UNIVERSIDAD POPULAR AUTONOMA DEL ESTADO DE PUEBLA

SISTEMAS COMPUTACIONALES

Desarrollo de un tutorial para contribuir a la disminución de contagio de virus en la U.P.A.E.P.

TESIS

Que para obtener el título:

Licenciado en Sistemas Computacionales

Presentan:

Claudia Malcón Cervera
María Alejandra Sarmiento Ramírez

Asesor:

Ing. Marco Antonio Carrasco Dávila

H. Puebla de Zaragoza 1995

Deseamos expresar nuestro agradecimiento con admiración y respeto a la Institución que nos formó:

UNIVERSIDAD POPULAR AUTONOMA DEL ESTADO DE PUEBLA

Al Ing. Marco Antonio Carrasco Dávila, por su colaboración y asesoría en la realización de esta tesis.

Al Ing. José María Bedolla Cordero, por el interés y el apoyo mostrado durante la realización de este trabajo.

A todas aquellas personas que de alguna manera, con su apoyo, consejos y colaboración, hicieron posible que este trabajo llegara a su fin.

A Dios, por permitirme realizar una meta más y acompañarme en cada momento difícil y feliz de mi vida.

A mis padres Susana y José Isabel, por su infinita confianza depositada en mí, por su comprensión y cariño. Muchas gracias

A Aliz, por tu insuperable apoyo, tu gran cariño, y enorme sacrificio para la realización de mi vida profesional. Gracias hermana, te quiero mucho.

A mis hermanos Charito y Miguel Angel, por su compañía y solidaridad en los problemas cotidianos. Los quiero mucho.

A Claudia, una gran amiga, por tu apoyo y valiosa ayuda para la realización de este proyecto. Gracias por tu inigualable amistad.

A Rubén, por tu amor y compañía. Gracias, te quiero mucho.

A mis grandes amigos y valiosos compañeros, con los cuales compartí tantas y bonitas experiencias Los recordaré siempre.

Alejandra

A Dios, por estar conmigo en todo momento y por permitirme tener a mi familia y amigos.

A mis padres Armando y Josefina, a mis hermanos Armando y Carolina, por el gran amor, confianza y apoyo que he recibido de ustedes. Dios los bendiga.

A mi abuelo, a mis tíos y primos, por el tiempo que hemos convivido y por el cariño y consejos brindados.

A Juan Carlos, por el cariño, comprensión y alegrías que me has brindado desde el momento en que nos conocimos.

A Alejandra, por tu amistad y por todos los momentos compartidos al realizar la tesis.

A mis grandes amigos, por todas las alegrías y tristezas compartidas, por el apoyo, confianza y comprensión. Los quiero mucho.

Claudia

INDICE

LISTA DE TABLAS

LISTA DE FIGURAS

INTRODUCCION

En esta tesis se presenta una investigación sobre los virus computacionales, a los que se les llama así, por su similitud con el funcionamiento de los virus biológicos

Los virus biológicos son pequeños organismos que infectan algunas células del organismo humano y modifican su información genética al irse reproduciendo dentro de las células afectadas, también pueden estar latentes en el organismo durante bastante tiempo sin que éste presente ningún síntoma de infección. Cuando sufren mutaciones resulta muy difícil detectarlos y, por lo tanto, difíciles de combatir una vez que se han presentado los síntomas.

Los virus computacionales son pequeños programas que infectan a otros programas ejecutables, modifican su estructura y se reproducen dentro de éstos También pueden estar latentes en el sistema (infectando discos y programas), y no presentan problemas durante largos periodos. Además algunos se modifican por sí solos para evitar que sean detectados fácilmente.

Actualmente en los Centros de Cómputo UPAEP hay un alto índice de propagación de virus computacionales debido a la gran cantidad de copias ilegales que se realizan entre los alumnos y a la falta de información real sobre estos programas, provocando la pérdida o alteración de archivos de datos o archivos ejecutables almacenados en discos, desplegando en la pantalla mensajes misteriosos o de burla, y causando una conducta anormal del sistema operativo y/o del sistema de trabajo utilizado

Para disminuir esta propagación se realizó este trabajo de investigación, enfocado principalmente a los alumnos de la UPAEP que inician en sus estudios de computación; además se desarrolló un tutorial en Visual Basic™, el cual contiene información sobre los virus computacionales, su origen, medios de contagio, funcionamiento y medidas de protección; además de prácticas de detección y erradicación de los mismos con los programas Norton Antivirus™, Central Point Antivirus™ y VirusScan™ y muestra los efectos de los virus por medio de simuladores

Dicho tutorial se proporcionará a los directores de carreras y a la dirección general de bachilleratos UPAEP, para que lo apliquen a sus alumnos.

Dado el objetivo principal de este trabajo, que es desarrollar la cultura computacional en los alumnos de la UPAEP para no utilizar copias ilegales de programas y disminuir la incidencia de contagio de virus, se presentan en el primer capítulo los conceptos básicos y fundamentales de virus computacional, sus similitudes

con los virus biológicos, su origen, mitos y realidades

En el segundo capítulo se presenta la situación que impera en los centros de cómputo UPAEP, las medidas que actualmente se están tomando para controlar el contagio de virus y los resultados que se han obtenido

En el tercer capítulo se presentan los medios de contagio más frecuentes elegidos por los virus para ejercer su acción de expansión

En el cuarto se esquematiza el funcionamiento de los virus, las fases de su ciclo de vida, sus lugares de almacenamiento, y las clasificaciones de los virus basadas en sus diferentes características: general, por la forma en que trabajan, por la parte que modifica el virus en su ataque y por la forma en que intentan ocultarse

En el quinto capítulo se presentan las medidas que se deben tomar para prevenir, detectar y erradicar los virus computacionales

En el sexto se presentan el análisis, diseño, implementación y manual del usuario del tutorial desarrollado en ambiente gráfico para ayudarle a entender el funcionamiento de los virus

En los apéndices se explica sobre la estructura y manejo de discos, archivos, memoria y el listado del tutorial. Al final se incluye un glosario con los términos utilizados en el desarrollo de esta investigación

Es importante aclarar que este estudio sólo abarca a los virus en las computadoras IBM™ PC o compatibles utilizando el sistema operativo MS-DOS™

CAPITULO 1. VIRUS COMPUTACIONALES

Dado el objetivo principal de este trabajo, que es desarrollar la cultura computacional en los alumnos de la UPAEP para no utilizar copias ilegales de programas y disminuir la incidencia de contagio de virus, se presentan en este capítulo los conceptos básicos y fundamentales de virus computacional, sus similitudes con los virus biológicos, su origen, mitos y realidades

Un virus computacional es un programa con la habilidad de reproducirse por sí mismo, actúa como parásito, debido a que necesita agregar una copia de sí mismo a algún programa ejecutable, para poder propagarse Es desarrollado por un programador con la misma creatividad con la que desarrolla un procesador de palabras, una hoja de cálculo o un juego; por lo tanto, un virus no puede hacer nada que no haya sido escrito en su código de programación

Un virus puede o no dañar datos o a otros programas, esto es, no necesita realizar forzosamente acciones destructivas para ser considerado "virus" Es suficiente con que tenga la capacidad de reproducirse.

Algunos virus son agresivos y causan serios daños Otros son casi amistosos y divertidos (la minoría). Por ejemplo, el virus Cookie Monster, el cual interrumpe el trabajo del usuario desplegando ocasionalmente en pantalla el mensaje "I want a cookie" El autor de este virus no tenía pensado causar daño deliberadamente. Sin embargo, en otros casos, por errores en la programación del virus se producirán efectos drásticos y no intencionados, como el virus Arpanet que se reprodujo infinitamente más rápido de lo que su autor anticipó

La gran mayoría de los virus son los que causan severos daños. Como por ejemplo los que alteran archivos de datos. Estos virus buscarán una hoja de cálculo y cambiarán números o la posición del punto decimal, haciendo que cambien por completo todos los cálculos En archivos de texto un virus puede cambiar palabras o frases por otras diferentes.

Otros virus pueden cambiar un comando normal del DOS en el momento más inoportuno, causando un grave daño Por ejemplo, que cuando se da el comando para grabar un archivo, el virus lo cambie por el comando FORMAT, destruyendo todos los datos del disco en el cual se intentó grabar.

Aparte de cambiar comandos, los virus pueden también redefinir muchas teclas con las que se invoca a esos comandos DOS y algunos programas de aplicación tienen la facilidad de hacer que la tecla "A" actúe como la "Z", como una macro, esto es, que al presionar una tecla, se ejecuten una serie de instrucciones

Otra táctica adoptada por algunos virus es revolver la FAT La FAT desempeña el papel de índice del sistema, indica en dónde están localizados cada uno de los diferentes archivos Un virus puede tomar toda esta información y revolverla, o cambiar el nombre de los archivos y, en el peor de los casos, borrar la FAT, impidiendo la localización de los archivos

Los programas portadores de virus son

- los programas ejecutables (con extensiones COM, EXE)
- overlays y drivers (OVL, OVR, SYS y DRV)
- del sistema operativo (IBMBIO COM, IBMDOS COM y COMMAND COM)
- boot o en la tabla de partición de un disco

Sólo cuando uno de estos programas es ejecutado es que el virus se activa

Según Nombela (1990, Pág. 23) "*Las fases de actuación de un virus son las siguientes*

1) Infección el virus llega a la computadora dentro de un programa contaminado contenido en algún disco. El usuario, inconciente del peligro potencial, ejecuta el programa infectado, con lo que el virus toma el control del sistema operativo de la computadora

2) Latencia los programas ejecutables que utilicemos en la computadora durante esta etapa serán modificados por el virus para incluir en ellos una copia de sí mismo, de tal forma que si copiamos uno de esos programas en un disco y lo llevamos a otra computadora, la infección se propagará a ésta

3) Activación Una vez que se da una determinada circunstancia, como por ejemplo la llegada de cierta fecha o cuando el número de infecciones ha alcanzado una determinada cifra, el virus se activa y comienza su acción destructora"

1.1. Analogía entre virus computacionales y virus biológicos

La denominación de virus corresponde a la similitud que tienen este tipo de programas con sus homónimos biológicos.

Los virus biológicos son células parásitas infecciosas que entran en otras células por encima del control del núcleo, forzándolo a recibir las órdenes del virus El núcleo celular infectado es forzado a emitir órdenes al resto de las células, mismas que ayudan a que se reproduzcan en vez de producir su alimento

En un muy corto periodo de tiempo, la célula infectada produce miles de virus La célula muere y los miles de virus nuevos son liberados en otras células para invadirlas Este proceso continúa hasta que los virus o las células que los contienen son destruidos

Los virus computacionales entran al programa, infectando e instalándose en una localidad donde puedan tomar el control de las órdenes para dirigir al programa desde el sistema operativo Entonces el programa infectado permanece inactivo y sus instrucciones son interceptadas y usadas por el virus en su contra para duplicarse El

virus usualmente hace dos o tres copias de sí mismo, por cada orden del sistema Retorna el control al programa anfitrión, el cual empieza a ejecutarse normalmente, aunque después de que se ha duplicado el código del virus, la ejecución del programa se va haciendo cada vez mas lenta

La forma por la cual un virus biológico se propaga es por contagio Esto es, los virus están habitualmente presentes e infectan sólo a algunas personas a la vez, o van y vienen atacando a una población sana, hasta debilitarla

Aunque el virus computacional esté presente, sólo infecta a algunos archivos, hasta que debilita al sistema haciéndolo más lento, destruyendo el programa anfitrión o todos los programas de la computadora

1.2. Origen de los virus

Según Nieto (1991, Págs 18-23) *Se ha pretendido otorgar a John Vonn Newmann la paternidad de los virus, debido a que en su libro titulado Theory and Organization of Complicated Automata, de 1949, expone la idea de una porción de código que se reproduce y por lo tanto está "vivo" Años más tarde, en 1955, en su obra The Computer and the Brain hace una disertación teórica sobre la posibilidad de crear un programa autómata capaz de reproducirse a sí mismo.*

Estos primeros indicios teóricos de autorreproducción no parecen ser lo bastante sólidos para establecer el origen

La clave en el origen de la difusión del fenómeno vírico se ha querido situar en una serie de artículos publicados en la revista americana Scientific American, firmados por A K Dewdney El primero de la serie, fechado en 1984 se tituló "Juegos del ordenador en el juego de la Guerra Nuclear dos programas hostiles entablan, sin que intervengan activamente los usuarios, batallas de bits para obtener el control de la memoria". Estos dos programas se ponen en marcha mediante un programa ejecutor llamado MARS (Memory Array Redcode Simulator). Ayudado por David Jones, fueron desarrollando programas cuya única función era producir una copia de sí mismo cien unidades de memoria más allá de su posición actual, transfiriendo después el control a la nueva copia

Por otro lado, John F Scoch, del Centro de Investigación de Xerox™, en Estados Unidos, creó un gusano Este programa experimental fue ideado para obtener el máximo rendimiento de una red de computadoras interconectadas de Xerox™ Un programa supervisor se encargaba de cargar el gusano en

máquinas inactivas para asumir su control y, en combinación con otros gusanos residentes en otras máquinas, hacer funcionar grandes programas de aplicación en el sistema multiprocesador resultante

En el texto de este primer artículo, Dewdney insta a los lectores a que reflejen sus ideas de programas autoprotectores y autorreparadores y establece las normas y reglas del juego Jamás hubiera imaginado el autor lo que acontecería

No se debe interpretar que Dewdney fue el inventor de los virus, más bien se debe ver como un impulsor involuntario de este tipo de programas al difundir un inocente y creativo juego

Otras versiones juegan con la paradoja ¿Qué fue primero, el virus o el antídoto? Insinúan que los virus proceden de fabricantes de programas que los combaten Esta idea no resulta demasiado sólida, dada la gran cantidad y variedad de programas contaminantes que circulan en el ambiente computacional

Probablemente también se puede otorgar el título de iniciadores de virus a los fabricantes de software, como medida de protección para evitar la copia de sus productos sin obtener beneficios Es evidente la pérdida económica que este delito produce en la industria del software, sin embargo, los virus han disminuido la compra, más que alentarla Tal parece que los "autores originales", "programadores resentidos" o "despedidos" los han anexado "completamente gratis" a cierto software con el fin de crearle mala imagen e impedir no sólo la copia ilegal sino la compra legal. Esto es tanto o más difícil de probar que la versión anterior, pero no menos coherente, porque si se supiera que un software X trae virus para impedir copias ilegales, posiblemente pocas personas se atreverían a comprarlo

Por lo tanto, resulta difícil establecer el verdadero origen de este tipo de programas Probablemente no surgieron de forma aislada en un único lugar y como idea de un único programador, sino que son el fruto de la ocurrencia simultánea de distintos programadores en varios países.

1.3. Mitos y realidades

Las computadoras pueden contagiarse de un virus de la misma forma en que se contagia usted

Según Levin (1991, Pág 5) "*Muchos usuarios creen erróneamente que los virus computacionales tienen alguna forma de vida electrónica o que emplean inteligencia artificial Otros creen que pueden propagarse de computadora en computadora sin requerir contacto físico entre sistemas distribuidos Otros creen que pueden vivir dentro*

de los circuitos de sus computadoras incluso después de que se haya cortado la corriente

Al contrario que sus correspondientes biológicos, los virus computacionales no pueden flotar en el aire ni adherirse a la piel e infectar otros sistemas por medio de tales contactos Por último, como todo programa, los virus no pueden actuar cuando la computadora esté apagada"

Los virus son una epidemia fuera de control

En la actualidad mucha gente está creando nuevos virus y, al mismo tiempo, se están reproduciendo deliberadamente los virus ya existentes en el ambiente computacional, sin embargo, existen programas antivirus (referirse al glosario) para contrarrestarlos.

Gran parte de la propagación es por programas infectados que aún no han mostrado síntomas. Cualquier persona que conecte su computadora con otra, por medio del teléfono o con una red, o que intercambie discos o los transporte de un sistema a otro, puede hacer que se reproduzcan los virus, deliberada o inocentemente

Los virus pueden propagarse en todo tipo de computadoras

Falso. Según Devorak (1989, Pág. 115) "*Los virus están limitados para una familia de computadoras; por ejemplo, un virus diseñado para propagarse en las IBM™ PCs no puede infectar un mainframe IBM™ 4300, ni tampoco a una Commodore™ C64, ni tampoco una Apple Macintosh™*"

Los virus dañan el hardware

Según VIRUS-L (1992) "*La habilidad de los virus para dañar el hardware o de poner en un cierto peligro a los usuarios, atrae periódicamente la atención popular, la cual ha sido muy exagerada. En teoría, un virus puede causar que un disco duro esté girando continuamente hasta que se dañe por la alta temperatura generada. Pero esta es una escena poco probable.*

Algunos tipos de monitores pueden ser dañados por un virus que repetitivamente esté enviando señales luminosas a alguna posición de la pantalla

En realidad, es virtualmente imposible que el software dañe el hardware sin que el usuario esté conciente de que algo está muy mal antes de que el daño físico pueda ocurrir"

El uso del correo electrónico es peligroso

La habilidad de los virus para dañar el correo electrónico ha sido también exagerada. Debido a que en esta comunicación lo que circulan predominantemente son datos y no programas, es que se tienen pocas y difíciles oportunidades de que los virus se escondan o que se propague una infección.

Los sistemas de correo electrónico que sólo transmiten datos en vaivén en modo texto (ASCII) están ahora relativamente a salvo de fenómenos dañinos potenciales

Hay un riesgo significativo de infección sólamente en sistemas que permiten transferir archivos ejecutables

A pesar de que los virus no pueden actualmente infectar datos, sí pueden viajar con ellos, los virus pueden estar programados para activarse y transmitirse por sí mismos cuando una línea electrónica esté abierta y se use software para llevar a cabo la transferencia Mientras los virus atacan y se esconden en programas, incluyen instrucciones para propagarse por si los datos transferidos contienen cierto código de programación.

Los boletines informativos (BBSs) propagan los virus rápidamente

Los boletines informativos son medios grandiosos para conocer nuevos amigos, conseguir información, y adquirir virus si no se tiene cuidado. Debido a su bajo costo, cada vez se incrementa más el número de usuarios

Debido a que su propósito principal es actuar como medio para el intercambio de datos (y a menudo programas), los boletines informativos son muy vulnerables a infecciones virales. Pero no permita que lo asuste esta epidemia y se aleje de este maravilloso medio; tenga cuidado al usar sus servicios

Los discos de respaldo serán destruidos si se respalda un virus

No Suponga que un virus se respaldó con otros de sus archivos Los respaldos son una forma de datos y no pueden dañar su sistema Usted puede rescatar los archivos importantes de sus respaldos sin activar el virus.

Una computadora se contagia de virus si introduzco un disco infectado

Falso. Según Nombela (1990, Pág 71) "*Para que un virus pueda propagarse en una computadora, no basta con que se introduzca un disco infectado. Es necesario que se ejecute alguno de los programas infectados contenidos en el disco Mientras esto no suceda, el virus no contagia la computadora. Entonces, se puede efectuar cualquier tipo de acceso a un disco con archivos contaminados sin que represente problema; por ejemplo efectuar un comando DIR para ver el contenido del disco no puede hacer nunca que el virus contagie la computadora. Cuando la situación es a la inversa, sí pueden propagarse los virus: si su computadora es la que está contaminada y efectúa un comando DIR para ver el contenido de un disco sano, el virus puede aprovechar el acceso al disco para contaminarlo, a menos que esté protegido contra escritura*".

Todos los virus destruyen programas

Falso Hay virus, como el Cookie Monster, que sólo interrumpe el trabajo del usuario desplegando en pantalla el mensaje "I want a cookie" y no destruye programas, sin embargo, la gran mayoría sí se dedican a destruir información si es que no se les detectó a tiempo Aunque no siempre destruyen, pueden bloquear la computadora, impidiendo al usuario grabar su información.

Los virus sólo se activan en ciertas fechas

Falso. Hay otros que se activan cuando se han hecho un número determinado de copias del virus.

Estoy a salvo si tengo el programa antivirus X

Según VIRUS-L (1992) "*Proteger su información con algún programa antivirus puede reducir significativamente el riesgo de ser infectada por virus. Sin embargo, no hay programa que pueda proteger contra todos los virus debido a que se siguen creando virus nuevos. Por lo que se recomienda usar más de un programa antivirus que tenga una fuente confiable, además de actualizarlo constantemente*".

Si coloco el atributo Read Only (sólo lectura) a archivos, los protejo de los virus

Falso. El atributo Read Only protegerá a sus archivos de unos cuantos virus, debido a que la mayoría de éstos pasa por alto el atributo e infecta normalmente. Colocar el atributo de sólo lectura a los archivos ejecutables no es mala idea, pero ciertamente no es una protección completa contra los virus.

Los sistemas de control de acceso (passwords) protegen a los archivos de los virus

Según VIRUS-L (1992) "*Todos los passwords y otros sistemas de control de acceso están diseñados para proteger los datos del usuario de otros usuarios y/o sus programas. Sin embargo recuerde que, cuando se ejecuta un programa infectado con virus, éste ganará los actuales derechos/privilegios. Por consiguiente, si el sistema de control de acceso le da el derecho de modificar algunos archivos, también se lo dará al virus. Por lo tanto, un sistema de control de acceso protegerá a sus archivos de los virus no más de lo que los protege usted*".

CAPITULO 2. ENTORNO DE LA INFORMATICA EN LA UPAEP

Dado el objetivo principal de este trabajo, que es desarrollar la cultura computacional en los alumnos de la UPAEP para no utilizar copias ilegales de programas y disminuir la incidencia de contagio de virus, se presentan en este capítulo la situación que impera en los centros de cómputo UPAEP, las medidas que actualmente se están tomando para controlar el contagio de virus y los resultados que se han obtenido.

En la UPAEP, tanto en el nivel profesional como en los bachilleratos, se imparten diversos cursos de computación como herramienta indispensable en el proceso de educación integral.

Las computadoras proporcionan al proceso educativo atributos tales como perseverancia, disponibilidad continua y programas individuales y seriados de enseñanza para permitir que el estudiante incremente su capacidad de pensar en forma lógica, formule procedimientos para la solución de problemas y mejore sus relaciones humanas

2.1. Entorno en los bachilleratos

En los bachilleratos UPAEP, a partir del tercer semestre, todos los alumnos inician sus estudios de computación

Dentro del plan de estudios están contempladas las siguientes materias

Tercer semestre	Introducción a la Computación
Cuarto semestre	Lógica Computacional
Quinto Semestre.	Programación I
	Taller de Programación I
	Laboratorio de Computación I
Sexto Semestre.	Programación II
	Taller de Programación II
	Laboratorio de Computación II

en las cuales se imparte historia de la computación, algoritmos, MS-DOS™, QuickBasic™, Turbo Pascal™, Word™ para DOS, Lotus™ para DOS, Turbo C™, dBase III plus™, Works™ para DOS

Al concluir sus estudios de bachillerato el alumno podrá recibir, anexo al certificado de estudios correspondiente, un diploma otorgado por la UPAEP, que acredite la capacitación técnica terminal "Técnico en Computación"

Este diploma sólo lo podrán recibir aquellos estudiantes que hayan cursado y aprobado todas y cada una de las materias correspondientes al plan de estudios del bachillerato, haber obtenido como mínimo 7 5 de promedio general de todas las materias que indica el plan de estudios para la capacitación técnica terminal y, solicitar la presentación de un examen que evaluará integralmente el conocimiento y aplicación de estas materias

En el Departamento de Computación de los bachilleratos se encuentra concentrado todo el software original; además en cada uno de los bachilleratos hay un centro de cómputo para que los alumnos realicen sus prácticas

A continuación se presentan las características del equipo existente en cada uno de los centros de cómputo y las medidas que se siguen para controlar el contagio de virus

Tabla 2 1 Centro de Cómputo del Bachillerato Mixto Centro

Cantidad	Procesador	Monitor	Drives	Disco duro	RAM	Mouse	Impresoras	Scanner	Modem	Multimedia
12	8086	Mono TTL	2 5¼" LD		640 Kb					
2	8086	Color CGA	2 5¼" LD		640 Kb					
16	80286	Color CGA VGA	2 5¼" HD		640 Kb					
8	80386	Color VGA	1 5¼" HD 1 3½" HD		2 Mb		5			
4	80386	Mono VGA	1 5¼" HD 1 3½" HD		1 Mb					
1	80386	Color VGA	1 5¼" HD 1 3½" HD	20 Mb	2 Mb	Si	1			
1	80386	Color VGA	1 5¼" HD 1 3½" HD	80 Mb	2 Mb	Si	1	1	1	
2	80486	Color SVGA	1 3½" HD	220 Mb	4 Mb	Si				Si

Fuente Entrevista con el encargado del Centro de Cómputo

El equipo de cómputo que opera en el bachillerato mixto centro se presenta en la tabla 2 1 Los casos de virus que se han tenido son Dark Avenger, Ping-pong, 15xx, Stoned (el más frecuente) y recientemente el Satán o Natas en los discos duros Las medidas que se siguen en el centro de cómputo son los discos de sistema operativo de los alumnos tienen instalado el archivo VSHIELD EXE del VirusScan™ o el Norton Antivirus™ para detectar la existencia de algún archivo con virus, al momento que se quiera ejecutar En el caso de que se detecte alguno, entregan los discos al encargado

del centro de cómputo para ser vacunados Algunas veces sí han perdido información, debido a que los alumnos no entregan los discos para vacunarlos a pesar de que saben que están infectados y, otras veces, por falta de información

Tabla 2 2 Centro de Cómputo del Bachillerato Femenil Centro

Cantidad	Procesador	Monitor	Drives	Disco duro	RAM	Mouse	Impresoras	Scanner	Modem	Multimedia
1	8086	Mono TTL	2 5¼" LD		640 Kb					
1	80286	Color VGA	1 5¼" HD 1 3½" HD	Si	2 Mb	Si	1			
8	80386	Mono VGA	1 5¼" HD 1 3½" HD		1 Mb		2			
2	80386	Color VGA	1 5¼" HD 1 3½" HD		2 Mb					
10	80486	Color SVGA	1 3½" HD	220 Mb	4 Mb	Si				Si

Fuente Entrevista con el encargado del Centro de Cómputo.

El equipo de cómputo existente en el bachillerato femenil centro se presenta en la tabla 2 2 Los casos de virus que se han tenido son Ping-pong y el Stoned (siendo también el más frecuente) Actualmente el virus más insistente es el Natas, que infecta tanto a los discos duros, como a los discos de las alumnas

Las medidas que se siguen son. en el disco de sistema operativo tienen instalado el VSHIELD EXE del VirusScan™ o el Central Point Antivirus™ para detectarlos Cuando los discos de las alumnas se infectan, en el centro de cómputo se vacunan

Tabla 2.3 Centro de Cómputo del Bachillerato Varonil Centro

Cantidad	Procesador	Monitor	Drives	Disco duro	RAM	Mouse	Impresoras	Scanner	Modem	Multimedia
2	8086	Mono TTL	2 5¼" LD		640 Kb					
2	80286	Color VGA	2 5¼" HD	Si	2 Mb	Si	1			
1	80386	Color VGA	1 5¼" HD 1 3½" HD		2 Mb					
7	80386	Mono VGA	1 5¼" HD 1 3½" HD		1 Mb		1			
10	80486	Color SVGA	1 3½" HD	220 Mb	4 Mb	Si	2			Si

Fuente Entrevista con el encargado del Centro de Cómputo

El bachillerato varonil centro cuenta con el equipo de cómputo indicado en la tabla 2 3 El virus que más ha contagiado es el Stoned Hace seis meses hubo mayor incidencia de virus debido a que los alumnos tenían pocos conocimientos de computación Se les explicó brevemente lo que son los virus para que pudieran combatirlos También se han infectado con Natas los discos duros y discos de los alumnos

Sí ha habido casos en los que los virus borraron archivos Pero también hay alumnos que ponen como pretexto a los virus para afirmar que éste les borró los archivos de tarea (evitar responsabilidad)

Por lo regular, nunca le ponen atención a este problema, hasta que les sucede, es entonces cuando se les vacunan sus discos y se les explica

Tabla 2 4 Centro de Cómputo de los Bachilleratos Sur

Cantidad	Procesador	Monitor	Drives	Disco duro	RAM	Mouse	Impresoras	Scanner	Modem	Multimedia
10	80386	Color VGA	1 5¼" HD 1 3½" HD		2 Mb		2			
16	80386	Mono VGA	1 5¼" HD 1 3½" HD		1 Mb		2			
4	80486	Color SVGA	1 3½" HD	220 Mb	4 Mb	Si				Si

Fuente Entrevista con el encargado del Centro de Cómputo.

El equipo de cómputo que opera en los bachilleratos sur se indica en la tabla 2 4. Se han dado pocos casos de virus debido a que la mayoría de las computadoras no tienen disco duro y sólo se trabaja con discos flexibles, además, arrancan las máquinas con sistemas operativos que les proporciona el centro de cómputo, los cuales inicializan el archivo VSHIELD EXE del VirusScan™ para detectar archivos con virus al momento de ejecutarlos Si se llega a detectar alguno, en el centro de cómputo se les vacuna De los pocos casos de virus, el Stoned ha sido el más frecuente Los alumnos no saben qué es realmente un virus, ni qué problemas les puede ocasionar

Se tiene una población estimada en mil trescientos alumnos en los seis planteles (bachillerato femenil centro, bachillerato varonil centro, bachillerato mixto centro, bachillerato femenil sur, bachillerato varonil sur y bachillerato mixto sur), de los cuales aproximadamente un 40% tienen su propia PC o algún familiar les permite utilizarla, lo que implica un potencial riesgo de contagio de virus

En general, los alumnos carecen de información exacta acerca de lo que son los virus computacionales y de lo que pueden ocasionar, teniendo entonces, poco cuidado con sus discos

Otras veces, ponen como pretexto que el virus les borró los archivos de tarea, para tratar de justificar el no haberla hecho

Aunque los discos de los alumnos se vacunen, se siguen contagiando debido a que ellos, algunas veces, rentan computadoras en lugares donde no se siguen las medidas adecuadas para prevenir los virus Como se mencionó anteriormente, aproximadamente un 40% de los alumnos tienen computadora con disco duro en casa o algún familiar se las presta, pero la mayoría de ellos tampoco toma las medidas adecuadas Y ya es grande la cantidad de alumnos que han pedido ayuda a los encargados de centro de cómputo debido a que estas computadoras están infectadas con el virus Natas, que es el de más contagio actualmente y el más dañino

2.2. Entorno en la Universidad

En las carreras profesionales de la UPAEP también se imparten diversos cursos de Computación, con excepción de Ciencias Políticas, Ciencias de la Comunicación, Derecho, Filosofía y Psicología (en el área de Humanidades), Odontología y Enfermería (en el área de Ciencias de la Salud)

Es importante recalcar que se cuenta con una carrera especializada en el área de Computación, esta es la Licenciatura en Sistemas de Información, la cual tiene un perfil administrativo debido a que, además de contar con las materias propias de computación y matemáticas, incluye muchas otras materias administrativas y contables en el plan de estudios

Dentro del plan de estudios de las carreras profesionales se contemplan las siguientes materias:

Area de Humanidades

Se enseña sistema operativo y paquetería, como Works™

Pedagogía

Tercer semestre Computación I
Cuarto semestre Computación II

Area de Ciencias de la Salud:

Se enseña sistema operativo y paquetería, como Works™.

Medicina

Primer semestre Informática médica

Area Económico-Administrativa

Se enseña sistema operativo y paquetería Works™, dBase™, Lotus™; en programación es Basic™ y Turbo Pascal™, además de varios paquetes contables

Contaduría Pública

Primer semestre	Computación I
Segundo semestre	Computación II
Tercer semestre	Tratamiento de textos
Cuarto semestre.	Hoja de cálculo
Quinto semestre	Base de datos
Sexto semestre	Programación
Séptimo semestre	Redes y multiusuarios
Octavo semestre	Paquetes contables I
Noveno semestre	Paquetes contables II
Décimo semestre.	Actualización computacional

Administración de instituciones

Tercer semestre	Computación I
Cuarto semestre	Computación II

Administración de Empresas

Tercer semestre	Computación I
Cuarto semestre	Computación II

Economía

Primer semestre	Computación

Area de Artes ·

Se enseña sistema operativo y, principalmente Autocad™, además de otros paquetes de diseño para ambiente Macintosh™

Diseño Gráfico

Tercer semestre	Introducción a la computación
Cuarto semestre	Diseño y computación

Arquitectura

Primer semestre	Computación
Tercer semestre	Diseño bidimensional por computadora
Cuarto semestre	Diseño tridimensional por computadora
Quinto semestre.	Diseño integral por computadora

Area Tecnológica

Se enseña sistema operativo y paquetería, como Works™, Lotus™, dBase™, Clipper™, Autocad™, lenguajes de programación como Turbo Pascal™, C™, Visual Basic™

Ecología y Protección ambiental

Primer semestre	Computación I
Tercer semestre	Computación II

Ingeniería Civil

Primer semestre	Computación I
Segundo semestre	Computación II
Tercer semestre	Computación III

Ingeniería Química

Primer semestre	Computación

Agronomía Fitotecnia

Segundo semestre	Computación

Agronomía Zootecnia

Segundo semestre	Computación

Ingeniería Industrial

Tercer semestre	Computación I
Cuarto semestre	Computación II
Quinto semestre	Computación III
Octavo semestre	Sistemas de información
Noveno semestre	Diseño de sistemas

Sistemas de Información

Primer semestre.	Programación Pascal
	Paquetería
	Introducción a la computación
Segundo semestre	Ingeniería de sistemas
	Lenguaje C I
	Arquitectura computacional I
Tercer semestre	Lenguaje C II
	Arquitectura computacional II
Cuarto semestre	Base de datos I
	Sistemas operativos
Quinto semestre	Redes informáticas
	Base de datos II
	Ingeniería de software I
Sexto semestre	Sistemas abiertos y conectividad
	Análisis numérico y graficación
	Ingeniería de software II

Séptimo semestre	Bases de inteligencia artificial
	Análisis y diseño de sistemas I
Octavo semestre	Análisis de diseño de sistemas II
	Tópicos actuales de informática I
Noveno semestre	Simulación
	Programación administrativa
	Administración y auditoría de centros informáticos
	Tópicos actuales de informática II

A continuación se presentan las características del equipo existente en los centros de cómputo y la forma en que controlan el contagio de virus

Tabla 2 5 Centro de Cómputo General

Cantidad	Procesador	Monitor	Drives	Disco duro	RAM	Mouse	Impresoras	Scanner	Modem	Multimedia
13	80286	Color VGA	2 5¼" HD	20 Mb	640 Kb	Si				
20	80386	Color VGA Mono	2 5¼" HD 1 3½" HD		1 Mb 2 Mb	Si				
15	80386	Color VGA	1 5¼" HD 1 3½" HD	40 Mb	4 Mb	Si				

Fuente Entrevista con el encargado del Centro de Cómputo

El centro de cómputo general cuenta con el equipo indicado en la tabla 2 5 Se encuentra dividido en tres salas

En la sala dos se tienen veintitrés computadoras Macintosh™, un scanner, un plotter, impresoras láser y de matriz de puntos.

En la sala tres están instaladas las quince computadoras 80386SX, con discos duros de 40 Mb Estas computadoras sí se han contagiado algunas veces, debido a que los alumnos, al ir a trabajar también a computadoras de otros centros de cómputo, traen sus discos infectados

En la sala uno es donde están las trece computadoras 80286 con discos duros de 20 Mb En los discos duros se instala el NAV (Norton Antivirus™), el cual detecta cuando un disco tiene virus, sonando la alarma Pero aun sonando la alarma, el catedrático permite que los alumnos sigan trabajando con el disco infectado para que continúen tomando la clase y, obviamente, llegan a infectar las computadoras del centro de cómputo. Las medidas que se siguen son vacunar todos los días las computadoras en un horario determinado.

Anteriormente, cuando los alumnos tenían discos infectados, se vacunaban en el centro de cómputo Lo que se hace actualmente es, que al principio del semestre, en los cursos de sistema operativo que se imparten a los alumnos se les enseña cómo vacunar los discos

Recientemente se han tenido graves problemas en el centro de cómputo, debido a que las computadoras se contagiaron con el virus Satán o Natas Pero la Universidad adquirió el antivirus VirusScan™, y con eso se ha logrado eliminar al virus

En las Macintosh™ no se ha tenido ningún problema con virus, debido a que los alumnos no tienen este tipo de computadoras en sus casas

Los alumnos no entienden bien lo que es un virus y hacen mal uso de ellos, aparte de estar mal informados, aunque algunas veces sí han perdido información, otras los alumnos afirman que el virus les borró sus archivos de tarea para justificar el no haberla hecho

Tabla 2.6 Centro de Cómputo de Sistemas de Información

Cantidad	Procesador	Monitor	Drives	Disco duro	RAM	Mouse	Impresoras	Scanner	Modem	Multimedia
16	80386	Mono VGA	1 5¼" HD 1 3½" HD		1 Mb					
14	80386	Color VGA	1 5¼" HD 1 3½" HD	40 Mb	2 Mb	Si	6			
4	80486	Color UVGA	1 3½" HD	325 Mb	8 Mb	Si				Si
16	80486	Color VGA	1 3½" HD	325 Mb	4 Mb	Si				

Fuente Entrevista con el encargado del Centro de Cómputo

El equipo que opera en el centro de cómputo de Sistemas de Información se indica en la tabla 2.6.; además se cuenta con tres computadoras Macintosh™, un equipo Tower™ Modelo 1632 con doce terminales, el sistema 36 de IBM™ y el sistema HP™ 3000

El virus más común en este centro de cómputo es el Stoned, pero desde hace un año se está utilizando el sistema operativo versión 6 2, el cual tiene incluido un antivirus, y por esta razón no se han presentado alumnos pidiendo que se les vacunen sus discos En las computadoras más actuales se utiliza la versión 6 22

En semestres anteriores sí se tenían serios problemas de virus, al grado de llegar a perder archivos en sus discos.

Las personas que van a trabajar al centro de cómputo que no son de la carrera de Sistemas de Información le tienen miedo a los virus, pero a los que sí son alumnos de la carrera se les explica una o dos veces cómo eliminarlos con el antivirus que tienen las computadoras y con eso es suficiente

Actualmente, también se han tenido problemas en el centro de cómputo, debido a que las computadoras que tienen disco duro se contagiaron con el virus Natas Pero ya se eliminó también con el antivirus adquirido por la Universidad

Tabla 2 7 Centro de Cómputo de Contaduría

Cantidad	Procesador	Monitor	Drives	Disco duro	RAM	Mouse	Impresoras	Scanner	Modem	Multimedia
69	80486	Mono VGA	1 5¼" HD 1 3½" HD	200 Mb	4 Mb	Si				
1	80486	Mono VGA	1 5¼" HD 1 3½" HD	200 Mb	4 Mb	Si	5	1		Si

Fuente Entrevista con el encargado del Centro de Cómputo

El equipo del centro de cómputo de Contaduría se presenta en la tabla 2.7 De las cinco impresoras con que cuenta, tres son láser y dos de chorro de tinta (una a color)

Casi nunca han tenido problemas con virus Sin embargo, cada quince días se vacunan las computadoras con el VirusScan™, se borran archivos inservibles o se instala el software que haga falta

En este centro de cómputo únicamente se permite trabajar a los alumnos de la carrera de Contaduría. Los profesores enseñan a los alumnos cómo vacunar sus discos e ideas generales de lo que son los virus En el último semestre de la carrera, en la materia de Actualización computacional, es donde se les enseña a fondo lo que son los virus

CAPITULO 3. MEDIOS DE CONTAGIO

Dado el objetivo principal de este trabajo, que es desarrollar la cultura computacional en los alumnos de la UPAEP para no utilizar copias ilegales de programas y disminuir la incidencia de contagio de virus, se presentan en este capítulo los conceptos básicos y fundamentales de los medios de contagio más frecuentes elegidos por los virus para ejercer su acción de expansión

Cuando comenzaron las computadoras el objetivo principal consistía en procesar grandes volúmenes de información en segundos Actualmente con el auge de las computadoras personales, la utilización de la línea telefónica para la transmisión de datos codificados a través del modem, las redes de área local (LAN), las redes públicas de computadoras y las comunicaciones vía satélite, unidas a la estandarización de sistemas operativos, protocolos de comunicación y lenguajes de programación, se ha dado lugar a la telecomunicación.

Las formas en que los virus y los programas que los contienen son transferidos de una computadora a otros sistemas de computadoras personales puede darse en una variedad de formas. El medio más común es la distribución vía discos. Otros métodos para transferir programas son el CD, las cintas, así como las telecomunicaciones.

Cuando se compra un programa de computadora, éste viene almacenado en CD o en discos flexibles Los discos de 5¼ y 3½ pulgadas son los más comunes. Después de recibir un programa en discos flexibles, la mayoría de los usuarios realizan copias de trabajo del programa en otros discos flexibles o copian el programa de los discos flexibles al disco duro. Un disco duro puede contener miles de programas, datos y otros archivos.

Entre los medios para transferir archivos están

Discos:

- Usuario a usuario
- Compañía a usuario
- Autor a usuario

Telecomunicaciones

- Sistemas de boletines informativos (BBS), redes
- Servicios de información, correo electrónico
- Upload (enviar) y download (bajar)

3.1. Discos

Según Mayo (1989, Pág 22) "*En el caso de la transferencia de discos, un virus puede entrar a una computadora personal de dos formas: 1) por un programa copiado del disco ó 2) a través del proceso de reproducción del virus si se ejecuta un programa infectado con virus que está almacenado en disco, es posible para el virus copiarse en otros programas almacenados en otros discos que sean introducidos a la computadora.*

Un caballo de Troya no puede reproducirse, sin embargo, si se activó, puede afectar el sistema computacional completo -no sólo el disco donde está almacenado el programa Un gusano contenido en un programa almacenado en un disco puede introducirse en la memoria y afectar la información que podría ser grabada después en el disco"

Se debe ser especialmente precavido si no conoce el origen del disco que está introduciendo en el drive de la computadora.

Ahora se comentará sobre los principales tipos de software -comercial, shareware, freeware y de dominio público *Software comercial* son los programas computacionales diseñados y desarrollados por compañías de buena reputación (como Microsoft y Borland), para la venta al público en general. Una manera fácil de identificarlos es: 1) por el precio del paquete, el cual es usualmente caro; 2) la calidad física de la documentación (profesionalmente impresa y encuadernada), y 3) el contrato de permiso que viene con el paquete, el cual prohibe la copia del programa

Es posible que los autores del software comercial incluyan virus en el código de los programas, los cuales se activen cuando se haya realizado un cierto número de copias del software, y de esta manera se protegen de las copias ilegales, "obligando" a los usuarios a comprar el software original y las empresas no presenten pérdidas económicas.

Por consiguiente, se debe ser cuidadoso con algunas copias del software comercial que ejecute en su computadora La distribución de copias es en la mayoría de los casos ilegal, y se está incurriendo en una práctica turbia conocida como piratería (copias y distribución de programas comerciales) Es posible que los programas hayan sido alterados para incluir un caballo de Troya o un gusano, o que los discos estén infectados con virus La persona que copió estos discos probablemente tiene muchas otras copias de paquetes de software comercial ilegales que han sido utilizadas por lo menos una vez en su sistema computacional. Es posible que se hayan infectado, aun sin su conocimiento, de algún virus No se deben colocar discos que contengan copias de software comercial en el drive, a menos que pueda seguir claramente las generaciones de copias de los discos originales

Shareware son los programas distribuidos a través de BBSs y servicios de información sin pagar por ellos en ese momento. Si el programa prueba ser útil, el usuario debe pagar al autor una cantidad que normalmente está especificada en la documentación, entonces se recibirá una documentación adicional, un soporte y,

posiblemente, la siguiente actualización sin costo alguno Se requiere de licencias de pago para su distribución comercial

Debido a que los programas shareware pueden ser distribuidos ilegalmente por personas diferentes al autor, pueden tener los mismos problemas que las copias ilegales de software comercial en el sentido de que pueden ser infectadas por virus en algún lugar de la ruta de distribución La mayoría de las copias de programas shareware están perfectamente limpias, sin embargo, siempre se debe tener cuidado Si tiene dudas sobre el programa shareware que recibe, puede ponerse en contacto con el autor para obtener una copia limpia La mayoría de los autores de shareware están concientes del problema de los virus, y toman medidas para asegurar que las copias que envían a los usuarios (ya pagadas) no estén infectadas Obtener el shareware directamente de los BBSs de los autores garantiza que los programas estén completos, actualizados y no corruptos

Puede haber algunos autores de shareware que coloquen virus "gratis" en sus programas, los cuales se activen si el usuario sigue utilizando el programa y después de un determinado periodo de tiempo no ha pagado la cantidad que está especificada, de esta manera el autor garantiza que el usuario le pague. En cambio, si el usuario paga la cantidad indicada en la documentación, el autor le proporciona el programa completo y libre de virus

Freeware es muy similar a shareware con la excepción de que no se paga una cantidad por el software El autor permite que el programa sea distribuido y utilizado sin recibir una compensación. Las mismas precauciones consideradas en el shareware se deben tomar en el freeware.

En el *software de dominio público* tampoco se paga una cantidad por obtenerlo El autor del programa no demanda derechos de autor, los usuarios son libres de hacer lo que quieran con los programas

Debido a que los programas están en el dominio público, los usuarios son libres de jugar con ellos, a menudo reescribiendo partes de él El resultado es que pueden haber muchas versiones diferentes de un mismo programa. Debido a que no hay forma de saber si se tiene una copia limpia del programa para ejecutarlo, sólo se deben usar aquellas copias que hayan sido obtenidas de fuentes confiables y usadas por otras personas a las que no les ocasionó problemas, o, como en el caso del shareware, ponerse en contacto con los autores para solicitarles directamente copias de sus programas; con esto se garantiza también que las copias del software recibido estén libres de virus

La diferencia entre el freeware y el software de dominio público consiste en que los autores de freeware retienen el control de la distribución del software, incluyendo la capacidad de cambiar la siguiente versión como software comercial o como shareware, en cambio, en el software de dominio público, el autor cede la propiedad al público (usuarios).

Las aplicaciones de shareware, freeware y software de dominio público son formas muy eficaces de reducir los gastos de software A veces estos programas de

bajo costo están muy por delante de sus correspondientes comerciales en términos de su facilidad de uso y de sus funciones Es equivocado denominar a ese software como *intrínsecamente malo y negar a autores competentes* la oportunidad de servir a los usuarios.

3.2. *Telecomunicaciones*

Telecomunicación es el medio popular de transferir programas entre computadoras personales Las computadoras personales equipadas con modems pueden conectarse a computadoras remotas, las cuales almacenan muchos programas y otros archivos que pueden ser bajados por sus usuarios

Hay dos clases de sistemas computacionales remotos los BBSs y los servicios de información

Los *BBSs* (Bulletin Board System: boletines informativos) son computadoras personales que están conectadas al servicio telefónico vía modem Otros usuarios de computadoras personales que están conectados al BBS pueden enviar y bajar programas y otros archivos o enviar mensajes a otros usuarios Lo que alguna vez nació como un simple juego, es día a día un factor determinante en el desarrollo e intercambio de *usuarios de computadoras* A través de estos servicios, los usuarios pueden obtener información, programas, asesoría e inclusive entretenimiento y una forma diferente de *convivir* con personas que en ocasiones jamás llegaría a conocer, ni siquiera por voz Es precisamente esto último lo que los hace interesantes. la oportunidad de intercambiar correspondencia con otras personas de una manera rápida y oportuna. Por medio de algunas redes públicas (vía telefónica) que se han ido desarrollando entre BBSs, es hoy posible escribir una carta a una persona, por ejemplo en Francia, y al día siguiente, o antes, recibir una respuesta. Por mucho que se apure un servicio de correo, tardará por lo menos varios días

El *operador del sistema* o SysOp es la persona que se encarga de poner a funcionar y mantener el boletín. Tiene que estar siempre pendiente de lo que sucede dentro del sistema, quién llama, qué le solicitan los usuarios, etc El SysOp es quien, inicialmente, define todos los parámetros dentro del sistema, esto es, las áreas de mensajes, las de archivos, el propio nombre del sistema y ciertas restricciones para uso, que pueden ser fijadas o no, dependiendo del caso

Un BBS se encuentra dividido en tres grandes secciones La primera es de mensajes públicos; la segunda, de mensajes privados, y la tercera, de una biblioteca de archivos. En algunas ocasiones se ofrecen otros servicios que pueden ser tan importantes como estos tres principales Algunos BBSs han integrado con bastante éxito bases de datos para consultas, áreas de entretenimiento e incluso ya hay algunos BBSs que ofrecen servicios de soporte de importantes compañías de software y de hardware así como mercados en línea, con extensos catálogos de bienes y servicios

puestos a la venta por empresas que se han dado cuenta de la importancia que pueden tener estos modernos medios de comunicación

Una de las partes más entretenidas y con mayor uso de cualquier BBS que se precie de serlo, es el área de mensajes públicos, donde los usuarios comparten experiencias, lanzan preguntas al aire para ver quién las contesta, hacen consultas técnicas y en general expresan su opinión sobre muchos temas. Para poder tener un orden y no tener que leer un mensaje de astronomía después de leer uno de filosofía, los BBSs están organizados de manera que existan ciertas áreas particulares sobre temas más o menos comunes. De esta manera se podrán encontrar áreas de programación, diversiones, de arte, de cocina, de ciencia y una muy larga lista de temas que en los BBSs se conocen como mesas redondas o foros de discusión.

Los mensajes privados se crean para mandar una carta o cualquier tipo de comunicación escrita a otro usuario del sistema para que sea leída exclusivamente por el destinatario. La única diferencia entre los mensajes privados y los públicos radica precisamente en la privacidad. Existe la opción de mandar un mismo mensaje a un grupo de usuarios y de desviar los que reciba hacia la cuenta de otro, para cuando salga de viaje, por ejemplo

Otra de las principales atracciones de un BBS son también las llamadas secciones de archivos, que son grandes (dependiendo del tamaño del BBS) colecciones de archivos clasificados por temas, donde podrá encontrar desde un pequeño programa para emular una calculadora, hasta algunos importantes documentos sobre temas especializados de programación como pueden ser la programación de aplicaciones para Windows™, desde pequeños juegos hasta poderosas hojas de cálculo, programas escritos por alguna firma comercial o por usuarios aficionados del mismo BBS; en general, estos se distribuyen de acuerdo con la filosofía del shareware

Un *sistema de información* se puede definir como un BBS de dimensiones mucho mayores, generalmente usan mainframes y otros grandes sistemas de computadoras, que pueden manejar miles de usuarios simultáneamente que se conectan por la vía telefónica Los sistemas de información tienen cientos de miles de programas y otros archivos disponibles a los usuarios, característica de un extenso sistema de correo electrónico, y grandes bases de datos disponibles para investigación. Los servicios ofrecidos a través de un sistema de información pueden variar desde consultar el clima hasta hacer inversiones en la bolsa de valores, consulta de bases de datos, compras en centros comerciales electrónicos, consulta de noticias, reservaciones de boletos de avión y muchas actividades más. Concretamente en *SPIN* (sistema de información que está estrenando líneas digitales de fibra óptica) existe una especie de supermercado, en el cual uno puede ir de una *tienda* a otra y seleccionar una gran variedad de artículos que puede adquirir con acuerdos como la ya tradicional tarjeta de crédito Ahí se puede encontrar desde una cinta para impresora hasta tal vez la computadora nueva

Compuserve es el servicio de información más grande del mundo y actualmente cuenta con más de quinientos mil usuarios, en su mayoría norteamericanos, quienes día a día se comunican al sistema para realizar alguna de las actividades mencionadas anteriormente

Los sistemas de correo electrónico se implementan en redes de área local de macrocomputadoras, minis y computadoras personales Los usuarios pueden enviar correspondencia a un receptor único o transmitirla a muchos usuarios del sistema

Los BBSs y servicios de información están encendidos la mayoría de las veces las veinticuatro horas de los trescientos sesenta y cinco días del año y se encuentran siempre esperando a que otra computadora se comunique, por teléfono, para establecer una comunicación y poder compartir datos y archivos

Tanto en los BBSs como en los servicios de información se cuenta con shareware, freeware y software de dominio público que los usuarios pueden obtener Sin embargo, si se baja información de un BBS o de un servicio de información, se deben tomar las mismas precauciones que para el manejo de programas en discos.

La mayoría de los operadores del sistema son cuidadosos al verificar los nuevos archivos que fueron subidos al BBS para detectar posibles virus Si el boletín obtiene una mala reputación por difundir software contaminado, rápidamente perdería sus usuarios Algunos programas de los BBSs incluyen la capacidad de scanearse automáticamente para detectar virus.

Existen BBSs piratas. Su propósito es difundir software cracked (software comercial con el número de serie o protección de copia alterados) Los operadores de BBSs piratas son muy discretos acerca de la identidad de los usuarios que conocen el número telefónico del BBS, y el software pirata a menudo está en áreas privadas del BBS, de manera que los demás usuarios no ven los archivos ilegales. Los BBSs piratas mantienen una sección de virus computacionales disponibles para bajar. Se debe siempre evitar utilizar software pirata Más allá de las cuestiones morales y legales, el software pirata está expuesto a los virus computacionales

> Según Solomon (1993, Págs. 20-21) *Estos BBSs piratas permiten que el usuario se registre; puede bajar un virus y entonces no le permitirá regresar para bajar algo más hasta que se envíe un virus nuevo al BBS Escribir un virus nuevo no es tarea difícil para aquellas personas que dominan la programación a bajo nivel, pero para el mayor número de hackers, es completamente difícil Entonces, en vez de escribir un nuevo virus, ellos simplemente reescriben uno existente Debido a esto, es que se tienen varias versiones de ciertos virus Por ejemplo, hay varias versiones del virus Stoned. El código actual es casi siempre el mismo, pero es el mensaje el que ha cambiado El mensaje original era:*

Your PC is now Stoned

Este es el mensaje que ha sido visto ocasionalmente cuando una computadora es infectada primero Hay otro mensaje que se ha visto sólo en el código del virus, que es

LEGALISE MARIJUANA

Actualmente ser presentan otras variantes, como por ejemplo

Your PC is now Sanded
Lysergic acid rules O K

La mayoría de las veces estos BBSs justifican su existencia diciendo que están ahí para capacitar a investigadores de virus manteniéndolos actualizados

Lo cierto es que, mientras estos boletines permanezcan, la propagación de virus conocidos irá en aumento Si todos fueran cerrados, quizá entonces la propagación de virus disminuiría poco a poco.

Los BBSs productores de virus son una forma de que los virus escapen de su cautiverio. Una vez que ellos están en un disco, el camino está abierto para propagarse lejos y rápido

Por lo tanto, se pueden obtener virus por medio de un BBS. También se puede obtener un virus de una red, pero alguien tiene que ponerlo ahí, ya sea por accidente, por prueba, porque ahí lo diseñaron por primera vez, por sabotaje o venganza

La manera más común en que un virus llega por primera vez a una PC es por vía discos. Por lo tanto, se debe tener más cuidado con el manejo de los discos que con el uso de modems.

CAPITULO 4. FUNCIONAMIENTO DE LOS VIRUS

Dado el objetivo principal de este trabajo, que es desarrollar la cultura computacional en los alumnos de la UPAEP para no utilizar copias ilegales de programas y disminuir la incidencia de contagio de virus, se presentan en este capítulo los conceptos básicos y fundamentales del funcionamiento de los virus, sus lugares de almacenamiento, y las clasificaciones de los virus basadas en sus diferentes características general, por la forma en que trabajan, por la parte que modifica el virus en su ataque y por la forma en que intentan ocultarse

4.1. Ciclo de vida de un virus

Para entender cómo funciona un virus, se explicarán cada una de las fases de su vida

Fase de creación

En esta etapa se incluyen el diseño y la programación del virus, así como la liberación al ambiente computacional, para iniciar su propagación

Los programadores de virus pueden liberarlos varias veces y en lugares diferentes, dando un impulso substancial a su propagación

Los autores de virus generalmente no nombran formalmente sus trabajos, el nombre de un virus puede basarse en el lugar donde fue descubierto o donde una mayor infección ocurrió, por ejemplo, los virus Lehigh y Alameda. Otras veces, el virus es nombrado por alguna frase o valor usado cuando se da a conocer, por ejemplo, los virus Brain y Den Zuk Algunas veces los virus son nombrados por el número de bytes que agregan a los archivos que infectan, tales como los virus 1704 y 1280. Otros se nombran de acuerdo al software por el cual el virus muestra una afinidad, como por ejemplo el virus del dBase

Fase de entrada del virus a la PC

Un virus puede entrar a una computadora personal por cualquiera de los medios de contagio que se explicaron en el capítulo tres

Fase de infección o contagio

La llegada del virus no tiene ningún efecto mientras su código no se ejecute Esto ocurre cuando el usuario ejecuta un programa infectado o cuando arranca la computadora con un disco de sistema operativo infectado

Es entonces cuando el virus ha de almacenar una copia de sí mismo en la memoria o en los discos, debido a que son susceptibles de ser ejecutados varias veces

Lo anterior no significa que el virus se vaya a activar en ese preciso momento, sino que la computadora ha sido "infectada" El virus puede actuar inmediatamente, o bien, esperar a que se den las señales propicias, indicadas en su código de programación El objetivo de la infección es garantizar que el código se ejecute más veces, para reproducirse o propagarse, o para retardar su acción más dañina Por ello, es normal que el virus elija para anidar programas o secuencia de código que el sistema ejecuta con frecuencia, aunque no siempre es así. Otros virus pueden tener más interés en la propagación a otros equipos, por lo que intentan anidar en programas de aplicación, susceptibles de ser compartidos por usuarios de otras computadoras

Existen tres tipos básicos de contaminación

1) Contaminación del sector de arranque (boot o sector 0)
2) Contaminadores del sistema operativo
3) Contaminadores de archivos ejecutables

Ocultamiento

Según Nombela (1990, Págs. 59-60) "*El virus necesita ocultarse para evitar ser descubierto y eliminado, y poder seguir realizando sus acciones nocivas sin que el usuario se dé cuenta Debe ocultar.*

a) su código; de manera que no pueda ser descubierto por la observación del contenido de los discos, y

b) sus acciones, excepto aquellas para las que ha sido diseñado. No todos los virus tienen interés en ocultarse Algunos son de acciones rápidas, y no tiene tiempo el usuario de observar nada antes de que el parásito actúe.

Para ocultar su código en el disco, el virus puede utilizar alguna de estas técnicas

1) Marcar el archivo donde está almacenado con el atributo de archivo oculto, lo que hará que no pueda ser listado, leído, ni modificado con alguno de los comandos internos del DOS (DIR, TYPE, COPY, etc. incluidos en el COMMAND.COM)

2) Almacenar el código en uno o varios sectores libres del disco, marcándolos como defectuosos en la FAT

3) Mediante técnicas de formateo no estándar, con las que se logra introducir sectores extraños, que permanecen ocultos al DOS, porque no los puede leer"

Control de la computadora

Según Nombela (1990, Págs, 62-64) *Para poder realizar sus acciones, especialmente la de propagarse a otros programas, el virus necesita, de alguna forma, controlar la computadora, aunque sea de forma momentánea o intermitente La forma en la cual va a ejercer este control influye radicalmente en el método elegido para la instalación y ocultamiento*

El virus puede tomar el control de dos maneras

a) inmediatamente antes de la ejecución de un programa de usuario. Si el virus se ha instalado en un archivo ejecutable, el código del virus será ejecutado antes que el de su programa portador El virus puede aprovechar ese momento para hacer copias de sí mismo en otros archivos ejecutables. Normalmente, el virus aprovechará también ese momento para instalarse en memoria y quedar residente, tomando completo control del sistema operativo. No obstante, el virus podría operar sin recurrir a esta técnica de instalación en memoria

b) a intervalos cortos, aprovechando el sistema de interrupciones del procesador Una vez que el virus está residente en memoria y, para que el virus pueda ejecutarse a intervalos regulares, necesita ser llamado en algún momento durante la ejecución de otro programa. Lo que se hace para ello es aprovechar la interrupción hardware de reloj, que se ejecuta a intervalos muy regulares

La interrupción de reloj es utilizada por la PC para actualizar la hora del sistema. Dicha interrupción se activa 18.2 veces por segundo, lo que quiere decir que varias veces por segundo se interrumpe el programa que en ese momento se estuviera ejecutando, para pasar a procesar las instrucciones que componen la rutina de atención a la interrupción

La computadora posee una tabla en la parte baja de su memoria que es la que le indica la dirección de memoria donde cada rutina de interrupción comienza Por consiguiente, cada vez que se produce la interrupción hardware de reloj, el procesador acude a esa tabla, extrae de ella la dirección de comienzo de la rutina de interrupción de reloj, y ejecuta dicha rutina

Lo único que el virus hace es modificar dicha tabla sustituyendo la dirección de comienzo de la rutina de reloj por la dirección de su propio código De esta forma, el procesador acude a esa tabla, extrae de ella la dirección y pasa el control al virus Esto es lo que llamamos "interceptar" una interrupción

Por este mecanismo, el virus asegura una constante actividad, que aprovechará para reproducirse contaminando a otros archivos del sistema

Lógicamente, y para que el usuario no se dé cuenta de que algo anda mal (por ejemplo, porque la hora del sistema no se actualiza), una vez ejecutado el código del virus, éste da un salto a la rutina de reloj auténtica, para que efectúe las tareas que le son propias.

Para que este esquema pueda funcionar, es imprescindible que el virus quede antes residente en memoria

Reproducción

Según Nombela (1990, Pág. 64) *Una de las características fundamentales que distinguen a un virus de otros programas dañinos es su capacidad de reproducirse, es probablemente su cualidad más temible, pues al haber muchas copias del programa, hace más difícil su total erradicación del sistema.*

La capacidad reproductora de los virus no es siempre la misma. Puede variar desde una única copia (la necesaria para su instalación permanente en el sistema) a una reproducción múltiple, en la cual cada copia realiza varias copias de sí misma, con lo que la propia función reproductora satura el sistema y agota la capacidad de memoria.

Para que la reproducción sea efectiva, la copia realizada ha de quedar permanentemente en alguna parte del sistema. Como la memoria RAM es volátil, sólo tiene sentido la copia en disco, infectando a otros archivos ejecutables

La reproducción tiene como objetivos la propagación a otros sistemas y lograr los fines para los que fue programados.

Si el objetivo es la propagación, tiene sentido dejar la copia dentro de algún programa que sea susceptible de ser compartido por otro sistema, y lista para que comience su actividad desde el mismo instante en que comienza la ejecución del citado programa Entre estos programas se cuentan también los que forman el sistema operativo, incluyendo el programa de carga (boot). En principio, no sería necesaria más de una copia por disco si se garantiza que el programa donde se encuentra la copia se ejecutará con prioridad a los demás La realidad es que el virus, en su afán por garantizar la propagación y no dejar al azar la posibilidad de que se ejecute un programa no contaminado,

intenta realizar copias de sí mismo en todos los archivos del disco susceptibles de ser ejecutados

Para copiarse, necesita en principio, hacer una reconstrucción de sí mismo, pues muy probablemente esté esparcido en varios trozos a lo largo del disco, con el objeto de ocultarse La propagación a otro sistema requiere la recuperación de la totalidad del código. Existirá, por tanto, alguna rutina recuperadora de las diversas partes, si es que está dividido

El proceso de reproducción se divide entonces en las siguientes fases

1) Búsqueda de una archivo dónde instalarse. En el caso de los contaminadores de boot, el proceso de búsqueda es innecesario, debido a que el programa a contaminar está claramente localizado en el sector 0 Pero en el caso de los contaminadores de sistema o de aplicaciones, se deberá buscar el archivo adecuado

El proceso consistirá en buscar archivos en el directorio, traerlos a memoria, infectarlos y volverlos a escribir en el disco La realización de todas estas operaciones requiere la utilización de las interrupciones del DOS

Este proceso provoca una actividad de la unidad de disco demasiado frecuente, alertando al usuario, el cual posteriormente detecta al virus Debido a esto, muchos virus contaminadores de archivos ejecutables se limitan a infectar dichos archivos en el momento en que son llamados para su ejecución por el usuario. En dicho momento la actividad del disco es algo normal, y un exceso de dicha actividad puede no ser fácilmente detectado

La llamada a la función 4bh de la interrupción 21h del DOS suministra al virus el nombre del posible archivo a contaminar y permite que se realice la contaminación o reproducción sin levantar sospechas. El programa contaminante puede simplemente cargar en memoria el archivo que se solicita, modificarlo, volverlo a escribir en el disco y dar luego control a la rutina original de la función 4bh

2) Comprobación de la existencia de copia realizada anteriormente, para evitar instalarse varias veces en un mismo programa y disminuir la probabilidad de ser descubierto. Además, es importante ahorrar tiempo, evitando realizar acciones inútiles, y ahorrar espacio, evitando llenar el disco con copias del virus innecesarias. La comprobación de copia puede consistir en observar el programa en el que se piensa copiar para ver si contiene alguna palabra clave o cadena determinada que identifique al virus.

Sin embargo, no todos los virus son tan cuidadosos Algunos, en su afán de contaminar todos los archivos ejecutables, derrochan su capacidad reproductora conduciendo a su propia ruina al ser fácilmente detectados

Propagación

La propagación es uno de los principales objetivos de los virus Por medio de la propagación el virus consigue multiplicar su actividad dañina, a la vez de hacerse publicidad entre los usuarios

La *mayoría de los virus más dañinos son programados en un intento para* propagarse lo más silenciosamente posible durante esta etapa Si un virus causa un fuerte efecto o un daño al software desde la primera vez que es ejecutado, podría ser rápidamente detectado sin tener la oportunidad de propagarse La mayoría de los virus dilatan sus síntomas para darse tiempo a propagar la infección lo más extenso posible antes de descubrirse

El virus Miguel Angel se reproduce sin manifestar ningún síntoma obvio, y entonces un día (el 6 de Marzo), destruye la FAT del disco duro Otro virus que se reproduce ampliamente sin mostrar síntomas es el Jerusalén, el cual sólamente borra archivos en algún día Viernes 13

Manifestación

En esta fase se manifiesta la presencia del virus Lo puede hacer de dos maneras:

1) Manifestarse con el único fin de dar un susto o una sorpresa Entre este tipo de manifestaciones tenemos las que hacen aparecer de forma periódica mensajes o dibujos en la pantalla y solicitan a veces la ejecución de una determinada acción, pulsación de una tecla, etc., borran el contenido de la pantalla, o le colocan algún objeto molesto que no se puede borrar.

2) Manifestarse con el fin de hacer daño. Estos daños suelen ser el formateo del disco (destruyendo toda la información contenida en él), el borrado del directorio o de la FAT, o el borrado o alteración de algún archivo aislado, entre otros

Fin del ciclo de vida de un virus

Afortunadamente, la mayoría de los virus alcanzan un fin prematuro debido a que el software antivirus detiene su crecimiento antes de que su propagación se extienda demasiado Otros virus alcanzan su fin como resultado de cientos de usuarios que experimentaron problemas y los combatieron fuertemente.

La propagación de un virus es bastante más complicada que hace algunos años y hay tantas personas trabajando en el tema que, entre la aparición de un nuevo virus y la correspondiente vacuna, no pasa mucho tiempo. Parece que el panorama se presenta prometedor. Sin embargo, interpuesta la barrera de las herramientas antivirus, es sólo cuestión de tiempo la aparición de virus más sofisticados y potentes, capaces de saltarse las protecciones que dichas herramientas establecen

Anatomía de un virus

Se utilizará un virus como un ejemplo que muestre cómo pueden ser creados Esta no es la única forma en que un virus puede crearse, sólo muestra el tipo de cosas que normalmente incluyen

Este virus tiene problemas, por supuesto Para algunas cosas es lento Para otras, el proceso incluido causará una gran cantidad de actividades que mantendrán funcionando al disco que está en el drive

A continuación, se explica paso a paso cómo trabaja este virus (ver figura 4 1)

Paso 1· Se detecta en qué unidad se está y se salva la información Se necesitará más tarde También se coloca el contador de cuántas copias del virus ha encontrado en 0

Paso 2 ¿Es este el día? Si lo es, entonces ir a la subrutina "hacer algo dañino" Si no, ocuparse de la de reproducción

Paso 3 al Paso 6 Este grupo de pasos es parte de la bomba lógica actual del virus Formatea el disco duro, generalmente la tercera unidad en un sistema (unidad C) Si no hay disco duro, se formatea el disco de la unidad con que se arrancó la computadora Una vez hecho esto, se puede abandonar No hay necesidad de que la víctima se entere de lo que está sucediendo; la persona se dará cuenta la siguiente vez que trate de cargar el sistema

Paso 7· Si no es el día, almacena la posición en la unidad actual (en el subdirectorio en que estemos) de manera que pueda regresar cuando sí lo sea

Paso 8: Inicializa una variable para la unidad en la que se está trabajando. Esta marca el principio de el bucle más alejado de la estructura de el virus. Este ciclo hará que el virus se mueva a través de las unidades disponibles en el sistema destino.

Paso 9 al paso 14· Encontrar la siguiente unidad en secuencia Si no hay una siguiente unidad, se habrá terminado Si hay un siguiente unidad, ¿hay disco? Si no, empezar este grupo de pasos otra vez Si hay un disco, entonces moverlo al directorio raíz

Paso 15 Inicializa el apuntador al principio del stack del directorio Este apuntador se usará para guardar la ruta del siguiente subdirectorio con el que se va a trabajar Entonces empieza el segundo bucle, el cual moverá al virus a través de cada subdirectorio en turno

Paso 16 Inicializa el apuntador del archivo Este se usará para guardar la ruta del archivo en el directorio actual con el que se trabajará dentro de poco Entonces comienza el tercer ciclo, el cual mueve al virus a través de cada archivo en el directorio actual

Paso 17 al Paso 19 Selecciona el archivo con el que se va a trabajar Se asegura de que no es un archivo borrado, y se determina si es un subdirectorio

Paso 20. Si es un subdirectorio, se agrega su posición en el stack del subdirectorio e incrementa el apuntador del stack

Paso 21 al Paso 22 Se asegura de que el archivo no está aún infectado Si es así, agrega 1 al contador de cuántas copias ha encontrado

Paso 23. Si el contador marca 50 o más, va a una rutina peligrosa en los pasos 3 al 6

Paso 24 Si el archivo no está infectado, salva el sistema indicador y el byte de atributos para el archivo Coloca el byte de atributos a Hex '00' para aparentar que el archivo original está "normal" y permitir accesos ilimitados

Paso 25 Se copia el virus en ese lugar.

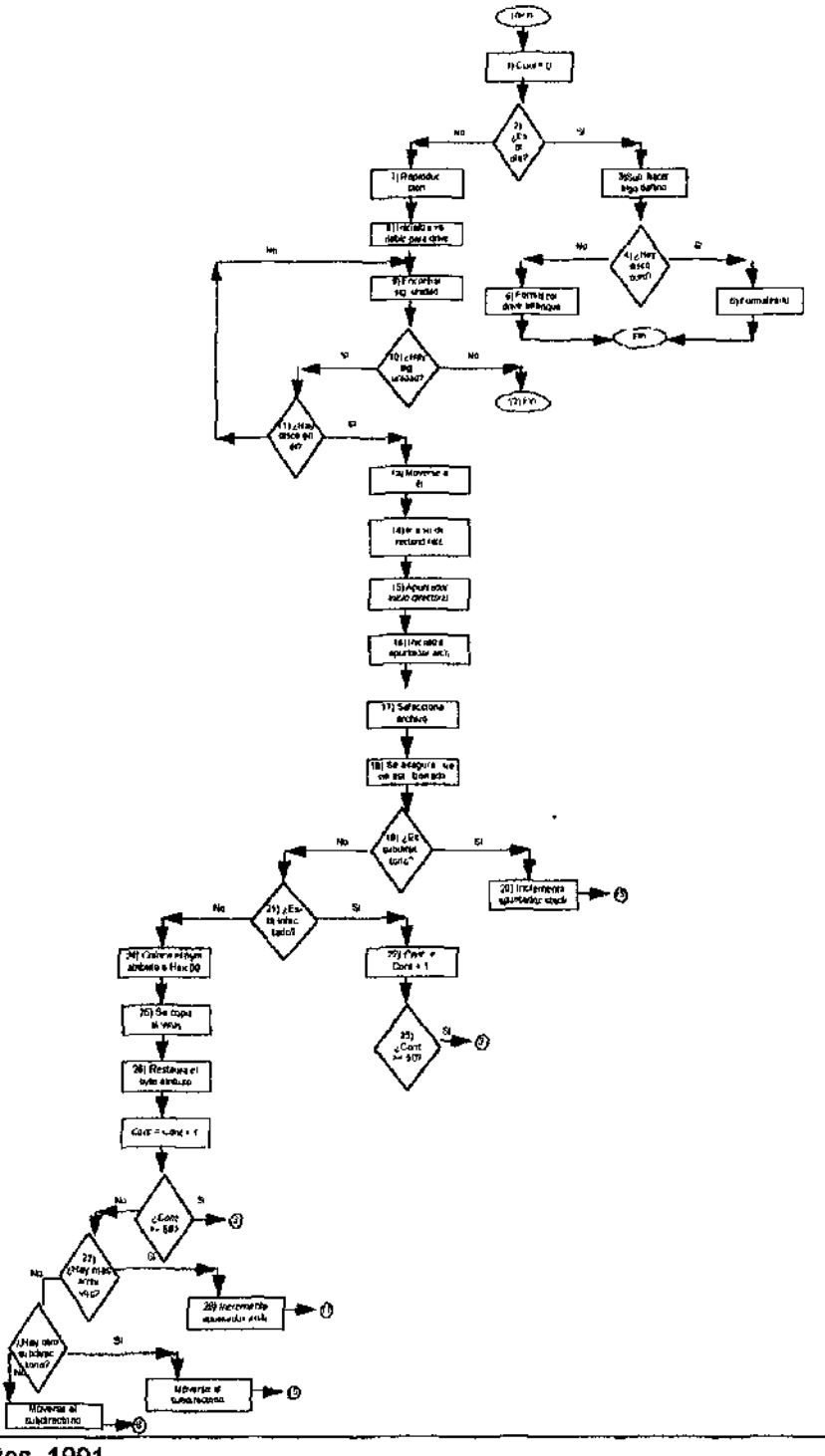
Paso 26. Cubre las rutas del virus de manera que nadie se dará cuenta de lo que ha hecho. Restaura el sistema indicador y el byte de atributos a la forma que tenían antes Cuando ha terminado la reproducción, agrega 1 al contador de copias y verifica si el contador sobrepasa el 50 y entonces destruye

Paso 27 al Paso 28. ¿Hay más archivos aquí? Si los hay, incrementar el apuntador del archivo y empezar el tercer bucle nuevamente

Paso 29 al Paso 30. ¿Hay otro subdirectorio en el stack? Si es así, moverlo, sacarlo de la pila y empezar el segundo bucle otra vez Si no, se ha terminado de trabajar con los archivos del disco, de manera que empieza el bucle principal nuevamente

(Las salidas están en los pasos 6 y 12)

Figura 4 1 Diagrama de flujo de un virus



Fuente: Fites, 1991.

4.2. Clasificación de los virus computacionales

Existen muchas clasificaciones de virus computacionales, basadas en sus diferentes características

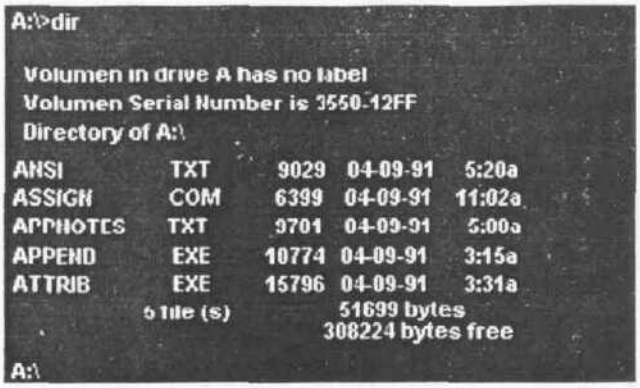
4.2.1. Clasificación general

Bugs

Son fragmentos de código de programas legales mal implementados que, debido a fallos lógicos internos, causan daño al hardware, al software del sistema o inutilizan los datos del usuario en forma accidental. Todos los programas pueden tener bugs Se requiere de un conjunto completo de condiciones para que el bug llegue a ser evidente. Algunos, sin embargo, son fáciles de notar

> Según Solomon (1993, Págs 7-9) *Por ejemplo, el MS-DOS™ contiene un bug muy destructivo que la gente algunas veces ha considerado erróneamente como virus, el cual ha estado desde la versión 2.0 Consiste en lo siguiente.*
>
> *Tome dos discos flexibles formateados. Asegúrese de que ambos contengan archivos, pero no los mismos Asegúrese de que no tendrá problemas si pierde archivos de los discos. Proteja contra escritura uno de ellos. Si se trata de discos de 5¼ pulgadas, la etiqueta protectora no debe ser transparente*
> *Coloque el disco no protegido en el drive A y teclee*
>
> *A <Return>*
> *DIR < Return>*
>
> *El drive hará click, emitirá un zumbido y en un par de segundos verá un directorio listado en la pantalla (ver figura 4 2.). Por ejemplo*

Figura 4.2. Listado del directorio del primer disco

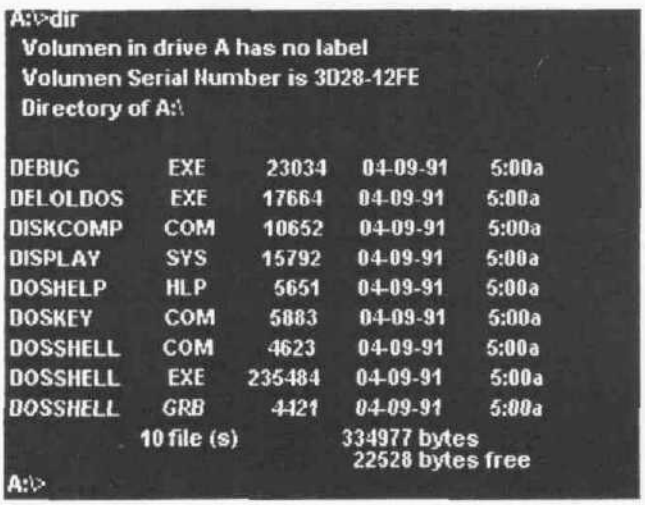


Fuente: Solomon, 1993.

Esto prueba que hay algunos archivos en el disco. Ahora reemplace el disco protegido en el drive y teclee

DIR <Return> (Ver figura 4.3.)

Figura 4.3. Listado del directorio del segundo disco



Fuente: Solomon, 1993.

Cuando el directorio se haya listado, teclee lo siguiente:

COPY CON Test.Txt <Return>

Este es un archivo de prueba <Return>
F6 <Return>

F6 es la tecla de Función F6; utilizando Ctrl-Z se tendría el mismo efecto.

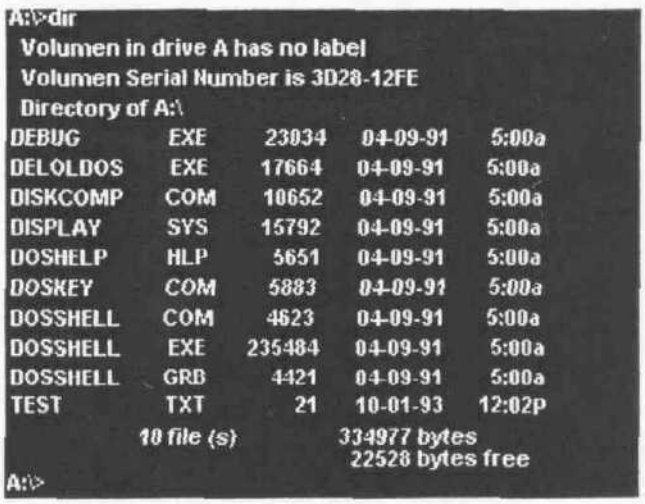
Usted debe observar ahora el siguiente mensaje:

Write protect error writing drive A
Abort, Retry, Fail?

Quite el disco del drive, reemplácelo por el disco no protegido contra escritura y presione R para Retry (intentar nuevamente). El drive zumbará por un segundo o dos y el prompt A> aparecerá. Ahora teclee

DIR <Return> (Ver figura 4.4.)

Figura 4.4. El directorio del primer disco, el cual ha sido sobrescrito por el directorio del segundo disco y el archivo TEST.TXT agregado



Fuente: Solomon, 1993.

Lo que usted debe visualizar es el directorio del disco protegido. El directorio original del disco ha desaparecido. Todos los archivos están todavía en el disco (uno o dos pueden ser corrompidos por el archivo Test.Txt) pero alguien especializado en la recuperación de datos podría recuperarlos. Este experimento puede no funcionar en su computadora particular. En una 486 de

un autor si funciona, pero en una NTC laptop del otro autor, sólamente funciona parcialmente El nuevo directorio aparece, pero el archivo Text Txt se pierde completamente

La variación en el funcionamiento puede ser causado por diferentes versiones de DOS. Este suceso es uno de los problemas con bugs -lo que es un bug en un tipo de computadora, no siempre lo es en otra, o se comporta completamente diferente

Camaleón

Es un programa que emula el funcionamiento de otros programas para obtener información del usuario y realizar alguna clase de daño

Cuando están adecuadamente programados, los camaleones pueden simular todas las acciones de programas de aplicación legítimos, de forma parecida a los programas de demostración, los cuales son simulaciones de programas reales de software.

Por ejemplo, un camaleón que simula el texto para pedir el login de un usuario en una red Novell En vez de que el usuario dé el login a la red, el programa camaleón colecta el nombre del usuario y su password. Entonces el camaleón puede ejecutar auténticamente el login de la red, alimentándola con los datos del usuario sin que se sospeche nada.

Por lo tanto, con un buen programa camaleón, su programador podrá conocer todos los passwords en una LAN, minicomputadora o mainframe Cada vez que un usuario cambie su password, el programa camaleón actualizará su lista.

Según Levin (1991, Págs 12-13) "*En una ocasión, un camaleón fue programado inteligentemente para emular un gran mensaje de apremio de toma de contacto con un sistema de multiusuarios para nombres y contraseñas de los usuarios. El camaleón grabó estos nombres y contraseñas en un archivo secreto y luego presentó un mensaje que indicaba que el sistema estaba inactivo temporalmente por motivos de mantenimiento Algún tiempo después, el autor del camaleón introdujo su propia contraseña confidencial, capturó la lista acumulada y así tuvo acceso a una multitud de loggins de usuarios para sus propios usos ilegítimos.*

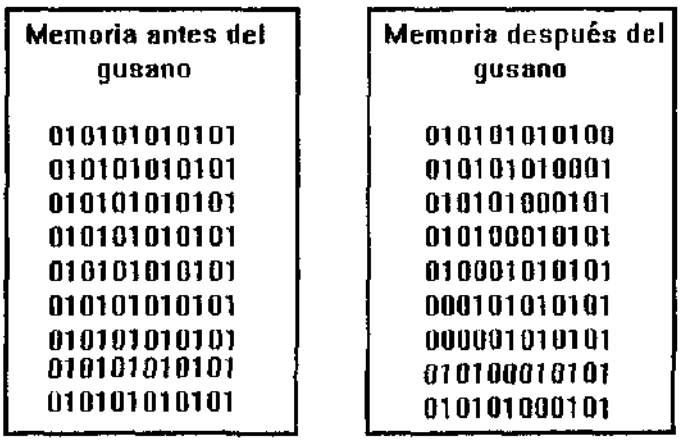
Otro programa clásico de camaleón fue el que simuló un programa bancario normal que el programador utilizó para desviar discretamente unas cuantas décimas de centavo en errores de redondeo a una cuenta secreta por cada transacción El botín resultante ascendió a cientos de miles, quizá millones de dólares"

Gusano

Según Nieto (1991, Pág 29) "*Un gusano es un programa que se transporta (desplaza) por sí mismo a través de la memoria interna y/o discos de una computadora (o en una red de computadoras), a diferencia del virus, que generalmente se adhiere a otros programas Está diseñado para que busque zonas de memoria desocupadas, hasta que consigue un desbordamiento físico de la memoria*" Otra diferencia

importante frente al virus es que los gusanos pueden tener porciones (segmentos) de ellos mismos ejecutándose en la memoria de diferentes máquinas y que mantienen *comunicación* con el programa gusano que los creó

Figura 4 5 Memoria antes y después del gusano



Fuente L Mayo, 1989

Estos programas no proliferan en una PC sino en redes públicas de comunicaciones y en redes de área local, y utilizan el correo electrónico como medio de propagación entre computadoras de una misma red Por lo tanto, un gusano requiere del ambiente de una red y de un autor que esté familiarizado con sus servicios y facilidades. A estos autores se les conoce como hackers porque se dedican a violar los mecanismos de seguridad en una red La tarea de un hacker es la siguiente accede a una de las computadoras de la red, a continuación analiza el sistema de conexión de las computadoras en busca de algún fallo de seguridad que permita pasar programas de una computadora a otra, por último, desarrolla el programa gusano que se encargará de penetrar una a una las demás computadoras de la red

Según L Mayo (1989, Pág. 8) "*Dependiendo de las intenciones del programador, el gusano podría cambiar todos los datos a ceros (ver figura 4 5.) o sutilmente alterar los datos por el intercambio individual de bytes de información almacenada Esta última técnica es más difícil de desarrollar, y potencialmente mucho más peligrosa. En muchos casos, los programas continúan ejecutándose aunque alguna parte del código ha sido alterada. Algunas faltas de ortografía en archivos de texto podrían asumirse como errores tipográficos. Sin embargo, imagine el caos que ocurriría si se alteran los datos de una hoja de cálculo que se usan en la planeación financiera, o si se alteran datos estadísticos*"

Los gusanos viajan en secreto a través de computadoras anfitrionas de la red, reuniendo información (posiblemente contraseñas o documentos) o dejando mensajes

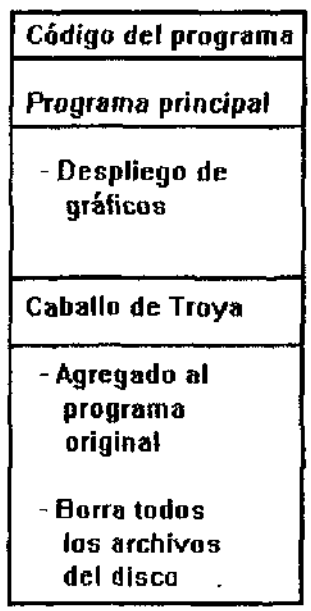
burlones, misteriosos, antes de trasladarse A menudo los gusanos borran todos los vestigios de sus visitas con objeto de permanecer invisibles ante los operadores de la red

El incidente Robert Morris-Internet que abarcó a seis mil computadoras a mediados de 1988 fue un gusano Fue diseñado para reproducirse lentamente, examinando la seguridad en el sistema computacional, pero un bug en el gusano causó que se reprodujera rápidamente, cada copia del gusano reinfectaba a otra computadora en la red hasta que saturó la memoria

Caballo de Troya

Tomaron su nombre de el infame caballo de Troya de tiempos pasados. Es un programa que aparenta ser legítimo mientras contiene otro programa que generalmente es malicioso (ver figura 4 6)

Figura 4 6 Caballo de Troya



Fuente L Mayo, 1989

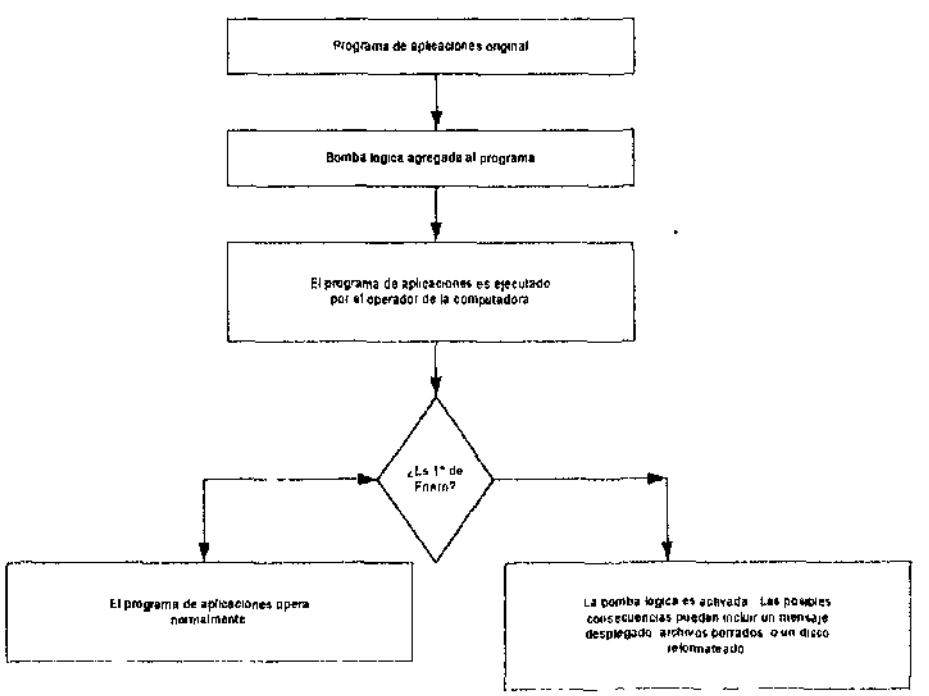
Como característica esencial de estos programas indicaremos que carecen del factor de autorréplica Por ello, su código maligno sólo se activa una vez al ejecutar el caballo de Troya que lo porta. Por ejemplo, un caballo de Troya podría ser un juego de computadora que reformatea el disco duro de la computadora cuando es ejecutado Se pueden utilizar también para extorsionar operaciones rutinarias, como el redondeo de cuentas en los procesos de actualización de cuentas bancarias, o para atacar los

sistemas de empresas introduciendo el programa malicioso por la puerta principal, disfrazado de publicidad o de información de utilidad Están limitados a los programas que los contienen y a los sistemas en que se pueden ejecutar, esto no sucede con los virus computacionales

Bomba lógica

Una bomba lógica es un programa muy corto que se agrega a un programa existente o, en algunos casos, una modificación hecha a un programa existente Se les llama así porque "explota" cuando ciertas condiciones son reunidas La condición o hecho que motiva la activación es variable y comprende desde una fecha determinada, por ejemplo un viernes 13, hasta secuencias especiales de teclas Si no se produce el suceso programado, el programa permanece oculto al usuario, sin ejercer más acción que ocupar una porción de la memoria Cuando llega el momento determinado, ejerce la acción para la cual se programó (ver figura 4 7)

Figura 4 7 Diagrama que muestra el seguimiento de una posible bomba lógica. Cuando la fecha es 1° de Enero, la bomba lógica se activa



Fuente L Mayo, 1989

La bomba lógica debe ser agregada al programa de aplicación por alguien con acceso al sistema y que tenga conocimiento para alterar el programa

Las bombas lógicas no afectan a las computadoras personales al mismo grado que lo hacen los caballos de Troya y los virus, debido a que las bombas lógicas son escritas para programas en particular corriendo en sistemas de hardware particular por una cierta razón maligna Sin embargo, las bombas lógicas aparecieron antes en el mundo de la PC

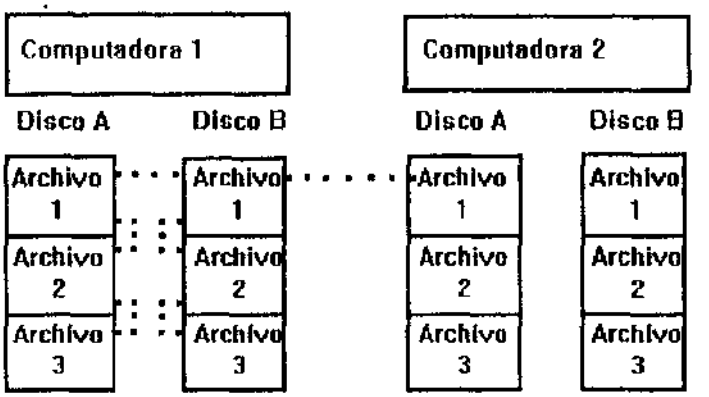
Un ejemplo es un procesador de palabras que fue distribuido con una particular PC para usarlo gratis por un tiempo limitado haciéndole una evaluación Los usuarios que decidieron el uso del procesador de palabras esperaron para registrarse con la compañía y pagar una cuota Entonces, los usuarios registrados recibieron una copia nueva del programa y la documentación relacionada Sin que los usuarios tuvieran conocimiento, una bomba lógica fue colocada en todas las copias de evaluación no registradas Cuando el programa fue ejecutado después haber concluido el periodo de evaluación, la computadora se bloqueó y el procesador de palabras procedió a borrar todos los archivos de texto almacenados en los discos de la computadora

La bomba lógica podría ser programada también para borrar o volver a calcular incorrectamente los registros, reformatear discos o realizar otras acciones análogamente destructivas

Virus

El motivo que ha originado la confusión de los virus con los programas escondidos en caballos de Troya o con bombas lógicas, es que muchos virus utilizan características similares a las de estos programas (ver figura 4.8)

Figura 4 8. Un virus computacional puede propagarse de archivo a archivo, de disco a disco y de computadora a computadora



Fuente L Mayo, 1989

Se trata, por ejemplo, de la posibilidad de estar contenidos en otros programas y permanecer ocultos a los ojos del usuario, o bien de sus condiciones de activación Como ejemplo, el virus Viernes 13 precisa para ejercer su acción destructiva que la

fecha del sistema coincida con el día trece del mes y con un viernes como día de la semana Por otro lado, se adhiere a la estructura de los archivos ejecutables para ocultarse, convirtiéndolos a su vez en caballos de Troya portadores del código del virus

En cuanto a los gusanos, la diferencia más significativa frente a los virus estriba en que los primeros ejercen su acción de copia sucesiva en la memoria interna de la computadora, mientras que los virus realizan su función de autocopia en los discos Esta función de copia es la que ha provocado la confusión

4.2.2. Clasificación en función de la parte modificada por el virus en su ataque

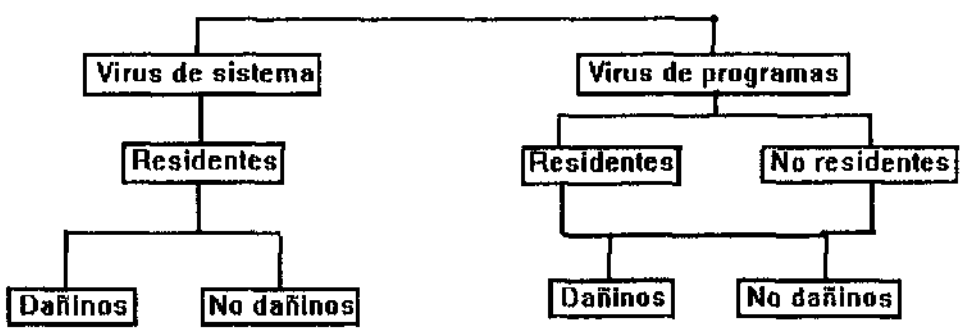
Virus de Sistema Operativo

Aquí se incluyen aquellos virus que son capaces de modificar el sector de arranque (boot) de los discos flexibles y duros, y la tabla de partición de los discos duros.

Virus de Programas

Dentro de esta división se incluyen los virus que son capaces de modificar la estructura de los archivos ejecutables con las extensiones COM, EXE, OVL, OVR, DRV, BIN, .DLL

Figura 4 9 Clasificación en función de la parte modificada por el virus en su ataque



Fuente Compumundo 92.

4.2.3. Clasificación por la forma en que trabajan

Algunos virus se alojan en las áreas más vulnerables de los discos que son el sector de carga (sector boot), la tabla de particiones en el caso de discos duros, en la tabla de asignación de archivos (File Allocation Table [FAT]), o en los sectores que ocupan los archivos ejecutables o programas de usuarios.

Cada técnica de infección proporciona notables ventajas y desventajas a los programadores Algunos métodos de contaminación son preferidos porque es menos probable que el software antivirus los detecte, sin embargo pueden ser complejos de diseñar Otros procedimientos pueden ser más fáciles de codificar y desarrollar, pero limitados en su capacidad de saturar sistemas completos

Virus contaminadores del sector de arranque (boot)

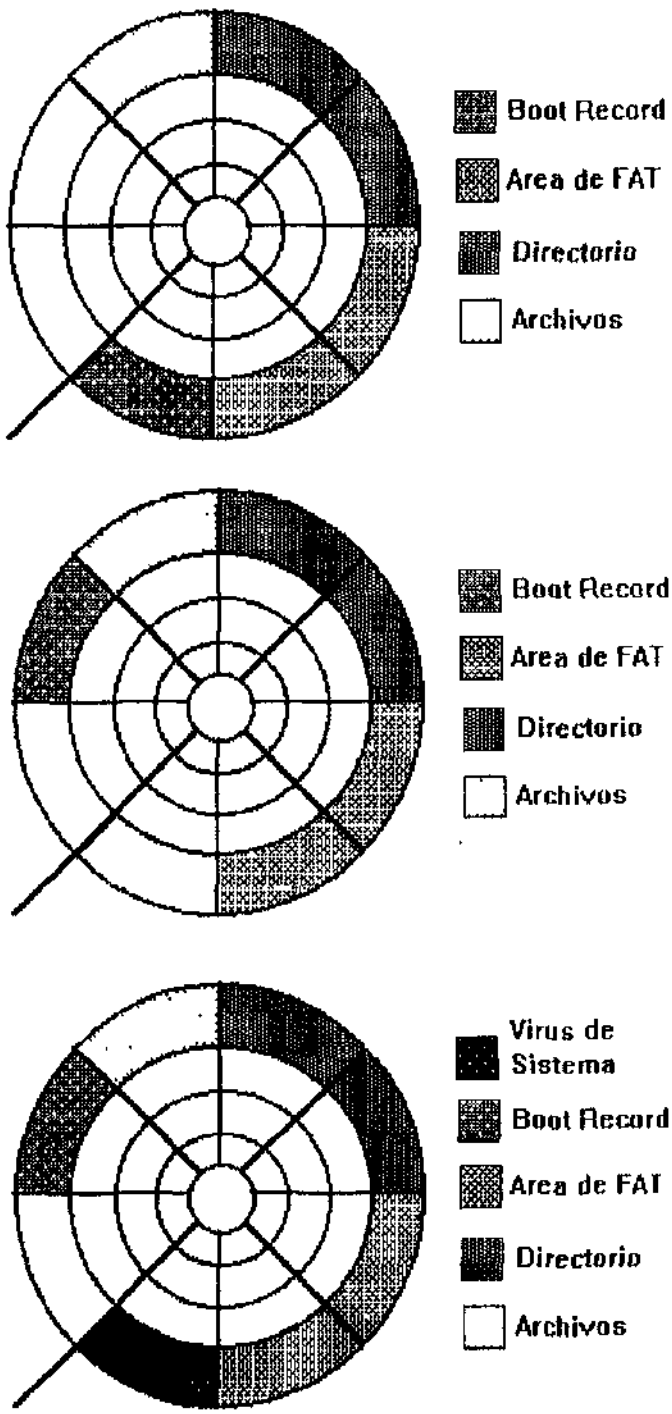
El sector de arranque es el primer sector en un disco flexible En un disco duro el primer sector lo ocupa la partición del DOS El sector de arranque contiene información acerca del disco (tal como el número de sectores en el volumen lógico) más un pequeño programa Cuando la computadora arranca, lee el sector de arranque en el disco de la unidad A o, si la unidad está vacía, lo lee de la unidad C, carga lo que encuentra en memoria y lo ejecuta Un virus del sector de arranque reemplaza el sector de arranque original (localizado en el sector 0 pista 0) con su propio código y lo mueve a otra parte del disco, de manera que pueda ser cargado después de que el virus haya finalizado su tarea y el proceso del sector de arranque original pueda continuar (ver figura 4 10)

Una vez que el virus ha infectado un sector de arranque, éste se ejecutará cada vez que la computadora arranque El virus se carga en memoria y se protege marcando esta parte de la memoria que utiliza El virus intercepta algunas interrupciones de la computadora (la interrupción 13h, y algunas veces otras) La interrupción 13h es la que controla la lectura y escritura de un disco, de manera que cada vez que se lea o grabe a un disco , el virus se ejecute primero Siempre que un disco sea accesado, el virus verificará si ya está instalado en él Si no está presente, entonces se instala Algunos virus sólo infectan discos flexibles, pero la mayoría infecta tanto discos flexibles como duros Si un virus ha infectado un disco duro o un disco flexible con DOS, habrá probablemente un gran número de discos infectados a su alrededor

Para los programadores de virus, la infección de los sectores de arranque de discos proporciona numerosas ventajas sobre todos los otros medios de infección, debido a que son cargados inmediatamente al arrancar la computadora, antes de que sea cargado el sistema operativo y el COMMAND COM, asumiendo un control total. Este tipo de virus pueden permanecer residentes y activos en todo momento, superando arranques en caliente (<Ctrl-Alt-Del>) y contaminar discos de arranque no infectados. Pueden controlar todas las acciones de los usuarios manteniendo el dominio sobre las medidas de software antivirus Por ejemplo, pueden cambiar listados de directorios para mostrar los tamaños correctos de los archivos cuando, en realidad, dichos tamaños han cambiado a consecuencia del código del virus añadido, engañando a los programas de software antivirus que comparan los tamaños de archivos

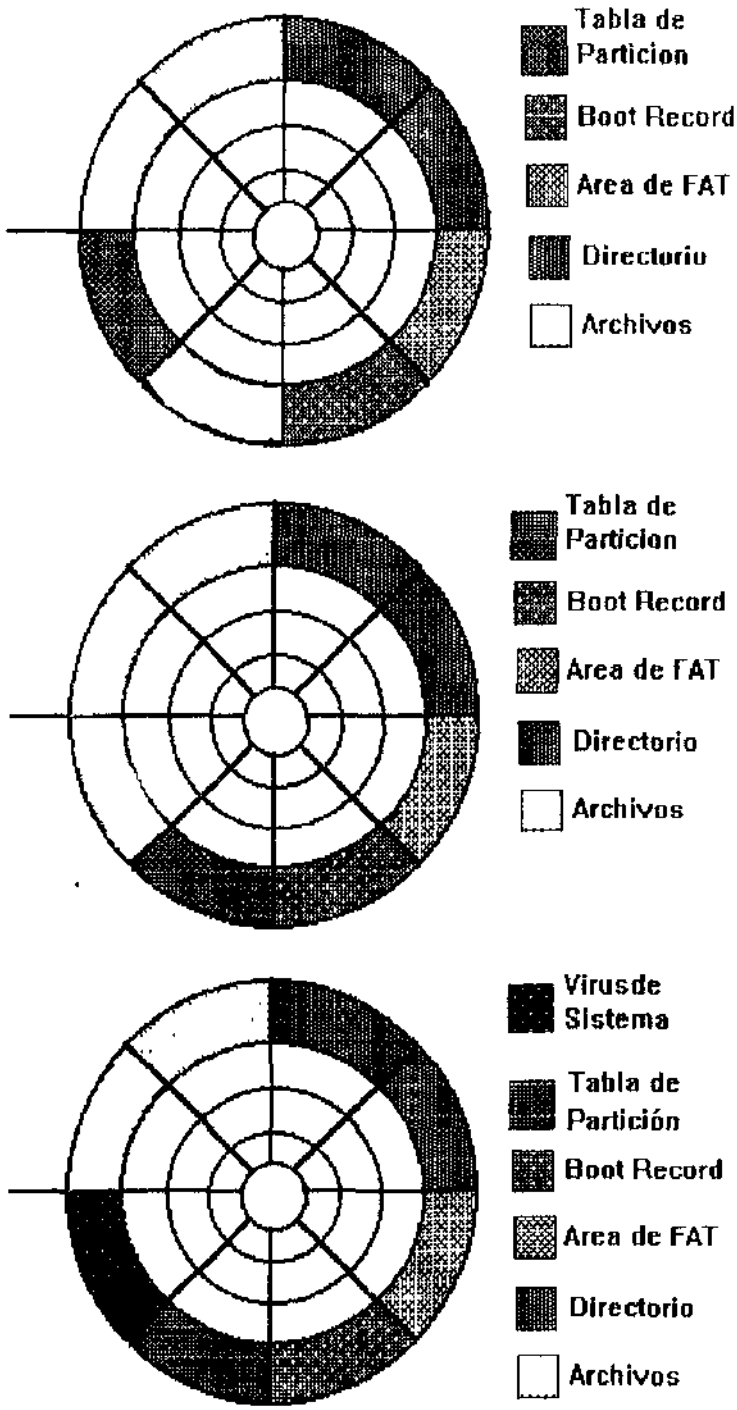
Ejemplos de este tipo de virus, son Alameda, Stoned, Brain, Search y el Ping-pong (virus italiano)

Figura 4 10 Contaminación del sector de arranque



Fuente Compumundo 92

Figura 4 11 Contaminación del sector de partición



Fuente: Compumundo 92

Virus contaminadores del sector de partición

El sector de partición es el primer sector de un disco duro Contiene información acerca del disco (tal como el número de sectores en cada partición y dónde comienza la partición del DOS) más un pequeño programa Cuando la PC arranca, lee el sector de partición en el disco y ejecuta el código Un virus de sector de partición es como un virus del sector boot con la excepción de que es más difícil de encontrar, muchas herramientas para examinar discos, tales como Debug, no permiten ver el sector de partición Los discos flexibles no tienen un sector de partición, de manera que un virus de sector de partición en un disco flexible tiene el mismo efecto que un virus del sector boot (ver figura 4 11)

El bloque de código del sector de partición es de sólo 446 bytes Por eso, el sector de partición original se esconde en un lugar conocido en el disco, y entonces se encadena a este sector el código del virus Esta es la técnica usada por el virus New Zealand (Stoned), descubierto en 1988

Virus contaminadores del intérprete de comandos (COMMAND COM)

El archivo COMMAND COM se carga después de que la PC haya terminado su proceso de arranque Esto significa que los dos archivos de arranque, MSDOS SYS e IO SYS ya han sido cargados y ejecutados, y que la computadora está preparada para empezar a realizar las órdenes del usuario. Una vez que aparece el prompt A> o C>, el usuario da la orden, COMMAND COM lo interpreta y realiza las funciones requeridas, luego vuelve a presentar el prompt en espera de instrucciones adicionales

Los virus diseñados para infectar el COMMAND.COM ofrecen una ventaja distinta a sus programadores como muchas órdenes introducidas en el teclado son pasadas a través del programa COMMAND COM, estos virus tienen la ventaja de examinar una gran mayoría de la interacción entre los usuarios y sus computadoras Pueden explotar las oportunidades para esconderse tras accesos normales de disco mientras se ejecutan órdenes internas del COMMAND COM (como DIR o COPY)

Por ejemplo, cuando el usuario quiere ver el contenido de un disco, teclea el comando DIR, las unidades de disco se activan para realizar funciones (leer) del directorio El usuario espera que los accesos a los discos sean dirigidos en ese momento; los virus corresponden a esas expectativas Antes de que la orden DIR del disco sea en realidad procesada, los virus del COMMAND COM se introducen, buscan e infectan otros archivos COMMAND.COM que encuentren y luego terminan las funciones normales de la orden DIR Aunque los tiempos de ejecución de las órdenes interceptadas por virus son mayores que los de las no infectadas, la mayoría de los usuarios no notan la diferencia

Los virus contaminadores del COMMAND COM, al igual que los virus del sector boot, son cargados desde el momento del arranque de la PC, permanecen residentes en memoria y tienen la capacidad de supervisar y controlar casi todas las interacciones usuario-computadora La diferencia básica entre estos dos tipos de virus es que los del sector boot se instalan primero, a un nivel mucho más bajo al que se instalan los

virus del COMMAND COM, proporcionándoles a los primeros la capacidad de influir en casi todas las interacciones del sistema, mientras que los segundos, instalados hacia el final del proceso de arranque, tienen acceso a menos facilidades, pero muy potentes

El programa COMMAND COM puede ser infectado como cualquier otro archivo COM

Ejemplo de este tipo de virus es el Lehigh, el cual atacó la Universidad Lehigh en Noviembre de 1988 Este virus causó daños en los discos duros después de haberse reproducido en cuatro archivos COMMAND COM adicionales

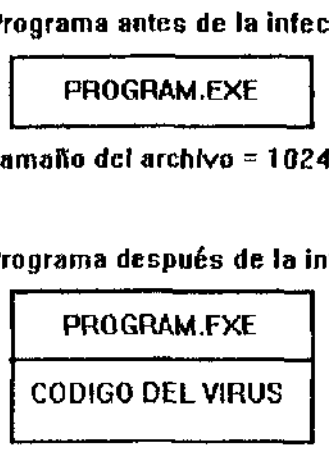
Contaminadores de archivos ejecutables (COM, EXE)

Este tipo de virus se agrega o inserta a un archivo ejecutable Esto es mayormente a archivos .COM y EXE, pero podría ser también a archivos SYS, DRV o a archivos de overlays (OVR, OVL)

Para infectar a estos archivos, el virus debe insertar su código de tal manera que éste sea ejecutado antes que el del programa que infectó Esto lo puede hacer de cuatro formas

a) Por añadidura Los virus agregan su código al final de los archivos ejecutables Los archivos ejecutables originales son modificados para que, cuando se ejecuten, el control del programa se pase primero al código del virus añadido, el cual se activa, y después de realizar las acciones para las que fue diseñado, devuelve el control a los archivos originales, los cuales continúan ejecutándose como normalmente lo harían (ver figura 4 12)

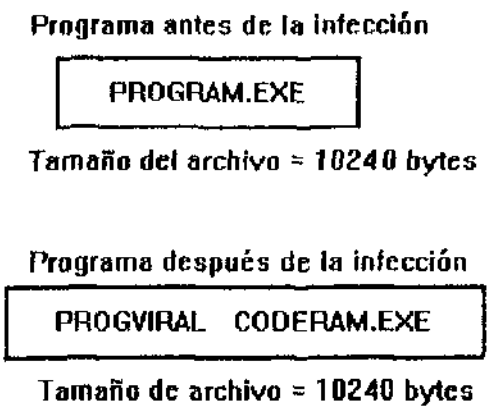
Figura 4 12 Contaminación de un archivo ejecutable por añadidura



Fuente Levin, 1991

b) Por inserción Los virus sitúan su código dentro del código no utilizado de los programas ejecutables originales Los archivos ejecutables originales son modificados de forma muy parecida a los de añadidura, excepto que el código del virus está ahora dentro de los archivos ejecutables originales, en lugar de ser agregados al final de los archivos El tamaño del código de este tipo de virus tiene que ser reducido al mínimo En muchos casos puede ser difícil encontrar cantidades suficientes de espacio del programa original no utilizado o incluso puede no estar disponible en los archivos ejecutables de destino (ver figura 4 13)

Figura 4 13 Contaminación de un archivo ejecutable por inserción



Fuente Levin, 1991

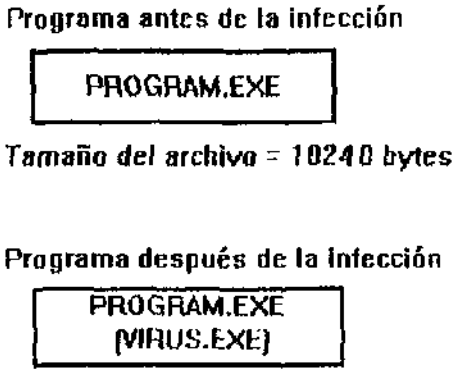
c) Por reorientación Se introducen virus centrales (centros de control) en una o más posiciones físicas de los discos, tales como áreas de partición del disco, sectores del disco marcados como dañados e inutilizables o como archivos escondidos ordinarios Estos virus, utilizando las técnicas de añadidura o inserción implantan diminutos programas virus entre los archivos ejecutables normales. Estos programas se activan cuando los programas originales infectados son ejecutados, reorientando el flujo del programa mediante las solicitudes de ejecución a sus virus centrales

La infección por reorientación también conserva el espacio en disco Las porciones del código del virus, que son convenientemente pequeñas, aumentan los tamaños de los programas en unos cuantos bytes o en nada si se utilizan infecciones de inserción, por lo que se pueden crear virus computacionales grandes y versátiles, sin preocuparse por las consecuencias de añadir kbytes a los archivos ejecutables originales.

d) Por sustitución o sobrescribiendo. Los virus escriben su código directamente sobre el código del programa original, destruyendo parte o todo de él El programa original ya no se ejecutará correctamente después de la infección Esta táctica tiene beneficios para los programadores de virus debido a que cada sustitución de un virus

sirve para eliminar archivos de programas válidos Sin embargo, el inconveniente de este método es que las infecciones son casi siempre descubiertas poco después de que hayan tenido lugar, promoviendo la rápida erradicación de los virus Debido a que los virus de sustitución empiezan a destruir los datos desde su primera ejecución, sus efectos son dañinos pese a la prontitud o eficacia con que sean eliminados (ver figura 4.14)

Figura 4 14 Contaminación de un archivo ejecutable por sustitución



Fuente Levin, 1991

A continuación se explica el proceso de contaminación a los archivos ejecutables *COM* y *EXE*

Contaminación de un archivo COM La mayoría de los archivos .COM tienen tres bytes al principio que hacen un jump (salto) al principio del programa actual El virus podría agregarse al final del archivo, parchando el jump de manera que ejecute el salto al código del virus, y la última instrucción del código del virus sea un salto al programa original Esto asegura que el programa original se ejecute en una forma aparentemente normal. El virus también puede anidarse en un bloque suficientemente grande de ceros en el código En tal caso, el salto al código del programa original aún asegura que el programa sea ejecutado en forma aparentemente normal (ver figura 4 15)

Según Nombela (1990, Pág 58) "*El proceso de contaminación consistirá entonces en*

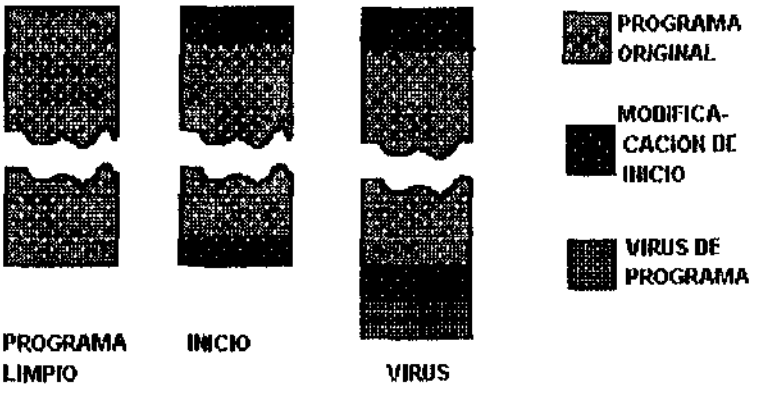
a) Abrir el archivo para que sea de lectura/escritura

b) Añadir el programa del virus al principio o al final del archivo

c) Guardar los primeros bytes en algún lugar apropiado del programa del virus, para que puedan ser sustituidos al final de la ejecución de éste

d) Sustituir los primeros bytes del archivo por la llamada al código del virus
e) Cerrar el archivo"

Figura 4 15 Contaminación de un archivo COM



Fuente Compumundo 92

Contaminación de archivos EXE

Según Nombela (1990, Págs 58-59) *Los archivos EXE contienen en su cabecera (header) información que necesita el DOS para el cálculo de las direcciones correctas de algunas instrucciones Se componen de dos partes una cabecera, que contiene información de control y reubicación, y un módulo de carga que contiene el código del programa, con algunas direcciones todavía incorrectas*

En la cabecera también se contienen los datos que son necesarios para localizar la primera instrucción del programa Estos datos son los valores que el DOS colocará en los registros del procesador y que determinarán de esa forma la dirección de comienzo Un virus puede aprovecharse de esta circunstancia y sustituir unos pocos bytes de la cabecera por los necesarios para que la dirección de comienzo de ejecución del programa sea la del código del virus, que se añadirá al final del módulo de carga La última instrucción del código del virus será un salto a la primera instrucción del programa onginal, que se habrá calculado con los datos contenidos en la cabecera (ver figura 4 16)

El proceso de contaminación consistirá entonces en:

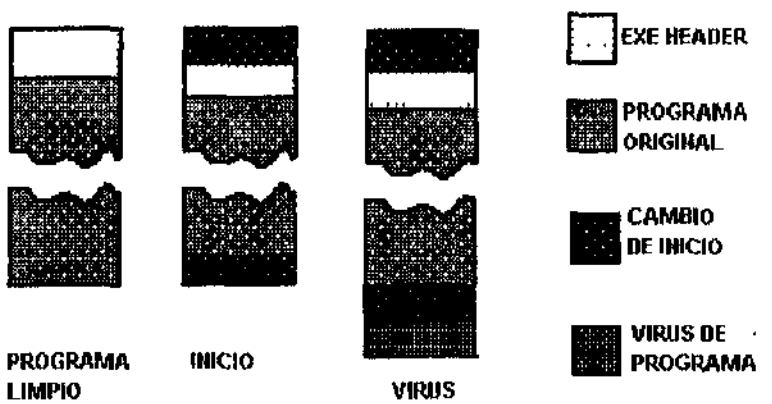
a) Añadir el código del virus a continuación del código del programa

b) Guardar determinados valores contenidos en el header en alguna variable dentro del código del virus

c) Sustituir los valores anteriores por los necesarios para que la primera instrucción que se ejecute cuando se transfiera el control al módulo, sea la de inicio del código del virus

d) Dentro del programa del virus deberá haber alguna rutina que permita realizar los cálculos necesarios para deducir los valores adecuados que se tendrán que colocar en los registros del procesador inmediatamente antes de ceder el control al programa original Para estos cálculos será necesario utilizar los valores originales contenidos en el header y que se guardaron durante el proceso de contaminación

Figura 4 16 Contaminación de un archivo .EXE



Fuente Compumundo 92

Otros puntos a considerar en la contaminación a los archivos ejecutables (.COM y EXE), son

Los virus de archivos ejecutables se activarán cada vez que se ejecute un archivo infectado El código del virus buscará un archivo no infectado, lo infectará y, después de esto, el programa original correrá normalmente

Debido a que los archivos COM tienen una estructura muy simple, se presta para ser infectada fácilmente. Es sólo ligeramente más difícil escribir un virus infector de archivos EXE porque la estructura de estos archivos es más compleja Muchos virus sólamente infectan archivos COM y un número menor infectan tanto archivos COM como archivos EXE.

Algunas veces se cree que un archivo infectado con un virus tendrá una fecha y hora cambiada Sin embargo, no es así Actualmente los paquetes de utilerías permiten, al igual que los virus, leer la hora y fecha de un archivo, y colocarles sus

valores originales después de hacerles algún cambio También le permiten cambiar el atributo de un archivo y después volver a colocar al atributo original

Sin embargo, esta situación es diferente en una red Los atributos colocados por un supervisor no pueden ser cambiados por un usuario "ordinario" La seguridad en una red puede ser efectiva contra los virus, debido a que el virus tiene los mismos privilegios de un usuario conectado a esa red

Virus contaminadores multipropósito

Es completamente posible que un virus sea del tipo infector del sector boot o partición e infector de archivos ejecutables A este virus se le llama multipropósito, sin embargo, no todos ellos trabajan de la misma forma

El virus Tequila infecta el sector de partición de un disco duro cuando es ejecutado desde un archivo infectado en un disco flexible Cuando la computadora es arrancada subsecuentemente, el virus queda residente en memoria e infecta todos los archivos EXE que sean ejecutados, ya sea desde el disco duro o desde un disco flexible

Exebug es un virus del sector de partición en discos duros e infecta sectores boot en disco flexibles, pero también puede ocasionalmente sobrescribir un archivo .EXE El archivo ejecutable sobrescrito ya no ejecutará sus funciones originales

Adoptando dos o más técnicas infecciosas, logran un nivel de supervivencia más alto y tienen menos problemas reproduciéndose que los que tienen los virus que poseen una única técnica

Cuando los virus multipropósito obtienen el control durante los tiempos de ejecución, normalmente inspeccionan los sectores de arranque, los archivos COMMAND COM y los demás archivos ejecutables para verificar si ya han sido infectados Si encuentra algo no infectado, entonces procede a agregarle una copia de sí mismo.

Virus residentes en memoria

La diferencia entre un virus contaminador de archivos ejecutables y un virus residente en memoria es que el segundo se instala por sí mismo en la memoria, generalmente reemplazando la función de la interrupción 21h del DOS La mayoría de los autores de virus se han fijado en la interrupción 21h, función 4b (cargar y ejecutar un programa) Esta función sólamente es llamada cuando DOS trata de cargar un archivo COM o .EXE, los cuales son exactamente los que el virus quiere infectar Esto significa que, una vez que el virus está instalado en memoria, tiene el control cada vez que el DOS realiza alguna acción El virus hará primero todo lo que quiera y después pasará la solicitud original a DOS, ya sea intacto o en una forma modificada, de manera que sólamente se necesita ejecutar el virus residente en memoria una vez para infectar a otros archivos Esto también significa que el comportamiento de la computadora bajo el control del virus puede ser impredecible

Virus contaminadores de la tabla de asignación de archivos (FAT)

Algunos virus podrán asumir el control de la FAT, reorganizando el almacenamiento del disco o dañando la habilidad de la FAT de apartar el lugar donde los datos están localizados en el disco En efecto, el virus vuelve a trazar el mapa del disco o lo destruye, de manera que el sistema operativo no puede encontrar la forma de localizar en el disco alguna parte de los datos que hayan sido salvados

Los virus que envían copias de sí mismos al área de memoria RAM, la memoria principal de trabajo de la computadora, pueden permanecer ocultos, pero listos para recibir en cualquier momento a los anfitriones que vengan, tales como un disco infectado que está siendo cargado en alguno de los drives

El peligro potencial de un virus no siempre es en proporción directa de su complexión, tamaño o sofisticación *Un simple virus que rápidamente modifica la FAT*, que formatea un disco duro, o que arrastra pocos bytes de datos al directorio principal puede ser fatal para las actividades de procesamiento de datos Aun si el peligro actual es pequeño, las consecuencias pueden ser serias

Virus compañero

Los programas son ejecutados por el COMMAND COM, en orden jerárquico Si se tienen dos archivos con el mismo nombre pero con diferentes extensiones, cuando se teclea el nombre de un programa en el prompt del sistema operativo, el COMMAND.COM ejecutará el archivo con extensión COM en vez del programa con extensión .EXE

Un virus compañero infecta buscando un archivo ejecutable, normalmente con la extensión EXE Entonces el virus crea un archivo escondido con el mismo nombre pero con la extensión .COM. Este nuevo archivo escondido contiene el virus y una instrucción para que se ejecute el programa con extensión EXE después de que el virus se ha ejecutado. De manera que un virus compañero simplemente se llama él mismo por medio del mismo nombre como otro archivo, excepto que éste tiene una extensión .COM Algo importante para entender los virus compañeros es que los cambios no son hechos al archivo EXE original. Esta técnica puede hacer fracasar los métodos de detección de virus que se basan en encontrar cambios en archivos ejecutables

4.2.4. Clasificación por la forma en que virus intenta ocultarse o encubrirse

Virus con tácticas sigilosas o stealth

Para que un programa pueda ser considerado un virus, todo lo que necesita hacer es copiarse por sí mismo Pero para que sea un virus exitoso, necesita ser tan discreto como sea posible

El término que se utiliza para los virus que intentan permanecer discretos es *stealth* Debe comprenderse que hay varios grados de stealth, y varios tipos de

mecanismos de programación que son utilizados para lograr los diferentes grados de stealth

Algunos virus son altamente visibles, por ejemplo, el virus Burger sobrescribe el principio de los archivos que infectan En consecuencia, el programa infectado ya no funciona, y el usuario lo nota inmediatamente Esto es llamado *stealth negativo* Aproximadamente el 10% de los virus conocidos tienen stealth negativo, y la razón debe ser porque hay algunos autores de virus que lo que les interesa es alardear que escribieron un virus Los virus del sector boot no pueden tener stealth negativo Si una vez que ellos han ejecutado su propio código, no pasan el control al sector boot original, entonces la computadora fallaría al cargar, lo cual sería obvio para el usuario Además, por supuesto, el virus no sería capaz de multiplicarse exitosamente

El siguiente nivel de stealth es necesario para que el virus se reproduzca del todo *El programa original debe poder ejecutarse después de la infección* Para lograr esto, el virus debe agregar su código al archivo y preservar toda la información necesaria para que el programa se ejecute propiamente, y para que también el virus se ejecute Aproximadamente el 90% de los virus lo logran Esto es llamado *no stealth* Si el virus no hace más que esto, sólo será moderadamente visible, debido a que los archivos tienen marcada una fecha y hora cuando son creados, si un archivo es modificado, entonces la fecha y la hora mostrarán cuándo la modificación tuvo lugar Sin embargo *la mayoría de la gente no observa las fechas y horas marcadas en los* archivos

Si la fecha y la hora originales no son conservadas durante la infección, su modificación podría ser notada por un usuario alerta Un método para evitar algún cambio es utilizar la interrupción 21h, función 57h Pocos virus utilizan métodos de bajo nivel para conservar la fecha y la hora

Si un virus utiliza el DOS para agregarse al archivo, y el disco está protegido contra escritura, DOS mostrará el error Abort, Retray, Fail. Esto será notado --el usuario puede preguntarse por qué está siendo escrito, cuando todo lo que el hizo fue tratar de ejecutar un programa Nuevamente, esto alertaría al usuario Es regularmente fácil evitar este problema

Los virus del sector de arranque no tienen que hacer nada de lo expuesto arriba, debido a que no son visibles como archivos

Un virus que se enfrenta con los dos problemas de arriba tiene *stealth elemental.* En suma, para poder clasificarse en este nivel, el virus no debe hacer nada llamativo Algunos virus siguen esta primera parte de la regla, pero entonces hacen algo más que los hace altamente visibles; por ejemplo, el virus Diamond (V1024) tiene un despliegue *que es activado cada hora cuando el virus está residente en memoria* Un *diamante* multicolores aparece de repente en la pantalla, rompiéndose en fragmentos, moviéndose alrededor de la pantalla

Es posible ocultar el incremento del archivo en varias formas La forma más obvia para hacer esto, es no tener un incremento en el tamaño del archivo en primer lugar El virus Zero-hunt busca un bloque de ceros contiguos en un archivo, y si lo

encuentra, sobrescribe esa parte del archivo con una copia de su código Como debe haber suficientes ceros para contener el código completo del virus, el archivo no crece del todo El virus coloca una pequeña rutina al principio del programa, la cual causa un salto y ejecuta su código Una vez que esto ha sucedido, el virus regresa el control al programa original El virus Rat utiliza una técnica similar, pero sólamente trabaja en archivos EXE, donde busca un bloque de ceros que muchos compiladores colocan al principio del archivo EXE, justo después de la cabecera (header)

Para la mayoría de la gente, la única forma que conocen para inspeccionar el tamaño de los archivos es con el comando DIR DIR utiliza la interrupción 21h, funciones 11h y 12h Si el virus intercepta la interrupción 21h, atrapa sus funciones y entonces puede sustraer la longitud del virus y pasar este valor falso a alguna llamada al programa, de manera que si el comando DIR es ejecutado, el resultado parece normal El virus Zero-Eater (También llamado Zero-bug) utiliza este método

Otra forma de informarse sobre el tamaño de un archivo es con la interrupción 21h, funciones 4eh y 4fh. Estas son las equivalentes a 11h y 12h, algunos programas como el SHELL del DOS utilizan estas funciones para averiguar el tamaño de los archivos También si un programa antivirus está checando el tamaño de los archivos, es probable que use estas funciones, debido a que es más fácil en la programación que las 11h y 12h El virus puede atraparlas y fingir estas llamadas también

Una tercera forma de averiguar el tamaño de los archivos, es con la interrupción 21h, función 42h, subfunción 2 Esta busca el final del archivo, y el tamaño de los archivos es regresado en los registros Un programa antivirus solapado podría utilizar esta llamada para determinar el tamaño del archivo, pero hay virus solapados que también sustraen esto, como el Tequila

Por supuesto, se pueden evitar tales trucos cargando la computadora con un conocido disco de DOS libre de virus. Muy poca gente actualmente hace esto antes de ejecutar su software antivirus Se asume que mucha gente no sigue las instrucciones en el manual, debido a que no lo leyeron, porque tomaron la decisión de que no es necesario leerlo o porque tienen una copia pirata y por lo tanto no tienen el manual a su alcance

Un problema con los tres métodos de arriba (desde el punto de vista de los autores de los virus), es que el virus debe estar en memoria para operar con discreción, de manera que el virus quizá no ha sido ejecutado todavía, o el usuario volvió a cargar la computadora con un disco limpio de DOS. La siguiente forma de evitar el aparente crecimiento en el tamaño del archivo, es aumentar el archivo, por ejemplo, el virus Number-of-the-Beast tiene 512 bytes de tamaño, y reemplaza el primer sector del archivo con una copia de sí mismo Pero como necesita ese sector original, lo almacena después del final del archivo, en el espacio entre el final del archivo y el final del cluster La mayoría de los discos duros tienen 2 Kb clusters, así que el 75% de los archivos tendrá el espacio disponible necesario. Un problema con este método, es que cuando se copia ese archivo a un disco flexible, el tamaño del cluster debe ser por lo menos de 1 Kb, y los discos de alta densidad tienen los clusters

de 512 bytes de tamaño Cuando se copia un archivo infectado a disco flexible, el virus será copiado, pero no todo el programa original

El virus V1963 (y V1963B, también llamado Necrophilia) necesita 1963 bytes, de manera que esta técnica no sería muy exitosa En vez de esto, el virus agrega un cluster a la cadena de la FAT, el cual utiliza para almacenar los primeros 1963 bytes del archivo original La entrada del directorio queda inalterada, de modo que si el virus no está en memoria, el tamaño del archivo no se mira sospechoso

En el caso de un virus stealth del sector boot, éste tendría que mostrar el sector boot original siempre que una solicitud fuera pedida para leer el sector boot El Brain fue el primer virus que hizo esto Pero el hecho de que con facilidad coloca (c) Brain como etiqueta del volumen del disco, además de notificar 3 Kb como sectores dañados en el disco, realmente lo descalifica como stealth intermedio

Para que un virus llegue a ser totalmente invisible a los programas antivirus, es necesario ir al *stealth avanzado*. Pero primero se describirán algunas técnicas de ocultamiento variadas

Ciertos programas antivirus trabajan interceptando las interrupciones, y entonces bloquean ciertas actividades, como son intentar escribir a archivos .COM o EXE Si alguno de los programas antivirus está en memoria, es obviamente una buena idea para el virus desactivarse antes de infectar algún otro archivo, sin causar una alarma para el usuario. Algunos virus, tales como Eight Tunes, detecta este producto utilizando su propia llamada ¿estás ahí?

Otra técnica que es vista algunas veces, fue inspirada por el hecho de que muchos programas rastreadores se verifican antes de ejecutarse, y si hay algún cambio al archivo, lo reportarán Esto significaría que un virus nuevo podría ser detectado en esta forma, de manera que algunos de los virus se abstienen de infectar tales programas. Una forma común es buscar las letras SC o SCAN en los nombres de archivos. Si es encontrado, entonces el virus no infecta ese archivo particular Otra cadena que ellos evitan es un archivo con TEST en el nombre.

Los virus que disimulan el tamaño de los archivos a menudo dejan una inconsistencia entre el tamaño reportado por el directorio y el número de elementos de la cadena FAT Cuando el comando CHKDSK es ejecutado, reportará estas inconsistencias y CHKDSK es un programa que es a menudo ejecutado cuando se sospechan problemas con el disco. Para evitar este reporte sospechoso por CHKDSK, por lo menos un virus verifica el nombre del programa que está siendo ejecutado, y si es CHKDSK, el tamaño del archivo stealth es desactivado

El último grado es el *stealth avanzado* Los virus que utilizan esta técnica aspiran a ocultar su existencia ante el software antivirus El ejemplo más conocido es el virus Frodo, también conocido como 4096, 4k e IDF. Frodo es muy mal interpretado. Hay reportes de que se desinfecta por sí mismo cuando lee, lo cual es más bien una forma curiosa de describir lo que hace actualmente De hecho, atrapa la interrupción 21h, y cuando son realizadas algunas operaciones a archivos, el virus cambia bruscamente su acción Cuando un programa utiliza DOS para leer, escribir o

buscar en el archivo, Frodo encuentra que esa llamada a DOS habría tenido lugar si Frodo no hubiera infectado el archivo, y regresa esa información para que DOS presente la llamada al programa El resultado es que con Frodo en la memoria, si se realiza una comparación byte-por-byte entre un archivo infectado y una copia limpia (en un disco flexible protegido contra escritura), la comparación no reportará diferencia Frodo marca los archivos agregándoles cien años a la fecha marcada y la existencia de esto es encubierta Como resultado, es difícil descubrir que Frodo está presente, y es difícil librarse de él

Frodo tiene también una forma ingeniosa de ocultarse en la memoria La mayoría de los programas que quedan residentes en memoria y capturan una interrupción, lo hacen cambiando la entrada en la tabla del vector de interrupciones Como resultado, algunas personas han creído que ésta es la única forma de hacerlo Pero Frodo no utiliza este método para evitar que los programas que verifican cambios en la tabla del vector de interrupciones lo detecten En vez de esto, Frodo parcha los primeros cinco bytes del manejador de interrupciones, con un salto al código de Frodo Después de que el código de Frodo es ejecutado, vuelve a parchar dejando el núcleo original del DOS como estaba antes, y lo salta

El virus Number-of-the-Best (llamado así porque tiene '666' en el código) tiene una longitud de 512 bytes (actualmente hay como una docena de versiones) También es un virus stealth avanzado, pero realiza este artificio por medio de la manipulación de las tablas de archivos de sistema dentro del DOS Los 512 bytes del virus son codificados de forma compacta Si hay algún intento de leer los primeros 512 bytes de un archivo infectado mientras el virus está en memoria, el virus trae los 512 bytes originales que ha colocado después del final de archivo, y los presenta en su lugar En contraste, el COMP del DOS que compara programas, y los checksummers criptográficos, son engañados pensando que el archivo es invariable a partir del original

También tiene una forma ingeniosa de esconderse en memoria Necesita precisamente 512 bytes de almacenamiento, los obtiene tomando los primeros buffers del DOS y convenciendo a DOS de que el segundo buffer es actualmente el primero Más aún, la mayoría de los mapeadores de memoria no reconocerán este orificio de 512 bytes en memoria, creen que es parte del DOS

Entre los virus del sector del boot, los virus Joshi y EDV utilizan técnicas de stealth avanzado Si alguno de estos virus está en memoria, y se intenta leer el sector que contiene el código del virus, el virus redirecciona la lectura a donde se encuentra el sector que reemplazó, de manera que el software antivirus no nota nada fuera de lugar

EDV tiene algunos artificios adicionales Si se busca el lugar donde colocó el sector que reemplazó, en el cilindro 39, cabeza 1 y sector 8, el virus regresa un sector no legible marcado como error, de manera que no se ve el sector boot en un lugar inusual Cuando el virus queda residente en memoria, primero trata de utilizar la

memoria arriba de los 640 Kb, si es que hay RAM superior, de manera que los mapeadores no lo vean

El virus Joshi sobrevive al <Ctrl-Alt-Del> Mucha gente piensa que el <Ctrl-Alt-Del> recarga la computadora, actualmente es sólo otra secuencia de teclas que puede ser remplazada por medio de la interrupción 9 Este artificio de Joshi le ha permitido sobrevivir a operaciones de limpieza de discos debido a las personas que piensan que todo lo que se tiene que hacer es recargar y formatear los discos duros a bajo nivel Esto, aparte de ser una medida excesiva, es innecesario, a menos que se realicen las cosas correctas en el modo correcto

Virus polimórficos

Un virus polimórfico es aquel en que dos infecciones del virus no parecen ser el mismo El código del virus actual cambia con cada infección

Un virus polimórfico consiste en dos partes el cuerpo encriptado y la variable *desencriptadora / cabecera (header)*

En cada momento de la infección el cuerpo principal del código es encriptado diferentemente, con trillones de encriptaciones diferentes posibles en algunos virus Antes de que este código pueda ser ejecutado, debe ser desencriptado por la cabecera desencriptadora, la cual es una parte del virus que no se encripta por sí misma En vez de ser encriptada, es variada de momento a momento usando diferentes instrucciones que ejecuten la misma función, consumiendo código que ocupa espacio sin afectar las funciones, el uso alternativo de los registros del procesador y trucos similares.

El grado de variabilidad de encriptación y desencriptación de la cabecera varía mucho con el virus. Algunos virus completamente polimórficos permiten billones de permutaciones diferentes, sin compartir constantes de cadenas buscadas Otros virus semipolimórficos pueden contener varias cadenas cortas comunes

En la primera semana de 1994 apareció en México un nuevo virus que fue bautizado como Natas, pero se sospecha que está emparentado con el virus Satán descubierto en agosto de 1993 Se trata de un virus polimórfico, es decir, que tiene *múltiples formas de infectar*

Los síntomas que se han observado con mayor frecuencia son que deshabilita los manejadores de disco haciendo imposible la lectura o escritura de archivos desde ellos e infecta la operación del archivo EMM386 EXE de Windows™

Para saber si la computadora está infectada por Natas hay que verificar el tamaño del archivo COMMAND COM Si éste ha aumentado en 4,744 bytes, seguramente se ha infectado por este virus

Otro síntoma es que aumenta cien años a la fecha de creación de los archivos Por esta razón es que Natas forma parte de los virus de *los cien años*

El virus Natas infecta la tabla de particiones, los archivos del sistema y los archivos ejecutables en general, es un virus muy activo de tipo stealth

Un antivirus que lo puede detectar y erradicar, tanto de discos duros como de flexibles es el Sistema Integral Antivirus de McAfee Consta de un programa llamado SCAN2, el cual, combinado con ciertos parámetros, permite detectar y eliminar el virus Natas tanto de la tabla de particiones, sector de arranque y archivos ejecutables, sin dañarlos

Para poder erradicar el virus Natas del disco duro, se debe utilizar el comando

A>SCAN2 C /ALL /SUB /CLEAN

Cuando el disco duro está comprimido (con STACKER o DBLSPACE), se debe utilizar el comando

A>SCAN2 C /ALL /SUB /ADL /CLEAN

Sin embargo, *como todo software antivirus, no detecta todas las mutaciones de* Natas Hay que estar actualizando constantemente el software para que éste sea lo más efectivo posible

Virus slow (lentos o torpes)

Este tipo de virus es diseñado con el objeto de hacer fracasar los métodos ckecksum (suma de verificación) de detección de virus. El virus puede sólamente infectar archivos al tiempo en que la modificación es improbable de ser notificada, tal como cuando un archivo está siendo copiado. O puede solamente infectar programas que se distinguen porque se modifican por sí mismos, tales como SETVER EXE Simplemente limitando la infección a discos flexibles normalmente derrotará los métodos checksum porque este tipo de precaución antivirus es generalmente empleado en disco duros

El virus Brain fue escrito antes de que los discos duros fueran comunes y sólamente fue diseñado para infectar discos flexibles Es un infector lento debido a que actualmente hay muy pocas computadoras con sólo drives para discos flexibles *Los virus lentos modernos pueden ser escritos deliberadamente para limitar la* infección a discos flexibles, aun cuando pueden ser virus infectores de archivos ejecutables o virus del sector boot El virus Starship es un buen ejemplo

Infectar sólamente cuando un programa está siendo copiado significa que la modificación no será notada por un checksummer debido a que el archivo no será incluido en las bases de datos de archivos a ser verificados o porque no se incluyen en la base de datos de archivos para los cuales los checksummers han sido diseñados Esto sucede comúnmente cuando software nuevo es instalado en el disco duro Cuando los nuevos programas son subsecuentemente agregados a la base de datos del checksummer, ya están infectados con el virus, y no cambian otra vez. La modificación (infección) sucedió cuando el checksummer no estuvo rastreando.

Los checksummers son a menudo instalados para ignorar modificaciones a archivos ejecutables, dejándolos completamente desprotegidos La razón de que estas modificaciones de programas sean excluidas de la lista de archivos es porque constantemente se dan falsas alarmas, aun si el programa no es excluido y la alarma es causada por un virus, es probable que sea ignorado

CAPITULO 5. MEDIDAS DE PROTECCION

Dado el objetivo principal de este trabajo, que es desarrollar la cultura computacional en los alumnos de la UPAEP para no utilizar copias ilegales de programas y disminuir la incidencia de contagio de virus, se presentan en este capítulo los conceptos básicos y fundamentales de las medidas que se deben tomar para prevenir, detectar y erradicar los virus computacionales

Existen dos tipos de medidas de protección: las medidas preventivas propiamente dichas, las cuales se deben seguir desde el momento de adquirir una computadora o cuando existe la plena seguridad de no estar infectado, y las medidas de contingencia, las cuales se deben tomar en el mismo momento en que se detecta un virus, para evitar su mayor propagación

El grupo de medidas de prevención no se debe seguir cuando se tenga duda o conocimiento de la existencia de un virus en la memoria de la computadora o en alguno de los discos, esto no haría sino propagar más su infección. En tal caso se debe pasar directamente al segundo grupo de medidas, las de contingencia, y seguirlas en el mismo orden en que aparecen

Dentro del primer grupo de medidas se realiza otra subdivisión las medidas que evitan que el sistema se contagie y las que averiguan si está contagiado o no. En caso afirmativo se pasa al grupo de medidas de contingencia

5.1. Medidas de prevención

1 No utilizar copias piratas

El medio más susceptible de contagio lo constituyen las copias ilegales de software que circulan entre los usuarios de las computadoras personales para conseguir todo tipo de programas Este detalle no se le escapa a los programadores de virus, aprovechando la masiva circulación de discos para colocar sus programas contaminantes.

2. *Se debe evitar que el software de la empresa salga y regrese a ésta* para evitar una posible contaminación, que provoque el contagio de todo el sistema.

3 Utilizar un sistema operativo fiable

Se debe tener la seguridad de que se está utilizando un sistema operativo que se encuentra en buenas condiciones (no contagiado) Las consecuencias de un fallo por esta causa pueden ser graves, porque cualquier programa que se utilice a continuación, quedará contagiado

Para las computadoras personales se deberá tener un disco flexible con un sistema operativo que sea copia del original, el cual será propiedad del usuario y no lo deberá utilizar ninguna otra persona Este disco deberá llevar siempre la etiqueta protectora o la pestaña contra escritura en su posición de sólo lectura

4 Apagar y volver a arrancar una computadora

Siempre que se utilice una computadora ajena o del dominio público, debe cargarla con el disco de sistema operativo de su propiedad

Cuando se ejecuta un programa contaminado con virus, éste se instala en la memoria interna (RAM), desde la cual dirige todas sus operaciones devastadoras Esta memoria sólo permanece activa mientras la computadora está encendida Por tanto, una sencilla forma de evitar que un virus siga actuando es apagar completamente la máquina durante unos 10 ó 15 segundos y luego arrancarla con su sistema operativo No es suficiente reinicializar la computadora con Ctrl-Alt-Del, debido a que hay virus que interceptan la entrada del teclado, como el Alameda y el Fu Manchu

5 No utilizar el disco duro como único lugar de almacenamiento

Debido a la gran cantidad de información que se puede almacenar en un disco duro, y a su acceso tan frecuente, es que tiene mayor tendencia al contagio, por lo tanto, se recomienda almacenar también en otros medios, como discos flexibles, discos compactos, etc , así como realizarles respaldos

6 Comprobar la seguridad de los discos flexibles

No debe copiarse directamente un disco flexible al disco duro Deben antes pasar unas pruebas de seguridad (medidas de detección) dependiendo de su procedencia, original o dudosa

7 Proteger los discos contra escritura

Cuando no se espera realizar operaciones de escritura, es aconsejable protegerlos La información que se almacena en un disco se puede dividir en tres clases los programas escritos en código fuente, los programas en código máquina o ejecutable y los datos o archivos de trabajo Se deben diferenciar los discos que contengan los programas ejecutables y no necesiten de operaciones de escritura, de los discos que contengan los archivos de datos, que no pueden infectarse directamente y cuya lectura/escritura es casi constante Los primeros deberán llevar siempre una etiqueta que evite su escritura, o su pestaña de protección de escritura activada Los

otros se caracterizan por la actualización continua de sus datos y no deben llevar protección

8 Asignar únicamente el atributo de sólo lectura a los archivos ejecutables

De la misma forma que el usuario puede cambiar el atributo del programa, el virus puede también variarlo y una vez cambiado introducirse en él Aunque la medida no sirva para todos los virus, sí puede desenmascarar alguno de ellos Es conveniente llevar un registro de los archivos con atributo de sólo lectura debido a que algunas vacunas no cambian el atributo al desinfectar el archivo, y aunque indica que ya eliminó al virus, realmente no lo hizo

9 Se debe tener mucha precaución si se utilizan computadoras rentadas, servicios de cómputo o envía la computadora a reparar en lugares en los cuales no se tiene cuidado con el problema de virus, y por lo tanto, se encuentran vulnerables a su ataque

10 Tome sus precauciones al adquirir software nuevo

No se preocupe si	Preocúpese si
* Al obtenerlo debe pagar por él	* Es parcial o totalmente gratis
* Proviene de una fuente confiable	* Es obtenido de un conjunto de bo-- letines
* El proveedor tiene un buen prestigio y un buen soporte de mantenimiento	* Llega sorpresivamente por medio del correo o una fuente no solicitada
	* Es adquirido a través de un amigo, vecino o compañero de trabajo

Pregunte al proveedor sobre la garantía de que el código esté libre de virus
En general, siempre adquiera software original de fuentes responsables

11 Si es indispensable intercambiar discos o ejecutar programas de computadoras diferentes a la propia, o si se cuenta con varias computadoras, es muy conveniente tomar una de ellas como máquina de pruebas, en donde se verifiquen todos los programas nuevos poniéndolos en cuarentena (aislarlos), y sólo cuando esté seguro de que están "sanos" podrá instalarlos en el disco duro

Si cuenta con una sola máquina, realice la misma operación, apagando la computadora cada vez que revise un disco

La computadora que utilice para revisar los discos, no debe tener información importante e imprescindible Deberá usar sólo discos que estén también en cuarentena y no discos que sean compartidos con alguna otra máquina

El aislamiento de una computadora de su ambiente es un poderoso método de protección contra virus Desafortunadamente tal aislamiento es irreal en muchos

ambientes computacionales, pero debería llevarse a cabo cuando adquiere un software nuevo

12 Si se tienen que utilizar los discos propios en otro sistema, revíselos antes de volverlos a introducir a su sistema, esto garantizará que se encuentren libres de virus sólo en cierta medida, debido a que las vacunas no van a detectar los nuevos virus (o sus nuevas versiones)

13 No permitir que gente extraña utilice su sistema sin que usted esté presente para supervisar las operaciones que se realizan, debido a que un virus puede llegar por error, aun de las personas con mejores intenciones

14 No adquiera programas de servicios públicos (BBS) o de redes que no se encuentran bien administradas y por lo tanto no estén tomando precauciones contra los virus

Si es necesario, pregunte al operador del sistema cuáles son las medidas antivirus que aplican

La mayoría de ellos lo hacen, debido a que la competencia entre los diversos servicios hace que quien distribuya copias infectadas entre los usuarios pierda su prestigio, *sin embargo, no está por demás que tome sus precauciones*

Si tiene que utilizar software de dominio público, siga los siguientes pasos:

1 Respalde la información contenida en el sistema y verifique que se pueda recuperar esa información.

2 Si el software está siendo masivamente distribuido, espere por lo menos dos semanas antes de instalarlo en su sistema y observe si en los medios de comunicación. se dieron malos comentarios en torno a dicho software

3 Si debe instalar en el disco duro de su sistema este tipo de software, realice antes un respaldo completo, haga una verificación del tamaño de todos los archivos almacenados, después instale y ejecute el nuevo programa y realice la comparación entre los archivos, para verificar si ha habido un cambio

15 Actualice constantemente su software antivirus

El software antivirus puede ser razonablemente efectivo por un tiempo, pero si no se actualiza, llega a ser ineficaz en la prevención de infecciones de un gran número de nuevos virus extraños que aparecen constantemente

16 Siga una política eficiente de respaldos

La realización periódica de copias de respaldo es una medida bastante efectiva, al menos para la seguridad de datos La copia de seguridad debe ser una rutina obligatoria, incluso fuera del entorno de los virus (los desastres no son sólamente ocasionados por virus; pueden ser desde fallas de operación hasta siniestros, tales como robo, incendio o sismo)

Procure respaldar por separado los programas y los datos

Mantenga un calendario y una rotación de discos de respaldo, de tal manera que, si algún respaldo está infectado o destruido, sea capaz de recuperarse con algún otro disco de respaldo en buenas condiciones La frecuencia de estos respaldos debe ser cuidadosamente planeada de acuerdo a las necesidades de la organización. En una compañía grande los respaldos deben realizarse por lo menos una vez al día Por otro lado, puede ser que nunca se necesite hacer respaldos a una computadora que sólamente se utiliza para jugar

Es importante poner a prueba el método con el que se van a realizar los respaldos, esto con el fin de asegurar que los datos respaldados puedan ser restaurados fiablemente.

Bajo la amenaza de los virus, las copias de seguridad van a desempeñar dos importantes funciones. una labor restauradora de los datos en caso de daños, y una labor de protección, porque permite la comprobación entre dos copias del mismo archivo, de parámetros tales como tamaño, atributo, fecha y hora de compilación o de última modificación, etc

Tampoco esta medida es completamente efectiva Una de las versiones del virus Viernes 13, concretamente la llamada Century-B, tiene la característica de esperar a que se realice un respaldo y, tomando de él la dirección del comando, llena los discos de información con basura en lugar de grabar los programas que se encuentran en el disco.

17 Convertir las medidas preventivas en política interna de la empresa

Para funcionar eficientemente, las normas de prevención deben establecerse como política en cualquier empresa (en este caso, en la UPAEP, sus centros de cómputo y alumnos). Si todos utilizan software original y evitan la entrada/salida de discos de la empresa al domicilio particular, supone una disminución del riesgo de contagio. Se debe educar y concientizar a todo el personal sobre el problema de los virus, esta es la clave más importante para una exitosa protección de virus

18 Restringir el acceso directo a la información reservada

Otro foco peligroso en el entorno empresarial es el personal descontento, dado de baja o despedido Antes de salir de la empresa ha podido introducir algún virus. Es conveniente controlar especialmente a estas personas en lo que se refiere a su acceso a información de valor para la empresa Es fundamental restringir lo más posible el acceso directo a la información reservada, elija convenientemente una clave de acceso (password) a su sistema.

Controlar el acceso a las computadoras es utilizado algunas veces como defensa contra los virus. Sin embargo, sólamente debe ser utilizado como parte de la estrategia, si su parte complementaria son los programas antivirus El control de acceso está diseñado realmente para proteger contra accesos no autorizados a computadoras, y más particularmente, a los datos y programas que contienen

Las medidas que se pueden utilizar para prevenir el acceso a los datos deben ser probadas para ver qué inconvenientes pudieran surgir

La forma más eficaz de prevenir el acceso a los datos por personas no autorizadas es encriptarlos, cualquier otra medida sólamente retrasará el acceso por un tiempo Sin embargo, aún se pueden encontrar productos con un bajo nivel de protección

El nivel más simple La forma más simple de control de acceso consiste en un programa ejecutado desde el archivo AUTOEXEC.BAT, el cual pide un password y no le permitirá utilizar la computadora hasta que se dé el correcto. Tales programas pueden hacerse fallar presionando alguna tecla durante el proceso de arranque (boot), o cargando la computadora desde un disco flexible. Sin embargo, un gran número de personas protegen sus sistemas de esta forma.

Algunos fabricantes colocan un password dentro de las computadoras. La mayoría de tales sistemas almacenan el password en el CMOS, pero basta con quitar la batería para que ya no lo pida. Pocos fabricantes están utilizando actualmente el chip EEPROM (Electronically Erasable Programmable Read Only Memory· memoria de sólo lectura programable y borrable electrónicamente) para almacenar parte del BIOS El código para comenzar la secuencia de carga (boot) en una computadora es almacenado en un EPROM, que sólamente puede ser borrado por un rayo ultravioleta y reprogramarlo utilizando una herramienta especial. Un EEPROM puede ser borrado y reprogramado por la computadora que lo porta Como el EPROM, una vez programado, un EEPROM conservará su contenido hasta que sea reprogramado

Protección del boot Con este tipo de protección el disco duro parece no estar ahí si se carga la computadora desde el disco flexible Si se teclea C. <Return> MS-DOS™ desplegará el mensaje Drive not ready or invalid drive specification (drive no listo o especificación de drive no válida)

Si se carga desde el disco duro, se debe pasar a través de un sistema de control de password y, si no se conoce el password, no se puede accesar el disco Este tipo de control de acceso no permite utilizar Ctrl-Break o Ctrl-C para quebrantarlo

Sin embargo, no se debe olvidar que estos sistemas tienen alguna debilidad y probablemente pueden ser evitados o pasados por alto en pocos minutos.

Encriptación. El siguiente nivel es la encriptación de los datos Si los datos en el disco son encriptados, aun cuando haya algún acceso a la computadora, los datos permanecerán encriptados Provisto de un algoritmo de encriptación (como RSA y DES) suficientemente poderoso (y con el password mantenido en secreto), el tiempo tomado para desencriptar los datos significará que no vale la pena el esfuerzo.

¿Cuál es el algoritmo suficientemente poderoso? No es aconsejable depender de un algoritmo que no ha sido analizado extensamente RSA es considerablemente más lento que DES, pero tiene sus ventajas, tales como la capacidad de llaves públicas y privadas de encriptación / desencriptación Más aún, hay códigos propietarios, cuyos vendedores aseguran a los usuarios que son muy poderosos, y los cuales son mantenidos en secreto para asegurar su continua eficacia Desafortunadamente, más

tarde la estrategia es condenada al fallo, debido a que alguien que quiere conocer el algoritmo, simplemente tiene que desensamblar el código que lo implementa

Algunos sistemas encriptan los archivos, otros sólamente encriptan la FAT y/o los directorios, mientras que algunos ofrecen ambas opciones La ventaja de que no se encripten los archivos es que el proceso de encriptación / desencriptación llega a ser mucho más rápido, pero al costo de una considerable pérdida en la seguridad Los datos desencriptados son accesibles utilizando un editor de sector de disco

El problema más grande con la encriptación es que un algoritmo poderoso como DES retrasará el tiempo de acceso a los datos a un nivel a veces inaceptable

19 Adoptar medidas preventivas en las empresas fabricantes de software

Existen unas pequeñas medidas preventivas que pueden aplicar los fabricantes de software

- Se deben mantener en secreto los trabajos preventivos que se están llevando a cabo, para eliminar la posibilidad de que alguien cree un virus que vaya dirigido precisamente contra esos trabajos.
- Resultaría de utilidad comercializar los discos sin espacio libre, para impedir así que se añadiese un código posterior y, por tanto, negar la entrada a un virus
- Deben depurar al máximo el contenido de los discos antes de comercializarlos
- *Resulta práctico que el propio programa comprobara su estado antes de ejecutarse*, por ejemplo, que con unos parámetros determinados introducidos en un algoritmo se obtuviese un valor comparable en cada ejecución y que en caso de cambio, se avisara al usuario.

5.2. Métodos de detección

1. Lleve un registro de la longitud de los programas

A medida que ejecuta los programas verifique las longitudes regularmente, con el fin de detectar cualquier actividad que podría indicar que existe un virus

Antes de ejecutar un programa se debe hacer una consulta de su tamaño y fecha de compilación para compararlo con las copias que se tengan almacenadas en los respaldos y originales, así como de sus atributos una vez terminada la ejecución

Mantenga un manual con el tamaño original de los archivos y verifíquelos contra los tamaños de los archivos actuales para ver si no ha habido un crecimiento no planeado

2. Inspeccionar periódicamente los discos

Realice inspecciones periódicas de los discos para comprobar si poseen sectores defectuosos, y el espacio libre que existe en el disco.

3 Revise los discos que ha respaldado

Lo peor que puede hacer es respaldar sus virus y restaurarlos junto con su información

4 Inspección de síntomas

Existen ciertos síntomas de infección; estos factores pueden ser

- Mayor lentitud en el proceso
- Mayor tiempo de respuesta
- Pérdida de espacio en la memoria
- Falta de espacio en memoria para la ejecución de programas que antes sí se podían ejecutar
- Anomalías en la pantalla
- Resultados inesperados en la ejecución de programas
- Alguna operación inesperada de entrada/salida en los discos (flexibles o duros). La unidad de disco flexible puede estar funcionando sin que el usuario haya solicitado dicho comando

5. Instalación de software de segundad

Los detectores y protectores ayudarán a delatar el virus en su periodo de incubación, antes de causar el daño para el que fue creado Los programas antivirus, vacunas y antídotos, por otro lado, permiten actuar sobre el propio virus y sobre los daños que ha cometido, en el caso de ser los apropiados para combatir ese virus

En todos los discos de arranque se debe introducir un detector de virus que sea llamado en el CONFIG.SYS, debido a que sus comandos son ejecutados, cuando la computadora se arranca, antes de que el COMMAND.COM sea cargado y antes de que los comandos del AUTOEXEC BAT sean ejecutados. Un ejemplo de esto es el programa Virus Intercept de Norton Antivirus™. Virus Intercept es una porción de Norton Antivirus™ que reside en memoria, observando los archivos leídos desde disco y anticipándose a un ataque de virus.

5.3. Planes de contingencia

El plan de contingencia incluye las medidas que se deben seguir en el caso de detectar la presencia de un virus

Estas medidas desbancan a las de prevención desde el momento en que se haya encontrado un virus en periodo de latencia o reproducción

En cualquier caso, los pasos a seguir son los mismos, siempre y cuando no se disponga de un programa antivirus que ahorre alguno de ellos, como los referentes a limpieza del disco, cuyo trabajo es más laborioso Son universales, es decir, se deben seguir independientemente del virus que haya infectado el sistema y en el mismo orden en que aparecen

1 Conservar la calma

No se gana nada desesperándose, es mejor estar lo más tranquilo posible para poder llevar a cabo los pasos necesarios en la erradicación del virus

2 Apagar totalmente la computadora

Se debe apagar la computadora con el interruptor No es suficiente con reiniciarla mediante la combinación de teclas <Ctrl-Alt-Supr> Existen virus que bloquean el teclado plenamente y puede llegarse a dar el caso de que el programa contaminante simule una desconexión permaneciendo en la memoria

3 Encender la computadora con otra copia de seguridad

Diez o quince segundos después, se encenderá de nuevo la computadora utilizando un sistema operativo original o una copia realizada con un sistema sano Se debe tomar la especial precaución de no volver a utilizar la copia habitual del sistema de arranque por si está contagiada

4 Hacer copias de seguridad de los archivos de datos y archivos no ejecutables

Habrá que realizar copias de seguridad, únicamente de los archivos de datos y de todos aquellos programas que no sean ejecutables, debido a que los ejecutables son los que ocultan los virus entre sus instrucciones

5 De preferencia, dar nuevo formato al disco infectado

Se debe formatear al disco infectado, salvo en el caso en que no se tengan copias de los programas originales que lo integran y se intente anular el virus sobre el mismo programa o disco La excepción de no formatear se deberá llevar a cabo si se trata de algún tipo de virus conocido y se sabe cómo actúa, dónde se esconde, cómo desactivarlo, o si se va a adquirir un programa antivirus que lo desactive

Si se va a reformatear un disco, bajo MS-DOS™ 5 0 o superior, se recomienda utilizar la opción /U junto con el comando FORMAT Esto le indicará al DOS que haga un formateo incondicional, y que no guarde el sector de arranque original del disco Esto se debe hacer para evitar una reaparición del virus al desformatear el disco, además de que algunos virus se esconden en los sectores que ellos mismos marcan como dañados. Esta sugerencia también es aplicable para cualquier formateador que formatee bajo el esquema "safe format".

6 Comprobar los discos originales con programas detectores

Si no se posee un programa detector, se debe buscar en el programa original la misma señal que llevó a confirmar la existencia de contagio En caso afirmativo, se deberá volver al primero de los pasos, siendo imprescindible comprar los programas de nuevo.

7 Volver a copiar la información no infectada

Se debe volver a copiar toda aquella información que se sustrajo en un principio por encontrarse al margen de la infección Esto incluye los archivos de datos de los que se hizo una copia de seguridad.

8 Volver a comprobar los discos con programas detectores

Una vez restaurado el disco con la estructura que tenía anteriormente, se debe pasar de nuevo por un detector buscando posibles restos de virus

9. Probar todos los discos utilizados con anterioridad a la infección

Este paso resulta conveniente, es muy posible que se detecte tarde la infección y se haya propagado a más discos

10 Avisar a otros usuarios del peligro de infección

Comunicar la posibilidad de infección a todas las personas con las que se haya tenido intercambio de información, y si se está conectado a alguna red, comunicar del peligro de contagio a su administrador

5.4. Antivirus

Actualmente existen alrededor de tres mil virus No todos son comunes, pero es importante protegerse de ellos, debido a la perturbación potencial y a los gastos que un brote de virus puede causar.

A medida que cierto número y variedades de virus desafían la protección que se le da al software, se buscan nuevas soluciones para solventarlo

El método tradicional para atacar a los virus con scanners basándose en software que busque lazos de unión con los códigos de virus, fue aceptado cuando nuevos virus empezaron a surgir a intervalos de algunos meses

Ahora, con la aparición de nuevos virus día con día, se cuestiona el acercamiento tradicional del software reactivo, detectando y erradicando principalmente a los virus que se conocen y buscando nuevos horizontes soluciones de antivirus basadas en el hardware

5.4.1. Software antivirus

Al software para detectar y eliminar virus se le conoce como software antivirus Existen infinidad de ellos en el mercado; pueden dividirse en dos categorías: *Virus no-específicos* y *Virus-específicos.*

El software para virus no-específicos, incluye:

- Checksummers

El software para virus-específicos, incluye

- Inoculadores
- Scanners (rastreadores)
- Software para eliminar virus

Checksummers No son para virus-específicos y no necesitan enterarse de nuevos virus, de manera que tampoco necesitan actualizarse como un scanner.

La mayoría de los checksummers utiliza una lista de los archivos a ser protegidos, los cuales normalmente comprenden todos los archivos ejecutables en la computadora Un buen checksummer utiliza entonces técnicas avanzadas para calcular una única suma de verificación (checksum) por cada archivo en la lista.

Algún cambio al archivo, incluso si se cambia un solo byte, resultará en un cambio a la suma de verificación De manera que, la siguiente vez que el checksummer sea ejecutado, reportará un cambio al archivo el cual tuvo al menos un byte alterado. Esto puede o no ser causado por una infección de virus.

Para ser efectivo, el checksummer debe ser encriptado En otras palabras, debe utilizar un algoritmo que produzca un multiplicador criptografiado para calcular la suma de verificación. Para ser realmente efectivo, debe utilizar una clave variable como parte de la rutina. Si la llave es suministrada por el usuario, las probabilidades de que un programador de virus adivine la clave son remotas y el checksummer debe ser muy seguro.

Si está bien escrito, será fácil instalarlo y en promedio tomará aproximadamente un minuto para ejecutarlo Normalmente el checksummer se ejecuta desde el archivo AUTOEXEC BAT, el cual es ejecutado cada vez que la computadora se arranca

Las desventajas de los checksummers son el número de falsas alarmas que pueden ser generadas. Algunos programas tienen archivos .EXE que se modifican por sí mismos Por ejemplo, MS-DOS™ tiene un programa llamado SETVER.EXE que se modifica por sí mismo, y el checksummer da una falsa alarma. Otra desventaja es que sólamente avisa después de que el cambio al archivo ha sido realizado, en otras palabras, después de que el virus está en la computadora.

Existe ya en el mercado un checksummer TSR (que permanece residente en memoria) Este mira cada archivo que es abierto por el sistema operativo, calcula la suma de verificación, la compara con la que tiene como referencia y, si las dos sumas son iguales, DOS (y la llamada al programa) permite accesar el archivo. Si son diferentes, el TSR emite una alarma Un checksummer TSR no es aún para virus-específico, pero tiene la ventaja de que si un archivo llega a ser infectado, entonces se sabrá tan pronto como se trate de ejecutar el archivo infectado, además de minimizar las probabilidades de que otros archivos lleguen a infectarse o de que el virus haga algún daño

Inoculadores La mayoría de los virus no intentan infectar archivos más de una vez, no es ese su fin ¿Cómo saben, entonces, que cierto archivo ya ha sido infectado? La respuesta es que incluyen un "código de identificación" en el archivo infectado.

Los inoculadores trabajan agregando el código de identificación al archivo, lo cual podría parecer una muy buena idea en teoría, pero no en la práctica.

Jerusalén es un virus muy común que puede infectar tanto a archivos .COM como a .EXE. El método que utiliza para verificar si ya ha infectado un archivo .COM funciona efectivamente, pero el código de identificación que utiliza para archivos EXE tiene un bug (falla) y estará reinfectando archivos ejecutables, mientras haya espacio disponible en la memoria No es raro que Jerusalén sea encontrado cuando se trata de ejecutar un archivo infectado, debido a que despliega el mensaje' Program too large to fit into memory (programa demasiado grande para caber en la memoria).

El problema con los inoculadores es que cada virus requiere de un código de identificación específico, a menudo en una localización exacta en el archivo Esto significa que, por ejemplo, si dos virus miran los últimos cinco bytes del archivo, y cada uno es buscado para una cosa diferente, entonces no se puede inocular contra ambos virus Algunos virus colocan la hora estampada de los archivos a sesenta segundos, otros a sesenta y dos segundos. Nuevamente, sería imposible hacer ambas a la vez Un gran número de virus buscan bytes particulares al comienzo del archivo y, si estos bytes fueron sobrescritos en el programa a ser inoculado, el programa no podría trabajar propiamente después

Scanners Un scanner es para virus-específicos, lo cual significa que las características de virus conocidos son programadas en él Si un nuevo virus aparece, el scanner no será capaz de detectarlo hasta que esas nuevas características sean agregadas a su base de datos de información de virus. Para permanecer efectivo, necesita ser actualizado regularmente

Cuando un virus es detectado, desplegará un mensaje de advertencia en la pantalla. La mayoría de los scanners pueden escribir un reporte a un archivo en disco En el caso de múltiples infecciones, puede proveer una lista de archivos infectados que necesita para ser limpiados

Un scanner "sabe" acerca de los virus debido a que la habilidad para identificarlos está incluida en su código Este reconocimiento se lleva a cabo buscando una cadena de caracteres que es única para cada virus.

Parte de la destreza de un buen programador de productos antivirus está en su habilidad de analizar al virus por sí mismo y escoger su propia cadena de identificación Los mejores programadores llevarán esto a un paso más lejos y encriptan su archivo de cadenas de tal manera que sea difícil ingeniárselas para desencriptarlas. Esto significa que un autor de virus encontrará mayor dificultad para establecer la cadena de identificación que un producto antivirus está utilizando para encontrar a su virus

Los virus polimórficos cambian su código con cada infección. Por ejemplo, si hay cien archivos en un disco duro infectados con el virus V2P6, entonces habría cien diferentes encriptaciones y no habría una cadena constante que el scanner pudiera buscar. Esto requiere técnicas más sofisticadas de búsqueda que puedan decir si el virus está presente sin tener que buscar una cadena

Para ayudar a prevenir falsas alarmas, la base de datos de las cadenas identificadoras de los virus debe estar encriptada de alguna manera. Si esto no es realizado, como sucede con algunos productos, entonces el usuario, si está utilizando dos productos antivirus, obtendrá muchas falsas alarmas. Esto sucede porque algunos productos no liberan la memoria cuando han terminado la búsqueda y el remanente de la cadena utilizada en esa búsqueda permanece en memoria, donde son encontradas por el otro producto y lo identifica como virus.

Hay dos tipos de scanners: *command line* (línea de comandos) y *TSR* (residentes en memoria). Como su nombre lo indica, el scanner command line es ejecutado desde el prompt del DOS

Un scanner TSR es generalmente cargado cada vez que la computadora se arranca y permanece en la memoria hasta que se apaga. Está vigilando constantemente el acceso a los archivos, incluyendo los discos flexibles, o archivos que sean bajados de una red o desde una conexión de modem y suena una alerta si un usuario intenta accesar un archivo o un disco infectado con un virus conocido.

Debido a que no necesita la acción de un usuario, también es útil donde los usuarios podrían olvidar o no conocen los requerimientos para verificar toda la entrada de discos a una computadora

Software para eliminar virus. La mayoría de las compañías que producen software antivirus, también incluyen herramientas para neutralizar cualquier virus que pueden identificar Cuando encuentra un archivo infectado, lo aísla y elimina el virus, y en la mayoría de los casos repara el archivo infectado, permitiéndole regresar a su operación normal. Si el archivo se encuentra infectado con un virus poco común, se mostrará un mensaje de advertencia, preguntándole al usuario si borra y rescribe el archivo infectado.

Control de daños

Cualquier programa antivirus que se precie debe ofrecer un control de los daños producidos, tanto en el aspecto preventivo como restaurador. Las técnicas preventivas incluyen la detección de intentos de acceso directo al disco, avisando de los programas que intentan realizar este tipo de operación sin autorización. Protegen contra escritura el disco duro mientras que comprueban el software de dudosa procedencia. Si lo peor ocurre y el virus borra los programas o formatea el disco, se podrá restaurar el daño si el programa antivirus provee de alguna utilidad de recuperación de archivos o conserva una copia de la FAT.

Funciones complementarias

A la par de estas medidas comunes de protección, algunos programas antivirus ofrecen características de ayuda adicional. Si el programa salva una copia de la memoria CMOS, se podrá usar para restaurar la configuración cuando las pilas de la computadora se gasten. Cuando accidentalmente se intenta copiar un archivo ejecutable sobre otro con el mismo nombre, dicho programa antivirus avisará.

Inconvenientes

Todas las funciones anteriores presentan algún inconveniente en su uso. Los programas de prevención requieren una costosa preparación antes de poder utilizarse correctamente La lista de programas autorizados debe ser actualizada constantemente para evitar que los nuevos programas adquiridos sean rechazados por el antivirus.

Los programas detectores son muy especiales y sólo suelen servir para un virus en particular. Una pequeña variación en el virus puede hacer que el detector quede obsoleto

Los programas de identificación no son excesivamente prácticos, debido a que el más leve cambio en la cadena de caracteres del virus puede anular la función del identificador.

Por último, aunque el programa antivirus tenga un control de daños, si el virus ha realizado un formateo a bajo nivel del disco, le será imposible recuperar la información almacenada

5.4.2. Hardware antivirus

Algunos proponentes comentan que ciertas técnicas de protección son posibles o se vuelven más confiables utilizando una tarjeta adicional de adaptador. Por ejemplo, la memoria únicamente de lectura en esa tarjeta tiene oportunidad de funcionar antes de que empiece la PC, asegurando virtualmente un medio ambiente exento de virus.

Mientras que los scanners tradicionales de software buscan una serie de programas para poder identificar y eliminar a los virus conocidos, el hardware no necesita conocer virus específicos para poder trabajar.

Ningún producto ataca a todos los virus; sin embargo, se les ha hecho la vida más difícil a los autores de los virus.

Una opción para mejorar la seguridad en la PC es alterar el hardware. Hay dos niveles principales con los cuales puede llevarse a cabo esto:

Firmware. El BIOS es donde la información esencial acerca de la computadora es grabada con la pequeña sección de código que es utilizada para el proceso de carga de la computadora al encenderla; a esto se le denomina firmware. Dado que una PC estándar cargará desde un drive si es que un disco es colocado en el A; esto es fundamentalmente inseguro

Una vez que la PC ha sido cargada desde un disco flexible, entonces no importa cuánto software de seguridad se tenga en el disco duro, como no ha sido ejecutado, entonces no está activo

Lo que tienen que hacer todos los intrusos es utilizar llamadas a funciones de bajo nivel para accesar el disco duro y desactivar por completo el sistema de seguridad *Esto no es el tipo de programación que un intruso (programador) común* sabría cómo hacer, pero no presentaría dificultades a un hacker.

Si se cambia el firmware, se puede lograr que sea imposible cargar la PC desde el drive Esto es realizado cambiando el ROM BIOS o agregando un ROM extra, ya sea en la tarjeta madre o en un slot de expansión si la tarjeta madre no tiene enchufe para ROM. Si se adopta este método, la ROM extra puede ser utilizada para desactivar el drive a nivel BIOS. Puede también ser utilizado para prevenir el acceso al disco duro a menos que la introducción de password haya sido seguida correctamente.

La siguiente etapa es colocar una tarjeta en la PC que controle los puertos de entrada / salida Previniendo el uso de los puertos entrada / salida 320h a 324h, llega a ser imposible escribir código para accesar el disco duro debido a que utilizaría uno de esos puertos Se puede controlar el uso de los drives, el puerto paralelo y la red en la misma forma. Este método funciona porque cambia la naturaleza esencial de la PC

Utilizar un tarjeta para controlar los puertos de entrada / salida, combinado con *la encriptación del disco duro (implementado en hardware en la misma tarjeta) provee* el más grande control posible sobre lo que fue previamente un sistema completamente abierto

Algunos productos de importancia en este campo son:

Según Computerworld México (Marzo 1993) "*Circuito de seguridad. Virustrap es un producto que será comercializado por Texas Instruments, funciona asegurando el circuito de todos los códigos ejecutables en el disco duro. Detecta e intercepta formatos de discos no requeridos, alteraciones de bloque de los archivos de los sistemas operativos, y detiene todo escrito hacia las áreas protegidas del disco duro.*

Debido a que ninguna parte del programa se aloja en la memoria de acceso aleatorio, se dice que no es posible ningún ataque al software. Sin embargo, Virustrap no es económico: se venderá al menudeo a 329 dólares por PC.

Thunderbyte es uno de los más antiguos productos antivirus basado en hardware; ha estado en el mercado desde 1990. Consiste en una tarjeta con un programa de configuración y un cable plano; el disco duro y el controlador después son unidos a través de la tarjeta añadida Thunderbyte Los niveles de seguridad se establecen por medio de un microcircuito en el adaptador. Este producto es efectivo porque se basa en algoritmos especiales que registran cualquier intento de contaminar un programa o un archivo de datos. A pesar de que el producto es un residente en RAM, el vendedor no acepta que puede ser atacado en ninguna manera por software Thunderbyte fue desarrollado en Holanda y actualmente es fabricado y distribuido por Glynn International en Brookline Mass".

Según PC Magazine en Español (Junio 1993, Pág 50) *Un producto con una técnica distinta es el dispositivo de bloqueo de disco C Cure de Leprechaun Software International en Marietta, Ga Este está incluido con el programa Virus Buster de la compañía, por 299 dólares Este producto se conecta al cable del disco entre la tarjeta de interfaz y el disco duro y actúa como una protección virtual contra la escritura que evita cualquier intento para escribir al volumen C: Sin embargo, este método requiere que se tenga al menos dos particiones en el disco duro; una dedicada exclusivamente a los archivos y programas ejecutables críticos y la otra reservada para los archivos de datos y programas no esenciales En efecto, el disco C se convierte en una fortaleza inexpugnable en la que el dispositivo C:Cure sirve como la compuerta de seguridad*

Si bien el método de C Cure puede ser demasiado restrictivo para la mayoría de los usuarios, tiene, como muchas de las soluciones de hardware, el potencial de construir una aplicación más amplia en muchos entornos de computación estructurados en los que la regla la constituyen tareas específicas de computación basadas en aplicaciones seleccionadas. La computación con estilo libre presenta demasiadas oportunidades para que virus muy dañinos invadan al sistema.

V-Card es un producto de Digital Enterprises en Gaithersburg, Md. Mantiene la información sobre el sector de arranque y la tabla de particiones, más 1,280K de "fotografías" de todos los archivos ejecutables críticos y software antivirus en ROM La V-Card puede desactivar los discos flexibles y funciona como el dispositivo de arranque si se daña el disco duro. En acción, el dispositivo provee una barrera física entre los archivos infectados y el disco duro. También elimina y retira las amenazas de virus al tiempo que evita la carga de archivos o el borrado sobre la marcha sin autorización

La porción de software de detección y eliminación de virus de V-Card tiene una licencia de Netz Computing en Israel También se incluye un programa de verificación de integridad y restauración para archivos Se vende en 495 dólares

La técnica de Western Digital es una solución en hardware que intercepta las peticiones de escritura al disco duro El controlador lógico de sistema WD7855 (introducido al mercado en noviembre de 1992) de la compañía interactúa con las características de administración de energía para las

interrupciones de administración del sistema (SMI) que vienen incluidas en los últimos procesadores 386SX, 386DX y 486

Incluida en este controlador está una tecnología genérica antivirus llamada Inmunizador, que protege las áreas críticas del disco y de los archivos ejecutables contra escrituras Además, verifica todas las peticiones de escritura para detectar actividad que parezca ser de virus. Cuando opera, el WD7855 pasa las peticiones de escritura al controlador de disco. El SMI, que también inspecciona esto, además de otros componentes que consumen energía, activa al Inmunizador, que verifica si la petición se dirige o no a un área protegida en el disco duro Una simple alerta hace que se le pregunte si quiere aceptar la petición de escritura o rearrancar

El sistema antivirus PC-cillin de la compañía Trend Micro Devices (en Torrance, California, E U.A.) se vende en 139 dólares junto con un dispositivo llamado Inmunizer Box (caja de inmunizador), que se conecta al puerto de la impresora Este es realmente un chip de ROM que se puede programar y borrar eléctricamente (EEPROM) que almacena el sector de arranque y el contenido de la tabla de partición

Si bien el PC-cillin intercepta y destruye los virus, se mantiene segura la información crítica de MBR en la caja de inmunizador, libre de virus, lista para restaurarla al disco duro si la infección la dañara.

Multix vende una solución de hardware en una tarjeta de 8 bits que intercepta o filtra la actividad de entrada / salida en el bus de la PC. Su tarjeta ViruStop PC Immunizer Card de 69 dólares se activa al arranque y rastrea automáticamente la memoria y los sectores de arranque para detectar actividad de virus. Después de un arranque limpio, se inspecciona toda la información que se mueve por el bus y se suspende la operación alertando si se encuentra alguna información que se sepa o se sospeche que es de un virus.

Mientras que ningún producto antivirus sea 100% efectivo, el hardware puede encontrarse en el borde.

En esencia, los productos basados en hardware protegen áreas específicas del disco duro, atrapando llamadas genéricas que con frecuencia son utilizadas por un virus. Esto es particularmente efectivo para detener a los virus en los sectores delanteros

El software antivirus reacciona a la presencia de un virus, pero el hardware bloquea la entrada del virus al sistema

CAPITULO 6. TUTORIAL DE VIRUS COMPUTACIONALES

Dado el objetivo principal de este trabajo, que es desarrollar la cultura computacional en los alumnos de la UPAEP para no utilizar copias ilegales de programas y disminuir la incidencia de contagio de virus, se presentan en este capítulo el análisis, diseño, implementación y documentación de un tutorial desarrollado en ambiente gráfico para ayudarle a entender el funcionamiento de los virus, también le permite realizar prácticas de detección y erradicación con los programas Norton Antivirus™, Central Point Antivirus™ y VirusScan™, y muestra algunos efectos de los virus por medio de simuladores

6.1. Análisis

Actualmente en los Centros de Cómputo UPAEP hay un alto índice de propagación de virus computacionales debido a la gran cantidad de copias ilegales que se realizan entre los alumnos y a la falta de información real sobre estos programas, provocando la pérdida o alteración de archivos de datos o archivos ejecutables almacenados en discos, desplegando en la pantalla mensajes misteriosos o de burla, y causando una conducta anormal del sistema operativo y/o del sistema de trabajo utilizado

En los alumnos de la UPAEP, que inician sus estudios en el área de computación, hay desconocimiento sobre los virus computacionales, sus medidas de prevención, detección y erradicación, y además no existe un tutorial a su alcance que les facilite el aprendizaje sobre los virus y sus efectos, por lo tanto, al realizar copias de programas, se contagian y pierden su información

Para solucionar este problema se desarrolló un tutorial en Visual Basic™, el cual contiene información sobre los virus computacionales, su origen, medios de contagio, funcionamiento y medidas de protección; además de prácticas de detección y erradicación de los mismos y muestra los efectos de los virus por medio de simuladores

Dicho tutorial se proporcionará a los directores de carreras y a la dirección general de bachilleratos UPAEP, con el fin de que lo apliquen los alumnos que inician sus estudios de computación

Los alcances del tutorial son los siguientes

- La información abarca sólo a los virus en PCs IBM™ y compatibles, utilizando sistema operativo MS-DOS™

- Los virus son explicados de manera tipificada, por lo que no se incluye una lista completa

- Los requerimientos para la ejecución del tutorial, son

a) Computadora IBM™ PC o compatible

b) Procesador 80286 o superior

c) Mouse

d) 1 Mb en RAM mínimo (2 Mb o más recomendables)

e) Monitor VGA color o SVGA color

f) MS-DOS™ versión 3 1 o superior, con SHARE EXE ejecutándose

g) Microsoft Windows™ versión 3 0 o superior

h) Disco duro con 6 5 Mb disponibles

- El software utilizado por el tutorial en las prácticas de detección y erradicación de virus es

- Norton Antivirus™

- Central Point Antivirus™

- VirusScan™

- No se realizan pruebas en BBSs, ni en red

- No se desarrollan virus, ni programas antivirus.

- Aunque el tutorial se desarrollará en modo gráfico, al ejecutar los simuladores, se cambiará a modo texto.

- La investigación está enfocada, primordialmente, a alumnos que inician su formación en el área de computación

- El tutorial será desarrollado en Visual Basic™ Es justificable porque.

a) Trabaja en ambiente gráfico

b) En los centros de cómputo de la Universidad se cuenta con el equipo que cumple con los requerimientos necesarios para ejecutar el tutorial

c) En la mayoría de los centros de cómputo de los Bachilleratos se dispone de diez computadoras que cumplen todos los requerimientos; además, se realizó una encuesta a los alumnos para averiguar quiénes tienen computadora en su casa o si puede accesar a alguna con algún familiar o amigo, obteniéndose resultados positivos aproximadamente en 40%

d) Se puede hacer un convenio con los centros de cómputo de la Universidad para que los alumnos del Bachillerato utilicen las computadoras para ejecutar el tutorial

e) A los alumnos de los bachilleratos se les puede dar el tutorial en grupos, utilizando el Datashow; el inconveniente es que la sección de cuestionarios no garantiza el aprendizaje de todos los alumnos si se contesta en grupos, en tal caso, se tendría que aplicar por escrito a cada alumno.

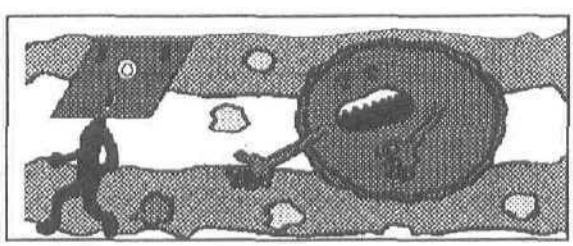
6.2. Diseño

A *continuación se presenta un catálogo de las imágenes desplegadas en las* pantallas del tutorial.

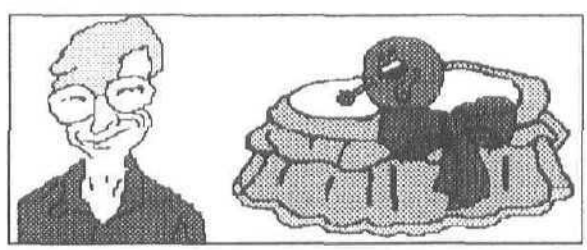
Las imágenes fueron almacenadas en formato de mapa de bits.

Junto a cada imagen se indica el nombre del archivo que la contiene, así como el tema y subtema del menú que representa y el nombre de la pantalla en la cual se despliega.

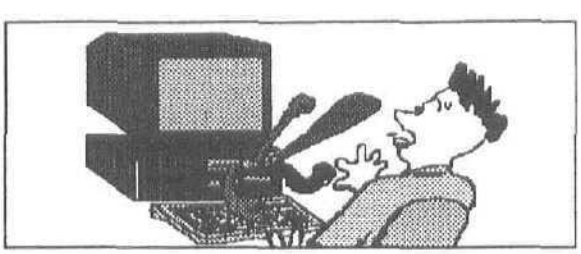
Catálogo de imágenes



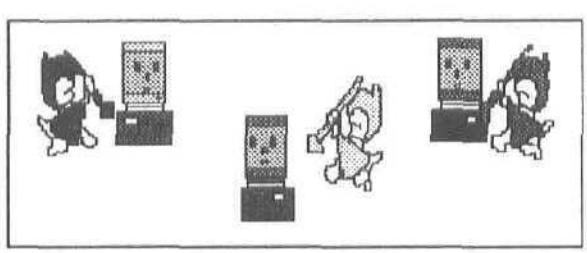
Nombre : IMAGEN1.BMP
Tema : Virus
Subtema : ¿Qué es un virus?
Pantalla : Efectos y fases de actuación



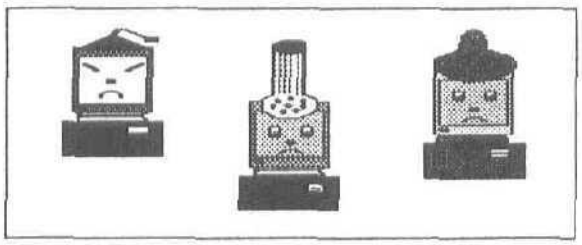
Nombre : IMAGEN2.BMP
Tema : Virus
Subtema : Origen de los virus
Pantalla : ¿A quién se otorga la paternidad de los virus?



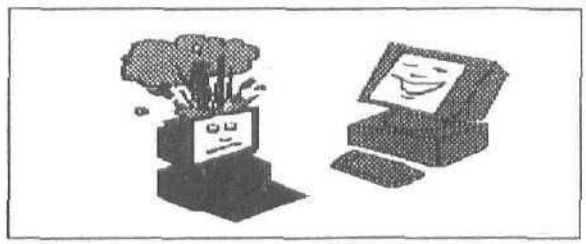
Nombre : IMAGEN3.BMP
Tema : Virus
Subtema : Mitos y realidades
Pantalla : Las computadoras se contagian de la misma manera que usted



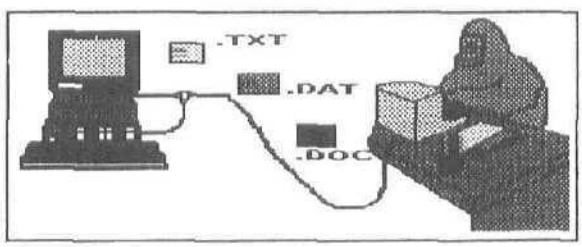
Nombre : IMAGEN4.BMP
Tema : Virus
Subtema : Mitos y realidades
Pantalla : Los virus son una epidemia fuera de control



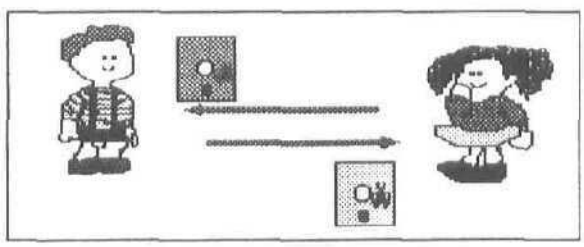
Nombre : IMAGEN5.BMP
Tema : Virus
Subtema : Mitos y realidades
Pantalla : Los virus pueden propagarse en todo tipo de computadoras



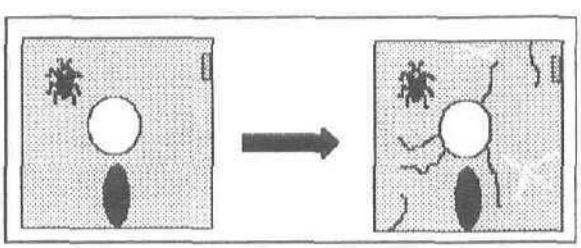
Nombre : IMAGEN6.BMP
Tema : Virus
Subtema : Mitos y realidades
Pantalla : Los virus dañan el hardware



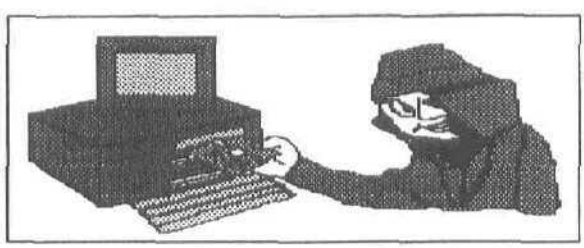
Nombre : IMAGEN7.BMP
Tema : Virus
Subtema : Mitos y realidades
Pantalla : El uso de correo electrónico es peligroso



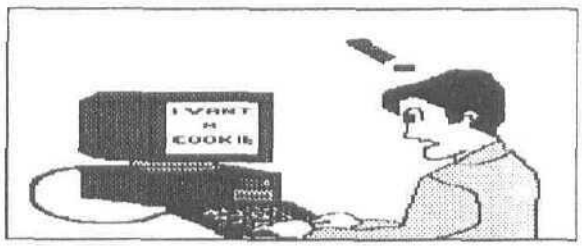
Nombre : IMAGEN8.BMP
Tema : Virus
Subtema : Mitos y realidades
Pantalla : Los BBBs propagan los virus rápidamente



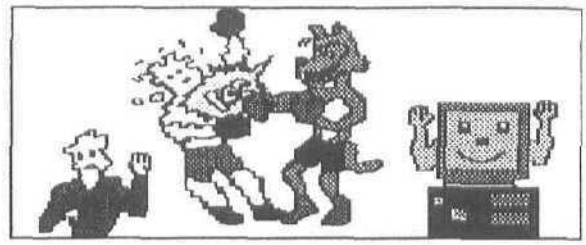
Nombre : IMAGEN9.BMP
Tema : Virus
Subtema : Mitos y realidades
Pantalla : Los discos de respaldo serán *destruidos si se respalda un* virus



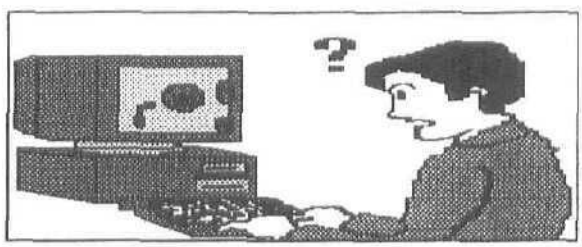
Nombre : IMAGEN10.BMP
Tema : Virus
Subtema : Mitos y realidades
Pantalla : Una computadora se contagia de *virus si introduzco un disco infec*tado



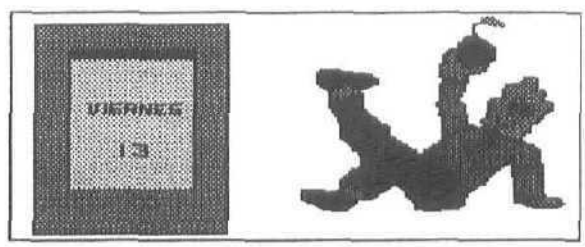
Nombre : IMAGEN11.BMP
Tema : Virus
Subtema : Mitos y realidades
Pantalla : Todos los virus destruyen programas



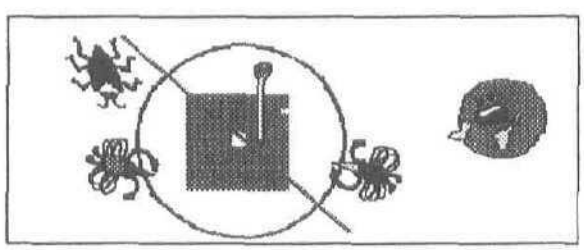
Nombre : IMAGEN12.BMP
Tema : Virus
Subtema : Mitos y realidades
Pantalla : Estoy a salvo si tengo el programa antivirus X



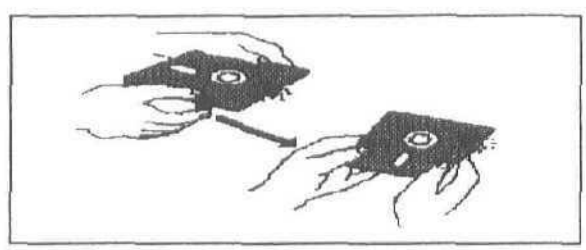
Nombre : IMAGEN13.BMP
Tema : Virus
Subtema : Mitos y realidades
Pantalla : Los sistemas con passwords protegen contra los virus



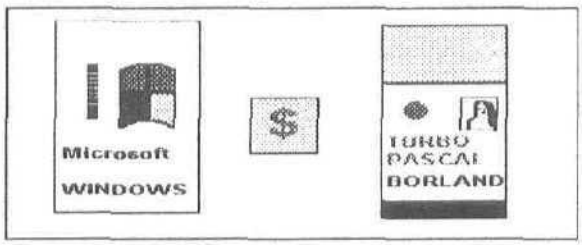
Nombre : IMAGEN14.BMP
Tema : Virus
Subtema : Mitos y realidades
Pantalla : Los virus sólo se activan en ciertas fechas



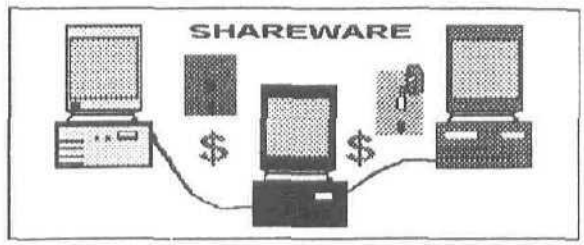
Nombre : IMAGEN15.BMP
Tema : Virus
Subtema : Mitos y realidades
Pantalla : Si coloco el atributo read-only protejo los archivos de virus



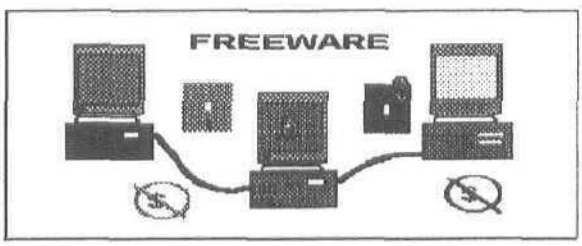
Nombre : IMAGEN16.BMP
Tema : Medios de contagio
Subtema : Transferencia de discos
Pantalla : Discos



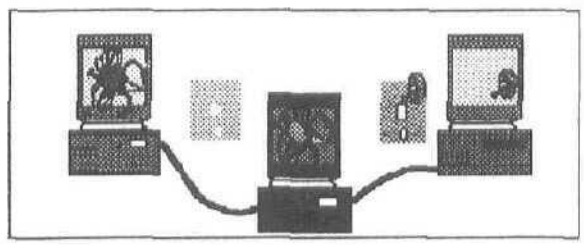
Nombre : IMAGEN17.BMP
Tema : Medios de contagio
Subtema : Transferencia de discos
Pantalla : Software Comercial



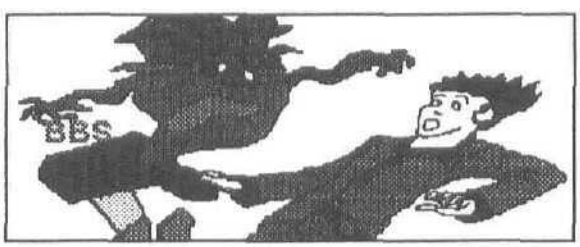
Nombre : IMAGEN18.BMP
Tema : Medios de contagio
Subtema : Transferencia de discos
Pantalla : Shareware



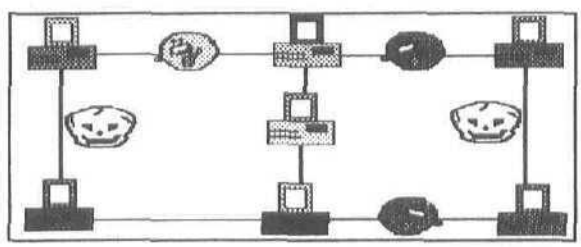
Nombre : IMAGEN19.BMP
Tema : Medios de contagio
Subtema : Transferencia de discos
Pantalla : Freeware



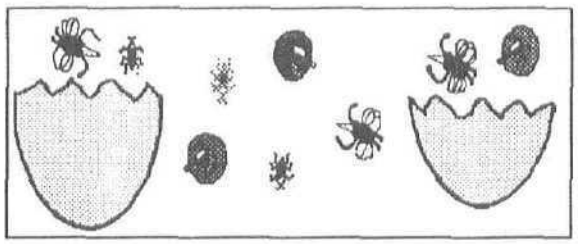
Nombre : IMAGEN20.BMP
Tema : Medios de contagio
Subtema : Transferencia de discos
Pantalla : Software del dominio público



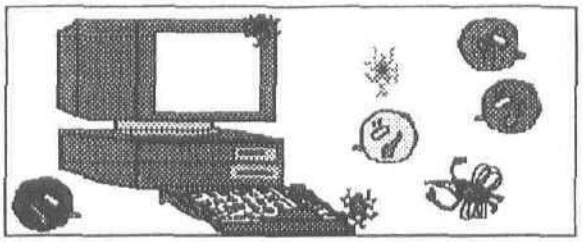
Nombre : IMAGEN21.BMP
Tema : Medios de contagio
Subtema : Telecomunicaciones
Pantalla : BBSs



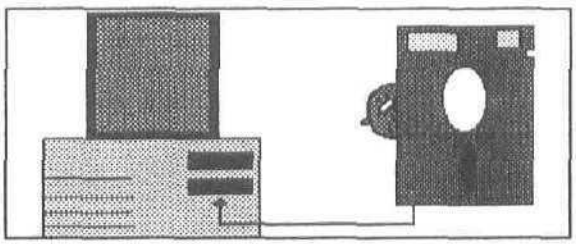
Nombre : IMAGEN22.BMP
Tema : Medios de contagio
Subtema :Telecomunicaciones
Pantalla : Sistemas de información



Nombre : IMAGEN23.BMP
Tema : Funcionamiento
Subtema : Ciclo de vida
Pantalla : Fase de creación

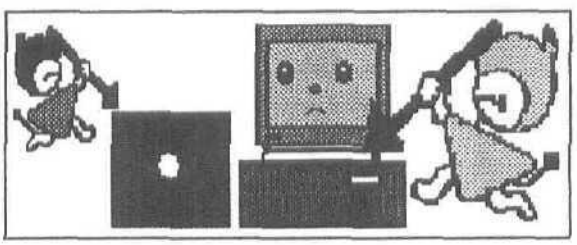


Nombre : IMAGEN24.BMP
Tema : Funcionamiento
Subtema : Ciclo de vida
Pantalla : Fase de entrada del virus a la PC

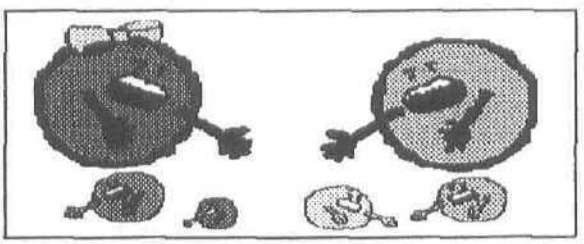


Nombre : IMAGEN25.BMP
Tema : Funcionamiento
Subtema : Ciclo de vida
Pantalla : Fase de infección o contagio

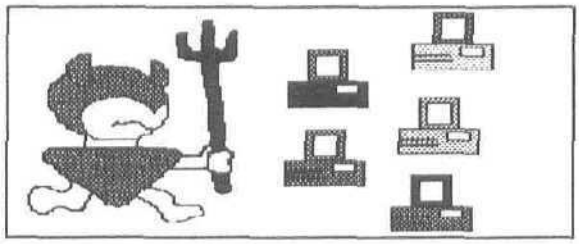
Nombre : IMAGEN26.BMP
Tema : Funcionamiento
Subtema : Ciclo de vida
Pantalla : Ocultamiento



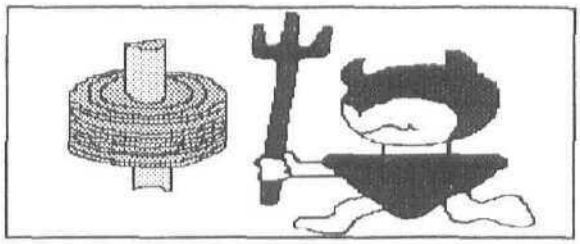
Nombre : IMAGEN27.BMP
Tema : Funcionamiento
Subtema : Ciclo de vida
Pantalla : Control de la computadora



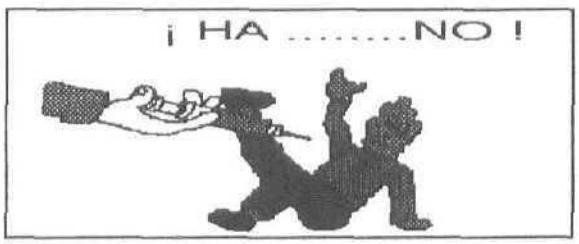
Nombre : IMAGEN28.BMP
Tema : Funcionamiento
Subtema : Ciclo de vida
Pantalla : Reproducción



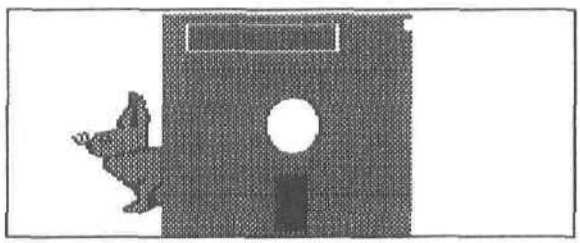
Nombre : IMAGEN29.BMP
Tema : Funcionamiento
Subtema : Ciclo de vida
Pantalla : Propagación



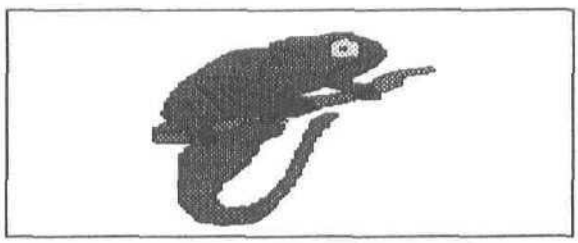
Nombre : IMAGEN30.BMP
Tema : Funcionamiento
Subtema : Ciclo de vida
Pantalla : Manifestación



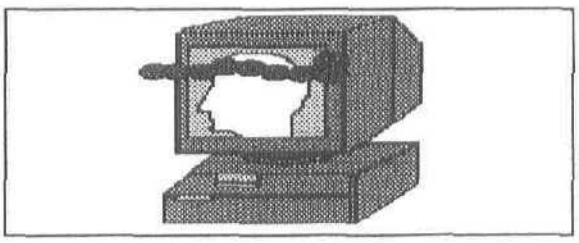
Nombre : IMAGEN31.BMP
Tema : Funcionamiento
Subtema : Ciclo de vida
Pantalla : Fin del ciclo de vida



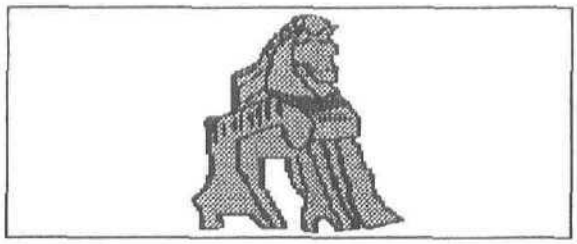
Nombre : IMAGEN32.BMP
Tema : Funcionamiento
Subtema : Clasificación general
Pantalla : Bug



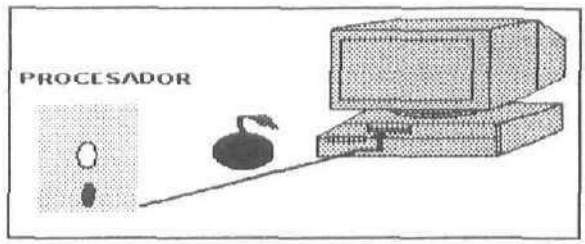
Nombre : IMAGEN33.BMP
Tema : Funcionamiento
Subtema : Clasificación general
Pantalla : Camaleón



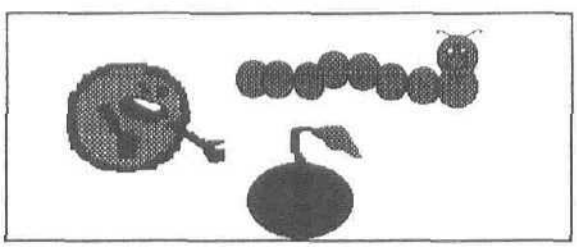
Nombre : IMAGEN34.BMP
Tema : Funcionamiento
Subtema : Clasificación general
Pantalla : Gusano



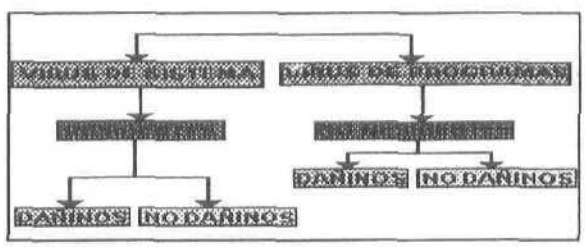
Nombre : IMAGEN35.BMP
Tema : Funcionamiento
Subtema : Clasificación general
Pantalla : Caballo de Troya



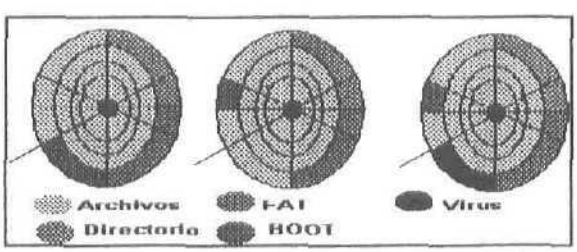
Nombre : IMAGEN36.BMP
Tema : Funcionamiento
Subtema : Clasificación general
Pantalla : Bomba Lógica



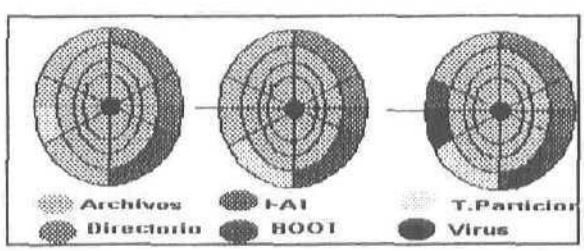
Nombre : IMAGEN37.BMP
Tema : Funcionamiento
Subtema : Clasificación general
Pantalla : Virus



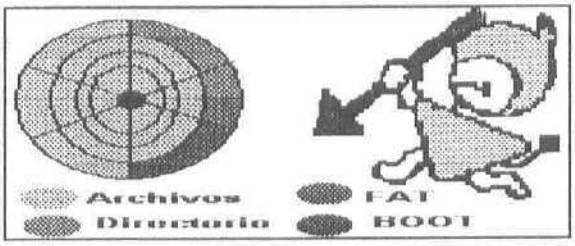
Nombre : IMAGEN38.BMP
Tema : Funcionamiento
Subtema : Clasificación por la parte que modifica el virus
Pantalla : Virus de sistema operativo, Virus de programas



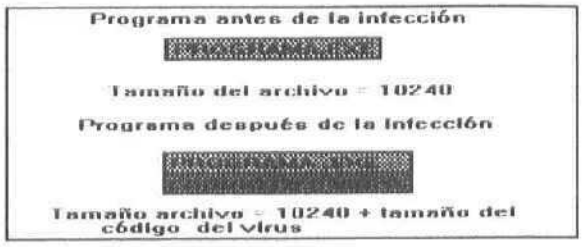
Nombre : IMAGEN39.BMP
Tema : Funcionamiento
Subtema : Clasificación por la forma en que trabajan
Pantalla : *Virus contaminadores del sector* de arranque



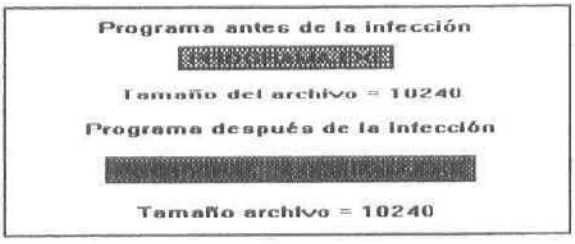
Nombre : IMAGEN40.BMP
Tema : Funcionamiento
Subtema : Clasificación por la forma en que trabajan
Pantalla : *Virus contaminadores del sector* de partición



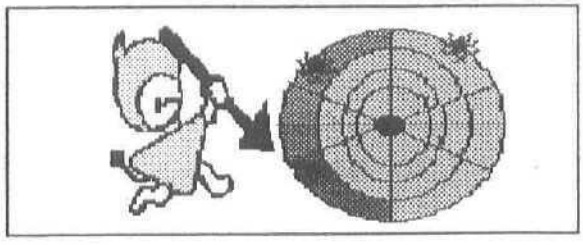
Nombre : IMAGEN41.BMP
Tema : Funcionamiento
Subtema : Clasificación por la forma en que trabajan
Pantalla : Virus contaminadores del intérprete de comandos



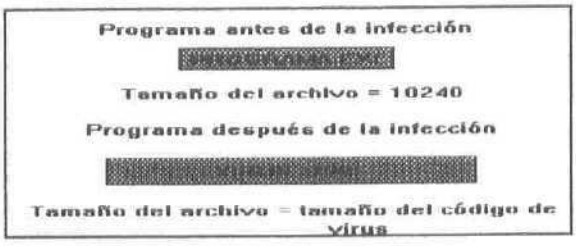
Nombre : IMAGEN42.BMP
Tema : Funcionamiento
Subtema : Clasificación por la forma en que trabajan
Pantalla : Contaminadores de archivos ejecutables por añadidura



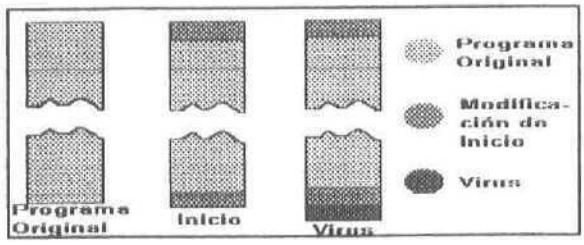
Nombre : IMAGEN43.BMP
Tema : Funcionamiento
Subtema : Clasificación por la forma en que trabajan
Pantalla : Contaminadores de archivos ejecutables por inserción



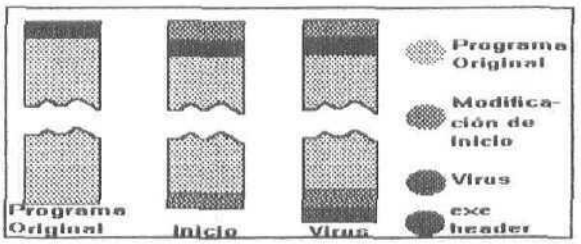
Nombre : IMAGEN44.BMP
Tema : Funcionamiento
Subtema : Clasificación por la forma en que trabajan
Pantalla : Contaminadores de archivos ejecutables por reorientación



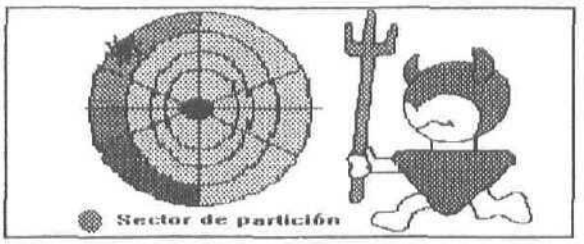
Nombre : IMAGEN45.BMP
Tema : Funcionamiento
Subtema : Clasificación por la forma en que trabajan
Pantalla : Contaminadores de archivos ejecutables por sustitución



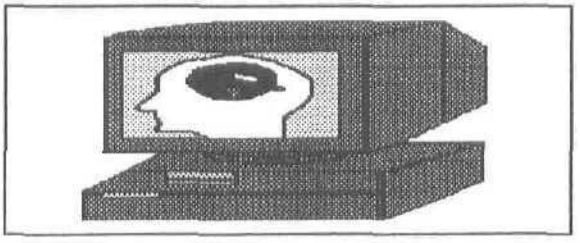
Nombre : IMAGEN46.BMP
Tema : Funcionamiento
Subtema : Clasificación por la forma en que trabajan
Pantalla : Contaminación de un archivo .COM



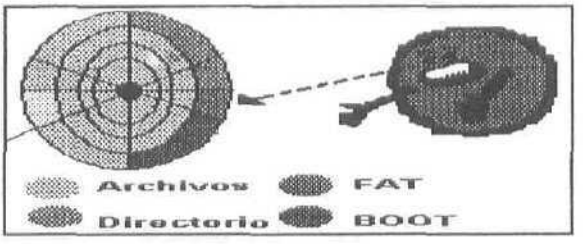
Nombre : IMAGEN47.BMP
Tema : Funcionamiento
Subtema : Clasificación por la forma en que trabajan
Pantalla : Contaminación de un archivo .EXE



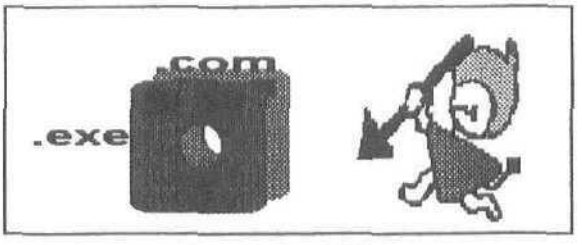
Nombre : IMAGEN48.BMP
Tema : Funcionamiento
Subtema : Clasificación por la forma en que trabajan
Pantalla : Virus contaminadores multipropósito



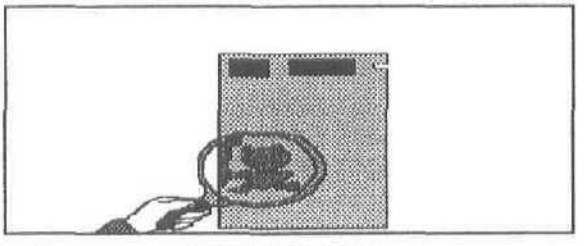
Nombre : IMAGEN49.BMP
Tema : Funcionamiento
Subtema : Clasificación por la forma en que trabajan
Pantalla : Virus residentes en memoria



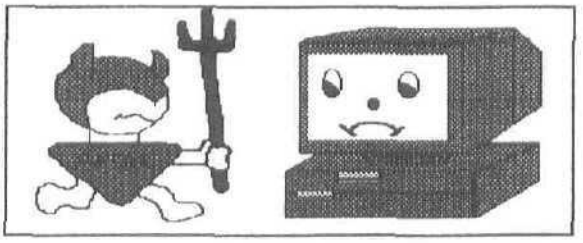
Nombre : IMAGEN50.BMP
Tema : Funcionamiento
Subtema : Clasificación por la forma en que trabajan
Pantalla : Contaminadores de la tabla de asignación de archivos



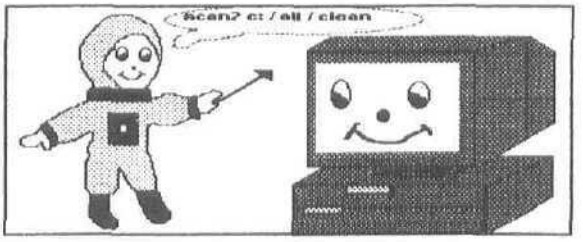
Nombre : IMAGEN51.BMP
Tema : Funcionamiento
Subtema : Clasificación por la forma en que intentan ocultarse
Pantalla : Virus compañero



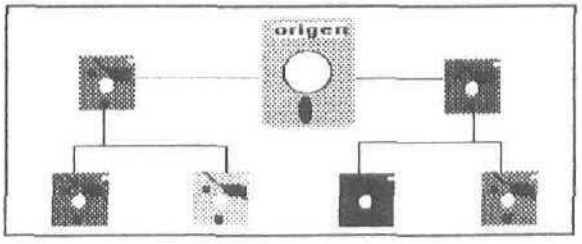
Nombre : IMAGEN52.BMP
Tema : Funcionamiento
Subtema : Clasificación por la forma en que intentan ocultarse
Pantalla : Virus con tácticas sigilosas o stealth



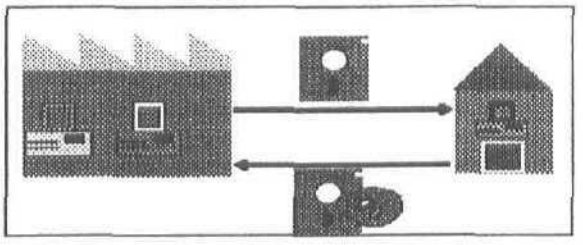
Nombre : IMAGEN53.BMP
Tema : Funcionamiento
Subtema : Clasificación por la forma en que intentan ocultarse
Pantalla : Virus polimórficos



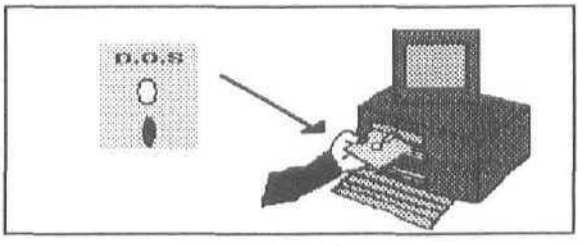
Nombre : IMAGEN54.BMP
Tema : Funcionamiento
Subtema : Clasificación por la forma en que intentan ocultarse
Pantalla : Virus slow



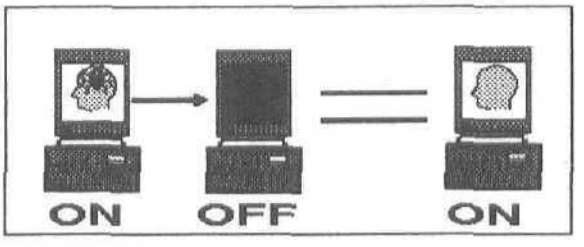
Nombre : IMAGEN55.BMP
Tema : Medidas de protección
Subtema : Prevención
Pantalla : No utilizar copias piratas



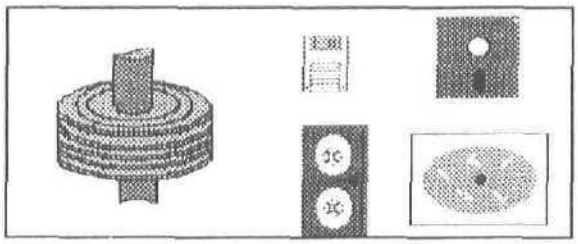
Nombre : IMAGEN56.BMP
Tema : Medidas de protección
Subtema : Prevención
Pantalla : Software de la empresa



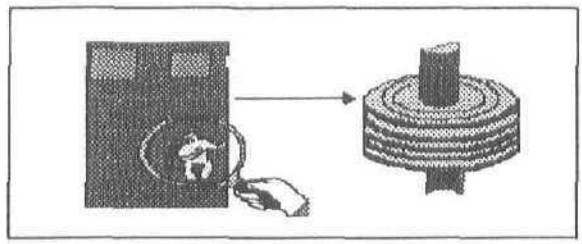
Nombre : IMAGEN57.BMP
Tema : Medidas de protección
Subtema : Prevención
Pantalla : Utilizar un sistema operativo fiable



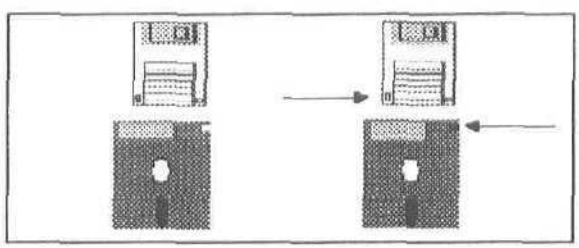
Nombre : IMAGEN58.BMP
Tema : Medidas de protección
Subtema : Prevención
Pantalla : Apagar y volver a arrancar la computadora



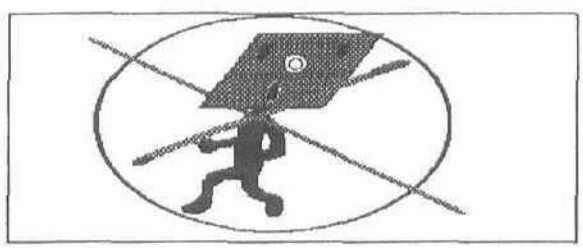
Nombre : IMAGEN59.BMP
Tema : Medidas de protección
Subtema : Prevención
Pantalla : No utilizar el disco duro como único lugar de almacenamiento



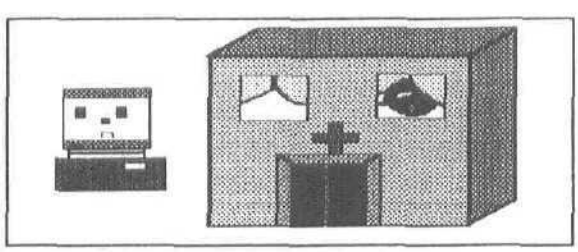
Nombre : IMAGEN60.BMP
Tema : Medidas de protección
Subtema : Prevención
Pantalla : Comprobar la seguridad de los discos flexibles



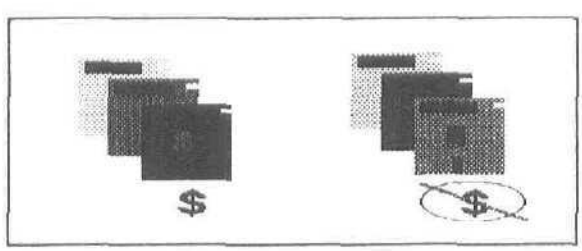
Nombre : IMAGEN61.BMP
Tema : Medidas de protección
Subtema : Prevención
Pantalla : Proteger los discos contra escrirura



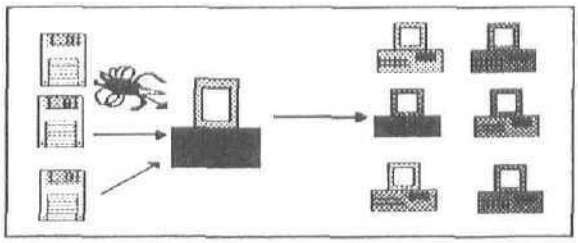
Nombre : IMAGEN62.BMP
Tema : Medidas de protección
Subtema : Prevención
Pantalla : Asignar el atributo de sólo lectura a los archivos ejecutables



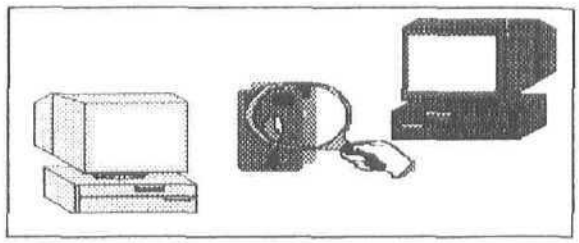
Nombre : IMAGEN63.BMP
Tema : Medidas de protección
Subtema : Prevención
Pantalla : Computadoras rentadas o en servicio



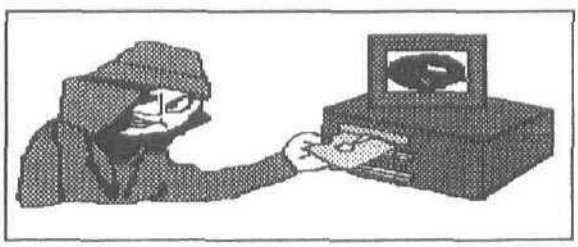
Nombre : IMAGEN64.BMP
Tema : Medidas de protección
Subtema : Prevención
Pantalla : Tome precauciones al adquirir software nuevo



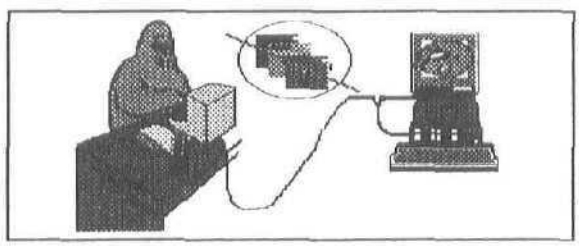
Nombre : IMAGEN65.BMP
Tema : Medidas de protección
Subtema : Prevención
Pantalla : Intercambio de discos



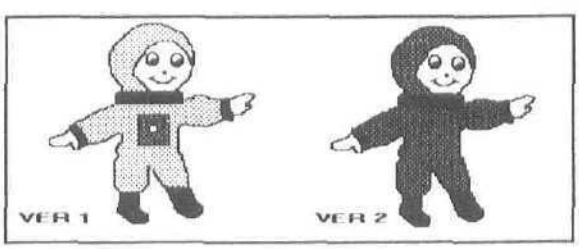
Nombre : IMAGEN66.BMP
Tema : Medidas de protección
Subtema : Prevención
Pantalla : Utilizar discos propios en otro sistema



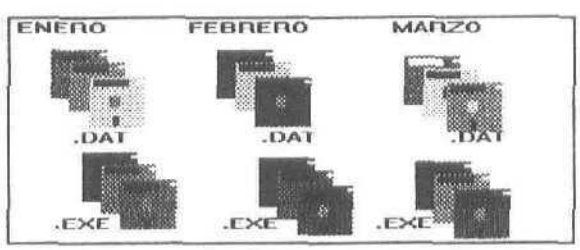
Nombre : IMAGEN67.BMP
Tema : Medidas de protección
Subtema : Prevención
Pantalla : Otras personas utilizan su *sistema*



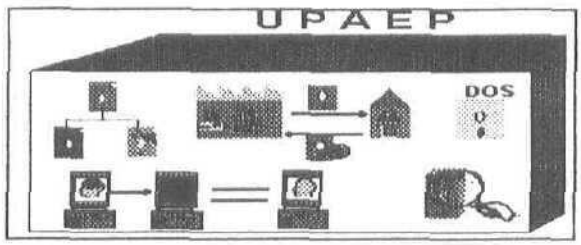
Nombre : IMAGEN68.BMP
Tema : Medidas de protección
Subtema : Prevención
Pantalla : Programas de servicios públicos (BBSs) o *redes*



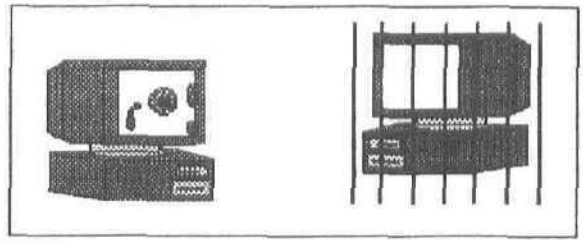
Nombre : IMAGEN69.BMP
Tema : Medidas de protección
Subtema : Prevención
Pantalla : Actualice constantemente su software antivirus



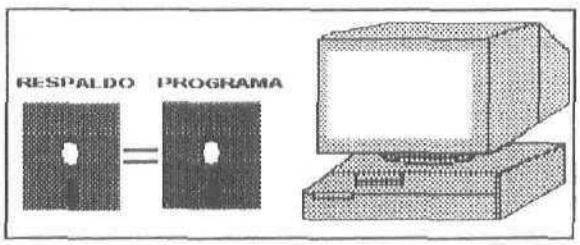
Nombre : IMAGEN70.BMP
Tema : Medidas de protección
Subtema : Prevención
Pantalla : Siga una política eficiente de respaldos



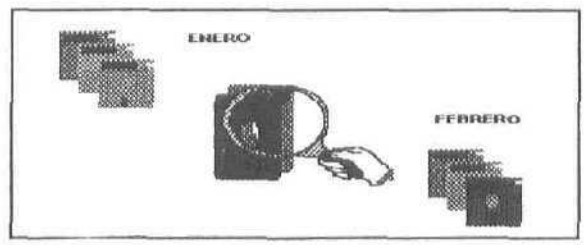
Nombre : IMAGEN71.BMP
Tema : Medidas de protección
Subtema : Prevención
Pantalla : Convertir las medidas preventivas en política interna de empresas



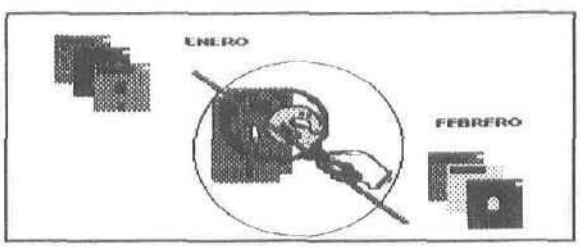
Nombre : IMAGEN72.BMP
Tema : Medidas de protección
Subtema : Prevención
Pantalla : Restringir el acceso directo a la información reservada



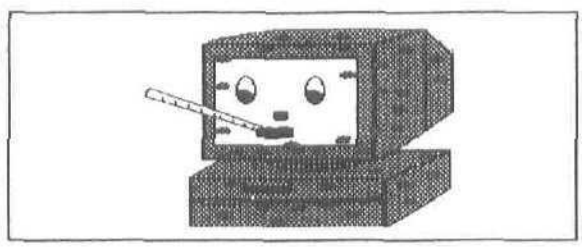
Nombre : IMAGEN73.BMP
Tema : Medidas de protección
Subtema : Detección
Pantalla : Lleve un registro de la longitud de los programas



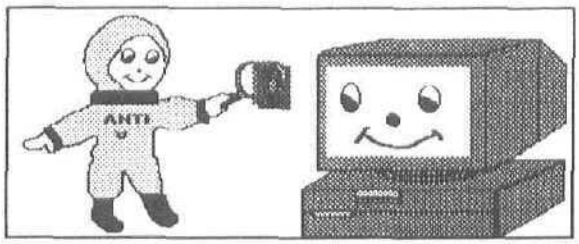
Nombre : IMAGEN74.BMP
Tema : Medidas de protección
Subtema : Detección
Pantalla : Inspeccionar periódicamente los discos



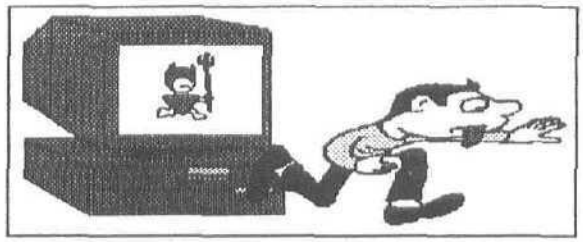
Nombre : IMAGEN75.BMP
Tema : Medidas de protección
Subtema : Detección
Pantalla : Revise los discos que ha respaldado



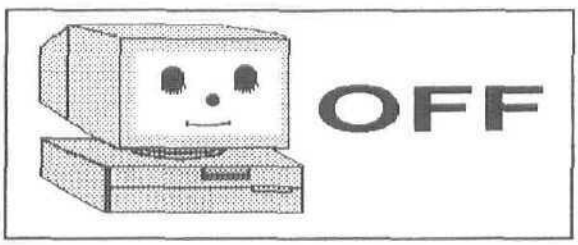
Nombre : IMAGEN76.BMP
Tema : Medidas de protección
Subtema : Detección
Pantalla : Inspección de síntomas



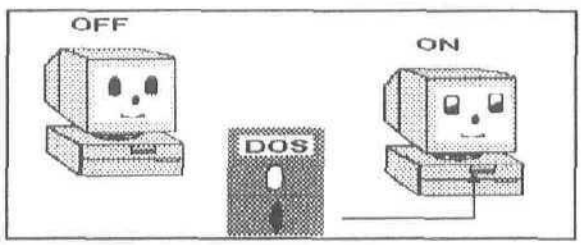
Nombre : IMAGEN77.BMP
Tema : Medidas de protección
Subtema : Detección
Pantalla : Instalación de software de *seguridad*



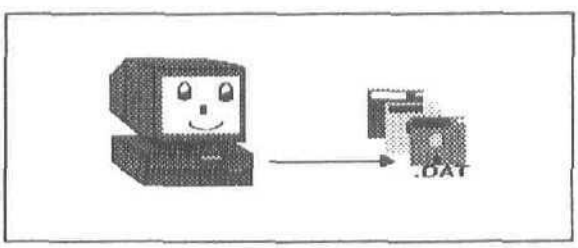
Nombre : IMAGEN78.BMP
Tema : Medidas de protección
Subtema : Erradicación
Pantalla : Conservar la calma



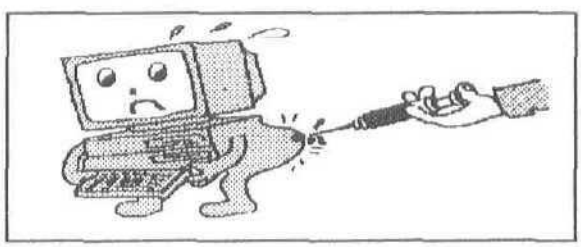
Nombre : IMAGEN79.BMP
Tema : Medidas de protección
Subtema : Erradicación
Pantalla : Apagar totalmente la computado*ra*



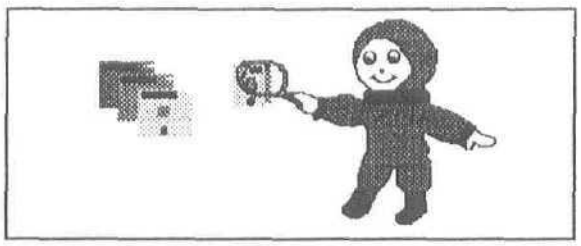
Nombre : IMAGEN80.BMP
Tema : Medidas de protección
Subtema : Erradicación
Pantalla : Encender la computadora con *otra copia de seguridad*



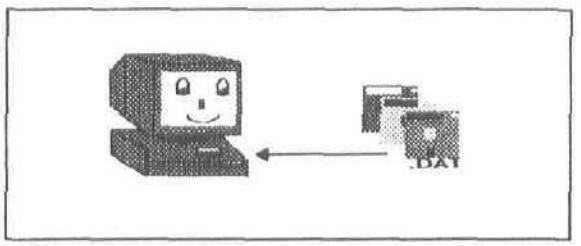
Nombre : IMAGEN81.BMP
Tema : Medidas de protección
Subtema : Erradicación
Pantalla : Hacer copias de seguridad de *archivos de datos y no ejecutables*



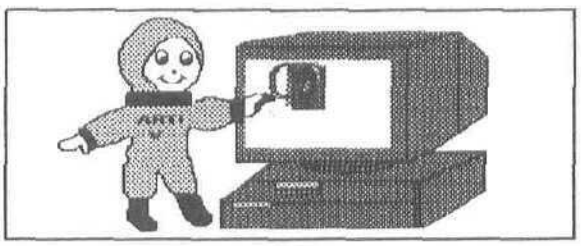
Nombre : IMAGEN82.BMP
Tema : Medidas de protección
Subtema : Erradicación
Pantalla : De preferencia, dar nuevo formato *al disco infectado*



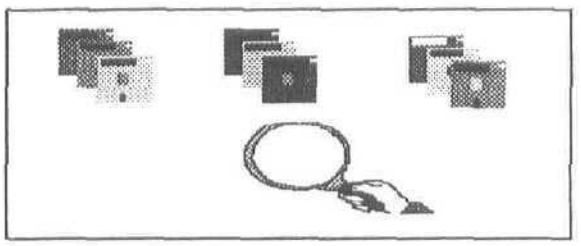
Nombre : IMAGEN83.BMP
Tema : Medidas de protección
Subtema : Erradicación
Pantalla : Comprobar los discos originales con programas detectores



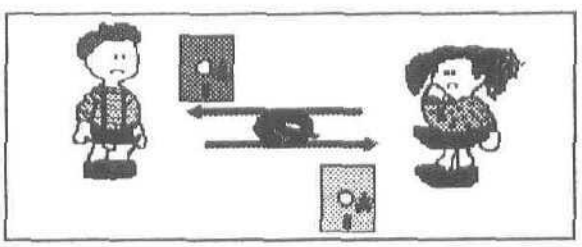
Nombre : IMAGEN84.BMP
Tema : Medidas de protección
Subtema : Erradicación
Pantalla : Volver a copiar la información no infectada



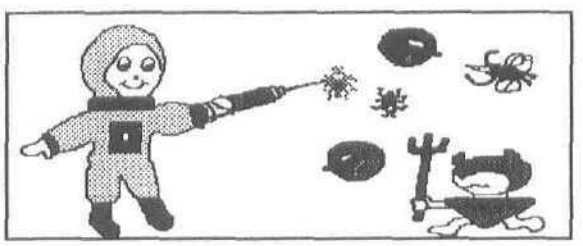
Nombre : IMAGEN85.BMP
Tema : Medidas de protección
Subtema : Erradicación
Pantalla : Volver a comprobar los discos con programas detectores



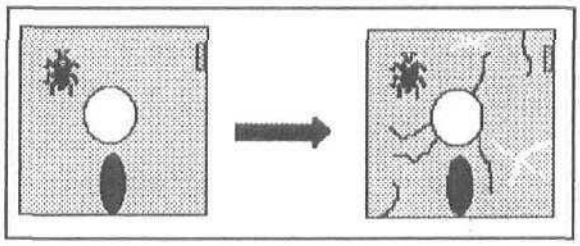
Nombre : IMAGEN86.BMP
Tema : Medidas de protección
Subtema : Erradicación
Pantalla : Probar todos los discos utilizados con anterioridad a la infección



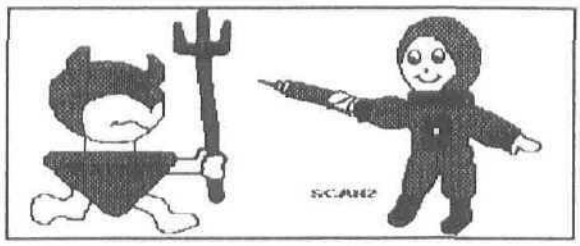
Nombre : IMAGEN87.BMP
Tema : Medidas de protección
Subtema : Erradicación
Pantalla : Avisar a otros usuarios del peligro de infección



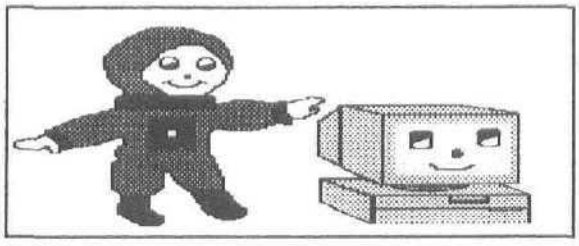
Nombre : IMAGEN88.BMP
Tema : Medidas de protección
Subtema : Software antivirus: virus no específico
Pantalla : Checksummers



Nombre : IMAGEN89.BMP
Tema : Medidas de protección
Subtema : Software antivirus: virus específico
Pantalla : Inoculadores



Nombre : IMAGEN90.BMP
Tema : Medidas de protección
Subtema : Software antivirus: virus no específico
Pantalla : Scanners



Nombre : IMAGEN91.BMP
Tema : Medidas de protección
Subtema : Software antivirus: virus específico
Pantalla : Software para eliminar virus

6.3. Implementación

Al implementarse el tutorial se le realizaron pruebas para verificar su correcto funcionamiento, las cuales permitieron hacerle mejoras al sistema, tales como:

- El tutorial proporciona al usuario dos oportunidades para registrar su nombre; si no lo hace así, se terminará la sesión.
- Al finalizar cada tema, el tutorial presentará al usuario un cuestionario que deberá contestar. Si lo aprueba, se le permitirá accesar el tema siguiente, de lo contrario, lo regresará al principio del tema.
- Si el usuario desea accesar un tema sin haber recorrido los que le preceden, el tutorial le presentará los cuestionarios de esos temas. Sólamente si los aprueba le permitirá visualizar el tema escogido.

- Siempre que el usuario esté contestando el cuestionario, no se le permitirá abandonar la sesión del tutorial.

- En el caso de que el usuario escoja la opción Salir, se presentará una pantalla con un mensaje que indica si desea realmente terminar la sesión del tutorial; esto permite al usuario decidir continuar con la sesión por si erróneamente escogió la opción de Salir Siempre que decida terminar la sesión, se graba en un archivo el número de pantalla en que se quedó; esto permitirá visualizar los temas ya aprobados en otra sesión del tutorial.

- Se colocaron barras de herramientas con botones, los cuales permiten accesar las opciones del tutorial utilizando el mouse o una secuencia de teclas que incluye Alt + la letra que aparece subrayada.

- Sólo se probó que las imágenes se visualicen correctamente en monitores VGA y SVGA color.

6.4. Manual del usuario

Instalación

Para instalar el Tutorial en su computadora debe utilizar el programa SETUP.EXE.

Antes de que ejecute el Setup, deberá asegurarse de que su computadora cumple con los requerimientos mínimos para ejecutar el Tutorial:

- Computadora IBM™ PC o compatible
- Procesador 80286 o superior
- Mouse
- 1 Mb en RAM mínimo (2 Mb o más recomendables)
- Monitor VGA color o SVGA color
- MS-DOS™ versión 3.1 o superior, con SHARE.EXE ejecutándose
- Microsoft Windows™ versión 3.0 o superior
- Disco duro con 6.5 Mb disponibles

Para empezar a instalar el Tutorial:

- Inserte el primer disco en el drive A
- Desde el Program Manager (Administrador de Programas) de Microsoft Windows™ o File Manager (Administrador de Archivos), escoja Run (Ejecutar) del menú File (Archivo)
- Teclee **a:setup**
- Siga las instrucciones en la pantalla

Empezando la sesión del Tutorial de Virus Computacionales

- Identifique la ventana TUTORVIR en el Program Manager (Administrador de Programas) y haga doble click en el icono TUTORVIR

Cómo utilizar el Tutorial

Opciones del menú

Virus

Esta opción presenta al usuario la información de qué es un virus, su origen, los mitos y realidades acerca de los virus, y cuatro simuladores para ver algunos de sus efectos.

Medios de contagio

Esta opción presenta al usuario las formas posibles en que se puede contagiar de virus, entre ellas están la transferencia de discos, los boletines informativos (BBSs) y los sistemas de información.

Funcionamiento

En esta opción se presenta la información referente al ciclo de vida de un virus y las diferentes clasificaciones que se han hecho de ellos

Medidas de protección

Esta opción despliega toda la información sobre cómo prevenir, detectar y erradicar a los virus, además de realizar prácticas en tres software antivirus diferentes Norton Antivirus™, Central Point Antivirus™ y VirusScan™.

Salir

Con esta opción se termina la sesión del tutorial, almacenando en un archivo los datos del usuario, así como en que tema se quedó

Accesar opciones del menú

Para accesar un comando del menú, puede hacerlo de dos maneras:

a) Presionando la secuencia de teclas Alt + Letra subrayada de la opción del menú elegida. Por ejemplo: Alt + V accesa el comando Virus del menú principal.

b) Hacer click con el botón izquierdo del mouse sobre la opción del menú elegida

Accesar información de cada tema

Para accesar la información de cada tema del tutorial, debe seguir los siguientes pasos.

a) Seleccionar una opción del menú principal, con esto aparecerá la primera pantalla del tema elegido. Dicha pantalla contiene en la parte superior una imagen

referente al tema; más abajo contiene un cuadro con información Aquí puede utilizar la barra de desplazamiento del mouse localizada a la izquierda del cuadro para desplazar el texto hacia arriba o hacia abajo y terminar de leerlo Y en la parte inferior se encuentra una barra de herramientas, la cual presenta dos botones. Regresa y Avanza.

b) Para poder visualizar las siguientes pantallas con información puede hacer click con el botón izquierdo del mouse sobre el botón Avanza localizado en la barra de herramientas o bien, presionar la secuencia de teclas Alt + A.

c) Para visualizar las pantallas anteriores puede hacer click con el botón izquierdo del mouse sobre el botón Regresa localizado en la barra de herramientas o bien, presionar la secuencia de teclas Alt + R.

Cuestionarios

Al finalizar cada tema, el tutorial llevará a cabo una evaluación de los conocimientos aprendidos; esto lo hará por medio de un cuestionario que usted deberá contestar.

El cuestionario se presenta en una pantalla diseñada de la siguiente manera. en la parte superior despliega la pregunta. Más abajo aparecen tres posibles respuestas marcadas con A, B o C, de las cuales usted seleccionará la que considere es la respuesta adecuada a la pregunta. En la parte inferior de la pantalla se encuentra una barra de herramientas, la cual presenta tres botones· Anterior, Siguiente y Evalúa.

Para pasar a las siguientes deberá hacer click con el botón izquierdo del mouse sobre el botón Siguiente localizado en la barra de herramientas o bien, presionar la secuencia de teclas Alt + S.

Puede regresar a las preguntas anteriores haciendo click con el botón izquierdo del mouse sobre el botón Anterior localizado en la barra de herramientas o bien, presionando la secuencia de teclas Alt + N

Por lo tanto, usted podrá avanzar o regresar en el cuestionario por si desea cambiar alguna de las opciones elegidas como respuesta

Una vez contestado todo el cuestionario, deberá hacer click con el botón izquierdo de mouse sobre el botón Evalúa localizado en la barra de herramientas o bien, presionar la secuencia de teclas Alt + E, para que el tutorial le indique si aprobó o no el cuestionario

De haberlo aprobado, podrá continuar con el siguiente tema; en caso contrario, el tutorial lo regresará al principio del tema.

Si usted quiere accesar temas posteriores a los que lleva aprendidos en el tutorial, este le pedirá que primero conteste los cuestionarios de los temas que no ha visto; en caso de aprobarlos sí le permitirá ver el tema que usted haya solicitado; en caso contrario tendrá que pasar antes por lo temas que no ha aprendido.

CONCLUSIONES

El virus no es culpable de todas las anomalías o fallas que pueden aparecer en la computadora, sobre todo si se trata de deficiencias de hardware Es probable que se trate también de un error humano.

Es importante que las medidas de detección, prevención y erradicación mencionadas en esta tesis se establezcan como reglas y procedimientos en la UPAEP, sus centros de cómputo y a nivel de alumnos (usuarios) Si éstas se siguen, no se logrará que la organización sea totalmente inmune a un ataque de virus, pero sí reducirán la probabilidad del contagio y minimizarán los esfuerzos (humanos, de tiempo y económicos) de recuperación de la información.

El problema de los virus estará por siempre. Sin embargo, si se llevan a cabo las medidas de prevención, detección y erradicación, el riesgo de contagio será mínimo Además, tan pronto como los usuarios tengan problemas de virus con las computadoras, otras personas estarán ofreciendo nuevas soluciones, por medio de hardware y/o software, a estos problemas.

Es primordial la educación y concientización de la existencia de estos programas virus y de los daños que pueden ocasionar. Se debe evitar, en la mayor medida de lo posible, utilizar copias ilegales de programas.

APENDICE A. ESTRUCTURA Y MANEJO DE DISCOS

La mayoría de las microcomputadoras tienen algún medio de almacenamiento de información permanente, ya sea cintas, cassettes, discos y CD

Los medios de almacenamiento más comunes son el disco duro, el disco flexible, también llamado "floppy" o "diskette" y los CD (compact disk)

Discos flexibles

Hoy en día existen dos tipos de discos comerciales:

a) de 5¼ pulgadas de diámetro, disponibles en versiones de 360 Kb y 1.2 Mb de capacidad

b) de 3½ pulgadas de diámetro, disponibles en versiones de 720 Kb y 1 44 Mb de capacidad.

Recientemente están entrando al mercado los discos flexibles con capacidades de 2.88 Mb, los cuales vienen contenidos en una cubierta de plástico rígido y sellada por una lámina metálica. También se han puesto a la venta discos de 3½ pulgadas que trabajan auxiliados por un rayo láser para la localización de los sectores, tecnología que se conoce como "floptical disk", y con la cual se consigue almacenar hasta 128 Mb de datos en un disco de baja densidad y 520 Mb en uno de alta densidad Por ahora este tipo de unidades son muy escasas, pero se espera que en pocos años gocen de gran aceptación.

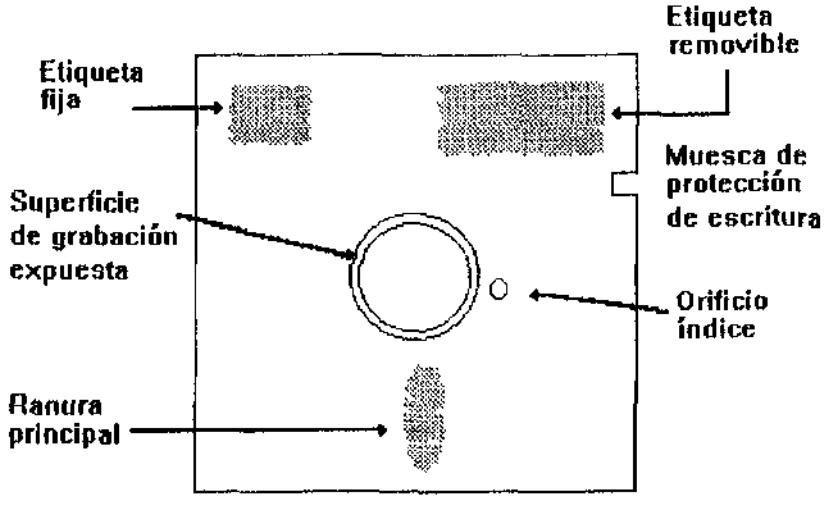
Estructura física de un disco

Un disco es un dispositivo de memoria externa, basado en la escritura / lectura de sectores y pistas sobre una superficie móvil magnetizada. Está fabricado con una lámina de plástico mylar recubierta de óxido magnético por ambos lados, y gira a una velocidad de trescientas revoluciones por minuto.

En la figura A 1 se observan las partes de un disco de 5¼ pulgadas y en la figura A.2. las partes de un disco de 3½.

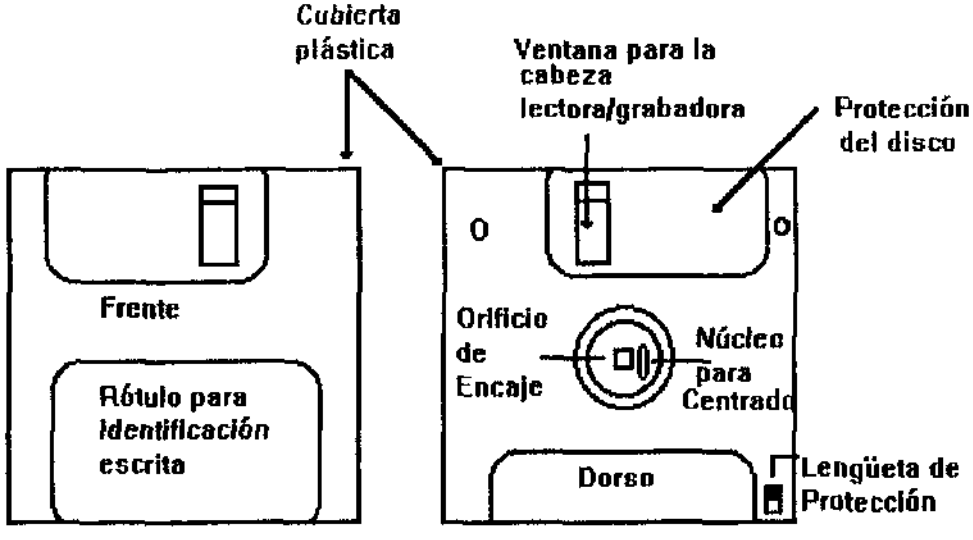
Para que una computadora pueda leer y grabar información en un disco, utiliza dos motores en el transporte del disco. Un motor hace girar el disco en el drive y el otro mueve la cabeza de lectura / escritura a través de la superficie del disco, hasta el lugar adecuado.

Figura A.1 Partes de un disco de 5¼ pulgadas



Fuente: PC Magazine en Español, Octubre 1993

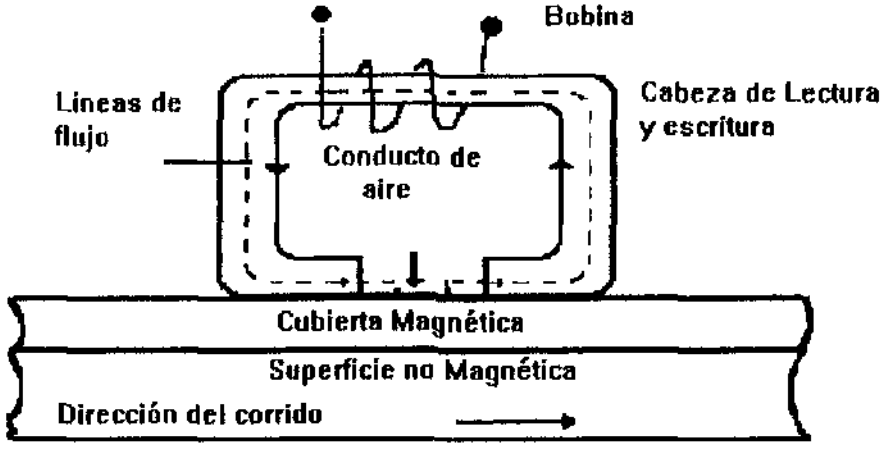
Figura A.2. Partes de un disco de 3½ pulgadas



Fuente PC Magazine en Español, Octubre 1993

La escritura de la información queda expresada en forma binaria, y está a cargo de una cabeza de lectura / escritura constituida por un núcleo de hierro suave de alta permeabilidad, con una bobina enrollada y una pequeña separación (ver figura A.3)

Figura A 3 Cabeza de lectura/escritura



Fuente: PC Magazine en Español, Octubre 1993

Al escribir sobre la superficie del disco fluye una corriente a través de la bobina, con lo que se establecen líneas magnéticas de flujo que llegan a la brecha de aire, el cual tiene una baja reluctancia al flujo magnético, lo que provoca que dichas líneas de flujo se desvíen y viajen por la cubierta magnética del disco en rotación

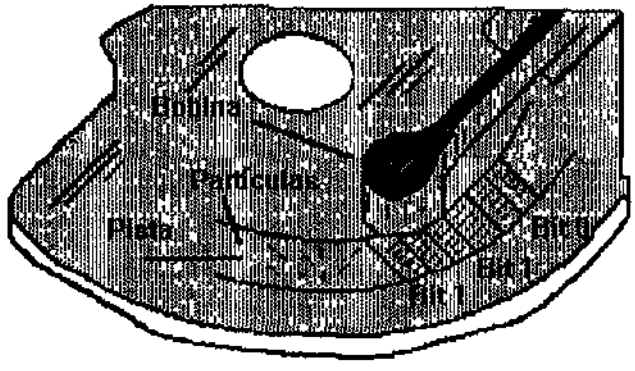
Conforme avanza el disco se magnetizan las partículas de cada pista, las cuales se ven obligadas a alinear sus polos magnéticos en la misma dirección, formando así una banda magnetizada que contendrá la información codificada en lenguaje binario (ver figura A.4.).

Dos de estas bandas contiguas magnetizadas integran lo que se conoce como un bit, que es la unidad básica de información Es decir, cada par de bandas magnetizadas representa el número binario 0 ó 1 Si las partículas magnéticas en ambas bandas están alineadas en el mismo sentido, el bit de datos representa un 0, y si están alineadas en sentido opuesto, representa un 1. Ocho pares de estas bandas magnetizadas contienen ocho bits o un caracter alfanumérico, el cual se ha tomado como la unidad de medida para la capacidad de almacenamiento de los diferentes medios magnéticos.

La operación de lectura es inversa a la de escritura, sólo que en este caso la bobina juega un papel de línea sensora. Conforme gira el disco, la superficie se desplaza cerca de la cabeza de lectura / escritura, y las bandas que han sido magnetizadas previamente producen un flujo a través del conducto de aire y en el

núcleo, induciendo una señal de voltaje que posteriormente se procesa y amplifica para los distintos tratamientos informáticos

Figura A.4 Bandas magnetizadas

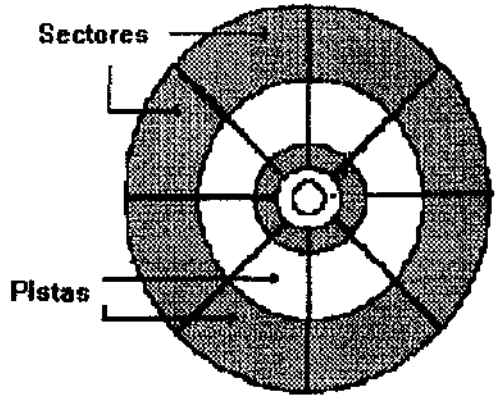


Fuente: PC Magazine en Español, Octubre 1993

Formateo

Un disco nuevo es como una hoja blanca, cuya superficie no dispone de renglones, por lo que no puede ser usada en esas condiciones, necesitamos formatearlo.

Figura A.5 Sectores y pistas de un disco



Fuente: PC Magazine en Español, Octubre 1993.

Para que el CPU pueda almacenar y accesar información en el disco, se precisa de un sistema de direcciones que identifiquen puntos en la superficie del disco (eje de coordenadas), por lo tanto, un disco debe ser preparado magnéticamente para que

pueda almacenar lógicamente y de manera organizada la información A la acción de "dibujar" magnéticamente en cada cara del disco una serie de círculos concéntricos llamados pistas, las cuales, a su vez son divididas en segmentos llamados sectores se le denomina formateo (ver figura A 5.).

El formateo se divide en dos etapas:

1 Formateo físico o de bajo nivel, que consiste en el "dibujo" magnético de pistas y sectores en cada cara del disco.

2. Formateo lógico o de alto nivel, el cual sigue inmediatamente al anterior, y consiste en dividir la capacidad de almacenamiento del disco en porciones que puedan ser manejadas por el sistema operativo

Tanto el formateo físico como el lógico, en el caso de los discos flexibles, están a cargo del comando FORMAT del sistema operativo.

Formateo físico o de bajo nivel. Durante el formateo físico se inicializa el disco, para lo cual un par de cabezas de lectura / escritura, encontradas respectivamente con las dos superficies, "dibujan" con marcas magnéticas cierta cantidad de pistas o tracks. Por ejemplo, un disco estándar de doble cara para una capacidad de 360 Kb, se formatea para cuarenta pistas numeradas de la cero a la treinta y nueve, cada una dividida en nueve sectores numerados del uno al nueve, cada uno de los cuales a su vez dispone de una capacidad de almacenamiento de 512 Kb (norma estándar IBM™), se tienen entonces cuarenta cilindros completos y una capacidad de almacenamiento de 368,640 bytes, que para abreviar simplemente se denominan 360 Kb

512 bytes por cada sector del cilindro x 2 caras = 1024 bytes, x 9 sectores por cilindro = 9,216 x 40 cilindros = 360,460 bytes totales en ambas caras del disco

Naturalmente que si el disco es de otra densidad o de otro diámetro, la capacidad de grabación de pistas y sectores también será otra En la tabla A.1. se muestra cómo se conforma la capacidad de almacenamiento de los discos de 5¼ y 3½ pulgadas en su densidad más popular.

Tabla A.1. Capacidad de almacenamiento de los discos de 3½ y 5¼ pulgadas

	5¼ Pulgadas	5¼ Pulgadas	3½ Pulgadas	3½ Pulgadas
	360 Kb	1.2 Mb	720 Kb	1.4 Mb
Cara	2	2	2	2
Pistas	40	80	80	80
Sectores por pista	9	15	9	18
Capacidad de almacenamiento.	368,640 bytes	1228,800 bytes	737,280 bytes	1474,560 bytes

Fuente: PC Magazine en Español, Octubre 1993.

Además de la delimitación del disco en sectores y pistas, es preciso disponer de un sistema de direcciones que permita almacenar y accesar de manera ordenada y lógica la información, es necesario entonces, numerar los elementos que componen el disco (cilindros, caras, pistas, sectores) Hay dos modos de direccionamiento que durante el formateo físico se determinan: la numeración física y la numeración lógica

En el caso de la numeración física, la tarjeta controladora del disco y las rutinas de la memoria ROM BIOS especifican el direccionamiento con base en tres coordenadas. cara, pista (cilindro) y sector, por ejemplo: lado 0, cilindro 14, sector 16 Sin embargo, para el sistema operativo (DOS) es mejor considerar los datos como si se trataran de una larga lista de unidades secuenciales, por lo que numera los sectores de la misma pista y cara, luego se numeran los sectores de la misma pista pero situados en la cara contraria, para continuar con el segundo sector de la cara 0, pista 1, etc Esta es la numeración lógica. Con este método se minimizan los movimientos de las cabezas y, por lo tanto, se optimiza el tiempo de acceso cuando se intentan leer sectores situados de forma ordenada

Llegando a este punto, cabe mencionar que la unidad controladora de disco flexible reconoce la posición del primer sector de cada pista mediante un pequeño orificio de indexación, ubicado cerca del centro del disco de 5¼, el DOS también reconoce la posición de éste por medio del orificio. Para ello se proyecta un haz de luz sobre la ventana del orificio índice, el cual sólo podrá pasar en el momento en que coincida con dicha ventana; cada vez que ello ocurre, durante la rotación se puede ir determinando la posición del disco.

Un sector (512 bytes) es la cantidad mínima que se puede leer o escribir en el disco; para ello, el DOS debe llevar un control del estado de cada uno (posición del sector, qué contiene, si está libre o físicamente dañado), lo que resulta muy costoso en cuanto a espacio de almacenamiento del propio disco, además de complicado y lento, dado que 512 bytes aún es una cantidad muy pequeña de información. Por lo tanto, el DOS agrupa un cierto número de sectores contiguos, llamados "cluster" (racimo), y los trata como un solo paquete de información en el disco. Se tiene, entonces, un tercer *método de direccionamiento de la información: mediante la numeración de clusters.*

Tabla A.2. Tamaño de un cluster en un disco

Tipo de disco	Tamaño de cluster
5¼	
360 Kb	2 sectores
1.2 Mb	1 sector
3½	
720 Kb	2 sectores
1 44 Mb	1 sector

Fuente: PC Magazine en Español, Octubre 1993.

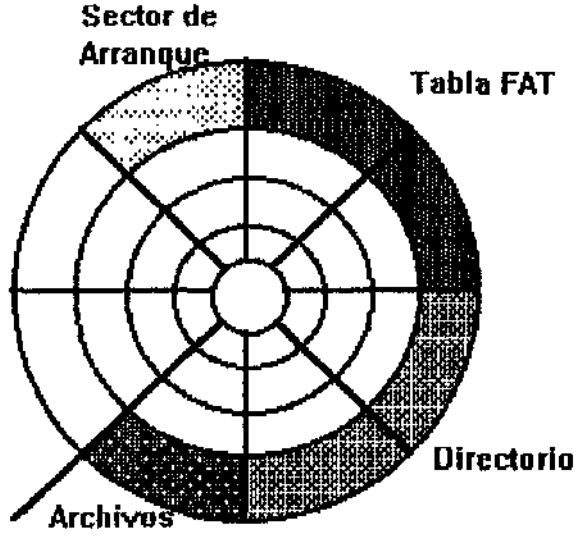
Formateo lógico o de alto nivel Una vez que se han creado las pistas y sectores de un disco, se precisa de un método que permita manejar eficientemente la información y llevar un recuento de su estado de organización Este método se define durante el formateo lógico.

Es importante mencionar que en esta etapa el DOS organiza la información en clusters, como unidad mínima de almacenamiento Naturalmente, los clusters no son una propiedad inherente al formateo físico del disco, sino un método del sistema operativo para optimizar el manejo de datos, por lo que el número de sectores (cada uno de 512 bytes) contenidos en cada cluster varía en función del tipo de disco (ver tabla A.2)

El formateo lógico consiste en la creación de un conjunto de índices que señalan en todo momento el estado del disco (qué zonas están ocupadas, sectores defectuosos, cuánto espacio disponible hay y en dónde) y que permiten direccionar la información. Para ello el disco se divide en dos zonas:

1. Area del sistema, dividida a su vez en.
   a) sector de arranque (boot sector),
   b) FAT (File Allocation Table: Tabla de localización de archivos) y
   c) directorio raíz (root directory)
2. Zona de Datos. En la figura A.6 se muestra una representación intuitiva de cómo quedarían distribuidas estas zonas, partiendo de la periferia hacia el centro del disco.

Figura A.6. Distribución de zonas en un disco



Fuente: PC Magazine en Español, Octubre 1993.

Sector de arranque

Cuando se acciona el interruptor de encendido de la computadora, los programas de arranque de la ROM le ordenan que lea el sector de arranque del disco,

para comenzar a cargar en la RAM el sistema operativo La computadora primero busca estas rutinas en el disco de la unidad A, y si no las encuentra, pasa enseguida a buscarlas en el disco duro

Si el usuario inserta un disco autoarrancable (es decir que contiene los tres archivos básicos del sistema operativo), al encender la máquina podrá cargar en RAM las rutinas que le permitan trabajar; pero si el disco no es autoarrancable, se emitirá un mensaje de error. Tanto el trabajo de cargar el sistema operativo como el de informar al DOS las características del disco, están a cargo del sector de arranque, para lo cual debe disponer de dos partes: 1) un programa muy corto de arranque y 2) una lista de las características clave del disco (número de bytes por sector, número total de sectores por pista, numero de cabezas de lectura / escritura, etc)

Debido a la importancia de estos datos, todos los discos del DOS, sean o no autoarrancables, deben de disponer de un sector de arranque, el cual siempre se ubica, en el caso de este tipo de discos, en el primer sector de la primera pista de la primera cara: sector 0, pista 0, cara 0 (ver tabla A 3.)

Tabla A.3 Mapa del sector de arranque de un disco DOS

Contenido
Reservado (3 bytes)
Nombre del fabricante y versión (8 bytes)
Bytes por sector (2 bytes)
Sectores por cluster (1 byte)
Sectores reservados (2 bytes)
Número de copias de la FAT (1 byte)
Número de entradas del directorio raíz (2 bytes)
Sectores totales (2 bytes)
Byte del formato del disco
Número de sectores por FAT (2 bytes)
Sectores por pista (2 bytes)
Número de cabezas (2 bytes)
Número de sectores ocultos (2 bytes)
Rutina de arranque (BOOT)

Fuente: PC Magazine en Español, Octubre 1993.

La Fat

La tabla de localización de archivos, FAT, es la segunda parte del sistema del disco, y consiste en un área que registra tanto el estado general de todos los clusters como el direccionamiento de los archivos, según la cadena de clusters que ocupa. Esta se actualiza cada vez que se graba o borra un archivo del disco.

En un disco, un archivo rara vez queda grabado en un bloque de sectores contiguos (a menos que esté recién formateado). Esto es así porque el DOS tiende a

distribuir los archivos por toda la superficie del disco, aprovechando los espacios libres que van quedando por otros archivos que se han borrado o modificado. En consecuencia, los archivos tienden a quedar fragmentados, por lo que precisan de un método de encadenamiento lógico que permita seguirles la huella.

Justamente, para conocer tanto el estado de cada cluster, como su contenido y la cadena de información que permite seguirle los pasos a cada uno de los archivos, el DOS construye un mapa o tabla llamada FAT. En la FAT se asigna una entrada para cada cluster que contiene la información respectiva, cuyo número de identificación corresponde con el número de dicho cluster; por ejemplo, el cluster 175 del disco está asociado con la entrada 175 de la tabla FAT.

Para entender mejor lo anterior, suponga un archivo llamado TEXTO.DOC, cuya entrada en el directorio correspondiente dice que comienza en el cluster 85. El DOS lee los sectores de este cluster; luego consulta la posición 85 en la FAT, para averiguar cuál es el número del siguiente cluster, por ejemplo el 110 Enseguida el DOS lee la siguiente porción del archivo en el cluster en que continúa el archivo Y así sucesivamente hasta que encuentra un código en particular (EOF = End Of File) que le indica que el archivo ha concluido.

Según el contenido de cada entrada en notación hexadecimal, se puede tener la información que se muestra en la tabla A 4 Por otra parte, puesto que la tabla FAT contiene los índices de los archivos y sin ella la información sería muy difícil de recuperar, se graba de manera adjunta una copia como protección contra una pérdida de los datos, en caso de daño de algunos de los sectores de la FAT original. Y por último , el número de sectores que ocupa la FAT depende del tipo y la capacidad del disco, información que viene almacenada en el primer byte de la FAT

Tabla A.4. Información hexadecimal de la FAT

Entrada de la FAT	Significado
0000	Cluster disponible
0000-FFEF	Cluster utilizado por un archivo
FFF0-FFF6	Cluster reservado
FFF7	Cluster defectuoso
FFF8-FFFF	Ultimo cluster

Fuente: **PC Magazine en Español, Octubre 1993.**

Directorio raíz

Este es un índice que el DOS crea en la tercera y última parte del área del sistema durante el formateo lógico. Tanto su tamaño como su posición quedan fijados durante esta etapa y no pueden alterarse posteriormente.

La cantidad de sectores que ocupa el directorio raíz es distinta entre un disco de baja densidad y uno de alta; por ejemplo, en uno de 360 Kb de 5¼ pulgadas se ocupan siete sectores, mientras que en uno de 1 2 Mb del mismo diámetro se usan catorce.

El directorio raíz dispone de un cierto número fijo de entradas, en donde se recoge la información esencial de cada archivo a almacenar en el disco, con lo que la cantidad de archivos posibles a almacenar queda limitada por ese número de entradas. En los discos de 360 Kb y 720 Kb el número de entradas máxima es de ciento doce, mientras que en los de 1 2 Mb y 1 44 Mb es de doscientos cuarenta y cuatro.

En la práctica, el directorio raíz se puede definir como el directorio de primer nivel en la estructura o árbol de archivos del disco, y se identifica con la diagonal inversa (\)

Tabla A.5. Información esencial de cada archivo en la entrada del directorio raíz

Campo	Longitud
Nombre	8 bytes
Extensión	3 bytes
Atributos	1 byte
Reservado	10 bytes
Hora	2 bytes
Fecha	2 bytes
Primer cluster	2 bytes
Tamaño	4 bytes

Fuente: PC Magazine en Español, Octubre 1993

En la tabla A 5. se observa cuál es la información esencial de cada archivo que se registra en cada entrada del directorio raíz El nombre y extensión es una cadena de hasta ocho y tres caracteres ASCII, respectivamente El punto de separación entre ambos no queda almacenado. El primer caracter de esta cadena tiene una importancia especial para el DOS. Por ejemplo, cuando se borra un archivo realmente lo único que se borra es el primer caracter, que se sustituye por un símbolo (sigma); también se borran sus entradas correspondientes en la FAT Esto permite recuperar posteriormente tal archivo por medio de algunas técnicas, siempre que la cadena de clusters en que se aloja no haya sido ocupada por otro archivo

En el campo de atributos se especifica la información que indica al DOS las características del archivo correspondiente, como son: si es de sólo lectura, si es oculto, si es archivo del sistema, etiqueta del volumen, si es subdirectorio o archivo.

Los 10 bytes que ocupa el "campo reservado" quedan para posibles usos futuros del DOS. Los dos siguientes campos señalan la hora y fecha en que fue creado o sufrió la última modificación el archivo correspondiente

El campo siguiente indica el primer cluster que ocupa ese archivo, es decir, actúa como punto de partida de la cadena de localización de la FAT A partir de esta información el DOS puede seguir el rastro del archivo, leyendo las correspondientes entradas de la FAT

El último campo contiene la información de cuántos bytes ocupa ese archivo.

Zona de datos

La zona de datos es donde finalmente van a ser almacenados los archivos y programas de los usuarios, y es la parte que sigue a continuación del área del sistema, prolongándose hasta el final del disco

En discos flexibles coincide el tamaño de un cluster con el tamaño de un sector En discos duros, el tamaño de un cluster suele ser de cuatro sectores

El DOS organiza la información en la zona de datos por clusters numerados secuencialmente, iniciando en todos los tipos de discos por el cluster 2, en consecuencia, el último cluster tendrá asignado un número que es mayor en uno al realmente existente, como espacio disponible para almacenamiento en el disco

Discos duros

Un disco duro es un dispositivo con alta capacidad de almacenamiento, es similar a los discos flexibles en varios aspectos En la actualidad los discos duros tienen una capacidad desde 20 Mb hasta 1 ó 2 Gigabytes; debido a esto, su manejo es un poco más complicado.

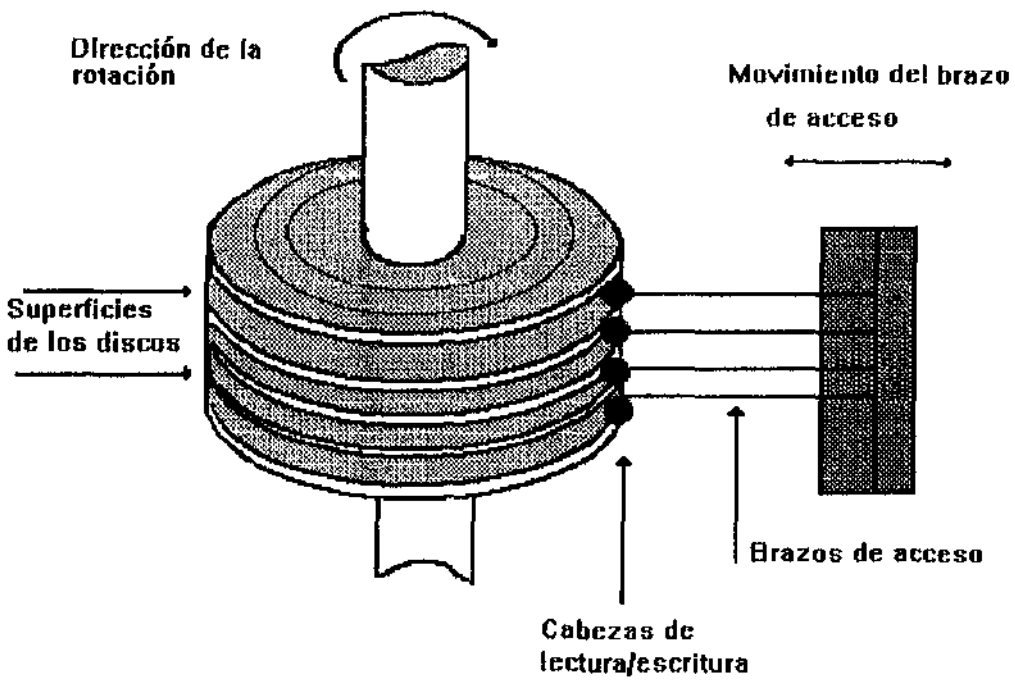
Físicamente un disco duro consta de varios platos rígidos y cabezas de lectura / escritura (una para cada lado de cada plato), situados en planos paralelos entre sí y con el mismo eje, encerrados en una caja sellada Se emplean brazos de acceso múltiples y cabezas de lectura / escritura en este tipo de discos. Los brazos se mueven al unísono hacia adentro y hacia afuera, entre los discos individuales. Frecuentemente se montan dos cabezas en cada brazo, para tener acceso a dos superficies (ver figura A 7) Debido a que los discos duros almacenan tanta información, sus superficies magnéticas son de alta calidad y su velocidad de rotación es mucho más alta en comparación con la de los discos flexibles (300 rpm contra 3600 rpm).

Para formatear un disco duro se requieren de tres pasos separados.

1) Realizar un formateo a bajo nivel Divide al disco en cilindros (es el equivalente de los tracks de los discos flexibles) y sectores Un disco duro típico tiene aproximadamente trescientos cilindros y diecisiete sectores por cilindro. El número de platos, el número de cilindros por plato y el número de sectores por cilindro determina el total de almacenamiento disponible en el disco.

2) El siguiente paso es particionar el disco usando el comando FDISK del DOS. Un disco duro puede ser dividido en una o más particiones, a cada una de las cuales se les asignará una letra comenzando por la C

Figura A 7 Disco duro



Fuente Sanders, 1988

Efectuar la partición de un disco duro es distinto a darle formato. Al hacer la partición de un disco se especifican las secciones del disco que podrá utilizar el DOS u otro sistema operativo Al dar formato al disco, el DOS prepara la partición existente para recibir archivos Es decir, que después de haber hecho la partición de un disco, todavía será necesario dar formato a cada partición antes de poder utilizarla.

FDISK graba la información del tamaño de la partición en el Master Boot Record (MBR primer sector de arranque), el cual indica dónde comienza el sistema operativo en el disco, qué tan grande es y si se encuentra activo. El MBR se almacena en el primer sector del disco Este comando sólo funciona en discos duros físicamente instalados, por lo tanto un disco flexible no puede ser particionado

3) Después de particionar el disco, se lleva a cabo un formateo a alto nivel con el comando FORMAT del DOS, el mismo programa para formatear un disco flexible. FORMAT crea el sector de carga del DOS y la FAT para cada partición del DOS. La partición primaria, generalmente el boot del drive C, contiene los archivos del DOS necesarios para cargar la computadora. Cada partición tiene también un directorio raíz como los discos flexibles

APENDICE B. ARCHIVOS

Un archivo es una unidad lógica de información en la que se almacenan programas o datos fuertemente relacionados entre sí, el significado de estos datos y su relación están definidos por el usuario.

Cuando se crea un archivo, se le da un nombre, que será la única referencia necesaria; para acceder posteriormente a los datos contenidos en él no hace falta saber su ubicación concreta dentro del disco La longitud de un archivo es variable y su contenido puede ser modificado cuando se necesite añadir nuevos datos al mismo. El tipo de información que contiene y el formato de los datos en su interior, son definidos por el usuario

Los nombres de los archivos identifican su contenidos Las extensiones ayudan a identificar qué tipo de archivo es. Cuando se crea un archivo, se puede elegir una extensión que ayude a su identificación La extensión no debe tener más de tres caracteres. La mayor parte de los programas que crean archivos añaden una extensión. Es recomendable usar dicha extensión.

El sistema operativo sólo conoce dos tipos de archivos: de programas y datos. Para el DOS, todos los archivos con extensión .EXE o COM son programas, y el resto son archivos de datos

Archivos .EXE

Estos archivos no pueden ser ejecutados inmediatamente después de ser cargados, pues el sistema operativo necesita realizar unas operaciones previas a su ejecución. Contienen un área al comienzo que se denomina "campo de encabezamiento" (header), el cual contiene información sobre ciertos parámetros que el DOS necesita para poder ejecutar el programa. El tamaño de esa área varía según el número de instrucciones que deban ser reubicadas durante la carga del programa. Antes de ceder el control al programa .EXE que se va a ejecutar, el DOS comprueba que éste contenga código ejecutable.

El tamaño de los archivos con extensión .EXE sólo esta limitado por el tamaño de la memoria de la máquina Al ejecutar un programa de este tipo, el código del programa, los datos y la pila se sitúan en segmentos distintos. El código del programa se sitúa a continuación del Prefijo del Segmento del Programa.

Archivos .COM

Los archivos COM son más compactos y rápidos que los programas EXE, puesto que no contienen información de reubicaciones y pueden tener una longitud máxima de 65,536 bytes (el tamaño de un segmento de memoria); menos la longitud del Prefijo de Segmento del Programa (PSP) que son 256 y una palabra (2 bytes) reservada para la pila de datos. El DOS no comprueba si los programas .COM contienen código ejecutable, como lo hace con los programas con extensión EXE Al ejecutar un programa .COM todos los registros de segmento de memoria apuntan al mismo segmento, que es el segmento que ocupa el código del programa, es decir, el código contenido en un archivo .COM es un fiel reflejo del código que se almacenará en memoria Lo único que se desconoce es la posición exacta dentro de la memoria donde estará ubicado.

APENDICE C. MEMORIA

La memoria provee de un almacenamiento temporal para programas y datos Físicamente es un chip existente en la tarjeta principal de la computadora Todos los programas deben ser cargados en la memoria para ser ejecutados

Toda la ejecución de programas y procesamiento de datos se realiza en la memoria Las instrucciones del programa son copiadas en la memoria desde un disco y después se les extrae de la memoria llevándoselas a un circuito electrónico para su análisis y ejecución.

Las instrucciones dirigen a la computadora para la introducción de datos a la memoria desde un teclado, disco o canal de comunicaciones

Cuando un dato entra en la memoria, el contenido previo de ese espacio de memoria se pierde Una vez que el dato está en la memoria, puede ser procesado (calculado, comparado y copiado). Entonces los datos pueden ser sacados desde la memoria a la pantalla, impresora, disco o canal de comunicaciones

Según Freedman (1994, Pág. 503) *"La memoria puede ser vista como un tablero electrónico con cada casilla del tablero conteniendo un byte de dato o instrucción. Puesto que cada cuadro tiene una dirección separada como una casilla de correo, el caracter individual dentro de la casilla puede ser manipulado independientemente del resto de las casillas. Debido a esto la computadora puede descomponer los programas en instrucciones y los registros de datos en campos, todos los cuales son almacenados como grandes bloques en discos "*.

La memoria permite que los datos sean desglosados y reordenados de cualquier manera prescrita (ver figura C 1.).

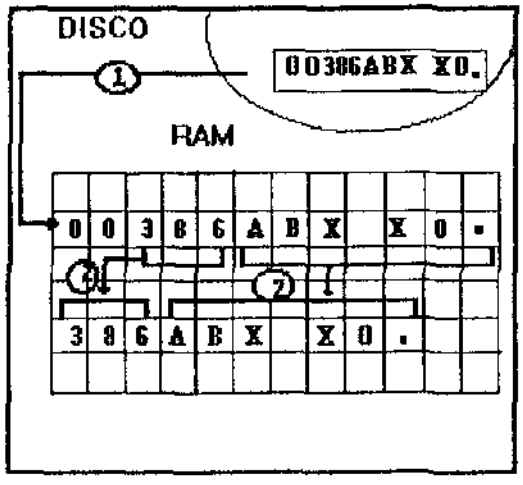
1) Un registro de datos completo es leído del disco y escrito en la memoria.

2) Los caracteres individuales son copiados del buffer de entrada al buffer de salida. A los datos numéricos se les eliminan los ceros precedentes con instrucciones de formato especiales que filtran los ceros no deseados

La computadora puede tener tres tipos de memoria·

- Memoria convencional
- Memoria extendida
- Memoria expandida

Figura C 1 Paso de datos del disco a la memoria de la computadora



Fuente Freedman, 1994

Memoria convencional

La memoria convencional es el tipo de memoria encontrada en todas las computadoras. La mayoría de las computadoras tienen al menos 256 Kb de memoria convencional y puede crecer a 640 Kb.

Las primeras computadoras sólo podían accesar 1 Mb de memoria RAM, de los cuales 382 Kb se reservan para el hardware y es conocida como *memoria alta*. En este espacio se encuentra la memoria del BIOS, del video y de otras tarjetas de expansión. Por lo general esta área no está ocupada (físicamente) en su totalidad por memoria; se diseñó con un espacio disponible en el cual las tarjetas de expansión pudieran colocar sus extensiones al BIOS, áreas de memoria para video, o para transferencia de datos a dispositivo Los 640 Kb inferiores se dedicaron al sistema operativo y a los programas del usuario Estos 640 Kb se conocen como la memoria convencional.

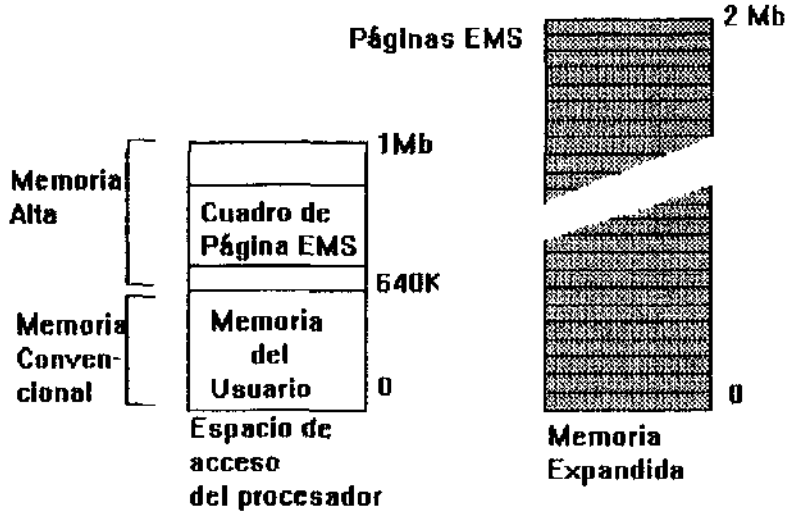
Para que la computadoras pudieran accesar a más de 1 Mb de memoria, se inventó la memoria expandida

Memoria expandida

Según PC Magazine en Español (Octubre 1993, Págs 92-93) *La figura C.2. muestra cómo trabaja la memoria expandida. El rectángulo de la izquierda representa 1 Mb de espacio de*

dirección al que el CPU puede tener acceso directamente. La memoria convencional se extiende de 0 Kb a 640 Kb, y la memoria alta se extiende desde 640 Kb a 1 Mb. El rectángulo en la derecha de la figura representa 2 Mb de memoria expandida, dividido en ciento veintiocho páginas de 16 Kb igualmente espaciadas. La clave es el espacio de 64 Kb reservado en la memoria alta para que sirva de marco de página de memoria expandida. El marco de página tiene espacio para cuatro páginas de memoria expandida de 16 Kb. Haciendo llamadas a un manejador, un programa de aplicación puede mapificar cualquiera de las cuatro páginas en el marco de página. La memoria expandida que se mapifica en el marco de página se puede leer y escribir, como si fuera la memoria normal. Enviando y recibiendo páginas del marco de página, un programa puede tener acceso a todas las páginas de memoria expandida que se le asignaron Otra manera de verlo es pensar que el marco de página sirve como una ventana para llegar a la memoria expandida. No puede tener acceso a toda la memoria de una vez, pero sí puede tener acceso a toda la memoria, enviando y recibiendo páginas, poco a poco, por medio de la ventana.

Figura C.2. Memoria expandida



Fuente: PC Magazine en Español, Octubre 1993.

Un punto importante que hay que tener en cuenta, es que no todos los programas pueden usar la memoria expandida, deben estar escritos especialmente para aprovecharla

La memoria expandida puede agregarse a cualquier computadora, aun a las máquinas con procesadores 8086 y 8088 Aunque las tarjetas de memoria expandida ya no son tan comunes, la memoria expandida está a la disposición hoy en día, porque las versiones 5.0, 6.0 y 6 2 del sistema operativo vienen con un manejador de memoria expandida (EMM386 EXE) que convierte la memoria extendida que se encuentra en las máquinas 386 y 486 a memoria expandida

Memoria extendida

Si bien la memoria expandida puede que ya no sea tan común, la memoria extendida sí lo es La memoria extendida se define como toda la RAM por encima de 1 Mb en las computadoras 286, 386 y 486. En apariencia, un programa de aplicación que quiera utilizar la memoria extendida para almacenar datos debe pasar mucho trabajo para hacerlo.

En primer lugar, el DOS no administra la memoria extendida como lo hace con la memoria convencional, así que es difícil para el programa poder saber cuándo es que otro programa está usando la memoria extendida que desea.

Los programas que quieran usar memoria extendida para almacenar datos pueden hacerlo si invocan los servicios de un administrador o manejador de memoria extendida (XMM), el cual se ocupa de los detalles asociados con la entrada y salida de los datos.

La mayoría de los programas que utilizan memoria convencional, no pueden usar memoria expandida, debido a que los números o direcciones que identifican posiciones dentro de la memoria extendida para los programas, son superiores a los que pueden reconocer. Los programas necesitan instrucciones especiales para reconocer las direcciones superiores de la memoria extendida.

Frecuentemente, a la memoria extendida colocada bajo el control de un XMM se le conoce como memoria XMS. Como la memoria expandida, la memoria extendida no se distribuye automáticamente a los programas. Para usarla, un programa tiene que decidirse a hacerlo, y tomar medidas especiales. Por lo tanto, no todos los programas usan la memoria XMS, pero el número de programas que sí lo hacen aumentan a diario.

APENDICE D. LISTADO DEL TUTORIAL

Los listados del programa así como los códigos fuentes y ejecutables se encuentran en poder de la Escuela de Sistemas Computacionales, para cualquier consulta o aclaración.

GLOSARIO

.EXE, .COM: Es la extensión de los archivos ejecutables Si se teclea el nombre del archivo sin la extensión, se ejecutará el programa.

.DRV: Es la extensión de una rutina de programación que contiene las instrucciones necesarias para controlar la operación de un dispositivo periférico

.OVL, .OVR: Es la extensión de los archivos overlays (traslape) Los archivos overlays permiten que un programa sea ejecutado en una computadora con menos memoria principal que el tamaño total del programa a ejecutar

.SYS: Es la extensión de los archivos en lenguaje máquina que son parte del sistema operativo o de otro programa de control. Puede referirse también a un archivo de configuración utilizado por tales programas.

Antivirus: Programas que tienen la finalidad de prevenir, detectar y erradicar virus

Archivo: Cualquier colección de datos que es tratada como una sola unidad en un dispositivo periférico. Conjunto de clusters necesarios para guardar la información

ASCII: American Standard Code for Information Interchange: Código estándar *americano para intercambio de información* Es un código de siete bits que permite ciento veintiocho combinaciones posibles de caracteres, de las cuales las primeras treinta y dos se usan para el control de impresión y transmisión. Como la unidad corriente de almacenamiento es el byte de ocho bits (doscientas cincuenta y seis combinaciones), y ASCII utiliza sólamente ciento veintiocho, el bit extra se usa como un bit de paridad o para símbolos especiales.

Atributo: Información que es contenida en el directorio de un disco y que clasifica el acceso a un determinado archivo. Los atributos típicos son leer / escribir, sólo lectura, archivo y oculto.

AUTOEXEC.BAT: AUTOmatic EXEcute BATch file (archivo por lotes de ejecución automática). Archivo del MS-DOS™ que si está en el directorio raíz, es ejecutado cada

vez que se arranca la computadora Contiene una lista de programas que se necesitan o se quieren ejecutar cada vez que enciende la computadora

BBS: Bulletin Board System (boletín informativo); su propósito es actuar como medio para el intercambio de datos (y a menudo, programas), por medio de PCs, módem y vía telefónica

Bit: Dígito binario. Un dígito simple de un número binario (1 ó 0). En la computadora, un bit es físicamente una celda de memoria (constituida por transistores o un transistor y un condensador), un punto magnético en un disco o una cinta, o un pulso de alto o bajo voltaje viajando a través de un circuito. Conceptualmente, un bit se puede pensar como una lámpara eléctrica, encendida o apagada Grupos de bits forman unidades de almacenamiento en la computadora, llamadas caracteres, bytes o palabras, que son tratados como un grupo. La unidad de almacenamiento más común es byte, constituido por ocho bits y equivalente a un caracter alfanumérico

Boot: Area del disco, en el cual se encuentra un programa escrito en lenguaje máquina que inicia el proceso de arranque de la computadora.

Checksum: Ver suma de verificación.

CHKDSK: Una utilidad del DOS que verifica el estado de un disco. También informa sobre la cantidad de memoria disponible.

Cilindro: Se llama cilindro al conjunto de pistas situadas perpendicularmente en la misma posición. En el caso de un disco flexible sólo hay dos caras, por lo que cada cilindro está formado por dos pistas, una colocada en el lado 0 y la otra en el lado 1.

Cluster: Es un grupo de sectores que es la mínima cantidad de espacio de almacenamiento que DOS puede asignar y utilizar. El número de sectores por cluster depende del tipo de disco que se utilice.

CMOS: Banco de memoria pequeña por batería en computadoras personales AT, que se utiliza para almacenar parámetros como hora, fecha, tipo de unidades, etc.

Código de identificación: Grupo de bytes utilizados para identificar un virus.

COMMAND.COM: Es el intérprete de comandos del sistema operativo MS-DOS™, contiene los comandos internos DIR, DEL, COPY, etc.

Correo electrónico: Telecomunicación de correspondencia entre puntos distantes Los sistemas de correo electrónico se implementan en redes de área local de

macrocomputadoras, minis y computadoras personales Los usuarios pueden enviar correspondencia a un receptor único o transmitirla a muchos usuarios del sistema Los sistemas sofisticados pueden invitar a los receptores a enviar una réplica si es que no han respondido dentro de un cierto marco de tiempo Con estaciones de trabajo multitarea, la correspondencia puede ser repartida y anunciada mientras el usuario está trabajando en una aplicación De lo contrario, la correspondencia es enviada a una casilla postal simulada en la computadora servidora de una red o en la computadora anfitriona, las cuales deben ser interrogadas por el receptor.

DES: Data Encription Standard (Estándar de cifrado de datos) Es un método de encriptación de datos, una técnica de cifrado estándar de NIST que embrolla los datos en un código impenetrable para la transmisión en una red pública Utiliza un número binario como clave de cifrado que ofrece más de setenta y dos cuatrillones de combinaciones. El número, que puede ser elegido al azar para cada transmisión, es usado como un patrón para convertir los bits en ambos extremos de la transmisión.

Directorio: Lista completa de archivos almacenados en disco. Los directorios crean la ilusión de compartimientos separados, pero son en realidad índices que apuntan a los archivos, los cuales pueden estar físicamente dispersos.

Disco o diskette: Son dispositivos para almacenar los programas del usuario. Físicamente el disco está dividido en anillos concéntricos o pistas, y cada pista en sectores o zonas donde almacenan centenares de bits de datos, que se manejan en grupo Cada vez que se accesa el disco para extraer o introducir información en él, se lee o escribe un sector entero a la vez.

DOS: Disk Operating System (Sistema operativo en disco).

Download: Descargar, bajar. Transmitir datos desde una computadora central a una computadora remota o desde un servidor de archivos a una estación de trabajo. Implica la transferencia de un archivo completo, más que la interacción a uno y otro lado en forma conversacional.

EEPROM: Electronically Erasable Programmable Read Only Memory (memoria de sólo lectura programable y borrable electrónicamente). Un chip de memoria que retiene su contenido sin potencia Puede ser borrado, tanto dentro de la computadora como externamente, y usualmente requiere más voltaje para el borrado que el común +5 voltios usado en los circuitos lógicos. Funciona como RAM no volátil, pero grabar en EEPROM es mucho más lento que grabar en RAM

EMM: Expanded Memory Manager (Administrador de memoria expandida). Controlador de software para PC que administra la memoria expandida En máquinas

8086 y 286, deben instalarse placas de memoria expandida En máquinas 386 o superiores el hardware tiene la capacidad de memoria expandida incorporada y sólo requiere el controlador o el administrador de memoria para activarla

EMS: Expanded Memory Specification (Especificación de memoria expandida). Una técnica para expandir la memoria más allá de un megabyte en PCs bajo DOS La versión 4 0 de EMS incrementa el total de memoria con la que las aplicaciones de DOS pueden trabajar desde uno a 32 Mb, suministrando una capacidad de conmutación de bloques que permite a segmentos de la memoria convencional apuntar a la memoria EMM En máquinas 8086 y 286, el EMS se instala conectando una placa de memoria EMS y agregando un controlador EMS al DOS. En máquinas 386 y superiores, el EMS es activado agregando un controlador de software llamado EMM.

EPROM: Erasable Programmable Read Only Memory. Son un tipo de microchip utilizado para almacenar datos incambiables Los chips pueden ser borrados sólamente con rayos ultravioleta

FAT: File Allocation Table (tabla de asignación de archivos) La parte del sistema de archivos del DOS y que lleva la cuenta de dónde están almacenados los datos en un disco Tiene la lista completa de clusters que ocupa cada archivo. Esta tabla se encuentra duplicada.

FDISK: Comando del DOS que particiona el disco duro en varios discos independientes La utilización del comando FDISK con la opción /MBR permite reconstruir la tabla de partición de los discos duros Esta medida es recomendable sólo cuando se tiene un virus de sector de arranque o tabla de partición

Gusano: Es un programa de computadora diseñado para "deslizarse" a través de la memoria o los discos de la computadora, alterando los datos que encuentra

Hacker: Nombre dado a una persona que accesa ilegalmente un sistema computacional. Dedica su tiempo a penetrar, a través del teléfono y desde una computadora situada en su propio domicilio, en sistemas informáticos en los cuales no está autorizado para acceder, bien con el fin de experimentar, bien por pura diversión o por afán de lucro

Hardware: Es el conjunto de elementos materiales y circuitos electrónicos de una computadora

IBMBIOS.COM: Basic Input / Output System. serie de programas básicos almacenados de forma permanente en la memoria interna de la computadora, que permiten al procesador controlar cada dispositivo periférico.

IBMDOS.COM: Es el programa que controla la ejecución de los archivos del disco

Inocular: Un método de protección de archivos contra infecciones de virus, insertando un "código de identificación" en el archivo Esta no es una buena forma de protección contra la acción de muchos virus

Interrupción: Es el método que el sistema operativo utiliza para señalar al procesador que hay una tarea a ser realizada.

Mainframe: Macrocomputadora. Se refiere a un gran sistema de computación, de aplicación general, donde el CPU es el centro de la mayoría de las actividades de procesamiento. Hay macrocomputadoras de escala pequeña, media y grande, manejando desde un manojo a varios miles de terminales en línea Las macrocomputadoras de gran escala pueden tener centenares de megabytes de memoria principal y centenares de gigabytes de almacenamiento en disco Las macrocomputadoras de media y gran escala utilizan computadoras más pequeñas como procesadores frontales que se conectan directamente a las redes de comunicaciones

MBR: Master Boot Record (primer sector de arranque), Indica dónde comienza el sistema operativo en el disco, qué tan grande es y si se encuentra activo El MBR se almacena en el primer sector del disco

Megabyte (Mb): Utilizado algunas veces para significar 1,000,000 bytes, pero en realidad son 1,048,576 bytes. Se utiliza como una medida de la memoria de una computadora o de la capacidad de los discos

Memoria: Almacenamiento de trabajo de la computadora, que físicamente es una colección de chips RAM. Es un recurso importante de la computadora, debido a que determina el tamaño y el número de programas que pueden ejecutarse al mismo tiempo, como también la cantidad de datos que pueden ser procesados instantáneamente

Módem: MOdulator-DEModulator (modulador-demodulador) Un dispositivo electrónico que adapta interna o externamente una computadora a una vía telefónica. Convierte los pulsos digitales de la computadora a frecuencias dentro del rango de audio del teléfono y los vuelve a convertir en pulsos en el lado receptor.

NIST: National Institute of Standards & Tecnology (Instituto Nacional de Normas y Tecnología) Es la agencia de definición de normas y estándares del gobierno de los Estados Unidos, anteriormente llamada National Bureau of Standards

Piratería: Copias ilegales de programas

Programa o software: Detallado conjunto de instrucciones, realizado por personas para dirigir a la computadora y que ésta funcione de manera que produzca el resultado deseado

Programa residente en memoria: Algún programa que, una vez cargado, realiza sus acciones y las termina pero no se quita de la memoria, y que puede volver a ejecutarse pulsando una secuencia de teclas.

PROM: Programmable Read Only Memory (memoria programable de sólo lectura) Un tipo de chip de memoria que contiene información que es programada por el cliente, en lugar de por el fabricante de chips

Protocolo de comunicación: Es un conjunto de normas y regulaciones que gobiernan la transmisión y recepción de datos

RAM: Random Access Memory (memoria de acceso aleatorio) Es lo mismo que memoria

Reluctancia: Resistencia de un circuito al flujo magnético

ROM: Read Only Memory (memoria de sólo lectura) Microchip de memoria especial dentro del cual la información es grabada (desde el momento de su fabricación) de manera que no puede ser cambiada o alterada.

RSA: (Rivest-Shamir-Adleman) Método de codificación (encriptación) de muy alta seguridad de RSA Data Security, Inc. Redwood City, CA, que utiliza una clave con dos partes La clave privada la guarda el propietario, la pública es la que utilizan los usuarios destinatarios Al codificar datos se utiliza la clave pública del destinatario, que sólo se puede descifrar por la clave privada del destinatario RSA es un cálculo muy intensivo, de esta forma se utiliza a menudo para crear un Digital Envelope (sobre digital), que mantiene una clave DES cifrada en RSA y datos cifrados en DES.

Sector: Cuando un disco es formateado, es dividido en círculos concéntricos Cada círculo es entonces subdividido en sectores Un sector normalmente tiene capacidad para 512 bytes de información

Sector boot: sector de inicialización o sector de arranque. Area del disco que contiene instrucciones y/o datos que hacen que la computadora localice y cargue el sistema operativo. Normalmente es el primer sector de la partición del disco.

Sistema operativo: Serie de programas internos que tienen como misión regular el funcionamiento de la computadora Facilita al usuario el manejo del equipo, gestionando los detalles internos, facilita a los programas del usuario el acceso a los distintos periféricos, a través de una serie de rutinas de servicio, y asegura que el funcionamiento de la computadora sea lo más eficiente posible.

Suma de verificación: Checksum. El valor numérico total de un bloque de datos, que se utiliza con propósitos de verificación de errores. Tanto los datos numéricos como los alfabéticos pueden utilizarse para calcular sumas de verificación, debido a que se puede sumar el contenido binario de los datos. Así como el dígito de verificación comprueba la precisión de un número único, una suma de verificación sirve para controlar todo un conjunto de datos transmitidos o almacenados. Las sumas de verificación pueden detectar tanto los errores en un único bit como algunos errores en múltiples bits.

Upload: Levantar. Transmitir datos de una computadora personal o una estación de trabajo a una computadora central o un servidor de archivos Levantar implica la transmisión de un bloque de datos completo, más que una sesión interactiva

Virus: Es un programa que se intercala dentro de otros, tomando el control del sistema operativo y capaz de propagarse creando duplicados de sí mismo.

Virus stealth: Virus que intentan esconderse por sí mismos eliminando señales de su presencia cuando están en memoria. Por ejemplo, si un comando DIR es realizado en una computadora donde un virus stealth está activo, reducirá el tamaño de los archivos infectados por el número de bytes que originalmente tienen los archivos.

XMM: eXtended Memory Manager (Administrador de memoria extendida). Evita que diferentes programas utilicen la misma parte de memoria extendida al mismo tiempo, y facilita que los programas utilicen la memoria extendida. MS-DOS™ incluye el administrador de memoria extendida HIMEM.SYS. HIMEM conforme a la versión 2.0 de Lotus™ / Intel™ / Microsoft / AST™ eXtended Memory Specification (XMS), especifica una forma estándar para que los programas utilicen la memoria extendida cooperativamente.

XMS: eXtended Memory Specification (Especificación de memoria extendida). Interfaz que permite a los programas DOS utilizar la memoria extendida de los equipos 286 o superiores. Si se tiene un sistema 80386 ó 80486 con memoria extendida y se utilizan programas que pueden tomar ventaja de la memoria expandida, se puede instalar EMM386.EXE. EMM386 es un driver que puede utilizar memoria extendida para simular memoria expandida.

BIBLIOGRAFIA

Compumundo 92
Apuntes del Taller de Virus Informáticos

Devorak, John C / Kane, Pamela
VIRUS Protection: Vital Information Resources Under Siege
Editorial Bantam Computer Books, 1989

Ferreyra Cortés, Gonzalo
Virus en las computadoras
Editorial Macrobit, 1991

Fites, Philip / Johnston, Peter / Kratz, Martin
The Computer Virus Crisis
Editorial Van Nostiand Reinhold, 1991

Freedman, Alan
Diccionario de Computación
Editorial Mc-Graw-Hill, 1994

Haynes, Colin
The Computer Virus Protection Handbook
Editorial SYBEX, 1989

H Baker, Richard
Computer Securiry Handbook
Editorial Mc-Graw-Hill, 1991

J Denning, Peter
Computer Under Attack. Intruders, worms and viruses
Editorial Addison Wesley, 1991

Levin, Richard B
Virus Informáticos: Tipos Protección Diagnosis Soluciones
Osborne Mc-Graw-Hill, 1991

L Mayo, Jonathan
Computer Viruses. What they are, how they work, and how to avoid them
Editorial Windcrest, 1989

Lundell, Allan
VIRUS! The Secret World of Computer Invaders That Breed and Destroy
Editorial Contemponay Books, 1991

Nieto, Pablo / Mur, Alfonso / Molina, Jesús
Virus Informáticos
Editorial Anaya Multimedia, S A , 1991

Nombela, Juan José / del Pino González, Luis M. / del Pino González, Javier
Virus Informático
Editorial Paraninfo, S.A , 1990

Norton, Peter / Nielsen, Paul
Inside the Norton Antivirus
Editorial Brady Publishing, 1993

Solomon, Dr, Alan / Kay, Tim
Dr. Solomon's PC Anti-virus Book
Editorial New-Tech, 1993

VIRUS-L / comp virus
Frecuently Asked Questions
1992

V Feudo, Christopher
The Computer Virus: Desk Reference
Editorial Business One Irwin, 1992

Publicaciones periódicas:

Computerworld México
Varios volúmenes

PC Magazine en Español
Varios volúmenes

PC World
Varios volúmenes

Personal Computing-México
Varios volúmenes

Otras referencias

Central Point Software
Manual Central Point Antivirus

Dittrich, Stefan
Acceso Rápido Visual Basic
Editorial Computec Marcombo, 1993

Maluf de Carvalho, José Eduardo
Microsoft Visual Basic
Serie Mc-Graw-Hill de Informática, 1992

McAfee Associates
Manual VirusScan

Microsoft
Manual MS-DOS 5.0

Microsoft
Manuales Visual Basic Profesional versión 3.0

Nelson, Ross
Guia completa de Visual Basic para Windows
Editorial Mc-Graw-Hill, 1994

Sanders, Donald H.
Informática Presente y Futuro
Mc-Graw-Hill, 1888

Symantec
Manual Norton Antivirus