

**INTRODUCCIÓN A LOS SISTEMAS**

**WILMER ESCALANTE  
GLORIA ESTOR  
ROBINSON LAPEIRA  
KERLIS PALLARES  
DANIEL TORRES**

**VIRUS INFORMATICO**

**VESPASIANO RODRIGUEZ  
Profesor**

**CORPORACIÓN UNIFICADA NACIONAL  
C. U. N**

**FACULTAD DE INGENIERIA  
PROGRAMA INGENIERIA TÉCNICA DE SISTEMAS**

**1er. SEMESTRE**

**SANTA MARTA D. T. C. H.**

**2.001**

## **JUSTIFICACIÓN**

En definitiva, sea cual fuere el motivo por el cual se siguen produciendo virus, se debe destacar que su existencia no ha sido sólo perjuicios: gracias a ellos, mucha gente ha tomado conciencia de qué es lo que tiene y cómo protegerlo.

## **OBJETIVOS**

- ✓ Ampliar nuestro conocimiento acerca de un virus.
- ✓ Identificar que es, que no es un virus y sus componentes.
- ✓ Conocer las consecuencias que puede presentar un virus.
- ✓ Darse cuenta de la importancia sistema computacional, los datos y su correcta protección.
- ✓ Obtener el conocimiento para de esta forma poder reaccionar adecuadamente si su sistema es infectado.

Crear el hábito de mantener copias de sostenimientos de datos y sistemas para evitar pérdida total del sistemas

## **CONCLUSIÓN**

Este trabajo está hecho con el fin de afianzar nuestro conocimiento acerca de lo que es en realidad un virus informático su impacto a nivel personal y de sistemas teniendo en cuenta la importancia que tienen los datos que se almacenan y el correcto manejo de las opciones informáticas que nos pueden ayudar a salvar parcial o totalmente de los datos que se encuentran en riesgo a causa de algunas de estas aplicaciones que ponen en peligro cualquier tipo de sistema protegido, si hablamos de virus nuevos, que por su tamaño tan imperceptible y las tantas maneras que encuentra para su propagación y reproducción pueden llegar y hacernos pasar un mal rato y obtener pérdidas irre recuperables.

## I. HISTORIA DE LOS VIRUS

Hacia finales de los años 60, Douglas McIlory, Víctor Vysotsky y Robert Moris idearon un juego al que llamaron **Core War** (Guerra en lo Central, aludiendo a la memoria de la computadora), que se convirtió en el pasatiempo de algunos de los programadores de los laboratorios Bell de AT&T.

El juego consistía en que dos jugadores escribieran cada uno un programa llamado *organismo*, cuyo hábitat fuera la memoria de la computadora. A partir de una señal, cada programa intentaba forzar al otro a efectuar una instrucción inválida, ganando el primero que lo consiguiera.

Al término del juego, se borraba de la memoria todo rastro de la batalla, ya que estas actividades eran severamente sancionadas por los jefes por ser un gran riesgo dejar un *organismo* suelto que pudiera acabar con las aplicaciones del día siguiente. De esta manera surgieron los programas **destinados a dañar** en la escena de la computación.

Históricamente los virus informáticos fueron descubiertos por la prensa el 12 de octubre de 1985, con una publicación del New York Times que hablaba de un virus que fue se distribuyo desde un BBS y aparentemente era para optimizar los sistemas IBM basados en tarjeta gráfica EGA, pero al ejecutarlo salía la presentación pero al mismo tiempo borraba todos los archivos del disco duro, con un mensaje al finalizar que decía "Caíste".

Bueno en realidad este fue el nacimiento de su nombre, ya que los programas con código integrado, diseñados para hacer cosas inesperadas han existido desde que existen las computadoras. Y ha sido siempre la obra de algún programador delgado de ojos de loco.

Pero las primeras referencias de virus con fines intencionales surgieron en 1983 cuando Digital Equipment Corporation (DEC) empleó una subrutina para proteger su famoso procesador de textos Decmate II, que el 1 de abril de 1983 en caso de ser copia ilegal borraba todos los archivos de su unidad de disco.

Uno de los primeros registros que se tienen de una infección data del año 1987, cuando en la Universidad estadounidense de Delaware notaron que tenían un virus porque comenzaron a ver "© Brain" como etiqueta de los disquetes.

La causa de ello era Brain Computer Services, una casa de computación paquistaní que, desde 1986, vendía copias ilegales de software comercial infectadas para, según los responsables de la firma, dar una lección a los piratas.

Ellos habían notado que el sector de booteo de un disquete contenía código ejecutable, y que dicho código se ejecutaba cada vez que la máquina se inicializaba desde un disquete.

Lograron reemplazar ese código por su propio programa, residente, y que este instalara una réplica de sí mismo en cada disquete que fuera utilizado de ahí en más.

También en 1986, un programador llamado Ralf Burger se dio cuenta de que un archivo podía ser creado para copiarse a sí mismo, adosando una copia de él a otros archivos. Escribió una demostración de este efecto a la que llamó VIRDEM, que podía infectar cualquier archivo con extensión **.COM**.

Esto atrajo tanto interés que se le pidió que escribiera un libro, pero, puesto que él desconocía lo que estaba ocurriendo en Paquistán, no mencionó a los virus de sector de arranque (boot sector). Para ese entonces, ya se había empezado a diseminar el virus Vienna.

Actualmente, los virus son producidos en cantidades extraordinarias por muchísima gente alrededor del planeta. Algunos de ellos dicen hacerlo por diversión, otros quizás para probar sus habilidades. De cualquier manera, hasta se ha llegado a notar un cierto grado de competitividad entre los autores de estos programas.

Con relación a la motivación de los autores de virus para llevar a cabo su obra, existe en Internet un documento escrito por un escritor freelance Markus Salo, en el cual, entre otros, se exponen los siguientes conceptos:

Algunos de los programadores de virus, especialmente los mejores, sostienen que su interés por el tema es puramente científico, que desean averiguar todo lo que se pueda sobre virus y sus usos.

A diferencia de las compañías de software, que son organizaciones relativamente aisladas unas de otras (todas tienen secretos que no querrían que sus competidores averiguaran) y cuentan entre sus filas con mayoría de estudiantes graduados, las agrupaciones de programadores de virus están abiertas a cualquiera que se interese en ellas, ofrecen consejos, camaradería y pocas limitaciones. Además, son libres de seguir cualquier objetivo que les parezca, sin temer por la pérdida de respaldo económico.

El hecho de escribir programas vírales da al programador cierta fuerza coercitiva, lo pone fuera de las reglas convencionales de comportamiento. Este factor es uno de los más importantes, pues el sentimiento de pertenencia es algo necesario para todo ser humano, y es probado que dicho sentimiento pareciera verse reforzado en situaciones marginales.

Por otro lado, ciertos programadores parecen intentar legalizar sus actos poniendo sus creaciones al alcance de mucha gente, (vía Internet, BBS especializadas, etc.) haciendo la salvedad de que el material es peligroso, por lo cual el usuario debería tomar las precauciones del caso.

Existen programadores, de los cuales, generalmente, provienen los virus más destructivos, que alegan que sus programas son creados para hacer notoria la falta de protección de que sufren la mayoría de los usuarios de computadoras.

La gran mayoría de estos individuos son del mismo tipo de gente que es reclutada por los grupos terroristas: hombres, adolescentes, inteligentes.

## II. QUÉ NO ES UN VIRUS

Existen algunos programas que, sin llegar a ser virus, ocasionan problemas al usuario. Estos **no-virus** carecen de por lo menos una de las tres características que identifican a un virus (dañino, auto reproductor y subrepticio). Veamos un ejemplo de estos no - virus: "Hace algunos años, la red de I. B. M., encargada de conectar más de 130 países, fue virtualmente paralizada por haberse saturado con un correo electrónico que contenía un mensaje de felicitación navideña que, una vez leído por el destinatario, se enviaba a sí mismo a cada integrante de las listas de distribución de correo del usuario. Al cabo de un tiempo, fueron tantos los mensajes que esperaban ser leídos por sus destinatarios que el tráfico se volvió demasiado alto, lo que ocasionó la caída de la red".

Asimismo, es necesario aclarar que no todo lo que altere el normal funcionamiento de una computadora es necesariamente un virus.

Por ello, daré algunas de las pautas principales para diferenciar entre qué debe preocuparnos y qué no:

### a) **BUGS (Errores en programas)**

Los bugs no son virus, y los virus no son bugs. Todos usamos programas que tienen graves errores (bugs). Si se trabaja por un tiempo largo con un archivo muy extenso, eventualmente algo puede comenzar a ir mal dentro del programa, y este a negarse a grabar el archivo en el disco. Se pierde entonces todo lo hecho desde la última grabación. Esto, en muchos casos, se debe a ERRORES del programa. Todos los programas lo suficientemente complejos tienen bugs.

### b) **FALSA ALARMA**

Algunas veces tenemos problemas con nuestro hardware o software y, luego de una serie de verificaciones, llegamos a la conclusión de que se trata de un virus, pero nos encontramos con una FALSA ALARMA luego de correr nuestro programa antivirus.

Desafortunadamente no hay una regla estricta por la cual guiarse, pero contestarse las siguientes preguntas puede ser de ayuda:

¿Es sólo un archivo el que reporta la falsa alarma (o quizás varios, pero copias del mismo)?.

¿Solamente un producto antivirus reporta la alarma? (Otros productos dicen que el sistema está limpio).

¿Se indica una falsa alarma después de correr múltiples productos, pero no después de bootear, sin ejecutar ningún programa?.

Si al menos una de nuestras respuestas fue afirmativa, es muy factible que efectivamente se trate de una falsa alarma.

### **c) PROGRAMAS CORRUPTOS**

A veces algunos archivos son accidentalmente dañados, quizás por problemas de hardware. Esto quiere decir que no siempre que encontremos daños en archivos deberemos estar seguros de estar infectados.

### III. QUE ES UN VIRUS

Un virus es simplemente un programa, elaborado accidental o intencionadamente para instalarse en la computadora de un usuario sin el conocimiento o el permiso de este.

Podríamos decir que es una secuencia de instrucciones y rutinas creadas con el único objetivo de alterar el correcto funcionamiento del sistema y, en la inmensa mayoría de los casos, corromper o destruir parte o la totalidad de los datos almacenados en el disco. De todas formas, dentro del término "virus informático" se suelen englobar varios tipos de programas.

Todos estos programas tienen en común la creación de efectos perniciosos; sin embargo, no todos pueden ser considerados como virus propiamente dichos.

Decimos además que es un programa parásito porque el programa ataca a los archivos o sector es de "booteo" o arranque y se reproduce a sí mismo para continuar su esparcimiento.

Algunos se limitan solamente a multiplicarse, mientras que otros pueden producir serios daños que pueden afectar a los sistemas. Nunca se puede 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, reproduciéndose una y otra vez cuando se accede a dichos archivos, dañando la información existente en la memoria o alguno de los dispositivos de almacenamiento del ordenador.

Tienen diferentes finalidades: Algunos sólo 'infectan', otros alteran datos, otros los eliminan, 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.***

La definición más simple y completa que hay de los virus corresponde al modelo D. A. S., y se fundamenta en tres características, que se refuerzan y dependen mutuamente. Según ella, un virus es un programa que cumple las siguientes pautas:

Es dañino

Es auto reproductor

Es subrepticio u oculto

El hecho de que la definición imponga que los virus son programas no admite ningún tipo de observación; está extremadamente claro que son programas,

realizados por personas. Además de ser programas tienen el fin ineludible de causar daño en cualquiera de sus formas.

Asimismo, se pueden distinguir tres módulos principales de un virus informático:

Módulo de Reproducción

Módulo de Ataque

Módulo de Defensa

#### IV. TIPOS DE VIRUS

Los virus se clasifican por el modo en que actúan infectando la computadora:

Programa: Infectan archivos ejecutables tales como .com / .exe / .ovl / .drv / .sys / .bin

Boot: Infectan los sectores Boot Record, Master Boot, FAT y la Tabla de Partición.

Múltiples: Infectan programas y sectores de "booteo".

Bios: Atacan al Bios para desde allí reescribir los discos duros.

Hoax: Se distribuyen por e-mail y la única forma de eliminarlos es el uso del sentido común.

Al respecto, se trata de virus que no existe y que se utiliza para aterrar a los novatos especialmente en la Internet a pesar que los rumores lo muestran como algo muy serio y a veces la información es tomada por la prensa especializada. Por lo general, como ya se expresó, la difusión se hace por cadenas de e-mail con terribles e inopinadas advertencias. En realidad el único virus es el mensaje.

Por último, cabe destacar que los HOAX están diseñados únicamente para asustar a los novatos (y a los que no lo son tanto). Otros como el mensaje del carcinoma cerebral de **Jessica, Jessica Mydek, Anabelle, Ana, Billy** y otros personajes imaginarios tampoco son reales como tampoco lo es la dirección [ACS@aol.com](mailto:ACS@aol.com), ya que fueron creados para producir congestión en la Internet.

A continuación se da un pequeño repaso a cada uno de ellos poniendo de manifiesto sus diferencias. La clasificación es la siguiente:

Virus 'Puro'  
Caballo de Troya  
Bomba Lógica  
Gusano o Worm  
Y Otros

Todos estos programas tienen en común la creación de efectos perniciosos; sin embargo, no todos pueden ser considerados como virus propiamente dichos.

### **a) Virus Puro**

Un verdadero virus tiene como características más importantes la capacidad de copiarse a sí mismo en soportes diferentes al que se encontraba originalmente, y por supuesto hacerlo con el mayor sigilo posible y de forma transparente al usuario; a este proceso de auto réplica se le conoce como "infección", de ahí que en todo este tema se utilice la terminología propia de la medicina: "vacuna", "tiempo de incubación", etc. Como soporte entendemos el lugar donde el virus se oculta, ya sea fichero, sector de arranque, partición, etc.

Un virus puro también debe modificar el código original del programa o soporte objeto de la infección, para poder activarse durante la ejecución de dicho código; al mismo tiempo, una vez activado, el virus suele quedar residente en memoria para poder infectar así de forma transparente al usuario.

### **b) Caballo de Troya**

Al contrario que el virus puro, un Caballo de Troya es un programa maligno que se oculta en otro programa legítimo, y que produce sus efectos perniciosos al ejecutarse este último. En este caso, no es capaz de infectar otros archivos o soportes, y sólo se ejecuta una vez, aunque es suficiente, en la mayoría de las ocasiones, para causar su efecto destructivo.

### **c) Bomba Lógica**

Se trata simplemente de un programa maligno que permanece oculto en memoria y que solo se activa cuando se produce una acción concreta, predeterminada por su creador: cuando se llega a una fecha en concreto ( Viernes 13 ), cuando se ejecuta cierto programa o cierta combinación de teclas, etc.

### **d) Gusano o Worm**

Por último, un gusano es un programa cuya única finalidad es la de ir consumiendo la memoria del sistema, mediante la realización de copias sucesivas de sí mismo, hasta desbordar la RAM, siendo ésta su única acción maligna.

La barrera entre virus puros y el resto de programas malignos es muy difusa, prácticamente invisible, puesto que ya casi todos los virus incorporan características propias de uno o de varios de estos programas: por ejemplo, los virus como el Viernes 13 son capaces de infectar otros archivos, siendo así virus puro, pero también realizan su efecto destructivo cuando se da una condición concreta, la fecha Viernes 13, característica propia de una bomba lógica; por último, se oculta en programas ejecutables teniendo así una cualidad de Caballo de Troya. De ahí la gran confusión existente a este respecto.

#### e) Virus De Macros

Esta entre las novedades surgidas últimamente en el mundo de los virus, aunque no son totalmente nuevos, parece que han esperado hasta 1995 para convertirse en una peligrosa realidad. Por desgracia, ya existe un número importante de virus de este tipo catalogados, que han sido escritos en WordBasic, el potente lenguaje incluido en Microsoft Word.

Estos virus sólo afectan a los usuarios de Word para Windows y consisten en un conjunto de macros de este procesador de textos. Aunque el peligro del virus se restringe a los usuarios de Word, tiene una importante propagación ya que puede infectar cualquier texto, independientemente de la plataforma bajo la que éste se ejecute: Mac, Windows 3.x, Windows NT, W95 y OS/2. Este es el motivo de su peligrosidad, ya que el intercambio de documentos en disquete o por red es mucho más común que el de ejecutables.

#### f) Virus Mutantes

Son los que al infectar realizan modificaciones a su código, para evitar ser detectados o eliminados (**NATAS** o **SATÁN**, **Miguel Angel**, por mencionar algunos).

#### g) Bombas de Tiempo

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

#### h) Auto reproducción

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

### **i) Infecciones del área de carga inicial**

Infectan los diskettes o el disco duro, alojándose inmediatamente en el área de carga. Toman el control cuando se enciende la computadora y lo conservan todo el tiempo.

### **j) Infecciones del sistema**

Se introducen en los programas del sistema, por ejemplo COMMAND.COM y otros que se alojan como residentes en memoria. Los comandos del Sistema Operativo, como COPY, DIR o DEL, son programas que se introducen en la memoria al cargar el Sistema Operativo y es así como el virus adquiere el control para infectar todo disco que sea introducido a la unidad con la finalidad de copiarlo o simplemente para ver sus carpetas (también llamadas: folders, subdirectorios, directorios).

### **k) Infecciones de programas ejecutables**

Estos son los virus mas peligrosos, porque se diseminan fácilmente hacia cualquier programa (como hojas de cálculo, juegos, procesadores de palabras).

La infección se realiza al ejecutar el programa que contiene al virus, que en ese momento se posiciona en la memoria de la computadora y a partir de entonces infectará todos los programas cuyo tipo sea EXE o COM, en el instante de ejecutarlos, para invadirlos autocopiándose en ellos.

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

## V. CARACTERÍSTICAS DE LOS VIRUS

El virus es un pequeño software (cuanto más pequeño más fácil de esparcir y más difícil de detectar), que permanece inactivo hasta que un hecho externo hace que el programa sea ejecutado o el sector de "booteo" sea leído. De esa forma el programa del virus es activado y se carga en la memoria de la computadora, desde donde puede esperar un evento que dispare su sistema de destrucción o se duplique a sí mismo.

Los más comunes son los residentes en la memoria que pueden replicarse fácilmente en los programas del sector de "booteo", menos comunes son los no-residentes que no permanecen en la memoria después que el programa-huesped es cerrado.

Los virus pueden llegar a "camuflarse" y esconderse para evitar la detección y reparación. Como lo hacen:

El virus re-orienta la lectura del disco para evitar ser detectado;

Los datos sobre el tamaño del directorio infectado son modificados en la FAT, para evitar que se descubran bytes extra que aporta el virus;

Los virus se transportan a través de programas tomados de BBS (Bulletin Boards) o copias de software no original, infectadas a propósito o accidentalmente. También cualquier archivo que contenga "ejecutables" o "macros" puede ser portador de un virus: downloads de programas de lugares inseguros; e-mail con "attachments", archivos de MS-Word y MS-Excel con macros. Inclusive ya existen virus que se distribuyen con MS-Power Point. Los archivos de datos, texto o Html **NO PUEDEN** contener virus, aunque pueden ser dañados por estos.

Los virus de sectores de "booteo" se instalan en esos sectores y desde allí van saltando a los sectores equivalentes de cada uno de los drivers de la PC. Pueden dañar el sector o sobrescribirlo. Lamentablemente obligan al formateo del disco del drive infectado. Incluyendo discos de 3.5" y todos los tipos de Zip de Iomega, Sony y 3M. (No crean vamos a caer en el chiste fácil de decir que el más extendido de los virus de este tipo se llama MS Windows 98).

En cambio los virus de programa, se manifiestan cuando la aplicación infectada es ejecutada, el virus se activa y se carga en la memoria, infectando a cualquier programa que se ejecute a continuación. Puede solaparse infecciones de diversos virus que pueden ser destructivos o permanecer inactivos por largos periodos de tiempo.

Asimismo, se pueden distinguir tres módulos principales de un virus informático:

Módulo de Reproducción

Módulo de Ataque

## Módulo de Defensa

### a) El módulo de reproducción

se encarga de manejar las rutinas de "parasitación" de entidades ejecutables (o archivos de datos, en el caso de los virus macro) a fin de que el virus pueda ejecutarse subrepticamente. Pudiendo, de esta manera, tomar control del sistema e infectar otras entidades permitiendo se traslade de una computadora a otra a través de algunos de estos archivos.

### b) El módulo de ataque

es optativo. En caso de estar presente es el encargado de manejar las rutinas de daño adicional del virus. Por ejemplo, el conocido virus **Michelangelo**, además de producir los daños que se detallarán más adelante, tiene un módulo de ataque que se activa cuando el reloj de la computadora indica 6 de Marzo. En estas condiciones la rutina actúa sobre la información del disco rígido volviéndola inutilizable.

### c) El módulo de defensa

Tiene, obviamente, la misión de proteger al virus y, como el de ataque, puede estar o no presente en la estructura. Sus rutinas apuntan a evitar todo aquello que provoque la remoción del virus y retardar, en todo lo posible, su detección.

## VI. EFECTOS Y DAÑOS

### a) DAÑOS DE LOS VIRUS

Definiremos **daño** como acción una indeseada, y los clasificaremos según la cantidad de tiempo necesaria para reparar dichos daños. Existen seis categorías de daños hechos por los virus, de acuerdo a la gravedad.

### b) DAÑOS TRIVIALES

Sirva como ejemplo la forma de trabajo del virus **FORM** (el más común): En el día 18 de cada mes cualquier tecla que presionemos hace sonar el beep. Deshacerse del virus implica, generalmente, segundos o minutos.

### c) DAÑOS MENORES

Un buen ejemplo de este tipo de daño es el **JERUSALEM**. Este virus borra, los viernes 13, todos los programas que uno trate de usar después de que el virus haya infectado la memoria residente. En el peor de los casos, tendremos que reinstalar los programas perdidos. Esto nos llevará alrededor de 30 minutos.

### d) DAÑOS MODERADOS

Cuando un virus formatea el disco rígido, mezcla los componentes de la **FAT** (File Allocation Table, Tabla de Ubicación de Archivos), o sobrescribe el disco rígido. En este caso, sabremos inmediatamente qué es lo que está sucediendo, y podremos reinstalar el sistema operativo y utilizar el último backup. Esto quizás nos lleve una hora.

### e) DAÑOS MAYORES.

Algunos virus, dada su lenta velocidad de infección y su alta capacidad de pasar desapercibidos, pueden lograr que ni aún restaurando un backup volvamos al último estado de los datos. Un ejemplo de esto es el virus **DARK AVENGER**, que infecta archivos y acumula la cantidad de infecciones que realizó. Cuando este contador llega a 16, elige un sector del disco al azar y en él escribe la frase: "**Eddie lives ... somewhere in time**" (Eddie vive ... en algún lugar del tiempo). Esto puede haber estado pasando por un largo tiempo sin que lo notemos, pero el día en que detectemos la presencia del virus y queramos restaurar el último

backup notaremos que también él contiene sectores con la frase, y también los backups anteriores a ese.

Puede que lleguemos a encontrar un backup limpio, pero será tan viejo que muy probablemente hayamos perdido una gran cantidad de archivos que fueron creados con posterioridad a ese backup.

## f) DAÑOS SEVEROS

Los daños severos son hechos cuando un virus realiza cambios mínimos, graduales y progresivos. No sabemos cuándo los datos son correctos o han cambiado, pues no hay pistas obvias como en el caso del **DARK AVENGER** (es decir, no podemos buscar la frase **Eddie lives ...**).

## g) DAÑOS ILIMITADOS

Algunos programas como **CHEEBA**, **VACSINA.44.LOGIN** y **GP1** entre otros, obtienen la clave del administrador del sistema y la pasan a un tercero. Cabe aclarar que estos no son virus sino troyanos. En el caso de **CHEEBA**, crea un nuevo usuario con los privilegios máximos, fijando el nombre del usuario y la clave. El daño es entonces realizado por la tercera persona, quien ingresará al sistema y haría lo que quisiera.

## h) SOFTWARE

- ☒ Modificación de programas para que dejen de funcionar.
- ☒ Modificación de programas para que funcionen erróneamente.
- ☒ Modificación sobre los datos.
- ☒ Eliminación de programas y/o datos.
- ☒ Acabar con el espacio libre en el disco rígido.
- ☒ Hacer que el sistema funcione mas lentamente.
- ☒ Robo de información confidencial.

## i) HARDWARE

- ☒ Borrado del BIOS
- ☒ Quemado del procesador por falsa información del sensor de temperatura
- ☒ Rotura del disco rígido al hacerlo leer repetidamente sectores específicos que fueren su funcionamiento mecánico.

## VII. SÍNTOMAS TÍPICOS DE UNA INFECCIÓN.

- ✓ El sistema operativo o un programa toma mucho tiempo en cargar sin razón aparente.
- ✓ El tamaño del programa cambia sin razón aparente.
- ✓ El disco duro se queda sin espacio o reporta falta de espacio sin que esto sea necesariamente así.
- ✓ Si se corre el CHKDSK no muestra "655360 bytes available".
- ✓ En Windows aparece "32 bit error".
- ✓ La luz del disco duro en la CPU continua parpadeando aunque no se este trabajando ni haya protectores de pantalla activados. (Se debe tomar este síntoma con mucho cuidado, porque no siempre es así).
- ✓ No se puede "bootear" desde el Drive A, ni siquiera con los discos de rescate.
- ✓ Aparecen archivos de la nada o con nombres y extensiones extrañas.
- ✓ Suena "clicks" en el teclado (este sonido es particularmente aterrador para quien no esta advertido).
- ✓ Los caracteres de texto se caen literalmente a la parte inferior de la pantalla (especialmente en DOS).
- ✓ Síntomas que indican la presencia de Virus
- ✓ Cambios en la longitud de los programas
- ✓ Cambios en la fecha y / u hora de los archivos
- ✓ Retardos al cargar un programa
- ✓ Operación más lenta del sistema
- ✓ Reducción de la capacidad en memoria y / o disco rígido
- ✓ Sectores defectuosos en los disquetes
- ✓ Mensajes de error inusuales
- ✓ Actividad extraña en la pantalla
- ✓ Fallas en la ejecución de los programas
- ✓ Fallas al bootear el equipo
- ✓ Escrituras fuera de tiempo en el disco

En la pantalla del monitor pueden aparecer mensajes absurdos tales como **"Tengo hambre. Introduce un Big Mac en el Drive A"**.

En el monitor aparece una pantalla con un fondo de cielo celeste, unas nubes blancas difuminadas, una ventana de vidrios repartidos de colores y una leyenda en negro que dice Windows '98 (No puedo evitarlo, es mas fuerte que yo...!!).

## **VIII. Estrategias de infección usadas por los virus**

### **a) Cómo se propagan los virus**

- ✕ Disquetes u otro medio de almacenamiento removible
- ✕ Software pirata en disquetes o CDs
- ✕ Redes de computadoras
- ✕ Mensajes de correo electrónico
- ✕ Software bajado de Internet
- ✕ Discos de demostración y pruebas gratuitos

### **b) Añadidura o empalme:**

El código del virus se agrega al final del archivo a infectar, modificando las estructuras de arranque del archivo de manera que el control del programa pase por el virus antes de ejecutar el archivo. Esto permite que el virus ejecute sus tareas específicas y luego entregue el control al programa. Esto genera un incremento en el tamaño del archivo lo que permite su fácil detección.

### **c) Inserción:**

El código del virus se aloja en zonas de código no utilizadas o en segmentos de datos para que el tamaño del archivo no varíe. Para esto se requieren técnicas muy avanzadas de programación, por lo que no es muy utilizado este método.

### **d) Reorientación:**

Es una variante del anterior. Se introduce el código principal del virus en zonas físicas del disco rígido que se marcan como defectuosas y en los archivos se implantan pequeños trozos de código que llaman al código principal al ejecutarse el archivo. La principal ventaja es que al no importar el tamaño del archivo el cuerpo del virus puede ser bastante importante y poseer mucha funcionalidad. Su eliminación es bastante sencilla, ya que basta con rescribir los sectores marcados como defectuosos.

### **e) Polimorfismo:**

Este es el método mas avanzado de contagio. La técnica consiste en insertar el código del virus en un archivo ejecutable, pero para evitar el aumento de tamaño

del archivo infectado, el virus compacta parte de su código y del código del archivo anfitrión, de manera que la suma de ambos sea igual al tamaño original del archivo. Al ejecutarse el programa infectado, actúa primero el código del virus descompactando en memoria las porciones necesarias. Una variante de esta técnica permite usar métodos de encriptación dinámicos para evitar ser detectados por los antivirus.

#### **f) Sustitución:**

Es el método más tosco. Consiste en sustituir el código original del archivo por el del virus. Al ejecutar el archivo deseado, lo único que se ejecuta es el virus, para disimular este proceder reporta algún tipo de error con el archivo de forma que creamos que el problema es del archivo.

Ejemplos de virus y sus acciones

Happy99: Programa enviado por mail, abre una ventana con fuegos artificiales. Manipula la conectividad con Internet.

Melissa: Macrovirus de Word. Se envía a sí mismo por mail. Daña todos los archivos .doc

Chernobyl (W95.CIH): Borra el primer Mb del HD, donde se encuentra la FAT. Obliga a formatear el HD. Además intenta rescribir el BIOS de la PC lo que obliga a cambiar el mother. Se activa el 26 de abril.

Michelangelo: Virus de boot sector. Se activa el 6 de marzo. Sobre escribe la FAT, dejando el disco inutilizable.

WinWord.Concept: Macrovirus que infecta la plantilla Normal.dot. Hace aparecer mensajes en la pantalla y mal funcionamiento del Word.

FormatC: Troyano que infecta el Word, al abrir un archivo infectado formatea el disco rígido.

Back Orifice2000 (BO2K): Funcionalmente es un virus y sirve para el robo de información. Permite tomar control remoto de la PC o del servidor infectados, con la posibilidad de robar información y alterar datos.

VBS/Bubbleboy: Troyano que se ejecuta sin necesidad de abrir un attachment, y se activa inmediatamente después de que el usuario abra el mail. No genera problemas serios.

## IX. FORMAS DE OCULTAMIENTO

Un virus puede considerarse efectivo si, además de extenderse lo más ampliamente posible, es capaz de permanecer oculto al usuario el mayor tiempo posible; para ello se han desarrollado varias técnicas de ocultamiento o sigilo. Para que estas técnicas sean efectivas, el virus debe estar residente en memoria, puesto que debe monitorizar el funcionamiento del sistema operativo. La base principal del funcionamiento de los virus y de las técnicas de ocultamiento, además de la condición de programas residentes, la interceptación de interrupciones. El DOS y los programas de aplicación se comunican entre sí mediante el servicio de interrupciones, que son como subrutinas del sistema operativo que proporcionan una gran variedad de funciones a los programas. Las interrupciones se utilizan, por ejemplo, para leer o escribir sectores en el disco, abrir ficheros, fijar la hora del sistema, etc. Y es aquí donde el virus entra en acción, ya que puede sustituir alguna interrupción del DOS por una suya propia y así, cuando un programa solicite un servicio de esa interrupción, recibirá el resultado que el virus determine.

Entre las técnicas más usuales cabe destacar el ocultamiento o *stealth*, que esconde los posibles signos de infección del sistema. Los síntomas más claros del ataque de un virus los encontramos en el cambio de tamaño de los ficheros, de la fecha en que se crearon y de sus atributos, y en la disminución de la memoria disponible.

Estos problemas son indicadores de la posible presencia de un virus, pero mediante la técnica *stealth* es muy fácil (siempre que se encuentre residente el virus) devolver al sistema la información solicitada como si realmente los ficheros no estuvieran infectados. Por este motivo es fundamental que cuando vayamos a realizar un chequeo del disco duro arranquemos el ordenador con un disco de sistema totalmente limpio.

### a) El módulo de reproducción

Se encarga de manejar las rutinas de "parasitación" de entidades ejecutables (o archivos de datos, en el caso de los virus macro) a fin de que el virus pueda ejecutarse subrepticamente. Pudiendo, de esta manera, tomar control del sistema e infectar otras entidades permitiendo se traslade de una computadora a otra a través de algunos de estos archivos.

### b) El módulo de ataque

es optativo. En caso de estar presente es el encargado de manejar las rutinas de daño adicional del virus. Por ejemplo, el conocido virus **Michelangelo**, además de producir los daños que se detallarán más adelante, tiene un módulo de ataque que se activa cuando el reloj de la computadora indica 6 de Marzo. En estas

condiciones la rutina actúa sobre la información del disco rígido volviéndola inutilizable.

### **c) El módulo de defensa**

tiene, obviamente, la misión de proteger al virus y, como el de ataque, puede estar o no presente en la estructura. Sus rutinas apuntan a evitar todo aquello que provoque la remoción del virus y retardar, en todo lo posible, su detección.

### **d) Formas De Infección**

Antes de nada, hay que recordar que un virus no puede ejecutarse por sí solo, necesita un programa portador para poder cargarse en memoria e infectar; asimismo, para poder unirse a un programa portador necesita modificar la estructura de este, para que durante su ejecución pueda realizar una llamada al código del virus.

Las partes del sistema más susceptibles de ser infectadas son el sector de arranque de los disquetes, la tabla de partición y el sector de arranque del disco duro, y los ficheros ejecutables (\*.EXE y \*.COM). Para cada una de estas partes tenemos un tipo de virus, aunque muchos son capaces de infectar por sí solos estos tres componentes del sistema.

En los disquetes, el sector de arranque es una zona situada al principio del disco, que contiene datos relativos a la estructura del mismo y un pequeño programa, que se ejecuta cada vez que arrancamos desde disquete.

En este caso, al arrancar con un disco contaminado, el virus se queda residente en memoria RAM, y a partir de ahí, infectará el sector de arranque de todos los disquetes a los que se accedan, ya sea al formatear o al hacer un DIR en el disco, dependiendo de cómo esté programado el virus).

El proceso de infección consiste en sustituir el código de arranque original del disco por una versión propia del virus, guardando el original en otra parte del disco; a menudo el virus marca los sectores donde guarda el *boot* original como en mal estado, protegiéndolos así de posibles accesos, esto suele hacerse por dos motivos: primero, muchos virus no crean una rutina propia de arranque, por lo que una vez residentes en memoria, efectúan una llamada al código de arranque original, para iniciar el sistema y así aparentar que se ha iniciado el sistema como siempre, con normalidad. Segundo, este procedimiento puede ser usado como técnica de ocultamiento.

Normalmente un virus completo no cabe en los 512 bytes que ocupa el sector de arranque, por lo que en éste suele copiar una pequeña parte de sí mismo, y el resto lo guarda en otros sectores del disco, normalmente los últimos, marcándolos como defectuosos. Sin embargo, puede ocurrir que alguno de los virus no marquen estas zonas, por lo que al llenar el disco estos sectores pueden ser sobrescritos y así dejar de funcionar el virus.

La tabla de partición está situada en el primer sector del disco duro, y contiene una serie de bytes de información de cómo se divide el disco y un pequeño programa de arranque del sistema. Al igual que ocurre con el *boot* de los disquetes, un virus

de partición suplanta el código de arranque original por el suyo propio; así, al arrancar desde disco duro, el virus se instala en memoria para efectuar sus acciones. También en este caso el virus guarda la tabla de partición original en otra parte del disco, aunque algunos la marcan como defectuosa y otros no. Muchos virus guardan la tabla de partición y a ellos mismos en los últimos sectores de disco, y para proteger esta zona, modifican el contenido de la tabla para reducir el tamaño lógico del disco. De esta forma el DOS no tiene acceso a estos datos, puesto que ni siquiera sabe que esta zona existe.

Casi todos los virus que afectan la partición también son capaces de hacerlo en el *boot* de los disquetes y en los ficheros ejecutables; un virus que actuara sobre particiones de disco duro tendría un campo de trabajo limitado, por lo que suelen combinar sus habilidades.

Con todo, el tipo de virus que más abunda es el de fichero; en este caso usan como vehículo de expansión los archivos de programa o ejecutables, sobre todo .EXE y .COM, aunque también a veces .OVL, .BIN y .OVR. AL ejecutarse un programa infectado, el virus se instala residente en memoria, y a partir de ahí permanece al acecho; al ejecutar otros programas, comprueba si ya se encuentran infectados. Si no es así, se adhiere al archivo ejecutable, añadiendo su código al principio y al final de éste, y modificando su estructura de forma que al ejecutarse dicho programa primero llame al código del virus devolviendo después el control al programa portador y permitiendo su ejecución normal.

Este efecto de adherirse al fichero original se conoce vulgarmente como "engordar" el archivo, ya que éste aumenta de tamaño al tener que albergar en su interior al virus, siendo esta circunstancia muy útil para su detección. De ahí que la inmensa mayoría de los virus sean programados en lenguaje ensamblador, por ser el que genera el código más compacto, veloz y de menor consumo de memoria; un virus no sería efectivo si fuera fácilmente detectable por su excesiva ocupación en memoria, su lentitud de trabajo o por un aumento exagerado en el tamaño de los archivos infectados. No todos los virus de fichero quedan residentes en memoria, si no que al ejecutarse se portador, éstos infectan a otro archivo, elegido de forma aleatoria de ese directorio o de otros.

La autoencriptación o *self-encryption* es una de las técnicas víricas más extendidas. En la actualidad casi todos los nuevos ingenios destructivos son capaces de encriptarse cada vez que infectan un fichero, ocultando de esta forma cualquier posible indicio que pueda facilitar su búsqueda. No obstante, todo virus encriptado posee una rutina de desencriptación, rutina que es aprovechada por los antivirus para remotoizar el origen de la infección.

El mayor avance en técnicas de encriptación viene dado por el *polimorfismo*. Gracias a él un virus no sólo es capaz de encriptarse sino que además varía la rutina empleada cada vez que infecta un fichero. De esta forma resulta imposible encontrar coincidencias entre distintos ejemplares del mismo virus, y ante esta técnica el tradicional método de búsqueda de cadenas características se muestra inútil.

Otra técnica básica de ocultamiento es la intercepción de mensajes de error del sistema. Supongamos que un virus va a infectar un archivo de un disco protegido

contra escritura; al intentar escribir en el obtendríamos el mensaje: "Error de protección contra escritura leyendo unidad A Anular, Reintentar, Fallo?", por lo que descubriríamos el anormal funcionamiento de nuestro equipo. Por eso, al virus le basta con redireccionar la interrupción a una rutina propia que evita la salida de estos mensajes, consiguiendo así pasar desapercibido.

#### **e) VIRUS EN INTERNET**

En ocasiones se propagan rumores que dan por cierto noticias de dudosa procedencia. Más o menos esto es lo que ha sucedido de un tiempo a esta parte con el virus por correo electrónico de Internet conocido por Good Times. Lógicamente las primeras noticias de esta maligna creación aparecieron en la «red de redes», en un mensaje alarmante que decía que si algún usuario recibía un mensaje con el tema «Good Times» no debía abrirlo o grabarlo si no quería perder todos los datos de su disco duro. Posteriormente el mensaje recomendaba que se informara a todo el mundo y se copiara el aviso en otros lugares. En esta ocasión el rumor es totalmente falso, aunque todavía sigue existiendo gente que se lo cree y no es raro encontrar en algún medio de comunicación electrónica nuevo reenvíos del mensaje original. De hecho, es totalmente inviable la posibilidad de una infección vía correo electrónico.

El riesgo de contraer un virus en la Internet es menor que de cualquier otra manera, tanto los mensajes de correo, como las página WEB transfieren datos. Sólo si se trae un software por la red y lo instala en su máquina puede contraer un virus

Una infección se soluciona con las llamadas "vacunas" (que impiden la infección) o con los remedios que desactivan y eliminan, (o tratan de hacerlo) a los virus de los archivos infectados. Hay cierto tipo de virus que no son desactivables ni removibles, por lo que se debe destruir el archivo infectado.

## X. PREVENCIÓN, DETECCIÓN Y ELIMINACIÓN

Una buena política de prevención y detección nos puede ahorrar sustos y desgracias. Las medidas de prevención pasan por el control, en todo momento, del software ya introducido o que se va a introducir en nuestro ordenador, comprobando la fiabilidad de su fuente. Esto implica la actitud de no aceptar software no original, ya que el pirateo es una de las principales fuentes de contagio de un virus, siendo también una practica ilegal y que hace mucho daño a la industria del software.

Por supuesto, el sistema operativo, que a fin de cuentas es el elemento software más importante del ordenador, debe ser totalmente fiable; si éste se encuentra infectado, cualquier programa que ejecutemos resultara también contaminado. Por eso, es imprescindible contar con una copia en disquetes del sistema operativo, protegidos éstos contra escritura; esto ultimo es muy importante, no solo con el S.O. sino con el resto de disquetes que poseamos. Es muy aconsejable mantenerlos siempre protegidos, ya que un virus no puede escribir en un disco protegido de esta forma. Por último es también imprescindible poseer un buen software antivirus, que detecte y elimine cualquier tipo de intrusión en el sistema.

Debido a que los virus informáticos son cada vez más sofisticados, hoy en día es difícil sospechar su presencia a través de síntomas frecuentes. De todas maneras la siguiente es una lista de síntomas que pueden observarse en una computadora de la que se sospeche esté infectada por alguno de los virus más comunes:

Operaciones de procesamiento más lentas.

Los programas tardan más tiempo en cargarse.

Los programas comienzan a acceder por momentos a las disqueteras y/o al disco rígido.

Disminución no justificada del espacio disponible en el disco rígido y de la memoria RAM disponible, en forma constante o repentina.

Aparición de programas residentes en memoria desconocidos.

La primera medida de prevención a ser tenida en cuenta es, como se dijo anteriormente, contar con un sistema antivirus y utilizarlo correctamente. Por lo tanto, la única forma de que se constituya un bloqueo eficaz para un virus es que se utilice con determinadas normas y procedimientos. Estas normas tienden a controlar la entrada de archivos al disco rígido de la computadora, lo cual se logra revisando con el antivirus todos los disquetes o medios de almacenamiento en general y, por supuesto, disminuyendo al mínimo posible todo tipo de tráfico.

Además de utilizar un sistema antivirus y controlar el tráfico de archivos al disco rígido, una forma bastante eficaz de **proteger los archivos ejecutables** es utilizar un programa **chequeador de integridad** que verifique que estos archivos no sean modificados, es decir, que mantengan su estructura. De esta manera, antes que puedan ser infectados por un virus convencional, se impediría su accionar.

Para prevenir la infección con un **virus de sector de arranque**, lo más indicado es no dejar disquetes olvidados en la disquetera de arranque y contar con un antivirus. Pero, además, puede aprovecharse una característica que incorpora el setup de las computadoras más modernas: variar la secuencia de arranque de la PC a "**primero disco rígido y luego disquetera**" (C, A). De esta manera, la computadora no intentará leer la disquetera en el arranque aunque tenga cargado un disquete.

Algunos distribuidores o representantes de programas antivirus envían muestras de los nuevos virus argentinos a los desarrolladores del producto para que los estudien o incluyan en sus nuevas versiones o upgrades, con la demora que esto implica.

En consecuencia, la detección alternativa a la de scanning y las de chequeo de actividad e integridad resultan importantes, ya que pueden detectar la presencia de un virus informático sin la necesidad de identificarlo. Y esta es la única forma disponible para el usuario de detectar virus nuevos, sean nacionales o extranjeros. De todas maneras, **existe una forma de actualizar la técnica de scanning**. La misma consiste en incorporarle al antivirus un archivo conteniendo cadenas de caracteres ASCII que sean trozos de código (strings) significativos del sector vital de cada nuevo virus que todavía no esté incorporado en la base de datos del programa.

De todas formas, esta solución será **parcial**: la nueva cadena introducida sólo *identificará* al virus, pero no será capaz de erradicarlo.

Es muy importante que los "strings" que se vayan a incorporar al antivirus provengan de una fuente confiable ya que, de lo contrario, pueden producirse falsas alarmas o ser ineficaces.

Algunos de los antivirus que soportan esta cualidad de *agregar* strings son Viruscan, F-Prot y Thunderbyte.

La NCSA (National Computer Security Association, Asociación Nacional de Seguridad de Computadoras) es la encargada de certificar productor antivirus.

Para obtener dicha certificación los productos deben pasar una serie de rigurosas pruebas diseñadas para asegurar la adecuada protección del usuario.

Antiguamente el esquema de certificación requería que se detectara (incluyendo el número de versión) el 90 % de la librería de virus del NCSA, y fue diseñado para asegurar óptimas capacidades de detección. Pero esta metodología no era completamente eficiente.

Actualmente, el esquema de certificación enfoca la amenaza a las computadoras empresariales. Para ser certificado, el producto debe pasar las siguientes pruebas: Debe detectar el 100% de los virus encontrados comúnmente. La lista de virus comunes es actualizada periódicamente, a medida que nuevos virus son descubiertos.

Deben detectar, como mínimo, el 90% de la librería de virus del NCSA (más de 6.000 virus)

Estas pruebas son realizadas con el producto ejecutándose con su configuración "por defecto".

Una vez que un producto ha sido certificado, la NCSA tratará de recertificar el producto un mínimo de cuatro veces. Cada intento es realizado sin previo aviso al desarrollador del programa. Esta es una buena manera de asegurar que el producto satisface el criterio de certificación.

Si un producto no pasa la primera o segunda prueba, su distribuidor tendrá siete días para proveer de la corrección. Si este límite de tiempo es excedido, el producto será eliminado de la lista de productos certificados.

Una vez que se ha retirado la certificación a un producto la única forma de recuperarla es que el distribuidor envíe una nueva versión completa y certificable (no se aceptará sólo una reparación de la falla).

Acercas de la lista de virus de la NCSA, aclaremos que ningún desarrollador de antivirus puede obtener una copia. Cuando un antivirus falla en la detección de algún virus incluido en la lista, una cadena identificatoria del virus le es enviada al productor del antivirus para su inclusión en futuras versiones.

En el caso de los virus polimórficos, se incluyen múltiples copias del virus para asegurar que el producto testeado lo detecta perfectamente. Para pasar esta prueba el antivirus debe detectar cada mutación del virus.

La A. V. P. D. (Antivirus Product Developers, Desarrolladores de Productos Antivirus) es una asociación formada por las principales empresas informáticas del sector, entre las que se cuentan:

Cheyenne Software

I. B. M.

Intel

McAfee Associates

ON Technology

Stiller Research Inc.

S&S International

Symantec Corp.

ThunderByte

#### **a. UN DISCO DE SISTEMA PROTEGIDO CONTRA ESCRITURA Y LIBRE DE VIRUS:**

Un disco que contenga el sistema operativo ejecutable (es decir, que la máquina pueda ser arrancada desde este disco) con protección contra escritura y que contenga, por lo menos, los siguientes comandos: FORMAT, FDISK, MEM y CHKDSK (o SCANDISK en versiones recientes del MS-DOS).

**b. POR LO MENOS UN PROGRAMA ANTIVIRUS ACTUALIZADO:**

Se puede considerar actualizado a un antivirus que no tiene más de tres meses desde su fecha de creación (o de actualización del archivo de strings). Es muy recomendable tener por lo menos dos antivirus.

**c. UNA FUENTE DE INFORMACIÓN SOBRE VIRUS ESPECÍFICOS:**

Es decir, algún programa, libro o archivo de texto que contenga la descripción, síntomas y características de por lo menos los cien virus más comunes.

**d. UN PROGRAMA DE RESPALDO DE ÁREAS CRÍTICAS:**

Algún programa que obtenga respaldo (backup) de los sectores de arranque de los disquetes y sectores de arranque maestro (MBR, Master Boot Record) de los discos rígidos. Muchos programas antivirus incluyen funciones de este tipo.

**e. LISTA DE LUGARES DÓNDE ACUDIR:**

Una buena precaución es no esperar a necesitar ayuda para comenzar a buscar quién puede ofrecerla, sino ir elaborando una agenda de direcciones, teléfonos y direcciones electrónicas de las personas y lugares que puedan servirnos más adelante. Si se cuenta con un antivirus comercial o registrado, deberán tenerse siempre a mano los teléfonos de soporte técnico.

**f. UN SISTEMA DE PROTECCIÓN RESIDENTE:**

Muchos antivirus incluyen programas residentes que previenen (en cierta medida), la intrusión de virus y programas desconocidos a la computadora.

**g. TENER RESPALDOS:**

Se deben tener respaldados en disco los archivos de datos más importantes, además, se recomienda respaldar todos los archivos ejecutables. Para archivos muy importantes, es bueno tener un respaldo doble, por si uno de los discos de respaldo se daña. Los respaldos también pueden hacerse en cinta (tape backup), aunque para el usuario normal es preferible hacerlo en discos, por el costo que las unidades de cinta representan.

**h. REVISAR TODOS LOS DISCOS NUEVOS ANTES DE UTILIZARLOS:**

Cualquier disco que no haya sido previamente utilizado debe ser revisado, inclusive los programas originales (pocas veces sucede que se distribuyan discos de programas originales infectados, pero es factible) y los que se distribuyen junto con revistas de computación.

**i. REVISAR TODOS LOS DISCOS QUE SE HAYAN PRESTADO:**

Cualquier disco que se haya prestado a algún amigo o compañero de trabajo, aún aquellos que sólo contengan archivos de datos, deben ser revisados antes de usarse nuevamente.

**j. REVISAR TODOS LOS PROGRAMAS QUE SE OBTENGAN POR MÓDEM O REDES:**

Una de las grandes vías de contagio la constituyen Internet y los BBS, sistemas en los cuales es común la transferencia de archivos, pero no siempre se sabe desde dónde se está recibiendo información.

**k. REVISAR PERIÓDICAMENTE LA COMPUTADORA:**

Se puede considerar que una buena frecuencia de análisis es, por lo menos, mensual.

Finalmente, es importante tener en cuenta estas sugerencias referentes al comportamiento a tener en cuenta frente a diferentes situaciones:

Cuando se va a revisar o desinfectar una computadora, es conveniente apagarla por más de 5 segundos y arrancar desde un disco con sistema, libre de virus y protegido contra escritura, para eliminar virus residentes en memoria. No se deberá ejecutar ningún programa del disco duro, sino que el antivirus deberá estar en el disquete. De esta manera, existe la posibilidad de detectar virus stealth.

Cuando un sector de arranque (boot sector) o de arranque maestro (MBR) ha sido infectado, es preferible restaurar el sector desde algún respaldo, puesto que en ocasiones, los sectores de arranque genéricos utilizados por los antivirus no son perfectamente compatibles con el sistema operativo instalado. Además, los virus no siempre dejan un respaldo del sector original donde el antivirus espera encontrarlo.

Antes de restaurar los respaldos es importante no olvidar apagar la computadora por más de cinco segundos y arrancar desde el disco libre de virus.

Cuando se encuentran archivos infectados, es preferible borrarlos y restaurarlos desde respaldos, aún cuando el programa antivirus que usemos pueda desinfectar los archivos. Esto es porque no existe seguridad sobre si el virus detectado es el mismo para el cual fueron diseñadas las rutinas de desinfección del antivirus, o es una mutación del original.

Cuando se va a formatear un disco rígido para eliminar algún virus, debe recordarse apagar la máquina por más de cinco segundos y posteriormente arrancar el sistema desde nuestro disquete limpio, donde también debe encontrarse el programa que se utilizará para dar formato al disco.

Cuando, por alguna causa, no se puede erradicar un virus, deberá buscarse la asesoría de un experto directamente pues, si se pidiera ayuda a cualquier

aficionado, se correrá el riesgo de perder definitivamente datos si el procedimiento sugerido no es correcto.

Cuando se ha detectado y erradicado un virus es conveniente reportar la infección a algún experto, grupo de investigadores de virus, soporte técnico de programas antivirus, etc. Esto que en principio parecería innecesario, ayuda a mantener estadísticas, rastrear focos de infección e identificar nuevos virus, lo cual en definitiva, termina beneficiando al usuario mismo.

## I. Consiga un programa antivirus

Actualizado, de los tantos que se ofrecen en el mercado, la mayoría de ellos muy efectivos, los que incluso permiten su actualización "en línea", vía Internet. Tal es el caso del Norton AntiVirus (por citar alguno, quizás el más popular). Si le interesa, puede bajar versiones "trial" (válidas por 30 días), de este programa en español desde aquí: Norton AntiVirus 5.0 para Windows 95 (12Mb) y Norton AntiVirus 5.0 para Windows 98 (12Mb) (es necesario registrarse primero para hacer el "download"). Alternativamente Ud. puede consultar nuestras sugerencias, más adelante en el tema "Software Detector".

- ✓ **Inicie** su computadora, por ahora solo para entrar al "setup" de BIOS y habilitar allí (opción *enable*) el arranque de su computadora a partir de un *disquete de inicio*. Esto es así, porque supuestamente Ud. habría configurado el arranque de su computadora a partir únicamente del disco rígido **C:** (justamente para evitar una infección a partir de disquetes contaminados y "olvidados" en la unidad **A:**)
- ✓ **Reinicie** su computadora con el *disquete de inicio* obtenido en el punto 2.

Cuando aparezca el indicador **C:\>\_ ejecute el archivo kill\_cih.exe** Este programa desactiva el virus de memoria, deteniendo así sus acciones de infección, para permitir la remoción por parte del antivirus. Es importante tener en cuenta, que este ejecutable **no elimina el virus**, sino que impide su proceso de infección, desactivándolo de memoria... hasta la próxima vez que se inicia la computadora.

Si su disco de inicio estuviese infectado, **es posible** que esta utilidad **no detecte** la infección, pero de todas formas es importante correrla antes de ejecutar el antivirus (o de actualizarlo por Internet), ya que si se intenta la desinfección antes, sólo se estará infectando al resto de los archivos con el virus. Entonces estará en condiciones de aplicar un potente antivirus de reconocida eficacia, sin prisa, configurándolo para que rastree **todo tipo de archivo**: ejecutables o no, incluyendo a los comprimidos.

**m. Si su computadora NO PUEDE reiniciarse:**

- ✓ **Encienda su computadora** e intente entrar al "setup" de BIOS. Pruebe el auto-reconocimiento de su disco rígido. Verifique que efectivamente la ROM BIOS reconozca a su disco rígido. Si su disco rígido es reconocido, continúe con el procedimiento anterior en el punto a.  
Si su rígido no es reconocido, **controle cuidadosamente** las conexiones físicas (conectores y cables bien enchufados). Una buena manera de hacerlo, es desenchufando y enchufando cada conector, uno por uno... sin olvidar ninguno.
- ✓ **Reinicie** su computadora con el *disquete de inicio* obtenido en el punto 2. Cuando aparezca el indicador **A:\>\_ escriba fdisk /mbr** y pulse ENTER. Si el daño estaba localizado en una partición del disco rígido, esta acción será suficiente para restaurarla y corregirla. Se comprueba reiniciando exitosamente la computadora.

Alternativamente, en el CD de instalación de Windows 95/98 **puede recurrir** a un programa llamado **ERU** (Utilidad de Recuperación de Emergencia) que es muy útil en estos casos, sin embargo es necesario **correrlo antes de que llegue el problema**, pues el ERU lo que hace es sacar una copia muy completa de los archivos del registro y de la configuración de sistema operativo, para poder hacer la restauración posteriormente.

- ✓ **Si las acciones anteriores fallan**, llega el momento de **intentar el formateo en bajo nivel** del disco rígido, operación muy delicada y específica para técnicos especializados, que no recomiendo la practique un usuario no calificado técnicamente.

## XI. SOFTWARE DETECTOR

El más grande impacto es localizado en las computadoras personales, dice *Viveros*, quien agrega que los usuarios pueden descargar programas anti-virus libre desde su empresa ubicada en el sitio <http://www.nai.com/> El virus puede venir a través del e-mail o en programas pirateados contaminados.

Si es Ud. usuario de Norton AntiVirus recientemente actualizado, de seguro está cubierto, como lo afirman sus fabricantes. Si su antivirus no posee el último archivo de definiciones, debería correr el "LiveUpdate!". Symantec aconseja que esa actualización se haga por lo menos con una frecuencia mensual. Nuevas definiciones de virus están disponible vía el LiveUpdate! en la publicaciones semanales.

Si tiene grandes sospechas de estar infectado, puede bajar una herramienta gratis para Windows 95/98 desde el sitio Symantec's web que detectará y eliminará el CIH virus.

### a. ¿Mi computadora puede contraer una infección cuando navego por internet?

Por el simple hecho de estar conectado a internet no se transfiere ningún tipo de virus informático. Existe quizá algún peligro, examinando páginas web o "bajando" archivos de la red.

Las páginas web que utilizan objetos *ActiveX* pueden contener virus, puesto que ellos son realmente ficheros ejecutables, recogidos por nuestro navegador y ejecutados en nuestras PC. Podrían eventualmente ser utilizados inescrupulosamente para propagar un virus.

La "seguridad" de los objetos *ActiveX* consiste simplemente en un **certificado digital de autenticidad**, "firmado" por quien ha creado el objeto. Pero un simple certificado de autenticidad **no puede garantizar** que no esté un virus presente.

También podemos recibir páginas que utilizan *Applets* de Java. Estos programas no llegan a ser descargados por nuestro navegador, se ejecutan en un entorno muy restringido, y no hay acceso a la PC, o al disco duro, con lo que resulta prácticamente imposible infectarnos con applets (al menos hoy por hoy).

Durante el proceso de descarga de ficheros, también es muy difícil recoger un virus, tenemos las mismas condiciones que con los applets de java, pero una vez que el fichero ha llegado completamente a nuestro PC, **debe ser chequeado antes de ejecutarse**, ya que podría contener un virus.

## b. ¿Qué hacer con los virus del correo electrónico?

Con estos podemos estar tranquilos, ya que un virus no puede copiarse ni romper nuestro disco duro tan solo por leer un correo electrónico, porque se trata simplemente de un archivo de texto (no ejecutable).

Una cosa muy diferente, son los ficheros adjuntos (attachments), ya que podemos recibir un fichero ejecutable que podría contener un virus. Lo mejor es **no ejecutar directamente los archivos desde nuestro navegador**, sino almacenarlos en nuestro disco duro y antes de ejecutarlos, chequearlos con un anti-virus confiable.

Es recomendable por lo mismo, **abstenerse en lo posible de enviar archivos adjuntos**, por idéntico riesgo que representa para nuestros correspondientes.

Si su programa de correo electrónico está configurado para leer los mensajes automáticamente con Microsoft Word, es posible recibir un virus-macro e infectar a nuestro Ms-Word. Si tiene esta opción activada; desactívala, y chequea los ficheros recibidos antes de ejecutarlos.

Finalmente, y por si quedara alguna duda, lo mejor es **tomar por norma** eliminar los ficheros recibidos por correspondientes desconocidos, aquellos que no hemos solicitado. No exponga sus datos a un riesgo innecesario por abrir (o ejecutar) un archivo desconocido.

## XII. ¿QUÉ ES UN ANTIVIRUS?.

No para toda enfermedad existe cura, como tampoco existe una forma de erradicar todos y cada uno de los virus existentes.

Es importante aclarar que todo antivirus es un programa y que, como todo programa, sólo funcionará correctamente si es adecuado y está bien configurado. Además, un antivirus es una herramienta para el usuario y no sólo **no será eficaz para el 100% de los casos**, sino que **nunca será una protección total ni definitiva**.

La función de un programa antivirus es detectar, de alguna manera, la presencia o el accionar de un virus informático en una computadora. Este es el aspecto más importante de un antivirus, independientemente de las prestaciones adicionales que pueda ofrecer, puesto que el hecho de detectar la posible presencia de un virus informático, detener el trabajo y tomar las medidas necesarias, es suficiente para acotar un buen porcentaje de los daños posibles. Adicionalmente, un antivirus puede dar la opción de erradicar un virus informático de una entidad infectada.

El modelo más primario de las funciones de un programa antivirus es la detección de su presencia y, en lo posible, su identificación. La primera técnica que se popularizó para la detección de virus informáticos, y que todavía se sigue utilizando (aunque cada vez con menos eficiencia), es la técnica de **scanning**. Esta técnica consiste en revisar el código de todos los archivos contenidos en la unidad de almacenamiento -fundamentalmente los archivos ejecutables- en busca de pequeñas porciones de código que puedan pertenecer a un virus informático. Este procedimiento, denominado **escaneo**, se realiza a partir de una base de datos que contiene trozos de código representativos de cada virus conocido, agregando el empleo de determinados algoritmos que agilizan los procesos de búsqueda.

La técnica de **scanning** fue bastante eficaz en los primeros tiempos de los virus informáticos, cuando había pocos y su producción era pequeña. Este relativamente pequeño volumen de virus informáticos permitía que los desarrolladores de antivirus escaneadores tuvieran tiempo de analizar el virus, extraer el pequeño trozo de código que lo iba a identificar y agregarlo a la base de datos del programa para lanzar una nueva versión. Sin embargo, la obsolescencia de este mecanismo de identificación como una solución antivirus completa se encontró en su mismo modelo.

El primer punto grave de este sistema radica en que siempre brinda una solución *a posteriori*: es necesario que un virus informático alcance un grado de dispersión considerable para que sea enviado (por usuarios capacitados, especialistas o distribuidores del producto) a los desarrolladores de antivirus. Estos lo analizarán,

extraerán el trozo de código que lo identificará, y lo incluirán en la próxima versión de su programa antivirus. Este proceso puede demorar meses a partir del momento en que el virus comienza a tener una dispersión considerable, lapso en el cual puede causar graves daños sin que pueda ser identificado.

Además, **este modelo consiste en una sucesión infinita de soluciones parciales y momentáneas (cuya sumatoria jamás constituirá una solución definitiva)**, que deben actualizarse periódicamente debido a la aparición de nuevos virus.

En síntesis, la técnica de scanning es altamente ineficiente, pero se sigue utilizando debido a que permite identificar rápidamente la presencia de los virus más conocidos y, como son estos los de mayor dispersión, permite una importante gama de posibilidades.

Un ejemplo típico de un antivirus de esta clase es el **Viruscan de McAfee**, que se verá más adelante.

En virtud del pronto agotamiento técnico de la técnica de scanning, los desarrolladores de programas antivirus han dotado a sus creaciones de métodos para búsquedas de virus informáticos (y de sus actividades), que no identifican específicamente al virus sino a algunas de sus características generales y comportamientos universalizados.

Este tipo de método rastrea rutinas de alteración de información que no puedan ser controladas por el usuario, modificación de sectores críticos de las unidades de almacenamiento (master boot record, boot sector, FAT, entre otras), etc.

Un ejemplo de este tipo de métodos es el que utiliza algoritmos **heurísticos**.

De hecho, esta naturaleza de procedimientos busca, de manera bastante eficiente, códigos de instrucciones potencialmente pertenecientes a un virus informático. Resulta eficaz para la detección de virus conocidos y es una de las soluciones utilizadas por los antivirus para la detección de nuevos virus. El inconveniente que presenta este tipo de algoritmo radica en **que puede llegar a sospecharse de muchísimas cosas que no son virus**. Esto hace necesario que el usuario que lo utiliza conozca un poco acerca de la estructura del sistema operativo, a fin de poseer herramientas que le faciliten una discriminación de cualquier falsa alarma generada por un método heurístico.

Algunos de los antivirus de esta clase son F-Prot, Norton Anti Virus y Dr. Solomon's Toolkit.

Ahora bien, otra forma de detectar la presencia de un virus informático en un sistema consiste en monitorear las actividades de la PC señalando si algún proceso intenta modificar los sectores críticos de los dispositivos de

almacenamiento o los archivos ejecutables. Los programas que realizan esta tarea se denominan **chequeadores de integridad**.

Sobre la base de estas consideraciones, podemos consignar que **un buen sistema antivirus** debe estar compuesto por **un programa detector de virus** - que siempre esté residente en memoria- y **un programa que verifique la integridad** de los sectores críticos del disco rígido y sus archivos ejecutables. Existen productos antivirus que cubren los dos aspectos, o bien pueden combinarse productos diferentes configurados de forma que no se produzcan conflictos entre ellos.

### XIII. MODELO ANTIVIRUS:

La estructura de un programa antivirus, está compuesta por dos módulos principales: el primero denominado **de control** y el segundo denominado **de respuesta**. A su vez, cada uno de ellos se divide en varias partes:

**Módulo de control:** posee la técnica **verificación de integridad** que posibilita el registro de cambios en los archivos ejecutables y las zonas críticas de un disco rígido. Se trata, en definitiva, de una herramienta preventiva para mantener y controlar los componentes de información de un disco rígido que no son modificados a menos que el usuario lo requiera.

Otra opción dentro de este módulo es la **identificación de virus**, que incluye diversas técnicas para la detección de virus informáticos. Las formas más comunes de detección son el scanning y los algoritmos, como por ejemplo, los heurísticos.

Asimismo, la **identificación de código dañino** es otra de las herramientas de detección que, en este caso, busca instrucciones peligrosas incluidas en programas, para la integridad de la información del disco rígido.

Esto implica descompilar (o desensamblar) en forma automática los archivos almacenados y ubicar sentencias o grupos de instrucciones peligrosas.

Finalmente, el módulo de control también posee una **administración de recursos** para efectuar un monitoreo de las rutinas a través de las cuales se accede al hardware de la computadora (acceso a disco, etc.). De esta manera puede limitarse la acción de un programa restringiéndole el uso de estos recursos, como por ejemplo impedir el acceso a la escritura de zonas críticas del disco o evitar que se ejecuten funciones de formato del mismo.

#### a. Módulo de respuesta:

la función **alarma** se encuentra incluida en todos los programas antivirus y consiste en detener la acción del sistema ante la sospecha de la presencia de un virus informático, e informar la situación a través de un aviso en pantalla.

Algunos programas antivirus ofrecen, una vez detectado un virus informático, la posibilidad de erradicarlo. Por consiguiente, la función **reparar** se utiliza como una solución momentánea para mantener la operatividad del sistema hasta que pueda instrumentarse una solución adecuada. Por otra parte, existen dos **técnicas para evitar el contagio de entidades ejecutables**: evitar que se contagie todo el programa o prevenir que la infección se expanda más allá de un ámbito fijo.

Aunque la primera opción es la más adecuada, plantea grandes problemas de implementación.

#### **XIV. ALGUNOS ANTIVIRUS.**

Certificado por la NCSA. Detecta más de 6.500 virus gracias a su propio lenguaje de detección llamado **VirTran**, con una velocidad de detección entre 3 y 5 veces mayor que los antivirus tradicionales.

Uno de los últimos desarrollos de S&S es la tecnología G. D. E. (Generic Decription Engine, Motor de Desenscriptación Genérica) que permite detectar virus polimórficos sin importar el algoritmo de encriptación utilizado.

Permite detectar modificaciones producidas tanto en archivos como en la tabla de partición del disco rígido. Para ello utiliza Checksumms Criptográficos lo cual, sumado a una clave personal de cada usuario, hace casi imposible que el virus pueda descubrir la clave de encriptación.

Elimina virus en archivos en forma sencilla y efectiva con pocas falsas alarmas, y en sectores de buteo y tablas de partición la protección es genérica, es decir, independiente del virus encontrado.

Otras características que presenta este antivirus, son:

Ocupa 9K de memoria extendida o expandida.

Documentación amplia y detallada en español y una enciclopedia sobre los virus más importantes.

Actualizaciones mensuales o trimestrales de software y manuales.

Trabaja como residente bajo Windows.

H. A. (Advanced Heuristic Analysis, Análisis Heurístico Avanzado).

##### **a) NORTON ANTIVIRUS.**

Certificado por la NCSA. Posee una protección automática en segundo plano. Detiene prácticamente todos los virus conocidos y desconocidos (a través de una tecnología propia denominada **NOVI**, que implica control de las actividades típicas de un virus, protegiendo la integridad del sistema), antes de que causen algún daño o pérdida de información, con una amplia línea de defensa, que combina búsqueda, detección de virus e **inoculación** (se denomina 'inoculación' al método por el cual este antivirus toma las características principales de los sectores de booteo y archivos para luego chequear su integridad. Cada vez que se detecta un cambio en dichas áreas, NAV avisa al usuario y provee las opciones de Reparar - Volver a usar la imagen guardada - Continuar - No realiza cambios - Inocular - Actualizar la imagen.

Utiliza diagnósticos propios para prevenir infecciones de sus propios archivos y de archivos comprimidos.

El escaneo puede ser lanzado manualmente o automáticamente a través de la planificación de fecha y hora. También permite reparar los archivos infectados por virus desconocidos. Incluye información sobre muchos de los virus que detecta y permite establecer una contraseña para aumentar así la seguridad.

La lista de virus conocidos puede ser actualizada periódicamente (sin cargo) a través de servicios en línea como Internet, América On Line, Compuserve, The Microsoft Network o el BBS propio de Symantec, entre otros.

## **b) VIRUSSCAN.**

Este antivirus de **McAfee Associates** es uno de los más famosos. Trabaja por el sistema de scanning descripto anteriormente, y es el mejor en su estilo.

Para escanear, hace uso de dos técnicas propias: CMS (Code Matrix Scanning, Escaneo de Matriz de Código) y CTS (Code Trace Scanning, Escaneo de Seguimiento de Código).

Una de las principales ventajas de este antivirus es que la actualización de los archivos de bases de datos de strings es muy fácil de realizar, lo cual, sumado a su condición de programa shareware, lo pone al alcance de cualquier usuario. Es bastante flexible en cuanto a la configuración de cómo detectar, reportar y eliminar virus.

## **c) Medidas antivirus**

Nadie que usa computadoras es inmune a los virus de computación. Un programa antivirus por muy bueno que sea se vuelve obsoleto muy rápidamente ante los nuevos virus que aparecen día a día.

Desactivar arranque desde disquete en el setup para que no se ejecuten virus de boot.

Desactivar compartir archivos e impresoras.

Analizar con el antivirus todo archivo recibido por e-mail antes de abrirlo.

Actualizar antivirus.

Activar la protección contra macrovirus del Word y el Excel.

Sea cuidadoso al bajar archivos de Internet (Analice si vale el riesgo y si el sitio es seguro)

No envíe su información personal ni financiera a menos que sepa quien se la solicita y que sea necesaria para la transacción.

No comparta discos con otros usuarios.

No entregue a nadie sus claves, incluso si lo llaman del servicio de Internet u otro.

Enseñe a sus niños las practicas de seguridad, sobre todo la entrega de información.

Cuando realice una transacción asegúrese de utilizar una conexión bajo SSL

Proteja contra escritura el archivo Normal.dot

Distribuya archivos RTF en vez de DOCs

Realice backups

## XV. DELITOS E INCIDENTES

**12 de diciembre de 1987.** El virus de **Navidad** Una tarjeta navideña digital enviada por medio de un BBS de IBM ataco las instalaciones en los EE.UU. por 90 minutos. Cuando se ejecutaba el virus este tomaba los Adress Book del usuario y se retransmitía automáticamente, además que luego colgaba el ordenador anfitrión.

Esto causo un desbordamiento de datos en la red.

**10 de enero de 1988.** El virus **Jerusalén** se ejecuta en una universidad hebrea y tiene como fecha límite el primer viernes 13 del año, como no pudieron pararlo se sufría una disminución de la velocidad cada viernes 13.

**20 de septiembre de 1988** en Fort Worth, Texas, Donald Gene un programador de 39 años será sometido a juicio el 11 de julio por cargos delictivos de que intencionadamente contaminó el sistema de por ser despedido, con un virus informático el año 85. Sera la primera persona juzgada con la ley de sabotaje que entro en vigor el 1 de septiembre de 1985. El juicio duro 3 semanas y el programador fue declarado culpable y condenado a siete años de libertad condicional y a pagar USD. 12000.

Su empresa que se dedicaba a la bolsa sufrió borro de datos, aproximadamente 168000 registros.

**4 de noviembre de 1988** Un virus invade miles de computadoras basadas en Unix en universidades e instalaciones de investigación militares, donde las velocidades fueron reducidas y en otros casos paradas. También el virus se propagó a escala internacional.

Se estableció que la infección no fue realizada por un virus sino por un programa **gusano**, diseñado para reproducirse así mismo indefinidamente y no para eliminar datos. El programa se difundió a través de un corrector de errores para correo electrónico, que se movió principalmente en Internet (Arpanet) y contamina miles de computadoras en todo el mundo contando 6000 computadoras en centros militares en los EE.UU. , incluyendo la NASA, la Fuerza Aérea, el MIT, las universidades de Berkeley, Illinois, Boston, Stanford, Harvard, Princeton, Columbia y otras. En general se determino que la infección se propago en las computadoras VAX de DEC (digital equipment corp) y las fabricadas por Sun Microsystems, que empleaban Unix.

Se halla al culpable Robert Morris, estudiante de 23 años, que declara haber cometido un error al propagar el gusano. Morris era el hijo de un experto en seguridad informática del gobierno.

El caso fue investigado por el FBI. Posiblemente se sentencie a Morris por 5 años de prisión y una multa USD. 250000.

**23 de marzo del 89** virus ataca sistemas informáticos de hospitales, variando la lectura de informes de laboratorio.

Y los últimos pero recordados vaccina, hacker, cpw543, natas, antiexe, etc.

Los delitos cometidos utilizando la computadora han crecido en tamaño, forma y variedad.

En la actualidad (1994) los delitos cometidos tienen la peculiaridad de ser descubiertos en un 95% de forma casual. Podemos citar a los principales delitos hechos por computadora o por medio de computadoras estos son:

- ✓ fraudes
- ✓ falsificación
- ✓ venta de información

Entre los hechos criminales más famosos en los E.E.U.U. están:

El caso del Banco Wells Fargo donde se evidencio que la protección de archivos era inadecuada, cuyo error costo USD 21.3 millones.

El caso de la NASA donde dos alemanes ingresaron en archivos confidenciales.

El caso de un muchacho de 15 años que entrando a la computadora de la Universidad de Berkeley en California destruyo gran cantidad de archivos.

También se menciona el caso de un estudiante de una escuela que ingreso a una red canadiense con un procedimiento de admirable sencillez, otorgándose una identificación como un usuario de alta prioridad, y tomo el control de una embotelladora de Canadá.

También el caso del empleado que vendió la lista de clientes de una compañía de venta de libros, lo que causo una perdida de USD 3 millones.

**Conclusión**

Estos hechos y otros nos muestran claramente que los componentes del sistema de información no presentaban un adecuado nivel de seguridad. Ya que el delito se cometió con y sin intención, utilizando siempre alguno de los diferentes tipos de virus.

**Manual publicado en**



**Con la autorización de sus autores**

<http://www.mundopc.net/cursos>