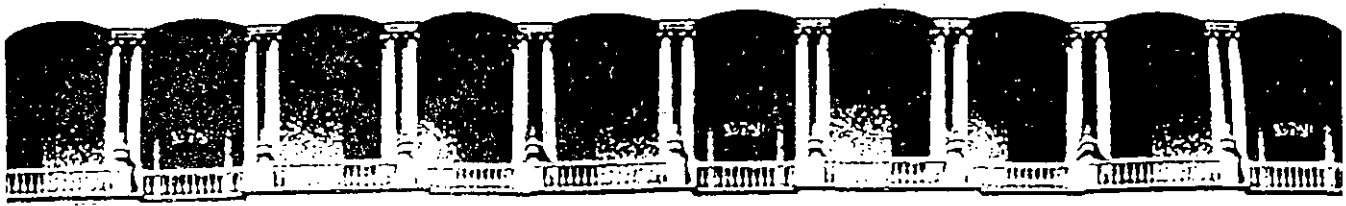


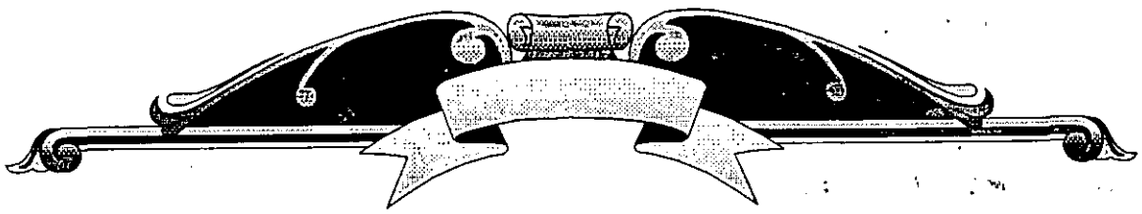
FACULTAD DE INGENIERIA U.N.A.M.
DIVISION DE EDUCACION CONTINUA

# VIRUS INFORMATICOS: TEORIA Y EXPERIMENTACION

**COMPLEMENTO**

(ACETATOS)

JULIO, 1994



# Virus Informáticos

DEC,FI,UNAM

Para que sea exitoso un virus de computadora debe incluir, al menos, las siguientes partes:

Uno o varios disparadores

Un sistema de control interno

Uno o varios sistemas de protección (ocultamiento)

Uno o varios sistemas de reproducción y contagio

Uno o varias misiones que cumplir

En forma adicional es frecuente encontrar rutinas de regeneracion para reconstruir las partes del virus que pudieran ser dañadas y programas portadores del virus que complementan la capacidad de reprodución y contagio.

Para que el virus surta algún efecto tiene por fuerza estar activo, es decir, debe ejecutarse. La ejecución debe pasar más o menos inadvertida para el usuario y puede ser iniciada automáticamente al ocurrir algún evento, por ejemplo, el arranque de la máquina o la ejecución de algún comando del sistema operaivo.

El virus es una amenaza potencial a la integridad del software de cualquier computadora y su patrón de operación es variado dependiendo del tipo de virus. Los efectos que causan pueden ser:

Cambiar el nombre del volumen del disco

Marcar sectores dañados en áreas no usadas del disco disminuyendo paulatinamente su capacidad.

Interferir con la operación de programas residentes en memoria RAM

Infectar al sistema operativo

Eventualmente cancelar el área de BOOT, FAT , DIRECTORY y área de datos

Provocar imágenes molestas en el monitor ó enviar mensajes

Borrar programas y archivos

Bloquear búfers a manera de no permitir la entrada y salida de los datos en los discos pareciendo una falla de software

Dañar físicamente la computadora

Destruir directorios de discos

Llenar de basura la memoria de la computadora

Formatear disquetes y discos duros

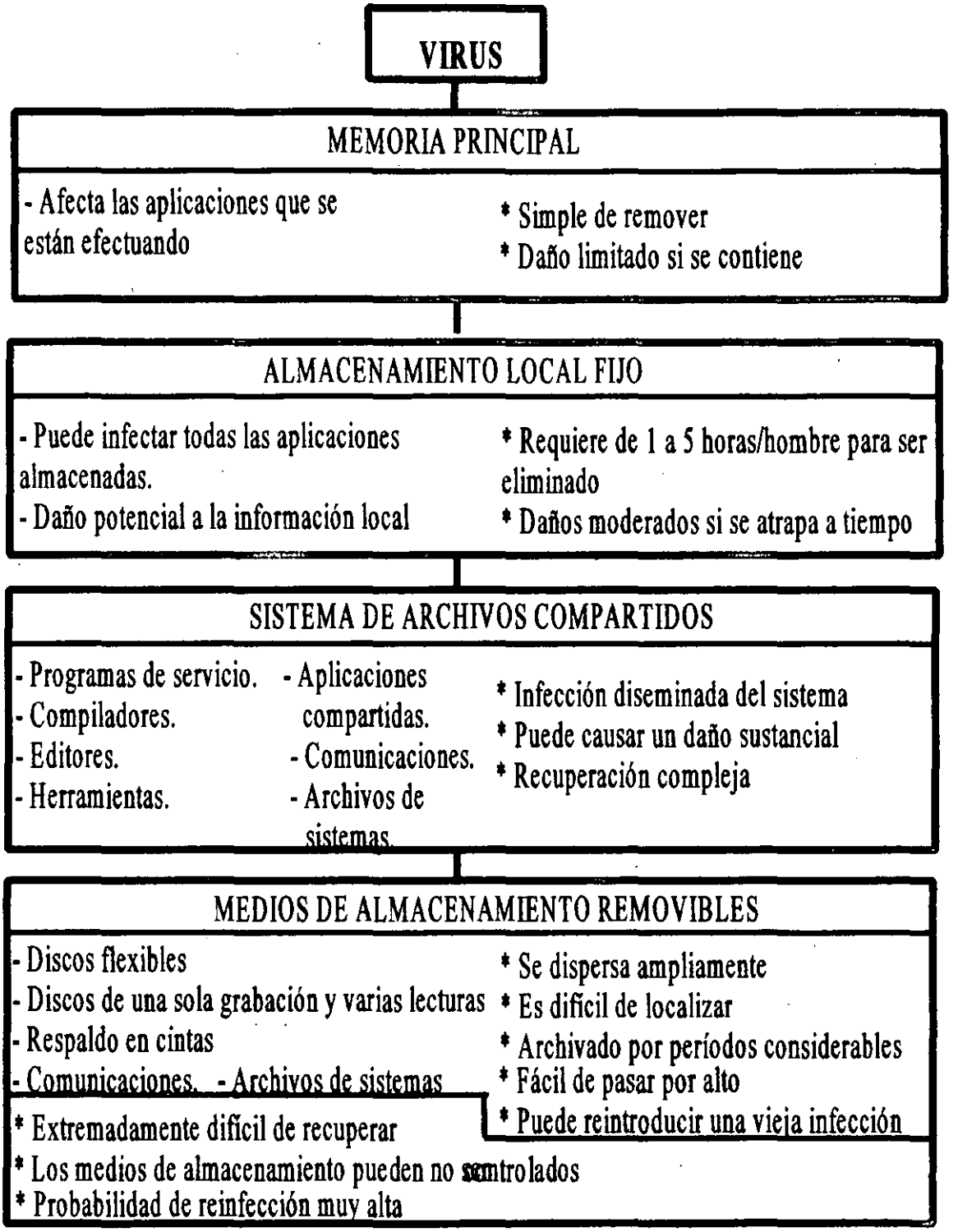
Resetear la computadora

Redefinir teclas

Inutilizar el teclado

Modificar la información en programas ó archivos

Disminuir la velocidad de procesamiento de la computadora


VIRUS
MEMORIA PRINCIPAL
- Afecta las aplicaciones que se están efectuando
* Simple de remover
* Daño limitado si se contiene
ALMACENAMIENTO LOCAL FIJO
- Puede infectar todas las aplicaciones almacenadas.
- Daño potencial a la información local
* Requiere de 1 a 5 horas/hombre para ser eliminado
* Daños moderados si se atrapa a tiempo
SISTEMA DE ARCHIVOS COMPARTIDOS
- Programas de servicio.
- Compiladores.
- Editores.
- Herramientas.
- Aplicaciones compartidas.
- Comunicaciones.
- Archivos de sistemas.
* Infección diseminada del sistema
* Puede causar un daño sustancial
* Recuperación compleja
MEDIOS DE ALMACENAMIENTO REMOVIBLES
- Discos flexibles
- Discos de una sola grabación y varias lecturas
- Respaldo en cintas
- Comunicaciones. - Archivos de sistemas
* Se dispersa ampliamente
* Es difícil de localizar
* Archivado por períodos considerables
* Fácil de pasar por alto
* Puede reintroducir una vieja infección
* Extremadamente difícil de recuperar
* Los medios de almacenamiento pueden no ser controlados
* Probabilidad de reinfección muy alta

Existen dos maneras de descubrir a un virus: utilizar un programa de protección o diagnosticar los sintomas de la precencia de este.

- Los sintomas con los que se puede sospechar la precencia de un virus son:
- La memoria RAM disminuye sin haber cargado algún programa
- El disco realiza accesos o se prende el foco rojo de la unidad sin existir alguna causa.
- El sistema se vuelve muy lento al estar trabajando
- El sistema operativo despliega mensajes de error inesperados, tales como INVALID DRIVE ESPECIFICATION
- Los tamaños de los archivos cambian sin motivo
- El número de archivos en el directorio del disco cambia sin razón.
- El copiar, borrar o renombrar archivos toma mucho tiempo.
- El teclado imprime caracteres extraños o de repente no trabaja

Aunque estos sintomas pueden deberse a una falla de los circuitos del sistema.

# Pasos a seguir cuando se detecta la presencia de algún virus

1) Apague completamene la computadora, no únicamente utilice Ctrl-Alt-Del

2) Encienda de nuevo la computadora utilizando un disco de arranque de DOS limpio. (Original)

3) En los discos flexibles o duros dañados, si no tenía un respaldo no infectado reciente y tiene necesidad de recuperar la información, respalde todos los archivos de datos que no sean ejecutables en otro disco flexible original formateado, que haya sido previamente verificado como no infectado

4) Inserte el disco de protección, vacuna o erradicación de virus y hágalo trabajar

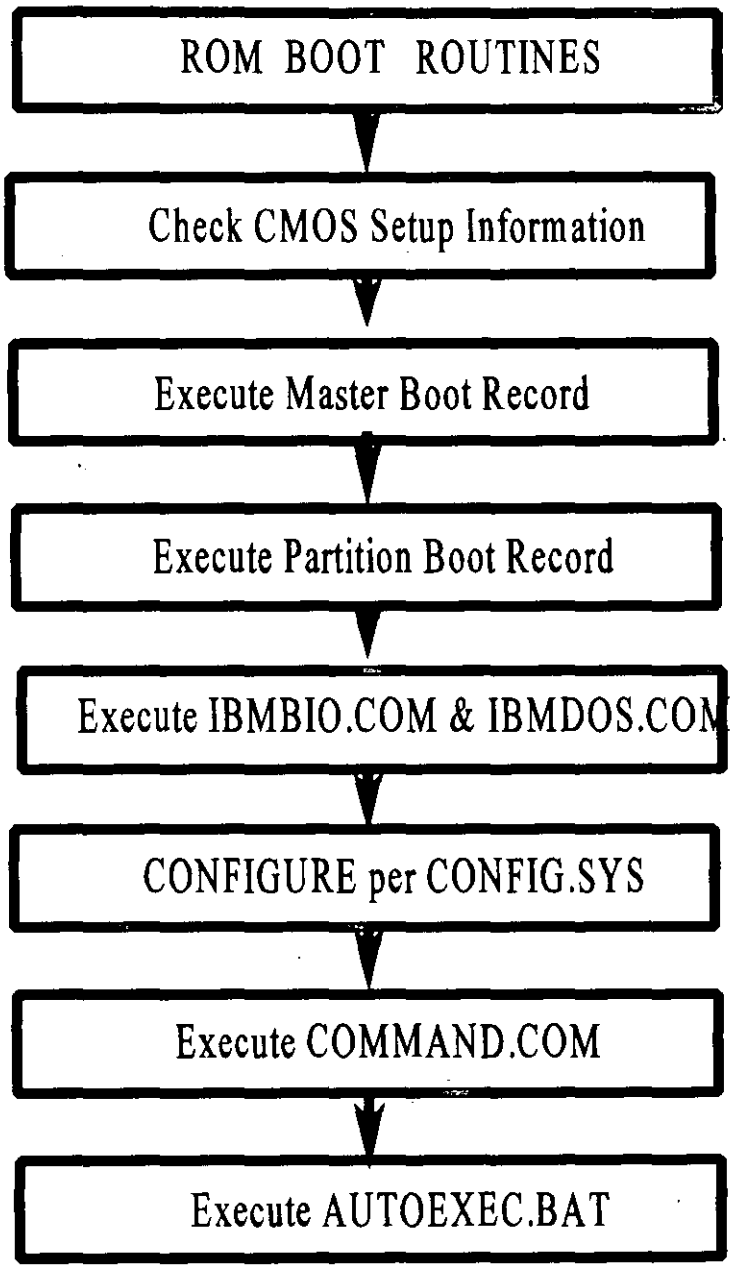
5) En caso necesario de formato al disco duro otra vez, desde el nivel más bajo y después utilice los comandos de DOS: FDISK y FORMAT

6) Restablezca los archivos de datos en el disco

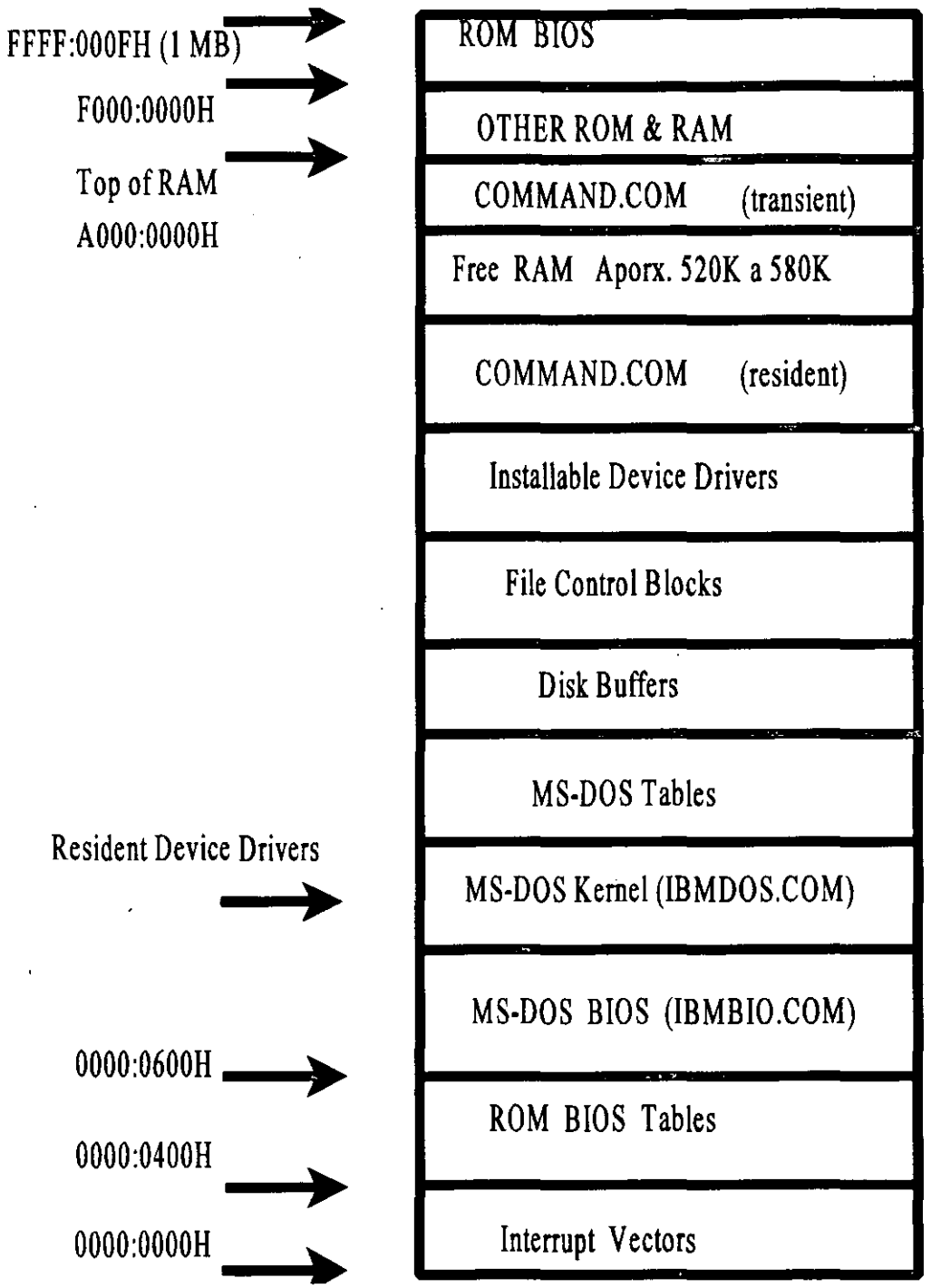
7) Verifique todos los discos flexibles que tiene con el programa de protección

Existen algunos virus que se almacenan en alguna parte de la memoria conocida como CMOS, y que guardan información permanente respaldados por una pila o batería. Si a pesar de haber realizado los pasos anteriores el virus permanece; entonces hay que destapar la máquina, quitar la pila, esperar mínimo una hora y volver a colocarla.

# IBM-PC BOOT PROCESS



# MAPA DE MEMORIA DE UNA IBM-PC



## ORGANIZACION LOGICA DEL DISCO

- ✓ Tabla de Particiones
- ✓ Area de BOOT
- ✓ FAT (File Allocation Table)
- ✓ Area de ROOT (Directorio raíz)
- ✓ Area de Datos (DATA)

# El BPB (Bios Parameter Block)

Ocupa los primeros 32 bytes del área de BOOT, a excepción de los formatos FE y FF, que contiene los siguientes datos:

| Offset | Longitud | Descripción |
|---|---|---|
| 3 | 8 bytes | Identificación del sistema OEM |
| 11 | 1 word | Bytes por sector |
| 13 | 1 byte | Sectores por cluster |
| 14 | 1 word | Sectores reservados |
| 16 | 1 byte | Copias de la FAT: 2 por disco flexible |
| 17 | 1 word | Entradas del directorio raíz |
| 19 | 1 word | Total de sectores en el disco |
| 21 | 1 byte | Identificador de formato |
| 22 | 1 word | Sectores por FAT |
| 24 | 1 word | Sectores por track o pista |
| 26 | 1 word | Lados o cabezas |
| 28 | 1 word | Sectores especiales |

# EL AREA DE DIRECTORIOS

El área de directorios está formada por espacios de 32 bytes que guardan los datos generales de cada archivo en el directorio raíz. Para un archivo, los datos están dados por:

| Offset | Descripción | Tamaño (bytes) | Formato |
|---|---|---|---|
| 0 | Nombre de archivo | 8 | Caracteres ASCII |
| 8 | Extensión del atributo | 3 | Caracteres ASCII |
| 11 | Atributo | 1 | Codificado bit |
| 12 | Reservado | 10 | No usado (ceros) |
| 22 | Tiempo | 2 | Codificado word |
| 24 | Fecha | 2 | Codificado word |
| 26 | Cluster inicial | 2 | Codificado word |
| 28 | Tamaño de archivo | 4 | Long word |

Para obtener la relación de sectores fisicos a lógicos:

Sector lógico = ( sector fisico - 1 ) + lado x sectores por track
+ track x sectores por track x lados por disco

Sector fisico = 1 + sector lógico MOD sectores por track

lado = ( sector lógico/sectores por track ) MOD lados por disco
track = sector lógico/( sectores por track x lados del disco )

# FAT ( File Allocation Table )

ORGANIZADA POR UNA TABLA DE NUMEROS ENTRE 0H Y 0FFFH

- Sector disponible: 000H

- Sector reservado: FF0h y FF6H

- Sector dañado: 0FF7H

- Ultimo registro del archivo: FF8H - FFFH

- Cualquier otro, es un registro intermedio

# IDENTIFICADORES DE DISCO

Para identificar el tipo de formato que tienen los discos, se verifica el byte correspondiente al primer elemento de la FAT o con el offset 21 en áreas de BOOT. Los diferentes formatos son:

SECTORES DE OVERHEAD

| Formato | Sectores | Boot | FAT | Directorio | Capacidad nonimal |
|---|---|---|---|---|---|
| FF | 320 | 1 | 2 | 4 | 160 Kbytes |
| FF | 640 | 1 | 2 | 7 | 320 |
| FC | 360 | 1 | 4 | 4 | 180 |
| FD | 720 | 1 | 4 | 7 | 360 |
| F9 | 1440 | 1 | 10 | 7 | 720 |
| F9 | 2400 | 1 | 14 | 14 | 1200 |

| Formato | Lados | Sectores | Tracks |
|---|---|---|---|
| FE | 1 | 8 | 40 |
| FF | 2 | 8 | 40 |
| FC | 1 | 9 | 40 |
| FD | 2 | 9 | 40 |
| F9 | 2 | 9 | 80 |
| F9 | 2 | 15 | 80 |

Existe otro formato que es el empleado para discos duros y se identifica con F8. Dado que los discos duros pueden ser de diferentes capacidades, estos datos se pueden localizar en el BPB del área de BOOT.

# COMANDOS DE DOS

ATTRIB

CHKDSK

COMP

DISKCOMP

FC

FDISK

FIND

MIRROR

RECOVER

UNDELETE

UNFORMAT

VERIFY

MSAV

VSAFE

# PROTECCION EN SISTEMAS DE COMPUTO

## VACUNAS

☹☹ Las vacunas pueden falsear la información, es decir, indicar la presencia de un virus cuando en realidad no existe (falsos positivos).

☹☹ La actualización en la base de conocimientos (virus) en el programa vacuna, sólo sirve para virus conocidos.

☹☹ No todos los programas pueden ser vacunados, ya que existen virus que dañan el archivo donde se alojan y al ser eliminados dejarán el archivo en malas condiciones.

☹☹ Al vacunar contra un virus esto puede permitir que otro virus entre: Caso Stoned y Ping pong.

En el caso de las vacunas que inmunizan:

☹☹ Los programas vacunados tardan más tiempo en cargarse ya que el código y datos del anti-virus aumentan su tamaño, además de que el proceso previo de verificación de suma total a la ejecución requiere más tiempo.

☹☹ No hay garantía de que las modificaciones de los archivos ejecutables no afectan negativamente a sus operaciones.

☹☹ Puede presentarse el caso de que la vacuna empleada para inmunizar esté contaminada con un virus que ésta no comtemple en su base de conocimiento.

☹☹ La conducta de las vacunas, parecidas a la de los virus, puede causar conflictos con otros sistemas de defensa viral.

☹☹ Los virus pueden detectar la presencia del código del programa vacuna en los archivos ejecutables destino y borrar o modificar los datos relacionados con la vacuna, o pueden corregir a los ejecutables inmunizados para saltarse el proceso de verificación.

# Virus Scanners

☹☹ Sólo pueden detectar un número limitado de virus y patrones de ataque conocidos. Esto significa que virus nuevos o modificados pueden estar activos, propagándose y completamente indetectables por los rastreadores.

☹☹ En una organización donde la información es de vital importancia y el tiempo muy valioso, el ejecutar el scanner implicará una pérdida de dinero.

☹☹ Generalmente éste tipo de programas requieren frecuentes y a veces costosas actualizaciones cuando se descubren nuevos virus o cuando antiguos virus se actualizan. Los nuevos patrones o signaturas de los virus tienen que ser agregados al código fuente del rastreador. Los usuarios que no utilicen versiones recientes estarán en peligro de un ataque o infección.

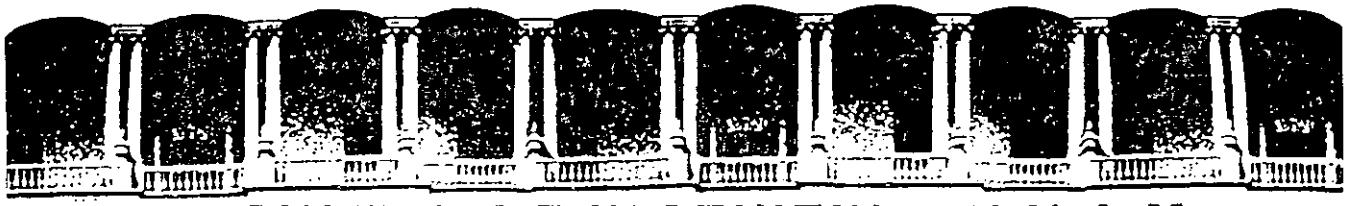
☹☹ Los rastreadores de virus ( virus scanners ) no son muy eficientes contra virus con la capacidad de evolucionar que empiezan a desarrollarse en la actualidad.

☹☹ Son más lentos cada vez que se actualizan. Los virus actuales también atacan hojas electrónicas o bases de datos, por lo que los lugares a buscar y patrones se incrementan, aumentando así el tiempo.

☹☹ Los rastreadores de virus ( virus scanners ) son superados fácilmente por los virus modernos que emplean las técnicas de codificación de datos para enmascarar sus patrones. Tales virus codifican sus signos reveladores bien encriptándolos o cambiándoles.

Como sus patrones cambian con cada nueva infección, no queda nada tangible para que los scanners de virus busquen o identifiquen.

☹☹ Producen falsos positivos para patrones cortos. Ya que puede presentarse el patrón en un archivo por casualidad sin que éste sea virus.



FACULTAD DE INGENIERIA U.N.A.M.
DIVISION DE EDUCACION CONTINUA

# VIRUS INFORMATICOS: TEORIA Y EXPERIMENTACION

COMPLEMENTO

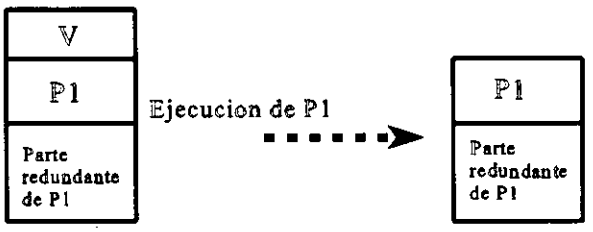
JULIO, 1994.

Palacio de Minería Calle de Tacuba 5 Primer piso Deleg. Cuauhtémoc 06000 México, D.F. Tel.: 521-40-20 Apdo. Postal M-2285

# Software con auto-defensa

La idea del sofware con auto-defensa es de algunos años atrás. Básicamente consiste en que el pograma se auto-verifica y automáticamente elimina la corrupción si es que la había.

La clave está en construir el programa con alguna clase de redundancia en él. Cuando se ejecute el programa, éste se verificará a si mismo, usando la misma clase de redundancia, y si no se encontró normal, detectará el error y corregirá éste, usando de igual forma la misma clase de redundancia para la corrección.

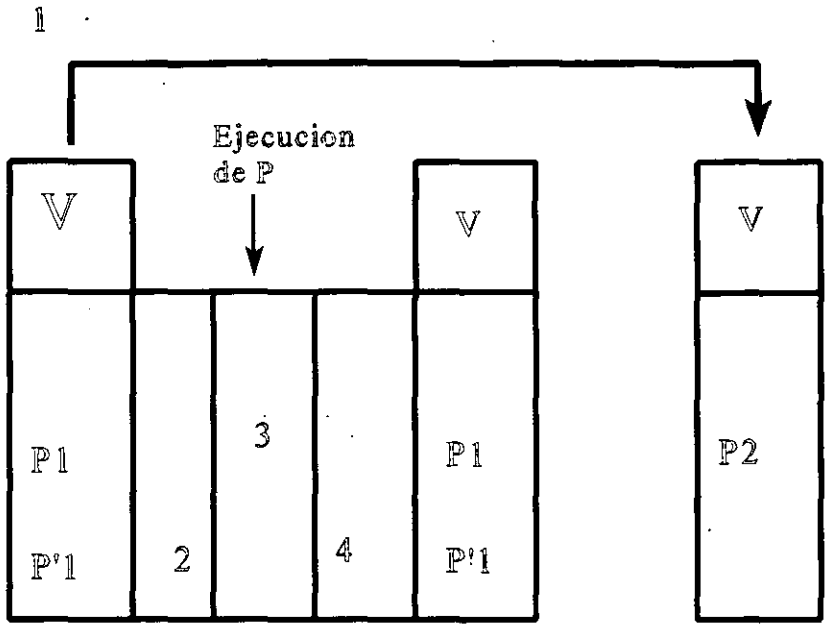



☹☹ El virus puede modificar la parte redundante del programa P1 para alojarse o propagarse.

☹☹ La detección puede fallar si se utiliza un método simple de checksum.

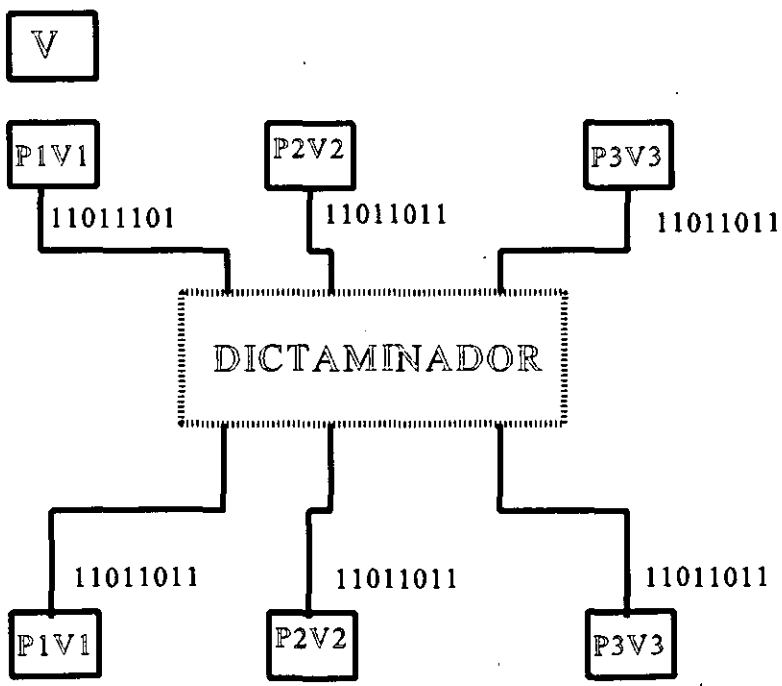
Existe una gran cantidad de técnicas diseñadas para aumentar la calidad del software que se auto-verifica, una de ella es Cryptographic checksum. Esta técnica puede variar en su implementación, es decir, puede comprobar sólo un sector al azar del archivo o el primero o el último. Otros seleccionan cinco o seis bloques cualesquiera. Estos esquemas pueden ser muy rápidos ya que no verifican toda la información pero tienden a fallar.

☹☹ Otro problema, es el tiempo invertido que el programa toma para mantenerse limpio. Esta es una situación de riesgo que hace que la auto-defensa falle.




## Software tolerante a fallas

Consiste en la ejecución de copias redundantes de programas. A continuación se presentará un ejemplo:



☹☹ El costo para la implementación es muy elevado. En el caso de este ejemplo, debe de haber tres diferentes programas, lo que implica tres diferentes programadores, también se necesita tener tres veces la capacidad de cómputo para tener la misma eficiencia.

☹☹ Difícil de elaborar. Ya que se tienen que implementar varios programas que hagan lo mismo, pero que sean totalmente diferentes entre si.

☹☹ Esta técnica no esta garantizada contra ataques intencionales.

# Control Total a cambios

Es un proceso de seguridad de calidad que verifica cualquier tipo de corrupción a través de un **guardia**. Normalmente se tienen dos ambientes, uno el **de investigación y desarrollo (R&D)**, y otro el de **ambiente de produccion (P).** El ambiente R&D es donde se hacen y se examinan los cambios. El ambiente P es donde se actualiza el uso de esos cambios día con día. Para que se tenga un total control a cambios existe un área entre los ambientes R&D y P llamada **control de cambio**, que contiene un conjunto de reglas acerca de como trabaja el sistema.


1. El control a cambios sólo puede aprobar o rechazar un cambio propuesto; este no puede hacer un cambio como si fuera propio.

2. El control a cambios sólo puede pasar fuentes desde el R&D a P. No puede pasar librerías en código ordinario, ejecutables o cosas similares, porque no se puede realmente determinar que tipo son los no fuentes.

3. El control de cambios es hecho vía humanos y por métodos de verificación automática. Se verifica que el cambio sea necesario y que sea el apropiado para un fin específico.

4. El cambio tiene que ser aprobado sobre un dato muestra desde el ambiente P para verificar que trabaja apropiadamente.

5. La operación del cambio debe ser evidente y obvia.

6. El cambio no debe tener código innecesario o datos complicados. Cualquier código innecesario puede contener virus u otro tipo de amenazas.

# Curas, Antidotos y Vacunas Comerciales

## Central Point Antivirus (CPAV)

El CPAV detecta, limpia e inmuniza cerca de 800 virus conocidos, además ofrece protección contra virus polymórficos creados de la mutación del virus Dark Avenger.

CPAV es un programa que funciona a base de menús desplegables en modo gráfico o de texto. Ofrece menús express o menús completos, los primeros se caracterizan por no ofrecer todas las opciones del producto. De esta forma los comandos se seleccionan a través del menú o bien, se pueden ejecutar en la línea de comando.

CPAV ofrece protección al área de BOOT, Tabla de Particiones y a la integridad de los archivos tanto de texto, como ejecutables. Además tiene dos programas TSR´S que monitorean la incursión de virus al sistema, un programa detector y limpiador, un programa de configuración, uno de instalación y varios de utilerias para la programación BATCH. Además ofrece una técnica de checksums para la protección de los archivos.

CPAV se puede ejecutar en WINDOWS, en el modo extendido del 386. El programa de instalación (INSTALL) verifica la existencia de WIN.INI y si existe crea un ícono de grupo llamado CPAV. El programa de instalación también hace las modificaciones necesarias a los archivos de inicialización del sistema (AUTOEXEC.BAT y CONFIG.SYS).

El producto utiliza los siguientes programas:

INSTALL.EXE: Realiza la instalación del producto, ofreciendo las opciones de crear un diskette de emergencia, desinstalar y configurar las opciones de los programas TSR VWATCH y VSAFE.

CPAV.EXE: Detecta y limpia virus. Algunas de las opciones que ofrece el menú principal (menú modo completo) son: Scan, Options, Configure, Help.

Si se desea utilizarlo en archivos BATCH el modo de empleo es:

CPAV [drive:] [drive:] | [ruta] /opciones

Las opciones son:

/S : Busca virus en discos y archivos.
/C : Busca y limpia discos y archivos de virus.
/I : Busca, limpia e inmuniza discos y archivos.
/R : Habilita la opción de Report.
/A : Busca todos los drives excepto A y B.
/E : Express Menu.
/L : Busca todos los drives locales excepto A y B.
/N : Muestra el texto del archivo CPAV.TXT, si existe.

Por ejemplo: CPAV /L /S buscará virus en todos los drives y archivos locales excepto el drive A: y B:

BOOTSAFE.EXE: Crea un archivo llamado BOOT.CPS donde almacena la información de la Tabla de Particiones y el área de Boot. Al momento de ejecución revisa la memoria en busca de virus, posteriormente válida la información contenida en el disco duro con la del archivo. S un virus alteró el área de boot o la tabla de particiones, BOOTSAFE ofrece las opciones de Regenerar (Rebuild), Actualizar (Update), Detener (Stop) y Continuar (Continue). Escoja Rebuild si usted no editó cualquiera de las áreas antes mencionadas, esta opción copia la información del archivo BOOT.CPS a las áreas afectadas y de esta forma elimina cualquier virus de boot o de la tabla de particiones. Escoja Update si editó cualquiera de estas áreas y no ha actualizado (BOOTSAFE C: /M) el archivo BOOT.CPS. Escoja Stop o continue si desea detener la ejecución del programa. La selección de las opciones se hace presionando la letra que indica el letrero de Warning entre corchetes. Por jemplo: [R] si se desea la opción Rebuild.

ISCPSTSR.EXE: Este programa se utiliza para verificar que VWATCH o VSAFE se hayan ejecutado e instalado. Si no fué así, regresa un ERRORLEVEL diferente de 99. Esto es especialmente útil cuando se tiene instalado una red LAN, y el adminostrador del sistema desea asegurarse que cada usuario que ingrese a la red este usando VSAFE o VWATCH.

Para MS-DOS copie el archivo iscpstsr.exe en la máquina a verificar y agregue las siguientes líneas al archivo AUTOEXEC.BAT:

```
iscpstsr
if erorlevel 99 goto sitsr
if errorlevel 0 goto notsr
goto fin
: sitsr
echo Gracias pormproteger al sistema contra virus
goto fin
: notsr
echo Por favor, ejecuta VSAFE o VWATCH para
     protección anti-virus.
goto fin

: fin
```

También se puede utilizar algún otro archivo de procedimiento por lotes, u otros programas, e incluso ejecutar vsafe ó vwatch en lugar de escribir un letrero en pantalla.

VSAFE.COM,
VWATCH.COM: Estos son programas residentes en memria, y se pueden instalar ya sea como manejador (como manejador use VSAFE.SYS ó VWATCH.COM) ó como TSR´S (use VSAFE.COM ó VWATCH.COM).

Vsafe, Vwatch y Vdefend (Parte del paquete PCTOOLS) son mutuamente excluyentes; instale el que mejor optimice su sistema. Utilice Vsafe para obtener el nivel más alto de protección antivirus.

Para instalar Vsafe como manejador agregue la siguiente línea DEVICE=C:\CPAV\VSAFE.SYS al archivo CONFIG.SYS. Para Vwatch agregue DEVICE=C:\CPAV\VWATCH.SYS. Todo lo anterior suponiendoque el producto se instaló en el subdirectorio C:\CPAV.

**Usando Vsafe:**

Tiene las siguientes opciones:

/1 : Formateo del disco duro a bajo nivel
/2 : Alerta contra programas que se vuelven residentes
/3 : Protección general contra escritura
/4 : Verifica archivos infectados
/5 : Alerta contra infección del sector BOOT del disco duro.
/6 : Protección del área de BOOT del disco duro.
/7 : Protección del área de BOOT de discos flexibles
/NE : No usar Expanded Memory
/NX : No usar Extended Memory
/Ax : Cambia teclas de configuración ALT-V como ALT-X
/Cx : Cambia teclas de configuración CTRL-V como CTRL-X
/N : Usese si algún driver de red es instalado después de Vsafe
/D : Deshabilita la creación de checksum
/U : Remueve Vsafe de memoria.

Las opciones por omisión son /1, /4, /5, /6.
Por ejemplo: Vsafe /1+/2-/3-/4+/5-/6+/7-/8- instalará Vsafe con protección de formateo del disco duro a bajo nivel, verificará los archivos antes de ejecutarlos, alertará contra la modificación del sector de Boot y protegerá el área de Boot del disco duro.

**Usando Vwatch:**

Tiene las siguientes opciones:

/NE : No usar Expanded Memory
/NX : No usar Expended Memory
/U : Remueve Vsafe de memoria
/D : Usa intercambio a disco.

Si sólo se cuenta con memoria convencional y se desea optimizarla, ejecute VWATCH /D lo cual minimiza el uso de memria usando intercambio a disco. Una parte del programa se carga en la memoria convencional, ocupando 7k. Cuando alguna parte del VWATCH se necesita este lee la información del disco. Esto trae como consecuencia degradación en el performanece del sistema.

## Norton Antivirus

Norton Antivirus se caracteriza por tener Virus Clinic y virus Intercept. virus Clinic busca algún virus. Si alguno es encontrado, dá la opción de reparar el archivo (si el archivo es reparable) o borrar el archivo. Puede buscar en todo el disco, directorios especificados o archivos individuales. Para revisar virus desconocidos, primero se deben inoculizar los archivos, después cada vez que el archivo es accesado es checado contra los datos de inoculación almacenados, y si alguno es cambiado pone alerta al usuario. Virus Clinic provee comandos para configurar Virus Clinic y virus Intercept y para manejar la lista de virus. También para poder restaurar los valores.

Virus Intercept monitorea constantemente el sistema en busca de virus, este es cargado en memoria cuando se arranca el sistema. Cada vez que se copia un archivo ó se ejecuta una aplicación, Virus Intercept checa el archivo en busca de cualquier virus definido. Si se localiza un virus se activa la bocina del sistema anunciando la presencia de un virus y la acción es detenida. En este momento se debe ejecutar Virus Clinic para determinar la extensión de la infección. Otra habilidad de Virus Intercept es la capacidad de "inoculizar" archivos. Esto consiste en calcular, la primera vez que se ejecuta un programa, los datos de inoculación y se guardan en el archivo de inoculación; y la próxima vez que se ejecute la misma aplicación se verifican los datos de inoculación para asegurarse que el código de la aplicación no ha sido modificado.

The Norton Antivirus es capaz de detectar 340 virus y 1,005 cadenas, con la opción de poder agregar nuevas definiciones de virus manualmente.

## Virus Intercept

Existen tres manejadores (device drivers) en The Norton Antivirus. Ellos requieren 1K, 6K y 39K de memoria respectivamente. Cada uno de estos dispositivos opera y detecta virus en DOS y Windows y se pueden optimizar si se instalan en la memoria alta.

### NAV&.SYS (1K)

Utilice este dispositivo si se tiene limitaciones de memoria, o se tienen varios TSR´S. Este driver detecta virus cuando un programa infectado esta por ejecutarse, pero no ofrece protección al área de BOOT y no despliega una alerta visual bajo Windows.

### NAV&.SYS /B [/A] (6K)

Realiza las mismas operaciones que el dispositivo de 1K, más la protección al área de BOOT. Y la alerta visual aparece bajo Windows (cuando NAVPOPUP.EXE es cargado). La opción /A causa que se busquen virus de área de BOOT en el drive B: en lugar de A:, al momento de presionar <CTRL+ALT+DEL>

### NAV_.SYS [/A] [/W] (39k)

Este driver realiza las mismas operaciones que los dos anteriores y también busca virus cuando se copian o mueven archivos. No permitiendo que archivos infectados entren al sistema. La opción /A causa que se busquen virus de área de BOOT en el drive B: en lugar de A:, al momento de presionar <CTRL+ALT+DEL>.

La opción /W previene que cualquier programa modifique la tabla de particiones y los sectores de BOOT sin conocimiento del usuario. Esta opción es molesta si se formatean constantemente discos flexibles o si se es aficionado a modificar estas áreas con algún editor del disco. Después de que se instala, NAV _.SYS previene cualquier lectura o escritura a el mismo. Consecuentemente no se puede ver, modificar, borrar o cambiar los atributos del archivo. Tampoco se debe marcar como archivo de solo lectura (READ-ONLY) porque The Norton Antivirus guarda su configuración y otra información en NAV_.SYS. La definición de los virus es leída en la memoria en tiempo de arranque.

Si se desea desactivar driver, sin modificar el archivo CONFIG.SYS, simplemente presione simultáneamente las dos teclas SHIFT al momento de arrancar el sistema y escuchar el primer BEEP. Sólo se puede instalar un driver, si se intenta instalar un segundo. Este desplegará el mensaje " Norton Antivirus already loaded"

Para instalar el dispositivo agregue una de las siguientes líneas al inicio del archivo CONFIG.SYS

DEVICE=C:\NAV\NAV&.SYS
DEVICE=C:\NAV\NAV&.SYS /B
DEVICE=C:\NAV\NAV_.SYS /W

**Virus Clinic**

Encuentra y remueve virus en archivos, directorios y drives.

USO:
NAV /A | pathname [/s] [/REFRESH] [/M-] [STOP]

NAV [/SOUND [+|-] ] [/BOX [+|- ] ] [/PRESENCE] [/BOOT drive...] [/M+]

| | |
|---|---|
| + | Activa opción |
| - | Desactiva opción |
| pathname | Cualquier drive válida ruta, directorio o archivo. |
| A | Busca en todos los drives |
| BOOT | Busca solamente en los sectores de BOOT y drives |
| BOX | Habilita/Deshabilita la alerta visible |
| REFRESH | Inoculate o reinoculate todos los archivos scaneados |
| S | Busca en subdirectorios |
| STOP | Detiene la búsqueda de virus si alguno es encontrado y traba el sistema aunque se presione CTRL-C |
| SOUND | Habilita/Deshabilita la alerta audible |
| M | Busca en memoria solamente (+), o salta la búsqueda en memoria (-) |

DOS Error Levels

| | |
|---|---|
| 1 | Virus encontrado en memoria |
| 2 | Virus Clinic puede estar infectado |
| 3 | Virus detectados durante la búsqueda |
| 4 | No virus detectados |
| 5 | Device driver NO esta activo en RAM |
| 6 | Device driver esta activo en RAM |
| 255 | Busca No completada |

Ejemplos:

nav /m+

Busca virus solamente en la memoria RAM

nav c:

Busca virus en memoria y en el disco C:

nav c:\dos /s

Busca virus en memoria, en el disco C:\dos y subdirectorios.