manera de saber los motivos que tuvo el intruso, y debe suponerse que sus intenciones son de lo peor. Aquella gente que irrumpe en los sistemas sin autorización causa mucho daño, aunque sea solamente para mirar su estructura, incluso sin que hubieran leído la correspondencia confidencial y sin borrar ningún archivo.

De acuerdo con un estudio de la Consultora “Ernst and Young” que integra a más de mil empresas, un 20% reporta pérdidas financieras como consecuencia de intrusiones en sus computadoras (Technology Review, Abril 95, pág. 33). Ya pasaron los tiempos en que la seguridad de las computadoras era sólo un juego o diversión.

1. QUÉ ES UN VIRUS

Es un pequeño programa escrito intencionalmente para instalarse en la computadora de un usuario sin el conocimiento o el permiso de éste. Se dice que es un programa parásito porque ataca a los archivos o sector de arranque (boot sector) y se reproduce a sí mismo para continuar su esparcimiento.

Algunos se limitan solamente a reproducirse, mientras que otros pueden producir serios daños que pueden afectar a los sistemas. Se ha llegado a un punto tal, que un nuevo virus llamado W95/CIH-10xx. o también CIH.Spacefiller (puede aparecer el 26 de cada mes, especialmente 26 de junio y 26 de abril) ataca al BIOS de la PC huésped y cambia su configuración de tal forma que se requiere modificarlo. Nunca se debe asumir que un virus es inofensivo y dejarlo “flotando” en el sistema.

Existen ciertas analogías entre los virus biológicos y los informáticos: mientras los primeros son agentes externos que invaden células para alterar su información genética y reproducirse, los segundos son programas-rutinas, en un sentido más estricto, capaces de infectar archivos de computadoras y reproducirse una y otra vez cuando se accede a dichos archivos, por lo que dañan la información existente en la memoria o en alguno de los dispositivos de almacenamiento de la computadora.

Tienen diferentes finalidades: algunos sólo “infectan”, otros alteran datos, otros los eliminan y algunos sólo muestran mensajes. Pero el fin último de todos ellos es el mismo: *PROPAGARSE*.

Es importante destacar que *el potencial de daño de un virus informático no depende de su complejidad sino del entorno donde actúa.*

Un virus es un programa que cumple las siguientes pautas:

- Es muy pequeño.
- Ejecutable o potencialmente ejecutable.
- Se reproduce a sí mismo.
- Toma el control o modifica otros programas.
- Convierte otros objetos ejecutables en clónicos víricos.

1.1 Cómo trabaja un virus

Por lo general, los virus se encuentran en la parte final del programa para infectarlo; es decir, modifican su correcto funcionamiento y por supuesto, incrementan el tamaño de éste. Son pequeños pedazos de código que por sí solos no significan nada, por lo que deben encontrar un lugar donde puedan reproducirse para así continuar su ciclo de vida. El lugar donde pueden reproducirse es en el sector de arranque, en los programas ejecutables o en ambas partes. Otros programas considerados como virus son los macrovirus los cuales infectan archivos de información; la aparición de éstos generó alarma en los ámbitos de seguridad informática, puesto que rompían una parte del paradigma establecido en el cual los archivos que podían ser infectados por virus eran solamente los ejecutables o potencialmente ejecutables (.EXE, .COM, .BAT, .PIF, .SYS, etc.). En la actualidad la mayoría de los macrovirus están escritos con el lenguaje de programación de macros del Microsoft

Office para Windows (recordemos que el Word Basic es un subconjunto del lenguaje Visual Basic) y pueden ser desarrollados para cualquiera de sus aplicaciones (Word, Excel y Access). Los macrovirus cumplen también con la norma D.A.S. (Daño, Autorreproductores y Subrepticios).

Los virus necesitan tener el control sobre sí mismos y el programa anfitrión para que puedan funcionar. Es por esta razón por lo que se añaden en el punto de inicio de un proceso a realizarse o punto de entrada del archivo, de esta manera, antes de que se pueda ejecutar el código del programa, se ejecuta el del virus.

El virus se reproduce cuando el ambiente es apropiado para “activarse” esto es: una fecha específica, a una hora determinada, por cierta cantidad de ejecuciones, por el tamaño del archivo de información o por una combinación de teclas. Éstas son las condiciones necesarias para que causen daño.

1.2 Propiedades de los virus

Además de la característica principal de estos programas, que es su facultad de duplicación, existen otras particularidades de los virus, como son las siguientes:

Modifican el código ejecutable: aquí aparece el adjetivo “contagio”. Para que un virus contagie a otros programas ejecutables, debe ser capaz de alterar la organización del código del programa que va a infectar.

Permanecen en la memoria de la computadora: cuando un usuario, inocente de las consecuencias, ejecuta en su computadora un programa con virus, éste se acomoda en la memoria RAM, con objeto de adueñarse de la computadora, y por así decirlo, tomar el mando.

Se ejecutan involuntariamente: un virus sin ejecutar es imposible que dañe una computadora. En ese momento está en reposo, en modo de espera, necesitando de alguien que ejecute el programa “portador”.

Funcionan igual que cualquier programa: un virus, al ser un programa de computadora, se comporta como tal, en ese sentido necesita de alguien que lo ponga en funcionamiento, si no, es software que estará solamente almacenado en un dispositivo magnético.

Es nocivo para la computadora: esto depende del virus con el que tratemos. Podemos encontramos con programas que destruyen parcial o totalmente la información, o bien programas que tan solo presentan un mensaje continuo en pantalla, el cual aunque no hace daño al final es muy molesto.

Se ocultan al usuario: claramente, el programador del virus desea que el usuario no lo advierta durante el máximo tiempo posible, hasta que aparece la señal de alarma en la computadora. Conforme pasa el tiempo, los virus van generando más y mejores técnicas de ocultamiento, pero también se van desarrollando los programas antivirus y de localización.

1.3 Orígenes

Los virus tienen la misma edad que las computadoras. Ya en 1949 John Von Neumann, describió programas que se reproducían a sí mismos en su libro “Teoría y Organización de Autómatas Complicados”. Es hasta mucho después que se les da el nombre de virus.

Antes de la explosión de la microcomputación se decía muy poco de ellos. Por un lado, la computación era secreto de unos pocos; por otro lado, las entidades gubernamentales, científicas o militares, que vieron sus equipos atacados por virus, se quedaron calladas, para no demostrar la debilidad de sus sistemas de seguridad, que costaron millones, al bolsillo de los contribuyentes. Las empresas privadas como bancos, o grandes corporaciones, tampoco podían decir nada, para no perder la confianza de sus clientes o accionistas. Lo que se sabe de los virus desde 1949 hasta 1989, es muy poco.

Se reconoce como antecedente de los virus actuales, un juego creado por programadores de la empresa AT&T, quienes desarrollaron la primera versión del sistema operativo Unix, en los años 60. Para entretenerse y como parte de sus investigaciones, crearon un juego, llamado “Core War”, que tenía la capacidad de reproducirse cada vez que se ejecutaba. Este programa tenía instrucciones destinadas a impedir el correcto funcionamiento de la memoria.

Al mismo tiempo, elaboraron un programa llamado “Reeper”, el cual destruía las copias hechas por Core Ware, un antivirus o antibiótico, en nuestra terminología actual. Conscientes de lo peligroso del juego, decidieron mantenerlo en secreto y no hablar más del tema. No se sabe si esta decisión fue por iniciativa propia o por órdenes superiores.

En 1982, los equipos Apple II comenzaron a verse afectados por un virus llamado “Cloner” que presentaba un mensaje en forma de poema.

Al año siguiente, 1983, el Dr. Ken Thomson, uno de los programadores de AT&T, que trabajó en la creación de “Core War”, rompió el silencio acordado, y dio a conocer la existencia del programa, con detalles de su estructura, en una conferencia ante la Asociación de Computación.

La Revista Scientific American a comienzos de 1984, publicó la información completa sobre esos programas, con guías para la creación de virus. Éste es el punto de partida de la vida pública de estos aterrantísimos programas, y naturalmente de su difusión sin control, en las computadoras personales.

Por esa misma fecha, 1984, el Dr. Fred Cohen hace una demostración en la Universidad de California, presentando un virus informático residente en una PC. Al Dr. Cohen se le conoce actualmente, como “el padre de los virus”. Paralelamente aparece en muchas PC's un virus, con un nombre similar a Core War, escrito en Small-C por un tal Kevin Bjorke, que luego lo cede a dominio público. ¡La cosa comienza a ponerse caliente!

El primer virus destructor y dañino plenamente identificado que infecta muchas PC's aparece en 1986. Fue creado en la ciudad de Lahore, Paquistán, y se le conoce con el nombre de BRAIN. Sus autores vendían copias pirateadas de programas comerciales como Lotus, Supercalc o Wordstar por sumas bajísimas. Los turistas que visitaban Paquistán, compraban esas copias y las llevaban de vuelta a los Estados Unidos de Norteamérica. Las copias pirateadas llevaban un virus. Fue así, como infectaron mas de 20 mil computadoras. Los códigos del virus Brain fueron alterados en los

Estados Unidos, por otros programadores, dando origen a muchas versiones de éste, cada una de ellas peor que la precedente. Hasta la fecha nadie estaba tomando en serio el fenómeno, que comenzaba a ser bastante molesto y peligroso.

Comienza la lucha contra los virus

En 1987, los sistemas de correo electrónico de la IBM, fueron invadidos por un virus que enviaba mensajes navideños y que se multiplicaba rápidamente. Ello ocasionó que los discos duros se llenaran de archivos de origen viral, y el sistema se fuera haciendo lento, hasta llegar a paralizarse por mas de tres días. El problema había llegado demasiado lejos y el Big Blue puso de inmediato a trabajar en los virus a su Centro de Investigación Thomas J. Watson, de Yorktown Heights, NI.

Las investigaciones del Centro T. J. Watson sobre virus, fueron puestas en el dominio público por medio de reportes de investigación, editados periódicamente, para beneficio de investigadores y usuarios.

El virus Jerusalem, según se dice creado por la Organización de Liberación Palestina, es detectado en la Universidad Hebrea de Jerusalem a comienzos de 1988. El virus estaba destinado a aparecer el 13 de mayo de 1988, fecha del 40 aniversario de la existencia de Palestina como nación. Una interesante faceta del terrorismo, que ahora se vuelca hacia la destrucción de los sistemas de cómputo, por medio de programas que destruyen a otros programas.

El 2 de noviembre de 1988, dos importantes redes de Estados Unidos se ven afectadas seriamente por virus introducidos en éstas. Más de seis mil equipos de instalaciones militares de la NASA, universidades y centros de investigación públicos y privados se ven atacados.

Para 1989 la cantidad de virus detectados en diferentes lugares sobrepasa los 100, y la epidemia comienza a crear situaciones graves. Una de las medidas tomadas para tratar de detener el avance de los virus, es llevar a los tribunales a Robert Morís Jr. acusado de ser el creador de un virus que infectó a computadoras del gobierno y empresas privadas. Al parecer, este muchacho conoció el programa Core Ware, creado en la AT&T, y lo difundió entre sus amigos. Ellos se encargaron de diseminarlo por diferentes medios a redes y equipos. Al juicio se le dio gran publicidad, pero no detuvo a los creadores de virus. La cantidad de virus que circula en la actualidad es desconocida.

Los virus conocidos son el resultado de investigaciones sobre programas autorreproductivos, que se habían iniciado a principios de los 80. La teoría básica de los “virus” fue expuesta en 1985 por Fred Cohen, en una memoria de titulación de la Universidad del Sur de California. Poco después se publicaba a nivel mundial el primer libro sobre el “Virus, enfermedad de los computadores”, de Ralf Burger. Este autor, al no poder apoyar sus tesis en pruebas concretas, desarrolló su propio virus y lo distribuyó a los 200 asistentes a una conferencia sobre el tema. En 1987, la revista Pixel publicó el código de un virus redactado en Basic. Seis meses después un virus pakistaní infectaba por primera vez una universidad: la de Delaware, en Estados Unidos.

En realidad, los creadores de éste (ingenieros pakistaníes) no pretendían hacer daño alguno. Su inofensivo virus (sólo reemplazaba el nombre de volumen del disquete por “Brain”) contenía incluso sus nombres, dirección y teléfono. Y se sorprendieron grandemente cuando supieron adonde había “viajado” su virus, ¡de disquete en disquete! Y más aún de la histeria que se desató a través de la prensa norteamericana.

1.4 Desarrollo del fenómeno virus

En los últimos años, el área informática ha experimentado un vertiginoso crecimiento, y con esto, los programas que las compañías distribuyen alcanzan con mayor rapidez el periodo de madurez. Hace algunos años, los usuarios comenzaron a grabar los programas, debido al alto precio de éstos, lo que llevó a los programadores de virus a encontrar el principal modo de distribución. Podemos, por otro lado, enunciar otras fuentes de desarrollo de los virus como son las redes, el freeware y shareware, las BBS, y la aparición de programas sencillos de creación de virus.

1.5 Ciclo de vida de los virus

Los virus son creados por un programador y colocados en programas ejecutables, de esta forma el contagio se inicia por uso de estos programas infectados. La forma de transmisión se realiza por medio de programas, usuarios, computadoras o red, si las condiciones son propicias como sería la utilización del programa en una fecha determinada. Por último, algunos programas de virus se modifican a sí mismos para no ser detectados.

2. CLASIFICACIÓN DE LOS VIRUS

Se intentará presentarle las ramas de esta gran familia, atendiendo a su técnica de funcionamiento:

- ***Bug-ware***

Son programas totalmente legales que realizan una serie de tareas concretas, por ejemplo, probadores de hardware o incluso antivirus. Si no se conoce bien su manejo, o tienen una programación complicada, pueden producir daños al hardware de la computadora o al software. Durante el año 1989 existieron muchas denuncias por parte de los usuarios en el sentido de que había aparecido un virus que actuaba en el procesador de textos *Wordperfect*. Llegó a dársele incluso un nombre: el *virus WP*. Más tarde se comprobó que las fallas eran debidas a la ignorancia de los usuarios, que llenaban la RAM de cadenas sueltas, por no conocer bien el manejo del programa. Es bien sabido que la computadora es el aparato tecnológico que más averías reales o aparentes recibe por la negación de sus dueños a leer el manual.

Queremos decir con esto, que los bug-ware no son virus. Parecen, pero no lo son. En un 90% de los casos, el virus es el mismo usuario.

- ***Caballo de Troya***

Es llamado como el caballo de Troya de la mitología griega. Los antiguos griegos eran incapaces de derrotar al ejército de Troya debido, entre otras razones, a las superiores capacidades tácticas y de combate del ejército troyano. Tras una larga y sangrienta batalla, el ejército griego parecía estar derrotado y retiró sus fuerzas. Después apareció un magnífico caballo de madera a las puertas de Troya, presumiblemente una oferta de paz del ejército griego a los ciudadanos de Troya. Se abrieron las puertas de Troya y el caballo de madera fue introducido para que todos lo vieran. La comunidad se regocijó con su victoria sobre los griegos.

Cuando cayó la noche y continuaban los festejos, un contingente de guerreros griegos salió del caballo de madera a través de una escotilla situada en el fondo y se abrió paso hasta las puertas de la ciudad. Los guerreros griegos abrieron las puertas e hicieron señales a los barcos que aguardaban. El ejército griego, con el elemento de la sorpresa de parte suya, invadió Troya y redujo a cenizas la ciudad.

Un caballo de Troya parece ser una aplicación inocente y útil que luego se revela como maligna. No hay nada que impida que se sigan realizando las misiones “benignas” de la aplicación original. Lo que sucede es que alguien ha desensamblado el original y ha añadido unas instrucciones de su colección. Una gran cantidad de virus informáticos en las primeras épocas se “incubaban” en una primera fase como caballos de Troya. Hoy en día a este tipo de programas los llamamos droppers o gérmenes. De todas formas, salvo en casos mixtos un caballo de Troya no se puede reproducir; su reproducción es la propia copia del programa por parte del usuario, así, depende totalmente del elemento sorpresa para actuar, y una vez localizado... la justicia se presenta bajo la forma de la orden DELETE del MS-DOS. Respecto a los programas inocentes que producen daños en la computadora, hablaremos de “Los doce del patíbulo (The dirty dozen)” y del “Hacked Report”, por ello para evitar inconvenientes con estos programas, lo mejor que puede hacer es no piratear.

- ***Camaleón***

Es un primito del caballo de Troya. Actúa como un programa parecido a otro de confianza, pero produciendo daños. La diferencia está en que el programa no se basa en uno ya existente, sino que diseña otro completamente nuevo. Esta técnica se utiliza, no en programas comerciales, sino en aplicaciones concretas. Bien programados son difíciles de eliminar pues reproducen fielmente al programa al que imitan. Un programa camaleón puede utilizarse, por ejemplo, para desviar los céntimos de las transacciones bancarias a una cuenta determinada; en este caso, lo mejor que puede hacer ante este tipo de técnica es... llamar a la policía.

- ***Bombas lógicas***

Actúa según un determinado tipo de condiciones técnicas. Imagine un virus que se haga presente cuando por ejemplo, haya un determinado número de megas ocupados en el disco duro; no suelen ser autorreproductores, ni se propagan de una computadora a otra. Es interesante observar la filosofía con la que están diseñados, en la cual existe un segmento de código maligno dentro de un programa aparentemente normal, que se mantiene latente sin ser detectado durante un tiempo determinado.

- ***Bomba de tiempo***

Parecido al anterior. Se conocen dos versiones: la que actúa en determinadas fechas, como un *Viernes 13*, o la que se activa tras una serie determinada de ejecuciones. Un ejemplo de esto sería también el virus del *moroso*, si una empresa no paga un programa legal, se activa el virus.

- ***Joke-program***

Ahora ya no se les ve mucho. Eran virus (se reproducían e infectaban) pero no producían realmente daños a la computadora, simplemente eran molestos. Seguro que le suena el *Virus de la Galleta*, o el *Come-come*, o el de la *Cadena*... Su época pasó, porque estaban diseñados en 8086 y con la aparición del 80286 se les acabaron los buenos tiempos. La fabricación de Joke-programs es el primer paso de un programador en el camino hacia los virus.

- ***Conejo***

También conocido como "*Peste*". En una red se puede dar un tipo determinado de trabajo que denominamos "*multitarea*", consiste en que las distintas órdenes (correo, impresiones, compilaciones...) siguen un orden determinado formando lo que conocemos como una "cola". De esa forma se ejecuta primero una, luego otra, y así sucesivamente mientras las que no se están ejecutando permanecen en la "cola" en una especie de lista de espera. Dentro de una red se pueden especificar preferencias para determinados usuarios que se saltan la "cola" por encima de otros.

Se puede dar el caso de que un alumno fabrique un programa para evitar todo lo anterior. Cuando le llegue el turno, su programa se dedicará a reproducirse de forma infinita, colapsando la red, y por lo tanto evitando cualquier posible preferencia de otro usuario; esto sería un programa *conejo*. La mayoría se autodestruyen una vez que han actuado.

- ***Gusanos***

No son exactamente virus informáticos, pero se les confunde frecuentemente con ellos, incluso en algunos casos se ha llegado a utilizar esta denominación como sinónimo de virus. Se dan en redes, de tal forma que se trasladan de una a otra terminal, se reproducen sólo si es necesario para el trabajo para el cual sido diseñados. Viajan a través de una red reuniendo información (contraseñas, direcciones, documentos...); también dejan mensajes, en su mayoría burlones, antes de desaparecer. No es raro que borren toda clase de vestigio de su paso por la red para no ser detectados por los operadores de sistema. De hecho, creemos que ya casi no se diseñan.

- ***Leapfrog o “Rana”***

Es un programa parecido al *Gusano* que a partir de una serie de datos conocidos, como la clave de acceso a una cuenta y el nombre de usuario, se dedica a recopilar información reservada. No tiene porque destruirse luego.

- ***Máscara***

Este programa asume la identidad de un usuario autorizado y realiza así las mismas labores del anterior, en realidad se considera una variante.

- ***Mockinbird***

Espera en un sistema de forma latente, interceptando las comunicaciones en el proceso de **login** o entrada. En ese momento se mete en la cuenta y comienza a actuar sin interferir en las operaciones lícitas que se estén realizando.

- ***Spoofing***

Una variación del anterior, observa lo que hace el usuario y lo repite de forma maliciosa buscando el bloqueo del sistema.

- ***Virus***

Básicamente, y sin entrar en más explicaciones, todo aquel programa que modifica maliciosamente a otro colocando una copia de sí mismo dentro de éste. Existen varias técnicas para conseguir esto:

- a) **Stealth**

Normalmente un virus realiza cambios al ejecutar su código, así puede ser detectado por un antivirus. Sin embargo, un virus puede camuflar dichos cambios para evitar la detección; en este caso el virus debe permanecer residente en memoria. Por supuesto, esto lo convierte en detectable por otros medios, pero no muy complicados. Un ejemplo claro de este tipo de virus es el veterano *Brain*. Para evitar problemas en la detección conviene utilizar previamente un disco o discos de sistema originales y, por supuesto, protegidos contra escritura. Asimismo, es recomendable emplear programas-herramienta originales y protegidos hasta la total erradicación del virus. De todas

formas, un *Stealth* poderoso es difícil de diseñar, pues sólo alcanza su máxima efectividad cuando está activo en memoria.

b) Tunnelling

Es una técnica que surgió de los anteriores. Para hacer fácil la explicación, podríamos decir que el virus averigua los puntos de vigilancia (interrupciones) que controla el antivirus y “pasa” tranquilamente por delante del sistema de defensa utilizando puntos (llamadas o funciones) no vigilados. Desde el punto de vista del programador, requiere conocimientos amplios de ensamblador.

c) Polimórfico

Cuando intentamos acabar con un virus, debemos vigilar todos los posibles lugares donde éste pueda esconderse. Llamamos a todo programa que cumpla con esta vigilancia “escáner”. Un virus polimórfico intenta escapar del escáner produciendo variadas copias totalmente operativas de sí mismo. Un método por ejemplo, es hacer una encriptación del código con una variación de los signos (leyendo un desplazamiento fijo en la tabla de Ascii). Otro método es producir varias rutinas de encriptación siendo sólo una visible (descriptor) en algún instante determinado. De hecho, más que un virus, es una técnica de encriptación. Actualmente, hay polimórficos muy sofisticados. El *Tremor* admite casi seis millones de variaciones.

Un virus bastante sofisticado de este tipo es el V2P6 del MSDOS, que varía la secuencia de instrucciones de sus copias con “basura” a la cabecera del virus (instrucciones de No Operación, o una instrucción que cargue un registro no usado con un valor arbitrario, mover 0 a A...). Por ello, el antivirus debe ser capaz de detectar una cadena muy concreta del virus. Existen también los MfE o compilador de polimórficos. En realidad no es un virus, sino un código que “muta” a otros virus que pasen por delante de él. Si la computadora está limpia no causa ningún daño.

La aparición de estos virus puso las cosas un poco difíciles a los antivirus entonces existentes, por la obligatoriedad de ser muy precisos en la detección.

d) Annored

Usan trucos especiales para hacer la búsqueda, desensamblaje y lectura de su código más difícil. Un buen ejemplo es el virus *Whale* (Ballena).

e) Companion (spawning)

Algunos no los consideran exactamente como virus, porque no se unen a un código de programa. Se aprovechan de una particularidad del MS-DOS hacia los ejecutables. En MS-DOS existen tres tipos de ejecutables: EXE, COM y BAT. Jerárquicamente un BAT se ejecuta con preferencia sobre un COM y éste sobre un EXE. Así se evitan problemas en caso de que aparezcan, por ejemplo, un WP.COM y un WP.BAT a la vez. Este tipo de virus, si ve que el programa se llama, por ejemplo, PEPE.EXE, crea un PEPE.COM dentro del cual va el código maligno. No son muy molestos y para eliminarlos basta con borrar el archivo del virus.

2.1 Por las formas en que se manifiestan

¿Pero cómo localizo un virus en mi computadora si las técnicas de ocultamiento son tan avanzadas? A continuación se explican los síntomas de infección más característicos de un virus:

Las computadoras personales se usan todos los días, a veces durante muchas horas, y los usuarios llegan a conocerlas íntimamente. Los usuarios están sintonizados con el flujo y reflujo de determinadas operaciones, reteniendo en el recuerdo la mayoría de éstas. Ellos conocen cuánto tardan las unidades de disco en almacenar ciertos archivos. Ellos saben cuando las operaciones van a ir despacio o velozmente. Los usuarios serios reconocen si sus PC's están funcionando bien. Al mismo tiempo, los usuarios pueden «sentir» cuando sus computadoras no están corriendo a la par.

Es posible (aunque no es recomendable) identificar a las computadoras infectadas con código de virus sin recurrir al uso de software sofisticado de protección y detección antivirus, pero los directores de sistemas y los usuarios finales deben aprender a reconocer los síntomas de aviso de las infecciones víricas. Los sistemas que muestren algunos de los rasgos listados en la sección siguiente, deben ser comprobados inmediatamente por diagnosticadores víricos expertos, especialmente cuando se evidencie más de una peculiaridad o cuando algunas computadoras muestren síntomas análogos.

Indicios de aviso de los virus informáticos

La siguiente es una lista de indicios comunes de avisos de virus informáticos:

- Las operaciones informáticas parecen lentas.
- Los programas tardan más de lo normal en cargarse.
- Los programas acceden a múltiples unidades de discos cuando antes no lo hacían.
- Los programas dirigen los accesos a los discos en tiempos inusuales o con una frecuencia mayor.
- El número de sectores dañados de disco aumenta constantemente.
- Los mapas de memoria (como la orden MEM del DOS 4.0) revelan nuevos programas TSR (residentes en memoria) de origen desconocido.
- Programas que normalmente se comportan bien, funcionan de modo anormal o caen sin motivo.
- Los programas encuentran errores donde antes no los encontraban.
- Programas aparentemente benignos, de «travesuras» divertidas se materializan misteriosamente y nadie reconoce haberlos instalado. Por ejemplo, agujeros negros, pelotas que rebotan, caras sonrientes o caracteres alfabéticos «lluviosos» empiezan a aparecer en la pantalla.
- Desaparecen archivos misteriosamente.
- Los archivos son sustituidos por objetos de origen desconocido o por datos falseados.

- Nombres, extensiones, fechas, atributos o datos cambian en archivos o directorios que no han sido modificados por los usuarios.
- Aparecen archivos de datos o directorios de origen desconocido.
- CHECKUP (u otro sistema de detección de virus) detecta cambios en objetos estáticos (archivos). Los cambios detectados en objetos dinámicos (archivos que se espera que cambien periódicamente, como archivos de datos de documento y de hojas de cálculo) no son necesariamente indicios de actividades víricas.
- Cambios en las características de los archivos ejecutables. Casi todos los virus de archivo, aumentan el tamaño de un archivo ejecutable cuando lo infectan. También puede pasar, si el virus no ha sido programado por un experto (típico principiante con aires de hacker), que cambien la fecha del archivo a la fecha de infección.
- Aparición de anomalías en el teclado. Existen algunos virus que definen ciertas teclas, las cuales al ser pulsadas, realizan acciones perniciosas en la computadora. También suele ser común el cambio de la configuración de las teclas, por la del país donde se programó el virus.
- Aparición de anomalías en el video. Muchos de los virus eligen el sistema de video para notificar al usuario su presencia en la computadora. Cualquier desajuste de la pantalla o de los caracteres de ésta, nos puede notificar la presencia de un virus.
- Se modifican el Autoexec.bat y el Config.sys. En ciertas ocasiones, los virus modifican dichos archivos para adaptarlos a su presencia, al igual que las aplicaciones de software.
- Reducción del tamaño de la memoria RAM. Un virus, cuando entra en una computadora, debe situarse obligatoriamente en la memoria RAM, y por ello ocupa una porción de ella. Por tanto, el tamaño útil operativo de la memoria se reduce en la misma cuantía que tiene el código del virus.
- Desaparición de datos. Esto es consecuencia de la acción destructiva para la que son creados casi todos los hermosos virus. Depende de la maldad del virus si se borran con la orden DEL, o mediante el uso de caracteres basura, lo que hace imposible su recuperación.
- El disco duro aparece con sectores en mal estado. Algunos virus usan sectores del disco para camuflarse, lo que hace que aparezcan como dañados o inoperativos.
- Aparición de mensajes de error inesperados. Lo más normal, es que en ciertos virus, el sistema operativo produzca errores inusuales, cosa que debe alertar al usuario.
- Reducción del espacio disponible del disco. Ya que los virus se van duplicando de manera continua, es normal pensar que esta acción se lleve a cabo sobre archivos del disco, lo que lleva a una disminución del espacio disponible por el usuario.

2.2 Por las zonas que afectan

Y ahora explicaremos un poco las distintas clases de virus desde el punto de vista del lugar donde atacan:

- ***BSI***

Contaminador del Sector de Arranque (Boot Sector Infector). Son los más comunes entre los virus de PC, los más peligrosos y por regla general los que más fácilmente se destruyen una vez detectados.

Cuando deseamos poner a funcionar nuestra computadora, bien desde el disco duro o desde el disquete de arranque, la computadora debe seguir una serie de instrucciones vitales para su funcionamiento, que obviamente se ejecutan en primer lugar. Algunas funciones, por su complejidad o dificultad de ejecución, se almacenan en la BIOS (Basic Input/Output System), sucediendo que muchos usuarios ni siquiera saben que existen estos procesos.

Todos estos archivos le indican a la computadora cómo realizar las funciones rutinarias.

El lugar donde se almacenan todas estas instrucciones se conoce como sector de arranque del disco (Boot). Un virus que altere o infecte de algún modo el sector de arranque será llamado BSI.

Infectar un sector de arranque ofrece múltiples ventajas para un virus-maker. Por una parte, el virus controlará el sistema de forma total porque se carga con el mismo sistema al conectar la computadora. De este modo el virus será lo primero que se ejecute antes que cualquier otro software. Pueden permanecer residentes en todo momento e incluso impedir el típico reseteo con CTRL-ALT-DEL. También, pueden falsear el tamaño de los archivos infectados para que un antivirus comparador no detecte cambios.

Un viejo truco para borrar un virus de este tipo cuando no se tiene una vacuna a mano es el siguiente: utilice unas utilidades Norton o unas Pctools o un programa Tool que le permita editar de alguna forma el Boot del disquete. En un disco limpio la parte final del Boot presenta (visible en Ascii) una serie de frases de error. Si el disco está infectado, estas frases no aparecerán, estando sustituidas por toda una serie de signos Ascii raros. Borre "a pelo" el Boot sustituyéndolo por ceros y grabe el cambio. Se supone que esto lo ha hecho arrancando antes de ejecutar el programa Tool desde una disquetera con un DOS limpio y protegido contra escritura. Una vez grabado el cambio, el virus habrá desaparecido, pero usted no tendrá Boot.

De lo anterior se deduce que este método nunca debe ser utilizado en disquetes de sistema (bootables). La falta de Boot en un disco de datos no suele ser peligrosa, y en último caso puede reponer un Boot limpio utilizando por ejemplo el Doctor Disco de las utilerías Norton, o cualquier programa similar.

En caso de doble disquetera, otro truco es (previa arrancada como describimos anteriormente), colocar el disco infectado en la unidad B: y desde A: con el disco del sistema operativo, ejecutar la orden SYS B: con lo que el virus será borrado al crearse un nuevo Boot. De todas formas el método anterior es más efectivo, sólo que éste sí puede usarse con discos bootables.

- **CPI**

Contaminador del procesador de órdenes. (C.P u's Infector). Existen múltiples versiones del sistema operativo DOS (MS-DOS, IBM-DOS, PC-DOS...). Básicamente los archivos de DOS pueden ser divididos en dos categorías. Tenemos archivos de apoyo al sistema de bajo nivel y archivos de programas de interfaz de usuario de alto nivel.

También tenemos una serie de archivos “ocultos” que se llaman IBMDOS.COM e IBMBIO.COM o bien IO.SYS y MSDOS.SYS según la versión de DOS. Los más comunes son los dos primeros. Estos archivos están protegidos contra escritura para evitar manipulaciones y permanecen ocultos, de tal forma que no aparecen ante una orden de directorio. Estos archivos sólo se activan ante la BIOS incorporada a la computadora.

Los programas centrales del procesador de órdenes se encuentran en el archivo COMMAND.COM. Este archivo se carga inmediatamente después del proceso de arranque. El COMMAND.COM interpreta las órdenes del usuario y avisa cuando no lo entiende. Todo virus que infecte archivos de órdenes centrales como el COMMAND.COM se denomina CPI's.

Para un virus-maker esto ofrece una gran ventaja, pues muchas de las órdenes que el usuario introduce en la computadora, deben pasar por el COMMAND.COM. Así, el contaminador posee un total dominio de todos los procesos que se vayan produciendo. No es pues nada raro que esta clase de virus se extienda con una enorme rapidez por el disco duro. Tampoco es extraño que un virus tipo BSI sea al mismo tiempo CPI. De todas formas un CPI se instala un poco después que un BSI, exactamente al final del proceso de arranque. Esto le hace perder una mínima parte de poder, pero no por ello deja de ser peligroso.

Un método para acabar con un CPI sería (previo arranque con sistema limpio), la sustitución inmediata del COMMAND.COM infectado del disco duro, teniendo cuidado de que el nuevo COMMAND.COM sea de la misma versión que el antiguo. Este truco sólo funciona nada más al aparecer la infección, pues como hemos dicho, estos virus se extienden con rapidez, y por lo tanto una vez extendido, es más difícil erradicarlos que solo cambiar el COMMAND.COM.

- ***GPI***

Contaminador de Propósito General (General Purpose Infector). Estos virus no están diseñados precisamente para infectar un determinado tipo de archivo de sistema, aunque nada impide que puedan hacerlo. Como ya hemos sugerido antes, no es raro que un virus tenga varias de esas propiedades. En algunos casos un GPI puede estar limitado a un tipo de archivo, como por ejemplo EXE y COM, que al ser ejecutables resultan más propicios. También son rápidos en la propagación.

Una vez extendidos resultan muy difíciles de erradicar, y el mejor método en este caso es una vacuna.

- ***MPL***

Contaminador Multipropósito (Multi Purpose Infector). Estos virus integran todas las características de los tres anteriores, resultando muy peligrosos.

Infectan en primer lugar los sectores de arranque y procesadores de órdenes, extendiéndose luego a archivos ejecutables, aprovechando en principio los ubicados en la memoria RAM (por haber sido cargados en el AUTOEXEC.BAT o en el CONFIG.SYS). Al tener varias propiedades aumenta su vida operativa. Al igual que el anterior, se impone una buena vacuna.

- ***FSI***

Contaminador de Archivo Específico (File Specific Infector). De forma similar que los CPI restringen las infecciones a archivos determinados. Podríamos distinguir dos tipos: los producidos por venganza (el típico empleado despedido que deja uno de éstos para fastidiar a la compañía), o bien alguien con una fijación por un lenguaje de programación (caso del virus *Dbase, Pascal...*). Se suele producir un pequeño retraso cuando el virus busca a su víctima pero nadie suele darse cuenta, una vez localizada ésta, la borran o le destrozan el formato.

- ***MRI***

Contaminador Residente en Memoria (Memory Resident Infector). Los BSI y CPI se pueden englobar como MRI, puesto que ambos permanecen activos en la memoria mientras se ejecutan. Pueden disfrutar de algunas de las ventajas de los CPI y BSI, ya que siempre están cargados y activos interfiriendo en todas las operaciones informáticas. Las salidas de pantalla e impresión pueden ser interceptadas, así como los archivos de datos, que resultan corrompidos.

2.3 Por su grado de mutación

Podemos distinguir varios tipos de virus polimórficos, por su tipo de encriptación:

- a) Oligomórfico que lleva un número fijo de descriptores, como por ejemplo el Whale (30 descriptores).
- b) Los que utilizan un descriptor con registros variables, como el Flip.2153.A.
- c) Polimórficos totales o puros, como el Tremor.
- d) Virus permutantes, que sólo varían algún signo de la cadena, como el Fly.
- e) Virus generados por el sistema de encriptación NukeE (NED), como el Tester.
- f) Virus basados en el Dark Avenger (MtE), como el CoffeShop.
- g) Virus basados en el sistema de encriptación Trident (TPE), como el Girafe.
- h) Virus basados en el Dark Slayer (DSME), como el Teacher.
- i) Virus basados en el Dark Angel (DAME), como el Trigger.
- j) Virus basados en el sistema Mark Ludwig (VME), como el Demo.

3. MÉTODOS DE PREVENCIÓN

Aunque las defensas técnicas son determinantes para combatir a los virus de las computadoras en el ambiente moderno, la historia ha demostrado que ningún método técnico por sí solo, es efectivo para proteger la información. Los sistemas son usados por personas, quienes deben tomar decisiones acerca de qué métodos utilizar y cómo emplearlos. En las defensas no técnicas, nos referimos a las políticas y procedimientos relacionados con la conducta humana, a las limitaciones de las técnicas debido al uso que hacemos de éstas, y a las acciones legales como castigo, disuasión y compensación.

3.1 Utilización en común limitada

La utilización en común limitada es una defensa técnica y de procedimiento porque en la gran mayoría de los ambientes de computación modernos, los usuarios hacen uso de información aunque las defensas técnicas traten de impedirlo. Por otra parte, muchas organizaciones emplean formas no técnicas de utilización en común limitada, sin proporcionar capacidades técnicas para hacer cumplir la política.

La utilización en común limitada restringe de manera efectiva la diseminación de los virus, si se usa de manera adecuada, pero casi ninguna organización lo efectúa de esta manera.

Aislamiento durante el ataque

Una estrategia general consiste en el aislamiento durante el ataque. En la IBM se dice que cuando se detecta un ataque en la red, “desconectan la clavija”. Eso no significa que estén a salvo. Si un virus se ha diseminado durante seis meses y causa daño hoy, desconectar la clavija de la red no ayuda. Por otra parte, si el ataque no es sutil ni lento, desconectar la clavija podría ayudar.

En muchas organizaciones no poseen una clavija, son 50 o más. Si va a optar por el aislamiento, tiene que saber cómo hacerlo. Debe haber alguien que sepa dónde está la clavija y requiere un plan de contingencia en el lugar para asegurar que la clavija se pueda desconectar. En la mayoría de las grandes organizaciones actuales, desconectarse de la red global resultaría desastroso, pues no tendrían acceso a los servicios, de modo que hay una relación entre utilidad y seguridad.

Separación de la función

Respecto a la separación de investigación y desarrollo de producción, se señalan muchos de los problemas y características de este método en la sección de control de cambios.

El disco AIDS

Es fundamental una política que no permita disquetes o cintas externos en las instalaciones, además de requerir que se verifiquen todos los programas que ingresen en una central de distribución u otros métodos de procedimiento similares. Esto nos remite a la historia del disco AIDS.

En 1989, uno de los más grandes intentos de extorsión a gran escala se inició cuando decenas de miles de disquetes infectados se enviaron a las personas que aparecían en la lista de correos de una revista de computación. Muchos de esos suscriptores trabajaban en empresas cuya política prohibía

el uso de “disquetes externos”. A pesar del control administrativo, hubo organizaciones donde cientos de usuarios pusieron estos disquetes en sus sistemas y los infectaron. Estas empresas pagaron varios meses-hombre de esfuerzo para deshacerse del problema, porque los empleados no respetaron la política establecida.

En este caso, el perpetrador fue atrapado porque los encargados de la lista de envíos tenían un registro de las personas que rentaban dichas listas y finalmente, por eliminación llegó al origen. Por desgracia, la captura del atacante no limitó el daño o compensó a las víctimas.

Prohibidos los discos externos

Un empleado llegó a la empresa con un disquete en la mano. El guardia de seguridad dijo: —“¿No leyó el memo? No se permite la entrada de disquetes externos”—. El empleado respondió: —“Éste no es un disquete externo, es interno. Me lo llevé a casa anoche y hoy lo traigo de regreso”—. El problema es que el empleado no comprendió lo que significaba la política de “prohibidos los discos externos”. Si va a utilizar controles administrativos y de procedimientos, debe educar a sus empleados para que sepan la importancia que tienen y por qué se establecen. Es común que esto no se haga. Se crea un reglamento sin ocuparse por explicarlo y las personas lo interpretan a su modo o lo ignoran.

Centrales de distribución

Otra técnica común es hacer que todo el software pase por una central de distribución antes de emplearlo dentro de la empresa. Ésta es una regla sensata, aunque sólo sea para asegurar que programas nuevos interactúen adecuadamente con el ambiente actual; no es una defensa eficaz contra los virus desconocidos, pero es el lugar idóneo para usar la tecnología de exploración. Aun cuando no detecte virus nuevos, será eficaz contra algunos ya conocidos y tendrá un costo muy bajo porque sólo se emplea en una unidad central. Por último, tales sistemas fallan porque, en la práctica, tienen problemas ocasionales y, si es el único mecanismo de defensa en el sistema, un error puede llegar a ser desastroso. Es demasiado frágil para depender de él.

Limitación de las fuentes de información

La eliminación del tablero de avisos es económica y bastante común como procedimiento de defensa. Algunos tableros de avisos tienen la fama de anunciar caballos de Troya, pero en la mayoría de los casos proporcionan información valiosa y vale la pena suscribirse a ellos. Una política común es la de “prohibido compartir”. Se darán algunos datos históricos. Ninguna distribución legítima de software o shareware de dominio público ha contenido algún virus hasta donde se sabe, pero casi todos los principales fabricantes de software comercial han repartido un virus en una distribución de software legítima, mientras varios fabricantes de hardware han distribuido discos con sistemas operativos precargados que contenían virus. Una revista especializada en PC distribuyó varios miles de copias de un virus entre sus lectores. Un importante distribuidor europeo de software electrónico distribuyó 60 mil copias de un virus entre sus clientes porque su analizador de virus no lo detectó. Así que, si vamos a tomar una decisión firme con base en los datos históricos, debemos establecer la política de comprar shareware y software de dominio público para evitar las infecciones virales y nunca comprar software “legítimo” envuelto en celofán.

Con seguridad, existen buenas razones para que el shareware y el software de dominio público nunca hayan sido infectados por algún virus. Cuando compra shareware o software de dominio público tiene el

nombre del autor, el cual está inscrito en ese software, por lo tanto tiene una muy buena razón para asegurarse de que esté bien, debido a que está en juego su reputación. Por otra parte, si trabaja para Microsoft e introduce un virus, nadie sabrá quien lo hizo y su nombre no aparecerá en el registro de derechos de autor. ¿Por qué iba a preocuparse si causa problemas? Por último, tratar de manejar la protección en un ambiente donde usted es el único que escribe un programa es muy fácil. En cambio, mantener la protección en un ambiente con miles de programadores no es tan sencillo. La probabilidad de que un virus se introduzca en un producto de Microsoft es mucho mayor que en el software de una empresa pequeña.

3.2 Controles administrativos

Los controles administrativos en general resultan muy baratos y por ello, son ineficaces. El problema principal parece ser que un solo error u omisión en la aplicación de una política puede ocasionar un colapso generalizado. A pesar de esta situación, el bajo costo de los controles administrativos los justifica como suplemento de las defensas técnicas.

El procedimiento no es efectivo como control de cambios, pero funciona en un sentido. Si es jefe en una corporación pública, sería responsable por no tomar las medidas adecuadas. Ahora tiene a quien correr.

3.3 Verificación interna

La verificación interna ha sido casi completamente ineficaz como defensa contra los virus y ha tenido un éxito mínimo en el rastreo de los atacantes. El primer problema es que las pistas de verificación interna existentes, no guardan información suficiente para seguir el progreso de un virus.

Muchos sistemas tienen dispositivos de control de acceso para informar de los intentos por violar los controles de acceso, pero un virus no tiene que hacer nada que no esté autorizado, de modo que este tipo de rastreo es ineficaz; sólo detecta ataques que no estén muy bien escritos.

Después, se tiene el análisis postmortem (es decir, después de muerto), el cual funciona bien, sólo que demasiado tarde. Ya sabe, llama al verificador, quien viene y le dice que su sistema computarizado no funciona y trata de establecer lo que está corrupto en el proceso. Puede ser la única forma de restablecer el sistema a su estado normal, pero en algunos casos tarda meses en resolverse y usted está fuera del negocio mientras se realizan las reparaciones.

3.4 Problemas en la red punto por punto

Ya se mencionó que los métodos de procedimientos tienden a presentar fallas, pero en ocasiones tales errores son bastante sutiles. Un ejemplo es el problema en las llamadas “redes de iguales”. Una red de iguales es aquella en la que dos “iguales” en diferentes lugares físicos en la red tienen derechos de acceso similares. El problema que presentan es que al volver equivalentes a los iguales en ubicaciones distribuidas, también lo efectúa en todos los mecanismos de protección relacionados con esos iguales. Debido a que la cadena de protección sólo es tan fuerte como el eslabón más débil, el proceso anterior distribuye la debilidad, de cualquier ubicación entre todos sus iguales.

Ya vimos un incidente de esta naturaleza en un importante departamento del gobierno Estados Unidos. Se establecieron estándares uniformes en toda la organización, pero un sitio tenía defensas de procedimientos muy estrictas y el otro poseía mayores defensas técnicas. Como resultado, un

virus entró en un sitio y, por medio de la red, se transmitió a un área equivalente en otro. Una vez establecida la infección, regresó vía la infección de iguales.

El virus Internet y la tarjeta de Navidad fueron eficaces porque operaban en redes iguales con problemas muy similares, y la mayoría de los virus que actúan en un solo sistema lo realizan en redes de iguales porque están diseñadas para que el proceso sea transparente.

Para que las defensas funcionen, en especial en las redes de iguales, los métodos y procedimientos deben ser uniformes o equiparables, lo cual plantea un problema, debido a que los procedimientos los realizan personas. Es muy difícil hacer que personas en dos lugares distintos físicamente hagan lo mismo, debido a las diferencias culturales y personales.

Respaldos de información

¿Qué es respaldar? Es copiar la información contenida en algún dispositivo a otro medio magnético de almacenamiento.

Esto es, si se tiene información almacenada en el disco duro de la computadora es recomendable copiarla a disquetes flexibles, a una cinta o a un cartucho removible, pues estos dispositivos se pueden almacenar en un lugar seguro.

Los respaldos como defensa

Los respaldos a menudo se recomiendan como un aspecto importante en la defensa contra los virus y se está de acuerdo en que, sin otras defensas en la ubicación, éstos son útiles contra la mayoría de los ataques, pero no están exentos de problemas. Como se señaló anteriormente, los respaldos son un refugio seguro para los virus y ello representa un problema considerable de diseminación y limpieza, pero hay muchos otros problemas con los respaldos en el ambiente actual:

- No siempre funcionan. Uno de los problemas principales es que los respaldos no aseguran la conveniencia de lo que respaldan.
- No se guardan el tiempo suficiente.
- Actúan como refugios seguros para los virus.

Al proporcionar refugio seguro para los virus, se debe estar seguro de lo que se respalda y consciente de que si tiene virus, éste se almacenará también. Al recuperar el respaldo, éste estará infectado y se volverá a contagiar la computadora.

Software de prevención

Un sistema de prevención intentará parar el virus en el mismo momento en que se produzca el ataque. Al respecto, un buen método es el de impedir el acceso al sistema a programas o usuarios que no dispongan de autorización.

Es necesario que un programa de éstos sea residente en memoria, o sea, en la RAM. De forma constante, se dedican a controlar las interrupciones del DOS para detectar el momento en que se produce una solicitud de actividad sospechosa. Si ésta se produce, salta inmediatamente en acción el

programa de seguridad informando de paso al usuario. Esto último se hace así, porque es posible que se trate de una operación benigna, en cuyo caso, debe ser el usuario quien decida.

Hasta hace poco, esta clase de sistemas no era de lo mejor del mundo. Por regla general ocupaban un espacio enorme de los 640 Kb de la memoria base, lo que provocaba que muchos usuarios prefirieran no instalar un programa vigilante.

Hoy en día, esto suele estar solucionado. Los programas generalmente ocupan no más de 20 Kb, e incluso en algunos casos los programas residentes vienen en forma de fichero SYS, con lo que se pueden instalar como un Device en el Config.sys. De todas formas, no se ha llegado aún a la perfección.

Productos certificados

El NCSA prueba y certifica que los exploradores de anti-virus pasen un número de pruebas rigurosas. En la evaluación se siguen los criterios siguientes:

- Pruebas realizadas por una organización independiente, así como por una organización imparcial.
- Pruebas realizadas con las últimas versiones de los productos.
- Se prueban la mayoría de los productos.
- Las diferentes plataformas de sistemas operativos son usadas en las pruebas.
- Las pruebas son publicadas.
- Expertos independientes son consultados.
- Grandes corporaciones que usan los anti-virus son consultados.
- Los resultados de las pruebas son publicados.
- La certificación puede ser revocada por fallas en el producto para mantener estos estándares.

El esquema de certificación de la NCSA para programas anti-virus puede ser consultada en la siguiente dirección de Internet.

<http://www.ncsa.com/avpdcert.html>

Dentro del software probado por NCSA, la lista proporcionada a continuación incluye las versiones más recientes disponibles al tiempo de prueba. Para la lista de todos los programas que desean obtener la certificación consulte la página de Internet.

Productos Certificados por NCSA	Tipos de Certificación		
	Demanda	Acceso	Limpiar
Computer Associates International (CAI)			
InoculateIT Personal Edition for Windows 95	Sí	Sí	Sí

InoculateIT Antivirus for Windows 95	Sí	Sí	Sí
InoculateIT for Windows NT Server	Sí	Sí	Sí
InoculateIT for NetWare	Sí	Sí	Sí
Vet Anti-Virus for DOS	Sí	Sí	
Vet Anti-Virus for Windows 3.x	Sí	Sí	
Vet Anti-Virus for Windows 95	Sí	Sí	
Vet Anti-Virus for Windows 98	Sí	Sí	
Vet Anti-Virus for Windows NT Workstation	Sí	Sí	
Vet Anti-Virus for NetWare	Sí	Sí	
<i>Data Fellows</i>			
F-Secure Antivirus for Windows 95	Sí	Sí	
Panda			
Panda Antivirus for DOS	Sí	Sí	
Panda Antivirus for Windows 3.x	Sí	Sí	
Panda Antivirus for Windows 95/98	Sí	Sí	Sí
Panda Antivirus for Windows NT Workstation	Sí	Sí	
Panda Antivirus for Windows NT Server	Sí	Sí	Sí
Panda Antivirus for OS/2	Sí	Sí	
Panda Antivirus for Netware	Sí	Sí	Sí
Symantec			
Norton AntiVirus for DOS	Sí	Sí	
Norton AntiVirus for Windows 3.x	Sí	Sí	Sí
Norton AntiVirus for Windows 95/98	Sí	Sí	Sí
Norton AntiVirus for Windows NT Workstation	Sí	Sí	Sí
Norton AntiVirus for Windows NT Server	Sí	Sí	Sí
Norton AntiVirus for NetWare	Sí	Sí	Sí
Norton AntiVirus for NT (AXP)	Sí	Sí	
NAV Corporate Edition DOS	Sí	Sí	
NAV Corporate Edition Windows 3.x	Sí	Sí	
Productos Certificados por NCSA	Tipos de Certificación		
	Demanda	Acceso	Limpiar
NAV Corporate Edition for Windows 95	Sí	Sí	
NAV Corporate Edition for Windows NT Workstation	Sí	Sí	
NAV Corporate Edition for Windows NT Server	Sí	Sí	
NAV Corporate Edition for Netware	Sí	Sí	
Trend Micro Inc.			
OfficeScan for Windows 95	Sí	Sí	
OfficeScan for Windows 98	Sí	Sí	
OfficeScan for Windows NT Workstation	Sí	Sí	

PC-cillin for Windows 95	Sí	Sí	
PC-cillin for Windows NT Workstation	Sí	Sí	
ServerProtect for Windows NT Server	Sí	Sí	
ServerProtect for NetWare	Sí	Sí	

Los productos listados anteriormente fueron probados en las plataformas mencionadas a continuación:

Plataforma	Versión
DOS	6.22
Windows	3.1
Windows 95	(4.00.950)
Windows 98	()
Windows NT Workstation	4.0
Windows NT Server	4.0
OS/2 Warp	3.0
NetWare	3.12

4. CONFIABILIDAD EN EL SOFTWARE DE PREVENCIÓN

Detección y erradicación de virus

4.1 Detección de virus

Los sistemas de detección comprueban el código del programa antes de ejecutarlo, de esta forma, el usuario podrá ser avisado de los posibles peligros del programa. Muchos de los programas antivirus del mercado integran ambos sistemas.

Se consideran dos sistemas de detección:

Detector antibomba. Explora archivos buscando rutinas peligrosas (órdenes de borrado de archivos, por ejemplo).

Detector antivirus. Un virus puede dejar rastros de su actividad, ahí es donde entran en escena esta clase de detectores. Son bastante eficaces, pues emplean algoritmos muy buenos. Existen dos tipos específicos:

a) Detectores de virus concretos

Buscan un número determinado de virus conocidos que llevan en su base de datos, por medio de lo que se conoce como “cadenas de detección”. El virus queda desde el primer momento identificado y se puede realizar una buena limpieza.

Inicialmente, un nuevo virus podría no ser detectado por este antivirus, pero hoy en día existen métodos para detectar los nuevos. Además, es obligatoria la renovación constante de esta clase de programas.

b) Detectores genéricos

Vigilan el tamaño de los archivos ejecutables.

El problema es que hay virus que pueden aumentar el tamaño de un archivo sin que se note, falseando dichos datos.

4.2 Comparando archivos

Los archivos tienen nombre, tipo, fecha y tamaño. Alguno de estos datos puede ser modificado al ser infectado, como podría ser el tamaño. En el sistema operativo se tienen programas que verifican si dos archivos tienen el mismo número de bytes, como sería el caso del DOS donde vienen programas de este tipo (DISKCOMP), los cuales comparan dos archivos supuestamente iguales byte a byte. Pueden detectar un cambio por pequeño que sea. Existen algunos realmente sofisticados que proporcionan incluso el offset donde comienza la diferencia, de éstos se tienen FC (File Compare) de las utilerías Norton.

Su mayor importancia radica en la fase previa del estudio de un virus. Con un programa de este tipo se puede averiguar dónde comienza éste y su tamaño, para de esa forma aislarlo y utilizar un antivirus.

4.3 Los programas antivirus

Inicialmente, cualquier sistema de seguridad es susceptible de ser invadido por un virus. Lo más normal es que un buen sistema de seguridad controle de manera óptima cualquier cambio producido en los archivos ejecutables.

Lo mejor que puede hacer ante cualquier duda sobre el sistema que debe elegir, es utilizar una copia de evaluación y elegir aquella que mejor se desempeñe. Pero fíjese que un buen antivirus no sólo debe ser de fácil manejo para usted, requiere una cantidad considerable de opciones de actuación y vigilancia para verificar que el programa en sí sea eficiente. Una forma válida de averiguar esto último, es comprobando su capacidad para detectar, no todos, pero por lo menos algún virus nuevo.

Considere lo siguiente:

- Compruebe que el manejo y la rapidez del antivirus sea lo bastante bueno como para que realice un “barrido” completo del disco duro, por lo menos una vez a la semana.
- Verifique que el programa y sus archivos de datos no queden residentes, por lo tanto al alcance de cualquier virus. Lo ideal es que el programa pueda ejecutarse desde un disquete, en ese sentido no utilice ningún archivo del disco duro para su funcionamiento.
- Compruebe que su ejecución sea exclusiva.
- Vea que vigile la mayor cantidad posible de archivos (ejecutables, de datos, overlays e incluso empaquetados).
- Debe comprobar los cambios en archivos ejecutables mediante CRC's (Cyclic Redundancy Checks).

Los programas antivirus se dividen en:

- a) *Programas de prevención.* Son aquéllos diseñados para interceptar el intento de acceso de un virus a la computadora mediante el monitoreo de la memoria, el sector de arranque y el área de archivos de modificaciones involuntarias.
- b) *Programas de detección.* Utilizan el proceso de identificación de un virus en la memoria, en el sector de arranque o en el área de archivos, mostrando en pantalla el nombre del virus, si existe alguno o bien, precisando que existe y no es conocido.
- c) *Programas correctivos.* Son aquéllos encargados de eliminar el virus, ya sea de la memoria, del sector de arranque o del área de los archivos.

Programas antivirus distribuidos comercialmente

- ***F-Prot Professional***

Integra una familia de productos encargados de rastrear, desinfectar, notificar y eliminar los virus a nivel cliente/servidor en las plataformas DOS, Windows, Windows 95, Windows NT, OS/2 y Netware. Se caracteriza por una detección y desinfección automática de los macrovirus, virus furtivos, polimórficos y de archivo, entre otros; además añade protección en tiempo real en cualquier plataforma o red y envía alertas virales por biper, fax, MHS Mail y SNMP a las estaciones de trabajo designadas en su red.

Asimismo F-Prot Professional para servidores bloquea el acceso de las estaciones detectadas/infectadas con virus; al tiempo que realiza programación de tareas de rastreo y desinfección para las horas de menos tráfico en la red.

En caso de encontrar virus, este producto despliega las instrucciones del usuario, además de que efectúa rastreos por inactividad de la red o PC. Esta familia de productos la componen:

- F-Prot Professional para DOS y Win 9.x.
- F-Prot Professional para Windows 95.
- F-Prot Professional para Windows NT.
- F-Prot Professional para Netware.
- F-Prot Professional para OS/2 Warp.

Compucilina de Solinfo

Es una herramienta preventiva, más que curativa, diseñada para mantener sus servidores y estaciones de trabajo libres de virus.

Es un sistema cuyo funcionamiento no depende del virus, es decir ofrece protección contra cualquier virus sin importar de cual se trate o de si es conocido o no.

La versión 5.1x conserva capacidades de seguridad, introducidas con las versiones anteriores; control de ejecución de software no autorizado; control de copia no autorizada del software protegido, diagnóstico rápido de virus en cualquier computadora con la mini-compucilina, además de propagación de revisiones periódicas en un equipo o en una red.

Con Compucilina también se pueden realizar los diagnósticos de consistencia lógica de discos duros y el control de acceso a la información del disco duro, lo cual permite definir hasta 32 usuarios para cada computadora.

Es un sistema que no afecta el desempeño de los equipos protegidos, ni genera alarmas innecesarias. Este producto se manifiesta cuando un virus real trata de atacar, en ese momento, genera un reporte con una historia detallada de todos los procedimientos que se llevan a cabo.

Otras de sus características son que la instalación en redes es totalmente automática, y con el programa disco es posible realizar diagnósticos de bajo nivel sobre los discos duros conectados a cualquier computadora.

El bloqueador de este antivirus restringe la ejecución de programas no autorizados; en tanto los algoritmos de detección de virus se mejoraron para que fuera mucho más rápido.

La mini-Compucilina solamente detecta y elimina virus conocidos, utilizando las últimas técnicas de antivirus tradicionales.

Con el despertador, esta función puede ser programada para que se active periódicamente y efectúe chequeos de todos los discos de una computadora.

InocuLAN de Cheyenne. División de Computer Associates

InocuLAN antivirus para Windows 95 es una tecnología de datos desarrollada específicamente para usuarios de Windows 95 en pequeñas empresas/oficinas en el hogar.

Este producto tiene una interfaz que facilita la protección antivirus para nivel de usuario; sus características adicionales incluyen la actualización de firmas antivirus, versiones mejoradas de software, un monitor de detección de virus en tiempo real y un asistente de limpieza de virus.

InocuLAN también incorpora apoyo a Microsoft Office 97, recuperación de desastres en un solo disco, una enciclopedia integrada de antivirus y apoyo para formatos encriptados y comprimidos.

Los Protection Suites mantienen libres de virus al Exchange Server y al Internet Information Server; con ello evitan que se propaguen a través del correo electrónico, las bases de datos de documentos o archivos bajados de Internet.

También codifica y autentifica datos sensibles para su transferencia escritorio a escritorio y respalda datos automáticamente. Está conformada por:

- Virus Scan. Detecta y elimina al 100% virus detectados en Internet, Intranets, macros, archivos de e-mail y de red.
- Protege a las PC de las applets destructivas de Java y ActiveX.
- PC Crypto. Utiliza una tecnología para codificación a 160 bits para proteger hojas de cálculo, mensajes de correo electrónico, documentación e información sensible a la que pueden acceder usuarios no autorizados.
- NetCrypto. Protege datos críticos de red, sin necesidad de administrar claves, lo que salvaguarda el nombre del usuario, palabras claves y correos electrónicos, entre otras cuestiones.
- QuickBackup. Respalda datos para desktop Windows 95.
- SecureCast. Automatiza la distribución Internet de los productos antivirus más recientes de McAfee.
- Bootshield. Protege la imagen del sector de arranque de la computadora, e inmediatamente reconoce cualquier modificación subsecuente. Advierte también al usuario de la presencia de cualquier virus en su computadora, con objeto de reiniciar su equipo y devolverlo de esa forma a su estado original.
- NetShield. Antivirus para servidores de red, amplía los servicios de seguridad sin arriesgar la operación de los servidores y se puede acceder a toda su funcionalidad desde una consola

bajo Windows. Una vez detectado algún archivo infectado, éste es marcado, aislado y eliminado, o simplemente se niega el acceso del virus, incluyendo macros de Word y Excel, sector de arranque, etcétera.

- WebScan. Provee protección a los servicios más comunes de Internet y correo electrónico. Permite la detección de virus genéricos y desconocidos del tipo de sector de arranque.
- WebShield. Detiene los virus en el Gateway.
- GroupShield. Antivirus para servidores de Exchange y Notes.

Norton Antivirus de Symantec

Norton Antivirus (NAV) ofrece protección automática contra virus para Windows 95, Windows NT, Windows 3.1 y estaciones de trabajo DOS. Esta solución resguarda todos los puntos de entrada de virus, incluyendo discos floppy compartidos, la Internet, anexos de e-mail y redes. Ofrece a los usuarios detección y reparación de virus, además de la protección contra virus desconocidos.

Norton Antivirus emplea tecnología heurística para analizar programas, detectar virus nuevos y desconocidos, por consiguiente, permite al usuario reparar el archivo infectado de inmediato.

La función Live Update de esta solución actualiza a los usuarios con las definiciones de virus más recientes, las cuales pueden programarse con anticipación.

ThunderByte de Microasist

ThunderByte elimina virus de archivos, sector de arranque y macro-virus para plataformas DOS, Windows 3.xx, Windows 95 y Windows NT, además de proteger los puntos de entrada para virus, incluyendo discos flexibles, redes, Internet y correo electrónico. Utiliza 4 Kbytes de memoria. Este antivirus se basa en siete métodos de detección, los cuales prevendrán que ningún virus afecte la información y funcionamiento de la PC:

- Análisis heurístico. Consiste en comparar una secuencia de código ejecutable en memoria, archivos o sector de arranque. Detecta virus conocidos y desconocidos.
- Reconocimiento de firmas. Cuenta con una base de firmas o huellas digitales suficiente, para detectar a la gran mayoría de virus.
- Análisis de integridad. ThunderByte indica si un archivo ha cambiado en relación con su tamaño, atributos, uso de memoria.
- Descriptación genérica.
- Detección automática.
- Creación de bitácora.
- Detección de macro-virus.
- Dentro de los procesos de corrección-prevencción, ThunderByte contempla tres aspectos:
 - a) Limpieza de archivos.
 - b) Protección del sector de arranque.

c) Detección y limpieza automática de macro-virus.

PC-cilling97

Es un sistema antivirus para Windows 95 e Internet, el cual incluye una protección de virus provenientes de servicios on line, como BBS e Internet, además de que utiliza la característica de monitor inteligente.

PC-cilling97 posee la habilidad de ajustar automáticamente el nivel de protección en función de la utilización de la PC. Este producto incorpora la tecnología que detecta y analiza virus desconocidos, polimórficos y aquéllos que incluyen técnicas de ocultamiento. También descubre virus antes de que puedan infectar archivos de sistema.

Enterprise Versión PC-cillin 4 en 1

Creado para soluciones antivirus en grandes corporaciones, integra en forma automática las plataformas DOS, Windows 3.x, Windows 95 y Windows NT Workstation; también cuenta con dos módulos principales: el administrador y el cliente; el primero se instala directamente en el servidor Netware o Windows NT Server y el módulo cliente se ubica en las estaciones de trabajo. Una vez instalado en la estación del usuario, PC-cillin realiza rastreos de virus en tiempo real, verificando la existencia de virus conocidos o desconocidos.

Además de la detección en tiempo real, cada cliente puede ejecutar rastreos manuales en cualquier momento o a intervalos preestablecidos por el administrador. Después de haber instalado la utilería de administración en el servidor, los clientes únicamente deben conectarse a la red para que se instale la protección en su sistema.

Server Proterct NT

Es la solución antivirus para proteger la información de servidores Windows NT. Realiza el chequeo automático del tráfico entrada/salida del servidor, además de que rastrea información almacenada en discos compartidos.

Entre las funciones que incluye están las siguientes: genera automáticamente mensajes de alerta configurables ante la detección de virus; rastrea archivos en distintos formatos de compresión; notifica al administrador de la red ante la detección de virus y posee una variedad de métodos de alerta.

Server Proterct NT puede configurarse para rastrear discos, directorios y archivos en cualquier momento. Permite la actualización automática en forma programada de todos los servidores a partir de un servidor actualizado, mediante FTP de Internet, conexiones a una BBS local o a través de disquete.

Server Proterct NT protege la información de servidores Novell Netware en una organización. Dentro de sus principales características destacan:

- Administración de dominio centralizada.
- Administración remota.

- Rastreo de virus en tiempo real.

Scan Mail for Microsoft Exchange

Detecta y elimina en tiempo real, virus en archivos adjuntos al correo electrónico e-mail, en el momento que lleguen a cualquier mailbox.

Scan Mail for Lotus Notes

Trabaja en tiempo real, detectando virus en archivos asociados al e-mail de Lotus Notes.

InterScan WebProtect

Es una solución antivirus y de seguridad diseñada para evitar infecciones de virus a través del servidor Microsoft Proxy. Este producto bloquea los Java Applets y Active X para suspender la ejecución de códigos peligrosos, para ello emplea un rastreo selectivo de archivos .JPG, GIF, JPEG, audio en tiempo real, animaciones, etcétera.

Dr. Salomon's Antivirus Toolking

Los productos de Dr. Salomon's Antivirus ofrecen diferentes herramientas que pueden ser utilizadas para generar una solución a la medida de sus necesidades. Cuenta con los siguientes anillos de protección:

- a) *Nivel 1.* Protección para terminales. Protege entradas de disquetes, archivos bajados de Internet, CD-ROM's y cualquier otro medio de almacenamiento. Esta solución soporta las plataformas Windows 3.x/DOS, Windows 95, Windows NT Workstation, OS/2 y Mac/System 7, mientras que los componentes son:
 - VirusGuard. Protección residente para MS-DOS en tan solo 9 Kb.
 - WinGuard. Repara de forma automática en cuanto detecta un virus y lo erradica, también avisa al administrador de la red si encontró virus.
 - FindVirus. Integra escáner bajo demanda para virus polimorfo y encriptado.
 - ViVerify. Incluye la función checksummer.
 - Scheduler. Programador de eventos.
 - Enciclopedia de Virus.
 - Magic Bullet. Disco con su propia rutina de arranque que puede emplearse para casos de emergencia, permitiendo al usuario arrancar en limpio y evitar una posible infección.
- b) *Nivel 2.* Protección para servidores. Monitorea las transacciones de archivos entre los clientes y el servidor, limpiando de forma automática y transparente para el usuario cualquier archivo que se escriba al servidor. Las plataformas soportadas son: Novell Netware, Windows NT Server, Dec Alpha NT, SCO UNIX y Sun Spare Solaris.

- Dr. Salomon's Antivirus Toolkit para Novell Netware es un sistema formado por 2NLMs nativos, FAM utilizado para llevar a cabo la limpieza de los archivos de forma transparente, mientras el usuario escribe o lee los archivos del servidor.
 - Salomon's Antivirus Toolking para Windows NT Server incluye NT Guard, un sistema similar a GinWard, además está diseñado para revisar las transacciones de archivos.
- c) *Nivel 3.* Protección para Groupware, además de limpieza en e-mail en forma automática y transparente.

4.4 Crear un disco de arranque

El primer paso en la detección y lucha contra un virus, instalado en un sistema de cómputo, es el de preparar un disquete que contenga los programas del sistema operativo necesarios para dar inicio el sistema desde la unidad A. El disquete deberá contener al menos, los siguientes programas:

- MSDOS.SYS
- IO.SYS
- COMMAND.COM
- SYS.COM
- FORMAT.COM
- FDISK.EXE
- CHKDSK.EXE
- DELTREE.EXE
- XCOPY.EXE

Posteriormente, debe dar formato al disquete en un equipo que no esté contaminado de la siguiente forma:

Format a: /s

Esto copiará los archivos MSDOS.SYS, IO.SYS y COMMAND.COM; los otros archivos localícelos en MS-DOS en su directorio \DOS o en Windows 95 en el directorio \windows\command y deberá pasarlos al disco con el comando copy o con el explorador de Windows.

La mayor parte de los programas antivirus permiten preparar un disco para detectar los posibles virus en su disco duro, para esto remítase al manual del producto. Este disquete debe protegerse contra grabación. La mayor parte de los programas antivirus, se distribuyen bajo el concepto de shareware lo que le permite probar los programas antes de comprarlos, una vez realizado lo anterior lo puede adquirir con licencia en alguna tienda de productos de cómputo.

4.5 Procedimiento recomendado para la correcta eliminación de virus

1. Apagar la computadora.

Iniciar el sistema desde la unidad A:, para ello se utiliza un disquete especialmente preparado y completamente libre de infecciones.

2. Correr desde A: el programa detector y eliminador de virus.
3. Seguir las instrucciones del programa y del manual correspondiente.

Efectos de algunos virus

- a) *Monkey*. Conocido también como stoned y empire. Simula un fallo total en disco duro, los usuarios suponen que éste ha tenido un error importante, ya que Windows no corre en la computadora y al tratar de arrancar simplemente “congela” la máquina.
- b) *Concept*. Es uno de los macrovirus, de nueva generación, que afectan a Word de Microsoft. Este virus modifica la función Guardar como.
- c) *Antiexe*. Es un virus no destructivo del sector de iniciación que puede causar daños accidentales de los archivos.
- d) *AntiCMOS*. Borra la información almacenada en un chip CMOS programable, donde se encuentran los datos de la PC.
- e) *Form*. Es un virus del sector de carga; el 18 de cada mes, marca a los sectores del disco duro como dañados, hace sonar las teclas cuando se presiona y visualiza un mensaje que no se puede reproducir.
- f) *Stealth*. No produce daños tangibles, pero después de haberse prendido la computadora, el virus utiliza su control de la memoria del semiconductor principal de la PC para esconderse. Aparentemente, puede afectar algunas de las operaciones de Windows.
- g) *Junkie*. Un virus “multipartito”, lo que significa que infecta archivos al igual que el sector de iniciación del disco duro. Puede causar conflictos de memoria.
- h) *El one_half*. Codifica la información del disco duro, así el virus puede leer los datos allí contenidos. Cuando la codificación del disco duro ha llegado a la mitad, despliega en pantalla el mensaje “one_half”. Si se intenta suprimir un virus sin el software antiviral adecuado, se perderán todos los datos debido a la eliminación de la clave de codificación.
- i) *Sat_Bug.Natas*. No causa daños, pero puede ser incompatible con el software de administración de memoria de la PC. Este virus está ampliamente difundido en México.
- j) *Ripper*. También conocido como Jack Ripper, corrompe los datos escritos en el disco duro pero sólo una vez de cada minuto.
- k) *WIN A HOLIDAY*. Este virus se filtra vía correo electrónico y borra toda la información del disco duro al leerlo. (Fuente: Contraloría).
- l) *AOL*. Solo se menciona que es muy peligroso y que no tiene remedio. (Fuente: Contraloría).

Es un virus que se filtra vía correo electrónico RETURNED OR UNABLE DELIVER. Ataca directamente a todos los componentes al intentar leerlo.

4.6 Cómo eliminar virus

Virus de archivo

- Arranque la computadora con un “disquete de arranque 100% libre de virus”. El arranque de la computadora debe ser total, es decir, no es suficiente realizarlo con las teclas Ctrl + Alt + Supr.
- Emplear un antivirus además de probar el disco duro, todos los disquetes y unidades de soporte magnético utilizados en ese sistema. El antivirus desinfectará todos los virus. Si no se contara con antivirus, se podría proceder a eliminar los archivos que con certeza están contaminados, sustituyéndolos por archivos originales procedentes de las copias de seguridad.

Virus de sector de arranque

- Arranque la computadora con un “disquete de arranque 100% libre de virus”. El arranque de la computadora debe ser total, es decir, no es suficiente realizarlo con las teclas Ctrl + Alt + Supr.
- Utilice un antivirus o en caso de no ser capaz éste de desinfectar el virus, reemplace los archivos de sistema por otros que sepa con certeza que están limpios. Puede hacer esto usando el comando Sys c: desde un disquete de arranque del sistema y con ese comando del sistema operativo.

Virus de tabla de partición

- Arranque la computadora con un “disquete de arranque 100% libre de virus”. El arranque de la computadora debe ser total, es decir, no es suficiente realizarlo con las teclas Ctrl + Alt + Supr.
- Utilice un antivirus o en caso de no poder éste desinfectar el sistema, destruya la tabla de partición y genere una nueva, motivo por el cual luego tendrá que recuperar todos los datos desde los backups.

5. RECUPERACIÓN DE DISCOS DAÑADOS

5.1 Herramientas para hacer un respaldo

Si la computadora presenta problemas con virus, éstos se eliminan con un antivirus. Si el sistema operativo quedó dañado se necesita hacer una copia de la información en un medio magnético, estando seguros de que no tiene virus.

¿Pero qué es un respaldo de información?

Un respaldo de información, al cual nos referiremos en adelante simplemente como respaldo, es una copia de los archivos ubicados en el disco duro a algún medio diferente a éste, el cual puede ser disquetes, cintas, unidades removibles u otro disco duro.

Un disco duro es un medio magnético de almacenamiento masivo de información, los datos pueden estar grabados y ser sensibles a daños por diversas causas; en un disco duro significa la pérdida total o parcial de la información contenida en un archivo o archivos, y ante algún daño, el único recurso para recuperar la información viene a ser una copia actualizada de ésta, es decir el respaldo actualizado de la información.

Causas que pueden originar daños en la información contenida en un disco duro

- Falla de la computadora. Como toda máquina no está exenta de fallas, algunas de éstas pueden repercutir en el contenido del disco duro.
- Falla en el disco duro. El disco duro es un componente mecánico y electrónico, sujeto a fallas mecánicas al grado de ya no funcionar, el cual por sus características de construcción algunas veces no permite reparación alguna.
- Fallas en el suministro de energía eléctrica. Si la computadora no cuenta con un sistema de los llamados de energía ininterrumpible, una falla en el suministro de energía ocasiona que la computadora no trabaje adecuadamente, lo cual impacta en el funcionamiento del disco duro y daña la información.
- Virus en la computadora. Existen virus cuyo objetivo es dañar el contenido de un disco duro. Algunos de éstos van dirigidos a dañar el FAT del disco duro, que es el área donde se guarda la ubicación de los archivos grabados, al dañarse este espacio es poco probable la recuperación de archivo alguno del disco.
- Errores de operación del usuario. También puede perderse información del disco duro por problemas en la operación por parte del usuario, como pueden ser: apagar accidentalmente la computadora a la mitad de un proceso o usar erróneamente los comandos del sistema operativo para borrar, dar formato o copiar.

5.2 Estrategias para hacer un respaldo

Todos los usuarios de sistemas de cómputo deben desarrollar un plan para respaldar regularmente los datos de sus computadoras. Se recomienda a cada usuario responsable del manejo de una computadora en su oficina, la realización de estos respaldos con objeto de que esta labor se efectúe de manera cotidiana. El periodo de respaldo debe hacerse basándose en la cantidad de actividad del sistema. Algunos usuarios encuentran que requieren de respaldos diarios, y otros consideran que

uno semanal es más conveniente. Los respaldos raramente son programados en periodos de más de una semana. Algunos usuarios establecen un plan mixto: ejecutan respaldos de disco semanalmente y respaldos diarios únicamente de los archivos que cambian.

Procedimientos de respaldo

Usted debería de respaldar en un dispositivo removible como un cartucho o cinta, el cual pueda sacarse de una unidad y guardarse en un lugar seguro.

Los respaldos efectuados en una unidad no removible, como un disco duro, están más propensos a daños.

Por el costo relativamente bajo de los discos duros, algunos usuarios desafortunadamente instalan dos discos duros en su computadora y respaldan uno con el otro. Algunos usuarios dividen un simple disco duro en dos particiones y respaldan una partición con la otra. Esta clase de “respaldos” se conocen como FALSOS, por el hecho de que si el sistema fuera sujeto a una pesada descarga de energía eléctrica o caída de voltaje, incendio, o cualquier otra clase de daño, el contenido de ambas unidades podría perderse parcial o totalmente.

Lo más conveniente es que ejecute sus respaldos en un plan rotativo. Se recomienda utilizar un sistema de respaldo de cinta o de unidad removible con un mínimo de tres cintas o cartuchos removibles por unidad o por PC, en las cuales respalde los datos de la primer semana en la primer cinta y la segunda semana en la segunda cinta. De esa manera, si la segunda cinta sufriera algún daño, podría utilizar el respaldo de la cinta de la semana anterior, para restaurar la información. La tercer semana, utilice la tercer cinta y guarde la primer cinta en un sitio donde pueda protegerse de incendio, robo, inundaciones o cualquier otro desastre. En la cuarta semana, empezará a rolar cada cinta, así que utilizará nuevamente la cinta uno. Esta opción detallada es aplicada si usted es de las personas que requiere respaldar semanalmente, en caso contrario si desea realizarlo diariamente puede aplicar este mismo rol de las tres cintas utilizándolas a diario, una cada día, rolándose después del tercer día.

En tanto, si el programa es para una actividad especial debe incluir una opción que permita respaldar todos los archivos relacionados con el programa, o bien que ubique todos aquéllos que tienen que ver con el programa en un subdirectorío específico. Posteriormente debe respaldar todo este subdirectorío en disquetes mediante el comando BACKUP del sistema operativo DOS, o el programa MWBACKUP de Windows.

Archivos específicos relacionados con programas de aplicación general:

Todos aquellos archivos generados con programas de aplicación general (Word, Excel, Power Point, etc.) pueden ser respaldados teniendo la costumbre de guardar la información tanto en el disco duro como en disquete, con la opción misma de “guardar” del programa, o bien con los comandos Copy y Xcopy del Sistema Operativo o con Explorador de Windows. A continuación describimos cómo hacer un respaldo utilizando estas herramientas en MS-DOS o Windows.

Debido a su gran capacidad de almacenamiento, un disco duro se encuentra organizado por directorios, éstos a su vez pueden contener subdirectorios y así sucesivamente. Para respaldar los archivos contenidos en un subdirectorío se necesita especificar todo el camino a seguir (PATH) para encontrarlos. Por ejemplo:

C:\NOMINA\REPORTES

La “C:” nos indica que se emplea el disco duro, la diagonal inversa “\” significa que son directorios. De esta forma para indicar el directorio raíz o principal se haría con C:\.

Esto sólo muestra el camino a seguir para encontrar los archivos. Para seleccionar aquéllos que se requieren respaldar se tienen que especificar sus nombres, se sugiere que para indicar todo un grupo de archivos se utilice el asterisco (*). Como posiblemente habrá notado, todos los archivos poseen un nombre y una extensión en el formato XXXXXXXX.XXX. Por ejemplo, un trabajo hecho en EXCEL podría llamarse “RELACION.XLS”, o uno hecho en Microsoft WORD (procesador de palabras) “CARTA.DOC”.

Mediante el uso del asterisco se pueden seleccionar diversos archivos, por ejemplo:

- Todos los archivos que se llamen “Disc”: DISC.*
- Todos los archivos que inician con “A”: A*.*
- Todos los archivos del subdirectorio sin excepción: *.*

Como se puede observar, el asterisco funciona como comodín, en ese sentido puede tomar cualquier valor. De esta forma, después de conocer como indicar el camino y seleccionar archivos, se utiliza para respaldar el comando BACKUP. Éste es útil cuando el número de archivos a respaldar son muchos o contienen demasiada información. En caso de ser pocos archivos y mínima la información que contienen (lo cual no significa que no sea importante) se utiliza el comando COPY. Cualquiera de los dos comandos anteriores copiará los archivos a la unidad de disco flexible (disquete) que se le indique, de la siguiente manera:

BACKUP [camino][Archivo Fuente][unidad de disquete] o

COPY [camino][Archivo Fuente][unidad de disquete]

La diferencia estriba en que el comando BACKUP solicitará disquetes conforme se vayan llenando, a diferencia del comando COPY el cual simplemente abortará el respaldo si no caben en uno solo.

La unidad de disquete se identifica generalmente como A:, aunque puede usarse B: para respaldarse a una segunda unidad en caso de existir ésta.

Por ejemplo, para respaldar la información de TODOS los archivos de un directorio llamado NOMINA:

BACKUP C:\NOMINA*.* A: o

COPY C:\NOMINA*.* A:

En este caso se recomienda emplear el comando BACKUP pues seguramente se trata de mucha información. En la descripción anterior, el comando BACKUP es para el sistema operativo MS-DOS, en el caso de Windows 95 se hace lo siguiente:

En Windows se incluye un programa que podrá utilizar para hacer copias de respaldo de los archivos del disco duro en un disquete, unidad de cinta u otro equipo de la red.

Para ejecutar Backup, haga clic en el botón “Inicio”, elija Programas, Accesorios y Herramientas del sistema y localice el ícono Herramientas de seguridad.

Si no se encuentra éste, presione el botón “Inicio”, seleccione Configuración, Panel de Control, Agregar o quitar programas, posteriormente elija la opción Instalación de Windows y de las alternativas existentes marque Herramientas para disco y dé un clic en el botón Aceptar; le va a pedir el CD-ROM de Windows 95, el programa es muy amigable y lo va a conducir por pasos para hacer su respaldo de la información.

Generalmente se tiende a pensar que no puede encontrarse un virus en la computadora, que eso sólo les sucede a quienes manejan mucho su equipo. No lo aprenda de la manera más dura, respalde su información.

Contenido de todo un disco duro

En el caso de servidores de red, resulta indispensable mantener un respaldo donde se pueda recuperar de una manera ágil y segura toda la información del disco duro, y que a la vez este proceso mantenga al servidor el mínimo tiempo posible fuera de la atención a las estaciones de trabajo.

Para estos respaldos pueden utilizarse las unidades de cintas de respaldo (casetes), con programas que generen un respaldo total del disco duro, por ejemplo cada dos meses, y elaborar un respaldo diario incremental, es decir uno donde sean grabados en cinta únicamente aquellos archivos cuya fecha de última modificación es posterior a la fecha del último respaldo total del disco duro, invirtiendo un mínimo de tiempo en el respaldo diario. Se pueden usar unidades removibles como las Jaz, Dito y Orb que permiten almacenar hasta 7 gigas de información compactada.

Si la información es de hasta 10Mb se requieren otros programas para hacer los respaldos en disquetes, de éstos existen muchos en el mercado como Backup Plus, Backup Assistant.

Si el disco tiene el sistema operativo dañado se utiliza el disco de arranque o el de seguridad que Windows 95 permite crear al instalar el sistema, de esta forma habrá acceso a los datos del disco y se podrá hacer un respaldo de la información importante en disquetes o en una unidad removible para que posteriormente se instale el sistema operativo.

5.3 Herramientas para reparar discos dañados

Si el disco tiene dañada la tabla de localización de archivos (FAT) el método anteriormente descrito no funcionará porque no se tiene acceso a los datos del disco dañado, para esto se utilizarán otros programas con los cuales se recuperará la información. Se describen algunos de éstos a continuación:

Norton Utilities para Windows 95/98

Es una colección de utilidades de diagnóstico y mantenimiento, Norton Utilities proporciona protección contra averías, solución de problemas en segundo plano (se pueden seguir utilizando otras aplicaciones), reparación básica de virus y actualizaciones en línea; además de nuevas utilidades de optimización con el fin de mejorar el rendimiento del sistema. Algunos de sus módulos se describen a continuación:

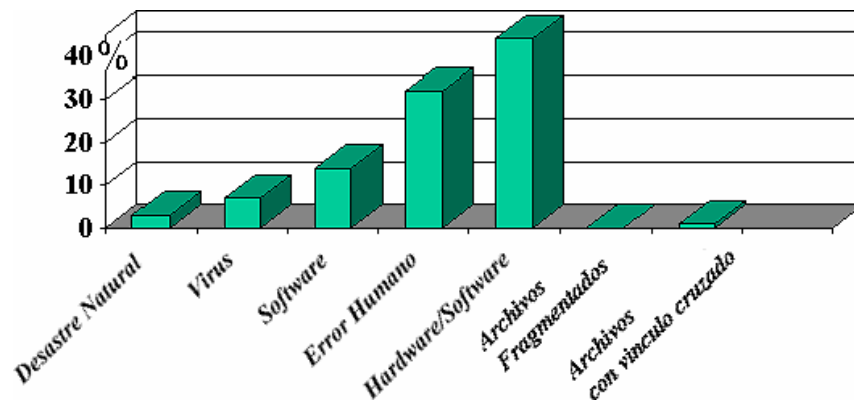
- *Norton WinDoctor*. Monitorea, limpia y está activo continuamente en el sistema, detecta en forma inteligente fallas en Windows y corrige los problemas dentro del Registro de Windows 95, archivos del sistema y aplicaciones de software. WinDoctor verifica problemas tales como atajos perdidos, capturas de registros inválidas, aplicaciones descompuestas y DLL faltantes. WinDoctor presenta una lista de problemas y los repara automáticamente o permite al usuario solucionarlos en forma manual.
- *Norton Web Services y LiveUpdate Pro*. Norton Web Services permite a los usuarios acceder a LiveUpdate Pro, una nueva utilidad basada en Internet que proporciona parches para Norton Utilities, así como para cualquier otra aplicación de software y de controladores de hardware en el sistema del usuario. LiveUpdate Pro permite instalar la actualización y también brinda la capacidad de deshacerla si es necesario.
- *Norton CrashGuard*. Proporciona la mejor protección contra averías. CrashGuard se ejecuta continuamente en el segundo plano, usando sólo 150K de memoria para interceptar averías y “desbloquear” aplicaciones. Cuando una aplicación tiene problemas, CrashGuard intercepta la avería, así los usuarios pueden guardar su trabajo. CrashGuard incluye Norton AntiFreeze que ofrece restaurar aplicaciones bloqueadas, incluso cuando el usuario se ve forzado a utilizar Ctrl + Alt + Supr.
- *Norton Zip Rescue*. Incluye la recuperación de fallas en el sistema y da la capacidad de guardar información rescatada en un Iomega Zip Disk. Permite a los usuarios recuperar sus sistemas arrancando desde Windows, en lugar de hacerlo desde DOS. El sensor de rescate en Norton System Doctor recomienda ahora actualizar los discos de rescate, cuando se detectan cambios en áreas críticas del sistema tales como el registro de arranque o CMOS.
- *Norton System Doctor*. Ayuda a mantener a las computadoras libres de problemas. Norton System Doctor le dice al usuario cómo reparar el error y qué utilidades de Norton Utilities debe utilizar, de igual manera también puede reparar automáticamente diversos problemas.
- *Speed Disk*. Proporciona la optimización de disco de manera inteligente, la ubicación de archivos en el disco con base en la frecuencia con la que se accede o modifica a éstos. Speed Disk coloca los archivos con los que se accede frecuentemente al frente del disco para obtener un acceso rápido, mientras que los archivos que raramente se utilizan los coloca al final del disco, dejando espacio libre en la parte media. Esto no sólo incrementa el rendimiento global del sistema, sino que también reduce el potencial para la fragmentación de archivos con el tiempo.
- *Nuts & Bolts Deluxe*. El conjunto más completo para la localización de averías, aunque tiene una integración débil con Windows 98. Detecta averías, optimiza y diagnóstica su sistema. Algunas de las tareas que realiza son las siguientes:
 - a) Sistema de optimización.

- b) Sistema de reparación y recuperación.
- c) Seguridad y recuperación de datos.
- d) Prevención de errores y protección de bloqueos.

Hard Drive Mechanic DELUXE

Pérdida de datos

Los eventos completamente imprevisibles como caídas de las unidades de disco duro físicas y lógicas son las causas principales de pérdida de los datos y de tiempo fuera de servicio de la computadora, incluso más que los virus, (véase el gráfico de Ontrack Internacional debajo). Estos eventos pueden atacar su PC y su sistema entero, incluyendo datos personales, periféricos, documentos compartidos, aplicaciones (contabilidad, finanzas, recursos humanos, etcétera).



El programa Hard Drive Mechanic puede automáticamente:

- Reparar/reconstruir el 98% de todas las caídas del sistema (FAT, particiones, raíz y arranque).
- Detectar al menos el 75% de todas las caídas de la unidad de disco duro físico, semanas antes de que los incidentes realmente ocurran, (sólo unidades S.M.A.R.T.).
- Reducir el costo de mantenimiento de su sistema en un promedio del 50%.
- Recuperar automáticamente su sistema de archivos del daño de los virus.

Muchas fallas mecánicas son consideradas típicamente predecibles. Ciertos componentes electrónicos pueden mostrar degradación antes de fallar y los problemas mecánicos son graduales y predecibles.

Con estos hechos en mente, IBM, Compaq y muchos otros importantes fabricantes de hardware desarrollaron tecnología para controlar aspectos falibles de una unidad de disco duro y la tecnología resultante, que permite predecir, se denomina Tecnología Auto-controladora de Análisis y Reporte (S.M.A.R.T.).

S.M.A.R.T. controla los aspectos clave de los componentes mecánicos y electrónicos de las unidades de disco duro, con la finalidad de proporcionar un sistema de advertencia temprana que otorgue suficiente tiempo de reacción para efectuar copia de seguridad de datos si un fallo fuera inminente.

Hard Drive Mechanic Deluxe es la primera aplicación exitosa de la tecnología S.M.A.R.T. para predecir eventos al usuario final. Diseñado para alertarle semanas y meses antes de un evento catastrófico, HDM Deluxe elimina la imprevisión del fallo de la unidad de disco duro, interpretando la información S.M.A.R.T. y presentándolo en un modo que le muestra la esperanza de vida de su unidad de disco duro.

Al incorporar inteligencia artificial, Hard Drive Mechanic Deluxe repara hasta 8 unidades en un mismo sistema automáticamente, sin que el usuario sea un experto.

HDM Deluxe contiene un procesador simple de archivos (SFP), el cual despliega un árbol del directorio de los archivos de su unidad permitiéndole seleccionarlos y ponerlos a salvo. Esto sin embargo, no es ningún SFP ordinario; posibilita especificar archivos individuales, directorios y subdirectorios individuales o la unidad entera. Una vez realizado esto, usted puede poner a salvo su opción de archivos, vía el puerto paralelo a otro PC, a los disquetes o a una segunda unidad de disco duro.

Lost & Found de PowerQuest

Lost & Found, favorece recuperar la información de discos dañados por fallas en el sistema lógico o incidentes. Una de las principales características de Lost & Found es que, en la mayoría de las ocasiones, no necesita enviar el disco a un centro de recuperación de datos.

Para llevar a cabo la recuperación de datos, no es necesario que el programa haya sido instalado anteriormente, ya que localiza la información y permite transferirla a un disquete, disco duro, disco de red o disco removible funcionando, aunque sectores críticos de información estén perdidos o dañados.

Asimismo, gracias a su sistema automático de respaldo, recobra los archivos aun después de dar formato al disco, siempre y cuando no se haya escrito sobre éstos, después de la eventualidad.

Esta solución analiza el disco y entrega un reporte con las posibilidades de recuperación de la información por códigos de colores. Mediante los diagnósticos entregados al usuario, éste puede prever posibles problemas. También incluye funciones como búsquedas seleccionadas, copiado de disco, navegador cluster y explorador de disco.

Por otra parte, puede reconocer y preservar archivos con nombre extenso cuando se están reestableciendo directorios o archivos, para mantener la facilidad de uso existente antes de la pérdida.

Los requerimientos del sistema son: procesador compatible con Intel x86; controladores IDE, EIDE o SCSI; 8MB en RAM; sistema FAT16 o FAT32 de archivos, y acceso de drive CHS o LBA.

5.4 Verificación de discos dañados

El usuario es quien conoce mejor su equipo de cómputo, por ello, en caso de detectar fallas en los componentes del sistema operativo o en la lectura de archivos del disco duro, debe hacer lo siguiente:

1. Verificar si tiene virus la computadora, si cuenta con un antivirus, éste debe estar actualizado. En algunos casos la actualización se puede a través de Internet, por ello, si tiene virus debe proceder a su limpieza.
2. Se puede hacer un diagnóstico con las Utilerías Norton y en caso de que falle Windows se ejecuta Norton Win Doctor; también si el disco presenta problemas con los archivos el Norton System Doctor.
3. Si tiene problemas con el sector de arranque o con el FAT, se utiliza Lost & Found o Hard Drive Mechanic siguiendo las instrucciones para recuperar la información del disco.

5.5 Instalación del sistema operativo

Para la instalación del sistema operativo en la computadora se deben tomar en cuenta las siguientes consideraciones:

MS-DOS

1. Dar formato al disco duro con `Format c: /s`.
2. Colocar el disco 1 en la unidad de disquetes y ejecutar el comando `instalar.exe`.
3. Seguir con los demás discos.

Windows 95

Definir un disco de arranque que reconozca el CD-ROM.

1. Crear un disco de inicio de w95.
2. Copiar las líneas referentes al CD-ROM del `autoexec` y `config` a éstos en a: (con el bloc de notas, copiando y pegando).
3. Copiar todos los archivos referentes al CD-ROM que el `autoexec` y `config` estén llamando.
4. Cambiar el path de estos archivos.
5. Guardar el `config` y `autoexec`.
6. Arrancar la computadora desde el disco creado.
7. Probar si reconoce el CD-ROM, en caso contrario, ejecutar `MSCDEX` con la misma línea que aparece en el `autoexec`.

8. Verificar de nuevo si reconoce el CD-ROM.

EJEMPLO:

Mis archivos del CD-ROM son mtmcdai.386, mtmcdai.sys y mscdex.exe (éste es común para todos).

Las líneas que yo tengo en el autoexec y config en el disco de arranque son:

Autoexec

```
rem ----- MTM ATAPI CD-ROM -----
```

```
rem - By Windows Setup - LH /L:1,36224 A:\MSCDEX.EXE /D:MTMIDE01 /L:D /M:10
```

```
rem ----- MTM ATAPI CD-ROM -----
```

Config

```
rem ----- MTM ATAPI CD-ROM -----
```

[COMMON]

```
DEVICEHIGH /L:1,15792 =A:\MTMCDAL.SYS /D:MTMIDE01 /L:SP
```

```
rem ----- MTM ATAPI CD-ROM -----
```

Para ejecutar el mscdex:

```
a:\mscdex /d:mtmide01 /l:d /m:10 (intro)
```

De esta forma se carga el mscdex.

Verificación del disco

Una vez que se reconoce el CD-ROM desde MS-DOS se procede a realizar lo siguiente:

Instalar W95 al 100% desde el CD-ROM.

Los pasos a seguir (no válido para la versión WIN95B-OSR2) son los siguientes:

Primero se lee todo el texto o se imprime, revisando todos los puntos antes de empezar, con esta opción queda MSDOS 7.0 y W95 por lo que no se aceptará MSDOS 6.22 o inferior, para esos juegos antiguos se emplea un disco de arranque de MSDOS 6.22.

1. Se debe hacer una copia de los archivos importantes y no olvidarse de: (Explorer, con xcopy de MS-DOS y con alguna otra utilidad de BACKUP).

Direcciones c:\windows*.WAB y Favoritos c:\windows\favoritos

Direcciones c:\windows*.PAB

Y algún otro archivo que se desee conservar. Si tienen dos HD es mucho mejor efectuar las copias en aquél que no se vaya a formatear. El disco D:\ se usa para guardar todos los programas originales a punto de instalar y así se instalan mas rápido.

2. Tomar nota de los datos del HD (setup de la bios por si acaso...) y comprobar que están las opciones LBA-NORMAL-LARGE o AUTO correctamente puestas. Se deben verificar los datos del fabricante del HD. ¡MUY IMPORTANTE!
3. Comprobar que existe copia de todos los programas que van a borrarse.
4. Verificar que se tiene el disco original (3 1/2) de W95 y el CD-ROM o el resto de discos.
5. Dar formato el HD c:\>format c:
6. Apagar la computadora y poner el disco de arranque en a:\>
7. Cuando la computadora busque la versión antigua de Windows, se inserta el disco del punto 5.
8. Seleccionar en comunicaciones sólo “Acceso telefonico a redes”.
9. Seleccionar únicamente las opciones de lo que vaya a utilizar.
10. Cuando se le pregunte el nombre de usuario, escribir el login en minúsculas junto con la contraseña.
11. Definir hora (GTM 06:00 Ciudad de México, Tegucigalpa).
12. Especificar la impresora.
13. Cuando se le pida, reiniciar el sistema.
14. Instalar los drivers del HD, si se tiene controladora con caché, seguir las instrucciones del fabricante.
15. Instalar los drivers de SVGA y la impresora (el sonido se instala sólo).
16. Instalar el módem.
17. Instalar todos los programas que se empleen.
18. Configurar RED. Configuración-Panel de Control-Red Aquí sólo se requiere instalar el “Adaptador de acceso telefónico” y el protocolo “TCP/IP”, en este último se debe dar un clic a Propiedades-Configuración DNS-Activar Host, poner todos los parámetros y reiniciar.
19. Instalar los UPDATES o PARCHES de W95 que se necesiten.
20. Sólo falta configurar el Acceso telefónico a redes con los datos de su proveedor.
21. Borrar todos los archivos con extensión .OLD, posteriormente ejecutar completos Scandisk y luego Defrag.
22. Instalar algún antivirus.

5.6 Verificación del sistema

Una vez instalado el sistema, se efectúan las pruebas necesarias en los programas, con la finalidad de verificar que se ejecuten adecuadamente.

BIBLIOGRAFÍA

Rodato, Jesús de Marcelo.

Guía de campo de los virus informáticos.

Ed. Alfaomega Grupo Editor, 1997.

Richard B. Levin.

Virus informáticos.

Ed. McGraw-Hill, 1992.

Cohen, Frederick B.

Curso abreviado de virus en computación.

Ed. Limusa, 1998.

Introducción.....	1
1. Qué es un virus.....	2
1.1 Cómo trabaja un virus.....	3
1.2 Propiedades de los virus.....	4
1.3 Orígenes.....	5
1.4 Desarrollo del fenómeno virus.....	7
1.5 Ciclo de vida de los virus.....	7
2. Clasificación de los virus.....	8
2.1 Por las formas en que se manifiestan.....	12
2.2 Por las zonas que afectan.....	13
2.3 Por su grado de mutación.....	16
3. Métodos de prevención.....	18
3.1 Utilización en común limitada.....	18
3.2 Controles administrativos.....	20
3.3 Verificación interna.....	20
3.4 Problemas en la red punto por punto.....	20
4. Confiabilidad en el software de prevención.....	25
4.1 Detección de virus.....	25
4.2 Comparando archivos.....	25
4.3 Los programas antivirus.....	26
4.4 Crear un disco de arranque.....	32
4.5 Procedimiento recomendado para la correcta eliminación de virus.....	32
4.6 Cómo eliminar virus.....	34

5. Recuperación de discos dañados	35
5.1 Herramientas para hacer un respaldo	35
5.2 Estrategias para hacer un respaldo.....	35
5.3 Herramientas para reparar discos dañados	38
5.4 Verificación de discos dañados	49
5.5 Instalación del sistema operativo.....	49
5.6 Verificación del sistema.....	45
Bibliografía.....	53