MINISTERIO DE DESARROLLO AGROPECUARIO
INSTITUTO NACIONAL DE AGRICULTURA
DR. AUGUSTO SAMUEL BOYD
DIVISA

SEMINARIO:

INTRODUCCIÓN AL USO DE COMPUTADORAS, SISTEMA OPERATIVO WINDOWS 3.1, EXCEL 4.0 Y WORDPERFECT 5.1 PARA MS-DOS

CONFERENCIA: ***DETECCIÓN DE VIRUS Y RECUPERACIÓN DE ARCHIVOS BORRADOS BAJO WINDOWS 3.1.***

EXPOSITOR: ***RAÚL ENRIQUE DUTARI DUTARI.***

FECHA: ***5 DE OCTUBRE DE 1993.***

HORA: ***8:00 A. M.***

LUGAR: ***OFICINA DEL DEPARTAMENTO DE PLANIFICACIÓN Y EVALUACIÓN DEL INSTITUTO NACIONAL DE AGRICULTURA.***

DIRIGIDA A: ***PERSONAL TÉCNICO Y ADMINISTRATIVO DE LA INSTITUCIÓN.***

DURACIÓN: ***2 HORAS.***

OBJETIVOS GENERALES

1. Crear conciencia del problema que representan los virus informáticos en el desarrollo de las ciencias computacionales.

2. Conocer algunas generalidades básicas acerca de los virus informáticos.

3. Crear conciencia acerca de la importancia que tiene el respaldo de la información, como medio seguro de salvaguardar la información.

4. Conocer algunas nociones fundamentales acerca del borrado y recuperación de archivos bajo Windows 3.1.

OBJETIVOS ESPECÍFICOS

1. Comprender, la manera en que el sistema operativo MS-DOS almacena la información en los medios de almacenamiento permanentes.

2. Conocer en que consisten los virus informáticos.

3. Definir las formas de acción que caracterizan a los virus informáticos.

4. Determinar los posibles daños que pueden provocar los ataques de los virus informáticos, en un sistema.

5. Conocer algunos mecanismos de protección contra los ataques de virus informáticos, utilizando las herramientas incluidas en el sistema operativo MS-DOS y en el Windows 3.1.

6. Determinar el procedimiento que sigue el sistema operativo MS-DOS al borrar un archivo.

7. Conocer algunos mecanismos de acción limitada para recuperar archivos borrados, que se incluyen en el sistema operativo MS-DOS y en el Windows 3.1.

TABLA DE CONTENIDOS

1. Observaciones Preliminares.

En la actualidad, existen dos problemas serios para todos aquellos que trabajan regularmente con computadoras, y que en un momento dado, pueden representar pérdidas importantes de información, de manera definitiva. Nos referimos a los virus informáticos y el borrado de archivos en el sistema.

Los virus informáticos son un fenómeno del cual se ha hablado mucho en la prensa y entre los usuarios de computadoras. No obstante lo mucho que se ha escrito y hablado a respecto, la información objetiva y veraz acerca del tema dista mucho de ser satisfactoria (y comprensible) para el usuario común de computadoras.

Se supone, que se comportan dentro de la computadora de una manera similar a la de los virus biológicos, al punto que mucha de la terminología que se utiliza para referirse a ellos, proviene del área de las Ciencias Biológicas.

Sin embargo, todos somos consientes que ellos representan un peligro latente contra nuestra información. Más de una persona que nos rodea conoce esta situación en carne propia, cuando todo o parte de su trabajo ha sido destruido su acción.

Por otro lado, un fenómeno similar de falta de información veraz y objetiva se presenta frente al problema más común que enfrentan los usuarios de las computadoras: el borrado o eliminación de los archivos, ya sea de manera accidental o intencional.

Lo más grave en ambos casos, es que el usuario promedio no sabe que ambos problemas, pueden ser controlados de manera casi absoluta, en la

mayoría de los casos, siguiendo algunas normas sencillas de uso seguro de las computadoras.

En tal sentido, esta conferencia pretende brindar al auditorio, una breve introducción a los temas antes mencionados, buscando realizar un acercamiento paulatino al tema, con el objeto de que el usuario común pueda comprender cómo se debe actuar frente a estos dos problemas, que tarde o temprano, debe confrontar todo usuario de las computadoras. Así, iremos intercalando en la exposición conceptos, definiciones, explicaciones y consejos acumulados a través de nuestra experiencia en el campo de la informática, con respecto a ambos temas.

Aunque los temas centrales de la ponencia son las herramientas antivirus y para recuperar archivos borrados de MS-Windows, eso no impedirá que, se agregue consejos adicionales acerca de otros tópicos del software, con el objeto de que este documento resulte de la mayor utilidad para todos sus posibles lectores.

2. Procedimiento General, De Almacenamiento De Información En Los Medios De Almacenamiento Permanentes, En El Sistema Operativo MS-DOS.

Para comprender mejor ambos temas (virus informáticos y eliminación de archivos en el sistema operativo), debemos conocer, el mecanismo que utiliza el sistema operativo para almacenar información dentro de los discos, a nivel físico y lógico.

2.1. Organización Física De Los Discos Flexibles Y Fijos.

La organización física de los discos fijos y flexibles es, fundamentalmente, la misma. En ambos casos, los datos y la información son almacenados dentro del disco a través de alteraciones magnéticas que sufre la superficie, a nivel de su polaridad, a las que se les asigna una información única (0 o 1, de allí el origen del sistema binario que utilizan las computadoras). Estas superficies son subdivididas, progresivamente, en cabezas, cilindros, sectores.

2.1.1. Cabezas, Caras O Superficies De Lectura/Escritura.

Esencialmente, constan de una o más superficies que se pueden magnetizar fácilmente. Cada una de estas superficies es magnetizada por una cabeza de lectura escritura, similar a las de las grabadoras de audio. Usualmente, se habla de manera indiscriminada de las superficies de lectura escritura del disco, o de sus cabezas.

2.1.2. Cilindros O Pistas.

Los campos magnéticos que se mencionaron previamente, son registrados en circunferencias concéntricas. Todas las superficies que son alcanzadas por las cabezas en un momento dado, son denominadas cilindros o pistas

2.1.3. Sectores.

Cada cilindro es dividido en una cantidad fija de secciones circulares, de igual tamaño. Estas secciones son denominadas, sectores y son la cantidad

mínima de información que puede leerse o escribirse en el disco, en una única acción del sistema.

2.2. Distribución Lógica De La Información Dentro De La Superficie De Los Discos Flexibles Y Fijos.

Para que el sistema operativo pueda utilizar eficientemente el disco, para almacenar información se requieren, adicionalmente a las estructuras físicas que lo sustentan a nivel electromagnético, estructuras lógicas de información que nos permitan manipular la información a nivel del sistema operativo.

Estas estructuras lógicas consisten en una tabla o índice que indica, en todo momento, las características de cada uno de los sectores del disco. Adicionalmente, las estructuras lógicas dentro del disco nos indican cómo está organizada la información dentro del mismo.

El conjunto de estructuras de información que almacenan los datos en el disco, así como la tabla de organización de la misma dentro del disco, se denomina formato lógico.

Cuando realizamos el formato del disco a nivel del sistema operativo, se realiza su formato lógico. En ese momento se definen dos zonas especiales dentro del disco: el área del sistema y la zona de datos.

2.2.1. El Área Del Sistema.

Existen una serie de sectores del disco flexible o fijo, que tienen un significado especial para el sistema. Ellos son:

- El sector de arranque.
- La tabla de localización de archivos.

2.2.1.1. El Sector De Arranque.

El sector de arranque es siempre el primer sector del disco flexible. En él esta la información necesaria para que informar al sistema si el disco en mención permite inicializar el sistema o no. No se puede ubicar en otro lugar del disco. Si por alguna razón se daña este sector en un disco, disquete debe ser eliminado, pues no se puede remediar esta situación.

En los discos duros, el primer sector contiene la información necesaria para ubicar al sistema en cuanto a cual es la sección del disco duro que se está utilizando, y donde está ubicado el correspondiente sector de arranque.

2.2.1.2. La Tabla De Localización De Archivos.

La tabla de localización de archivos, mejor conocida como F.A.T., es la tabla o índice antes mencionado, en ella se registran en todo momento:

- La cantidad de espacio libre de información, dentro del disco.
- Cuales sectores y racimos están ocupados o vacíos y donde están ubicados dentro del disco.
- Cuales partes del disco no pueden ser utilizadas para almacenar información, por estar defectuosas o dañadas.

2.2.2. La Zona De Datos.

La zona de datos, es el conjunto de sectores del disco duro donde se ubican las estructuras de datos que nos permiten almacenar la información útil dentro del disco.

3. Los Virus Informáticos.

A continuación haremos referencia al problema de los virus informáticos, tratando de mantener nuestra discusión dentro de los conceptos teóricos previamente ilustrados.

3.1. En Que Consisten Los Virus Informáticos.

Los virus informáticos son programas de computadora, escritos por programadores con amplia experiencia en el lenguaje ensamblador. Es decir, son conjuntos de instrucciones y datos que se ejecutan únicamente cuando están presentes en la memoria principal del sistema.

En tal sentido, no difieren mucho de cualquier otro programa que utilice el usuario promedio de las computadoras (hojas de cálculo, procesadores de palabras, bases de datos, etc.). Al igual que los paquetes comerciales, existe una gran variedad de virus informáticos, al punto que, a la fecha, se reportan más de 1800 virus identificados, aunque diariamente se reportan algunos más.

Estos programas tienen la característica de alterar internamente a los programas de computadora que contaminan, de modo que realicen acciones para las cuales no fueron diseñados originalmente. Estas acciones son, generalmente, de naturaleza autodestructiva frente a la información del sistema,

más no así frente a los equipos físicos que integran la computadora. Entiéndase: un virus, por lo general, no puede dañar el equipo físico de un sistema, sólo puede destruir su información.

Ahora, si estos programas pueden ser tan dañinos, la pregunta lógica es: ¿Porqué son creados?, pues sabemos que, de una u otra forma, los programas de computadora son creados por humanos. En tal sentido, no se puede dar una respuesta general que satisfaga todos los criterios. Sin embargo, podemos establecer algunos parámetros generales, que en conjunto, han provocado el fenómeno, a saber:

- **Pruebas del dominio de la programación:** De hecho, los primeros informes serios que existen acerca de programas que mostraran el comportamiento de los virus, proviene de la década de 1960. En esa época, los estudiantes avanzados de informática del Instituto Tecnológico de Massachusetts (M.I.T.), en sus ratos libres se distraían jugando “Core War”, un juego computacional de alta tecnología, que consistía en crear un programa capaz de infiltrarse en otra computadora, con el objeto de que el programa se autorreprodujera dentro de ella, hasta llenar la memoria del sistema y bloquearlo por completo. En 1984, el código fuente del juego fue impreso y comentado en una revista especializada y a partir de la fecha, es que se registra con más fuerza el fenómeno de los virus informáticos[1].

---

[1] NORTON, Peter y NIELSEN, Paul. Norton Antivirus. Traducido por Palmas Velasco, Oscar A. Primera edición. México D.F., México: Prentice Hall, 1993, página 14.

- **El movimiento punk cibernético:** La publicación de los códigos fuentes de los virus provocó que una serie de personas que tienen algún dominio de los lenguajes de programación (pero no tanto, como para llegar al nivel de los estudiantes del M.I.T.), y que tienen algún tipo de desorden mental, se dedican prácticamente a la creación de virus. Esta situación llega al punto que se les puede denominar como “programadores con malas intenciones”, y son mejor conocidos como “cracker”; se encuentran muy difundidos en Europa. Su obsesión es crear virus que sean cada vez más destructivos y difíciles de controlar[2].

- **Esquemas de protección:** Algunos programadores (muy pocos) crean los virus, y los distribuyen en copias ilegales de sus programas, con el objetivo de controlar la copia indiscriminada de sus productos y forzar a los usuarios a que les compren sus productos (que lógicamente, venden libres de virus). El ejemplo clásico nos lo da el caso del virus “Mente Paquistaní”[3].

- **Como un arma terrorista:** Algunas organizaciones terroristas se han servido de virus informáticos para atacar y hacer daño a los sistemas informáticos de los gobiernos contra los que luchan. Como ejemplo de ello, tenemos el virus “Jerusalén”, que fue

---

2 FERREYRA CORTÉZ, Gonzalo. Virus en las computadoras. Segunda edición. México D.F., México: Macrobit, 1991, página MF 4-6 y siguientes.

3 FERREYRA CORTÉZ, Gonzalo. Virus en las computadoras. Segunda edición. México D.F., México: Macrobit, 1991, página MF 4-3 y siguientes.

creado por la Organización para la Liberación de Palestina (O.L.P.), para destruir la información de los sistemas informáticos en todo Israel, el día 13 de mayo de 1988, en conmemoración del 40 aniversario de la desaparición del estado palestino[4]. Afortunadamente para el estado israelí, el virus fue detectado a tiempo y se pudo controlar. No obstante, se han reportado problemas similares en otros países con ese tipo de conflictos internos, como España.

- **Como arma político-militar:** Existen rumores (lógicamente, no confirmados) que la Agencia de Seguridad de los Estados Unidos desarrolla virus informáticos avanzados para ser empleados como armas de alta tecnología. De hecho, se especula que la espectacular ofensiva aérea que se dio a inicios de la Guerra del Golfo Pérsico, se debió a que los sistemas de radar de la defensa aérea de Irak quedaron virtualmente inutilizados por un virus informático, convenientemente infiltrado en sus computadoras[5].

---

4 NORTON, Peter y NIELSEN, Paul. Norton Antivirus. Traducido por Palmas Velasco, Oscar A. Primera edición. México D.F., México: Prentice Hall, 1993, página 70.

5 NORTON, Peter y NIELSEN, Paul. Norton Antivirus. Traducido por Palmas Velasco, Oscar A. Primera edición. México D.F., México: Prentice Hall, 1993, página 25.

3.2. Formas De Acción Que Caracterizan A Los Virus Informáticos.

Si como se ha mencionado previamente, los virus informáticos, similares a los programas que se utilizan comúnmente, surge la pregunta: ¿Cuales son las diferencias que existen entre los virus informáticos y los programas corrientes?

Las diferencias fundamentales que existen entre los virus informáticos y los programas de uso común (o aplicaciones), están en dos aspectos fundamentales:

- El procedimiento que siguen para activarse.
- Las acciones que realizan dentro del sistema.

3.2.1. Procedimiento Que Sigue Un Virus Para Activarse Dentro De Una Computadora.

Cuando utilizamos un programa común, tal como una hoja de cálculo o un procesador de palabras, el programa se activa solamente cuando el usuario se lo ordena al sistema, ya sea a través de una orden escrita en la petición de orden del sistema operativo (en los casos que se acostumbra trabajar con el MS-DOS), o a través de la activación de un icono que representa al programa (como es el caso más común dentro del MS-Windows 3.1).

En contraste, los virus generalmente se activan dentro del sistema de manera furtiva. El usuario que utiliza la computadora no se puede percatar de la intromisión. La intromisión puede realizarse por el procedimiento que explicaremos a continuación.

Es necesario que exista un disco infectado con el virus previamente para que la computadora pueda infectarse, o de lo contrario, no puede ocurrir la infección. Una vez se cumple esta premisa, el virus puede seguir, fundamentalmente, dos vías para infiltrarse en el sistema.

- Al ejecutar en el sistema un archivo que esté contaminado con el virus,

- Al provocar que el sistema se inicialize (que la computadora se inicia el proceso de carga del sistema operativo), provocando que la computadora lea el sector de arranque del disco (previamente infectado con el virus).

En ambos casos, el virus se aloja en la memoria de acceso aleatorio del sistema (R.A.M.), y se activa, manteniéndose en un estado oculto e inoperante, sin que el usuario común (desprevenido del problema) se percate.

3.2.2. Acciones Y Efectos De Un Virus Dentro De Un Sistema.

Una vez está activado un virus informático, el virus puede extenderse y atacar a muchos archivos en las unidades de disco conectadas al sistema. Luego, cuando ocurre un evento en particular, tal como una fecha u hora en especial, o un número específico de infecciones realizadas con éxito, el virus inmediatamente realiza acciones tales como:

- Destruir las áreas de almacenamiento lógico de la información de todo el sistema.

- Destruir las zonas críticas del sistema, tales como los sectores de arranque o las tablas de localización de archivos, haciendo de hecho, imposible llegar a las áreas de almacenamiento lógico de la información en el sistema.

- Generar falsos avisos, provocando que el usuario crea que los programas que anteriormente han funcionado de manera correcta, fallan de manera súbita.

- Inutilizar los programas, haciendo que graben basura dentro de los archivos que manipula el usuario (de hecho, el mismo estará destruyendo su información).

En el momento en que actúa un virus informático, contra la información del sistema es prácticamente imposible de recuperarla.

Es importante recalcar que el evento en particular que activa la acción del virus depende del virus particular que se encuentre en el sistema. Además, por lo general, el usuario no puede controlar la situación que activará la acción del virus (pues generalmente desconoce de su presencia).

3.3. Herramientas O Utilerías De Protección Contra Los Ataques De Virus Informáticos, Incluidos En El Sistema Operativo Ms-Dos Y En El Windows 3.1.

El sistema operativo MS-DOS, así como el Windows, poseen programas especiales que nos permiten controlar la acción de los virus informáticos, detectando y desinfectando, en la mayoría de los casos, a estos intrusos.

Estas utilerías, básicamente se dividen en dos grupos:

- Las que permanecen residentes en memoria mientras el sistema actúa normalmente (es decir, el comando Vsafe), advirtiendo e impidiendo (en la mayoría de las veces), la infección viral.

- Las que actúan cuando el usuario las activa intencionalmente, permitiendo la detección y eliminación de los virus del sistema.

3.3.1. Herramientas Residentes En Memoria O Antivirus Por Vigilancia Y Vacunas.

La herramienta residente en memoria que aportan el sistema operativo y Windows, es el comando VSAFE. Una vez es activado este comando, automáticamente se encarga de monitorear las zonas críticas del sistema, advirtiendo de cualquier acción que pueda atentar contra su seguridad. Además si encuentra en algún momento la presencia de un virus conocido, lo advierte y si es posible, lo elimina del sistema.

3.3.2. Herramientas Que El Usuario Activa Intencionalmente O Detectores/Limpiadores De Virus.

Las herramientas que aporta el sistema operativo para la detección intencional de los virus (en ambiente MS-DOS y en ambiente Windows), son los comandos MSAV y MSAVW. Una vez es activado uno de estos comandos, ellos revisan las partes de sistema críticas, reportando o eliminando (según lo que se les ordene), a los virus del sistema.

3.4. Limitaciones De Los Sistemas De Protección Contra Virus Informáticos, Medidas Preventivas A Tomar.

La mejor vacuna es la prevención, pues los virus están en constante actualización y los programas detectores y vacunas, de hecho, se actualizan posteriormente a su aparición en el mercado.

Además, los mismos esquemas de funcionamiento de los virus se están actualizando, de acuerdo a las últimas técnicas de programación estructuradas y por objetos, con el objeto de hacer más difícil su detección.

Todo esto hace que sea virtualmente imposible el prevenir la acción de los virus informáticos a través de un sistema antivirus 100% efectivo. En consecuencia, el secreto de la lucha contra los virus informáticos está en practicar lo que se ha dado en llamar la “computación preventiva”, que básicamente, se reduce a seguir dos simples reglas:

- Evite el intercambio de disquetes que contengan copias de programas. Utilice copias directas de sus originales, que deben estar convenientemente protegidas contra grabación, desde el momento en que se extraen de los paquetes en que se compran.

- Todo disquete que tenga que venir de una máquina distinta a la suya, deberá ser revisado, verificando que esta libre de virus. En caso de que los tenga si es posible, se le remueven, y en caso contrario (dependiendo del tipo particular de virus y de su ubicación), se deberá copiar los archivos no infectados a un disco limpio, o se desechará por completo (con todo y su información).

4. El Borrado De Archivos En El Sistema Operativo MS-DOS.

A continuación, analizaremos un poco los mecanismos que sigue el sistema operativo MS-DOS, para eliminar archivos.

4.1. Procedimiento Que Sigue El Sistema Operativo MS-DOS Al Borrar Un Archivo.

El sistema operativo, al borrar un archivo, coloca una marca especial en el primer carácter del nombre del archivo a borrar, dentro de la tabla de asignación de archivos (F.A.T.), este carácter lo identifica como borrado. Sin embargo, en ningún momento del proceso de eliminación del archivo, se modifican las zonas de datos asignadas al mismo.

Luego, la información que él contenía, permanece en el disco. Esta información es sobrescrita por el sistema operativo con información de otros archivos, únicamente en el momento que el sistema requiera estas zonas, por falta de espacio libre dentro del disco.

En consecuencia, en tanto el sistema operativo no tenga necesidad de escribir en los sectores que ocupa un archivo borrado, tendremos toda la información que el contiene intacta, con seguridad de poderla recuperar si es necesario.

4.2. Herramientas O Utilerías De Acción Limitada Para Recuperar Archivos Borrados, Incluidas En El Sistema Operativo MS-DOS Y En Windows 3.1.

La utilería para recuperar archivos borrados del sistema operativo es la orden UNDELETE del MS-DOS.

4.2.1. Herramientas Residentes En Memoria.

La herramienta residente en memoria que aportan el sistema operativo y Windows, es el comando UNDELETE.

El comando UNDELETE, al ser cargado como un programa residente en el sistema, cuando iniciamos la sesión, nos puede brindar varios niveles de protección contra el borrado de archivos.

4.2.2. Herramientas Que El Usuario Activa Intencionalmente.

Las herramientas que aporta el sistema operativo para la recuperación limitada de archivos borrados (en ambiente MS-DOS y en ambiente Windows), son los comandos UNDELETE y UNDELW.

En ambos casos, dependiendo de si el comando UNDELETE se a activado previamente o no, y del nivel de protección que estaba brindando, el programa, al ser activado, nos permitirá o no la recuperación del archivo teniendo o no que señalar cual es la primera letra del nombre del archivo.

4.3. Limitaciones De Las Herramientas Para Protección Contra El Borrado De Archivos Del MS-DOS Y Del Windows.

En caso de que el programa residente no se esté ejecutando en memoria, antes de borrar el archivo, la recuperación de estos dependerá de muchos factores, fundamentalmente, lo que ha sucedido en el sistema desde el momento en que se borró el archivo, hasta que se ordenó su recuperación. A saber, estos factores son:

- La cantidad de grabaciones que se han realizado.
- El tamaño de los archivos que se han manipulado.
- Si las estructuras de almacenamiento de datos a nivel lógico del disco presentan o no problemas (causados por la falta de mantenimiento lógico).

En consecuencia, la efectividad de estas herramientas está, al igual que en el caso de los virus, en la prevención. para tal efecto, el uso del UNDELETE como un programa residente, antes de que se realice la acción de borrar los archivos, es crucial para garantizar la seguridad de la recuperación de la información.

5. Comentarios Finales.

El conocimiento de estos problemas potenciales no nos debe amedrentar en cuanto a usar o no las computadoras en nuestro trabajo diario. Es cuestión de practicar una serie de normas simples, de computación preventiva, para

poder sentirnos libres, de hecho, de estas amenazas contra nuestra información. Entre ellas, tenemos:

- Cuando adquiera software de dominio público, procure revisarlo inmediatamente con un detector de virus, antes de instalarlo en su máquina.

- Manténgase informado acerca de cuales son los virus se están circulando en su medio, para estar prevenido en cuanto a las medidas de prevención específicas que requiere cada uno de ellos.

- Lleve una bitácora donde se controla a las personas con quienes se comparten archivos o discos, y manténgalos informados acerca de cualquier situación sospechosa en su sistema (evidentemente, para que esta recomendación sea funcional, el registro debe ser mutuo de las otras personas).

- Administre correctamente su disco duro, manteniéndolo libre de errores físicos y lógicos, al utilizar algún software de mantenimiento de sistema, como el SCANDISK, del sistema operativo, o el Norton Disk Doctor, de terceros fabricantes.

- Se recomienda implementar el uso del UNDELETE como un programa residente, de manera regular en el sistema.

- Mantenga siempre un disco de arranque con utilidades, de modo que pueda arrancar su máquina con ese disco y poder corregir problemas de virus y errores lógicos o físicos en el disco (lógicamente, ese disco debe estar absolutamente libre de virus, y contener todos los programas necesarios para tal fin).

- Evite que cualquier persona utilice su computadora, incluyendo a los vendedores de software con disco de demostración. En caso de que se incumpla la medida, se debe revisar completamente todo el sistema en busca de virus, de manera inmediata.

- Finalmente, mantenga un respaldo de toda la información de sus discos duros, de manera periódica, por si acaso llegan a fallar las recomendaciones anteriores.

Es importante recalcar que todas estas medidas, así como otras que se puedan implantar, no son una garantía absoluta de que nunca tendremos problemas con virus o archivos borrados. Sin embargo, su cumplimiento asegura que la mayoría de las causas de estos problemas estarán controladas, de modo que el peligro inherente a estos problemas, debe disminuirse al cumplirlas.

BIBLIOGRAFÍA

1. FERREYRA CORTÉZ, Gonzalo. Virus en las computadoras. Primera edición. México D.F., México: Macrobit, 1990.

2. FERREYRA CORTÉZ, Gonzalo. Virus en las computadoras. Segunda edición. México D.F., México: Macrobit, 1991.

3. MEJÍA M., Aurelio. Diccionario Técnico Actualizado. Primera edición. Medellín, Colombia: Divulgación Técnica Electrónica, 1991. 439 páginas.

4. MEJÍA M., Aurelio. Guía práctica para manejar el computador. Segunda edición. Medellín, Colombia: Divulgación Técnica Electrónica, 1992. 216 páginas.

5. Microsoft MS-DOS: Manual del usuario (versión 6.2). Sin traductor. E.U.A.: Microsoft Corporation, 1993. 272 páginas.

6. Microsoft Windows: Introducción (versión 3.1). Sin traductor. E.U.A.: Microsoft Corporation, 1992. 99 páginas.

7. Microsoft Windows: Manual del Usuario (versión 3.1). Sin traductor. E.U.A.: Microsoft Corporation, 1992. 716 páginas.

8. NORTON, Peter y NIELSEN, Paul. Norton Antivirus. Traducido por Palmas Velasco, Oscar A. Primera edición. México D.F., México: Prentice Hall, 1993. 313 páginas.

9. NÚÑEZ HERVÁS, Rafael. Utilidades Norton: Guía Práctica. Primera edición. México D.F., México: Macrobit, 1990. 222 páginas.

10. SCHILDT, Herbert. DOS 6 a su alcance. Traducido por Lirila, Terrez, Antonio. Cuarta edición. México D.F., México: McGraw-Hill, 1993. 428 páginas.

11. TAMAYO MARTÍNEZ, Jorge. Cómo y porqué actualizarse al DOS 6.2: Tomo 1. Primera edición. Barquisimeto, Venezuela: Enigma Editorial, 1994.