

MANTENIMIENTO DEL SOFTWARE CONTRA INFECCIÓN DE VIRUS INFORMÁTICOS

Rangel E.¹ & Pineda R.¹

¹ *Instituto Tecnológico agropecuario No. 25
S.E.P. / S.E.I.T. / D.G.E.T.A.*

Resumen

Este artículo es el resultado del "Anteproyecto de Investigación titulado: MANTENIMIENTO DEL SOFTWARE CONTRA INFECCIÓN DE VIRUS INFORMÁTICOS"; presentado en el Segundo Foro de Presentación de Anteproyectos de Investigación, organizado por el Instituto Tecnológico agropecuario No. 25 del 02 al 07 de febrero de 1998; en Cd. Altamirano, Gro. México. En términos generales, el presente trabajo consiste en el estudio de algunas medidas preventivas para reparar y proteger el software contra infección de virus informáticos; evaluando algunas estrategias para la protección del software, analizando el proceso de reparación del mismo software que haya sido afectado por un virus informático y evaluando aspectos clave, que permitan la prevención de virus informáticos en programas de cómputo residentes en memoria de la computadora.

1.- Introducción

"MANTENIMIENTO DEL SOFTWARE CONTRA INFECCIÓN DE VIRUS INFORMÁTICOS", es una propuesta que surge como inquietud, desde el momento en que los virus informáticos han entrado al software haciendo deterioros en el mismo. La preocupación es por parte de los programadores y personas que se encuentran relacionadas en el extenso mundo de la informática, ya que un virus representa un gran problema para el equipo de cómputo, también lo ha sido en mayor proporción hacia el software con el cual vamos a operar en la computadora, de ahí surge la inquietud o propósito de este trabajo; primero descubrir qué es un virus, cómo afecta en nuestro equipo, y principalmente, saber qué hacer en caso de que un virus estuviera afectando y de qué manera podemos proteger nuestro software al máximo contra un virus informático. Estas y mucho más inquietudes surgen a cualquier persona que esté relacionada con el ambiente de la informática, quienes pueden manifestar en forma de preguntas y que con esta investigación se ha realizado. En el presente trabajo, usted podrá responder a algunas sus dudas e inquietudes sobre cómo proteger al máximo el software, en cuanto a virus informáticos, pero además podrá conocer cómo reparar software, en caso de que haya sido afectado, ya sea por virus o por consecuencias secundarias, tales como: pistas o sectores defectuosos, los cuales usted conocerá cómo reparar. Es por ello, que el problema principal en el cual nos vamos a ubicar, es en protección contra virus informáticos; y como un aspecto de complementación es el mantenimiento del software ya que el propósito de este trabajo es brindar orientación acerca de cómo debemos reaccionar ante el problema que representa un virus informático; además de conocer los principales tipos de virus y de qué manera afectan tanto al hardware como al software, así como aprender algunos consejos prácticos para que el software no se contamine de virus. Fue preciso elaborar este proyecto para que el usuario tuviera métodos preventivos en cuanto a la problemática que representa un virus informático. La importancia en

la cual se enfocó, al empezar a elaborar este proyecto de investigación, es que se hizo una detallada investigación en la cuál como principal problemática se le dio prioridad a la función que los virus ejercen frente al software deteriorando o bloqueando, la información o deteriorando el contenido del software, por lo tanto consideramos que era de suma importancia que un usuario tuviera una guía para poder protegerse contra un virus y además poder detectar los mismos en el momento en que estos se presenten en el software o información de la computadora. Según estadísticas internacionales, más de un 80% de personas que se encuentran relacionadas en el ambiente de la informática han considerado que un virus es una problemática, ya que nunca lo han podido detectar en el momento mismo en que el software se infecta de estos virus, si no después ya que ocasionó perjuicios severos en el software; por eso es que hemos considerado importante este proyecto, ya que, se sugieren algunas indicaciones y/o consejos prácticos para poder detectar de inmediato un virus antes de que se presenten deterioros en el software el cuál representa un trabajo importante sobretodo para el programador y/o usuario que de él requiera. Con la elaboración de este proyecto, se beneficiarán todas aquellas personas que se encuentren relacionadas en el ambiente de la informática, ya que dicho ambiente está rodeado de software importante que se requiere de un mantenimiento y además de numerosos virus informáticos que cada día provocan más problemas en el software y que por medio de este proyecto, se considera es tarea de todos acabar con este tipo de problemas, desde el momento mismo que se presentan los virus informáticos, y no después que hayan ocasionado algún desperfecto. Es por ello, que en el presente trabajo, se les informa acerca de los virus informáticos más comunes el ambiente técnico, industrial y académico; para así estar alerta cuando alguno de ellos se presente.

2.- Objetivos

En virtud de esta investigación se tiene los siguientes objetivos general y específicos:

2.1. - Objetivo General

Estudiar medidas preventivas para reparar y/o proteger el software contra infección de virus informáticos.

2.2. - Objetivos Especificos

- Evaluar la protección del software contra virus informáticos.
- Evaluar y estudiar el proceso de reparación de software que haya sido afectado por un virus informático.
- Evaluar la prevención de virus informáticos en el software.

3.- Revisión De Literatura (Marco Teórico)

3.1.- Lo Que Es Un Virus Informático

Según Ferreyra (1992), un VIRUS INFORMÁTICO es un programa de cómputo que al ser activado ocasiona perjuicios severos a la información que se encuentra en el disco. Un virus es un programa que crea un programador al mismo tiempo de hacer un sistema; y el virus le sirve al programador para proteger su sistema contra la "Piratería" (Larry,1993). En cambio, Kazmier (1987) establece que cuando un programador hace un programa importante, crea su virus para protegerlo y en caso de que se lo llegaran a "piratear", este programa no dure mucho tiempo funcionando eficientemente en manos del desconocido (pirata). Un virus es un programa y nada más, que contiene instrucciones a realizar en la computadora. Los virus son programas ocultos que esperan determinada orden, tiempo, o proceso para activarse y ocasionar perjuicios severos tanto en el hardware como en el software.(Ferreyra,1992).

3.1.1.- Tipos De Virus

Un virus se activa al teclear una orden(como COPY) o comando (externo) o el nombre de un programa .EXE o .COM que ya esté infectado o que haya sido copiado teniendo la protección de plagio (piratería) como es un virus. Un virus siempre que se activa se va a la memoria de la computadora debido a que es un programa y todo programa se va directo a memoria de la computadora para llevar a cabo las rutinas que en este contiene. De ahí un virus puede ir directo a un disco o a una terminal, etc., todo depende de las instrucciones que contenga dicho virus (Ferreyra,1992).

En esta sección se analizaran los principales "tipos" de virus.

3.1.1.1.- Virus De Memoria

Estos virus cuando se activan se van a la memoria y de ahí ejecutan las instrucciones que ellos realizan por ejemplo: Echar a perder el disco duro, resetear la máquina (y así evitar que se use el software), deteriorando sectores o pistas de un disco duro o flexible, bloqueando la máquina, deteriorando la información en el disco, etc. Según Ferreyra (1992) este tipo de virus están ocultos en el disco generalmente no son localizables en el disco (aunque existen excepciones); es decir, para evitar que el contagio del virus lo mejor es apagar el equipo, para que dicho virus sea destruido, ya que este tipo de virus no se pueden localizar en disco, debido a que solo habitan en memoria. Un ejemplo de virus de memoria tenemos al virus ALIVE el cual poco a poco se va desarrollando y bloquea la máquina en determinado momento. Otro virus de memoria es el virus ROMSEANDIR, el cual al ser activado deteriora algunas partes del hardware y software como la configuración del BIOS de la computadora. Otro virus es el ALBANIAN el cual ocasiona desperfectos en discos a la tabla FAT a al BOOTSECTOR (Larry,1993).

3.1.1.2.- Virus En Disco

Este tipo de virus son los más fáciles de tratar o evitar ya que basta con solo tratarlo con una vacuna para que el virus se localice. La función principal de estos virus es que primero se van a la memoria y después se copian en el disco sin que uno se de cuenta de ello .Y una vez estando en el disco basta con teclear un archivo .EXE o .COM para que este virus se vaya nuevamente a la memoria y realice las

instrucciones que realiza como perjuicios severos en el software y hardware (Larry,1993). Un virus en el disco representa un gran problema cuando uno aun no se ha dado cuenta de que el virus ha sido activado por lo tanto provoca perjuicios severos y aun cuando ya ha sido eliminado del software mediante el uso de una vacuna los perjuicios ocasionados no se pueden reparar (Kazmier,1987). Un ejemplo de virus de disco esta el PIN-PON que se activa solo en procesadores de texto y va destruyendo la información. Otro virus es el NATAS.MBR que daña los discos del MASTER BOOT RECORD. Otros virus son: STONED, NATAS, WXYC, NOIL, etc., los cuales bloquean y destruyen la información (Kazmier, 1987).

3.1.1.3.- Virus Virtuales

Este tipo de virus no se encuentran ni en memoria ni tampoco en disco pero si pueden ocasionar severos perjuicios en el software. Un ejemplo de un virus virtual es por ejemplo un programa .EXE que requiera de una clave para entrar a operar y que al teclear una clave falsa entonces el programa pierde el control y ejecuta un bucle infinito el cual tiende a bloquear la máquina.

3.1.2.- *Cómo Afectan Al Software*

Un virus afecta en el software de muchos modos entre ellos tenemos:

3.1.2.1.- Deteriorando Los Discos Y La Información Que Contienen.

Un virus puede ocasionar deterioros en el disco duro y disco flexible. Los deterioros más frecuentes son los siguientes:

- * Deterioro físico en las pistas y sectores: Se refiere a que puede deteriorar el disco y la información a la vez pero el disco no puede ser utilizable (Larry,1993).

- * Deterioro lógico en la información: Se refiere a que puede deteriorar solo uno o unos cuantos archivos pero el disco puede seguir siendo utilizable (Larry,1993).

3.1.2.2.- Bloqueando La Máquina

Estos virus no afecta a la información ni tampoco causan deterioros en disco ni en el hardware. Su función principal es bloquear la máquina desactivando la interrupción del teclado y así evitar que siga trabajando el usuario hasta que se apague o resetee.

3.1.2.3.- Reseteando La Máquina

Estos virus no ocasionan ningún perjuicio en el software ni en el hardware pero la función que realizan es apagar la máquina automáticamente y volverla a encender para que así pierda el usuario la información y no dejarlo trabajar.

3.1.2.4. - Borrando Información Del Disco

Estos virus tienen una función especial por ejemplo al ponerle "DIR" (comando del DOS) a un disco que está contaminado con este tipo de virus, en lugar de los archivos aparecen algunos caracteres de la tabla ASCII.

3.1.2.5 - Mintiendo Al Usuario

Este tipo de virus informáticos, su función es hacer creer al usuario que la tarea o trabajo o alguna decisión a tomar es la correcta aunque en realidad no lo es. Por ejemplo si usted esta trabajando en un procesador de texto o en una hoja de cálculo y desea salir del paquete y salvar el documento entonces aparentemente se aprecia que ha sido guardado, pero en realidad (si el virus está activado) NO se guarda y eso se comprueba al salir del paquete y/o al buscar el archivo y éste no se encuentra en disco (Kazmier, 1987).

3.2.- Lo Qué Es Una Vacuna

Ferreira (1992) establece que cuando un programador crea un virus, este programador crea también la vacuna para dicho virus, por si acaso, se llegase a contagiar el mismo programador de su virus entonces ya poder quitarlo y poder seguir operando en el software.(Kazmier, 1987). Una vacuna (o antivirus informático) es un programa que localiza un virus informático, lo detecta y a su vez lo limpia, lo destruye y echa afuera del software. Una vacuna es un programa y nada más; el cual tiene determinadas tareas y es útil para un solo virus. Una vacuna solo es útil para un solo virus o para los virus que fue creado por el mismo programador (Kazmier,1987).

3.2.1.- Tipos De Vacunas

Existen varios tipos de vacunas entre ellas se encuentran las siguientes:

3.2.1.1.- Vacunas Para Memoria

Este tipo de vacunas se va a la memoria y de ahí queda residente ejecutando las tareas a realizar (detectar virus) y así el usuario puede estar trabajando y en el momento que se introduce un disco infectado, la vacuna activa una interrupción de sonido la cual quiere decir que el disco debe ser revisado para virus (Kazmier,1987). Un ejemplo de este tipo de vacunas tenemos a la utilidad NORTON.

3.2.1.2.- Vacunas Para Disco Y Memoria

Este tipo de vacunas al ser ejecutadas se van a la memoria de la computadora y comienzan el chequeo el cual consiste en verificar que la memoria no tenga virus (en caso contrario manda mensajes de apagar la máquina) y después verificar o checar que el disco en determinada unidad esté libre de virus, en caso contrario detecta y limpia el disco de virus (Kazmier,1987).

Entre las principales vacunas más eficientes se encuentran:

SCAN
KILLER
PCSCAN
NAVBOOT
SCAN2
SCANPM
NAV
MSAV
FINDVIRU
FPROT
SCANNAT

Este tipo de vacunas tienen la función de quitar el virus del disco pero no de la memoria. Sin embargo, una vez que ha quitado el virus de disco, la vacuna no puede reparar los perjuicios ya ocasionados en el software (Kazmier, 1987).

3.3.- Cómo Evitar La Infección De Un Virus

Para evitar la infección es necesario seguir algunos pasos necesarios de medidas preventivas. Por ejemplo:

- Apagar la máquina antes de usarla (si está encendida).
- Revisar de virus un disco antes de meterlo a la computadora.
- Proteger contra escritura los discos.
- Tener la seguridad de que cuando copien un disco que éste no tenga virus (Kazmier, 1987).

4.- Materiales Y Métodos

4.1.- Ubicación Del Trabajo

El trabajo se va a desarrollar en el laboratorio del ITA No 25, ubicado en la Región de Tierra Caliente, Municipio de Pungarabato, Estado de Guerrero.

4.2.- Materiales

Entre los materiales que se van utilizar durante el proceso del trabajo tenemos: Discos flexibles, discos duros, máquina con procesador 486 DX, software calificado para el uso de vacunas y software relacionado (vacunas informáticas, programas de prueba, por mencionar algunos).

4.3.- Ubicación De Las Variables

4.3.1.- *Prevención Y Protección Contra Virus Informáticos*

4.3.1.1.- Máquina Encendida

Un método que ha resultado eficiente para evitar la infección de virus es apagar la máquina antes de usarla (si es que está encendida) y arrancar con un sistema operativo libre de virus. Si una máquina está encendida y esta tiene virus en memoria entonces si uno llega y mete su disco y hace copia o realiza algunas tareas es probable que este disco se contagie del virus que contenga ; por lo tanto si antes de empezar a trabajar apagamos la máquina ; el virus se destruye al ser apagada, debido a que es un programa y todo programa en memoria se destruye al ser apagada la computadora.

Para que sea eficiente este método se debe apagar la computadora desde el botón POWER. Pero si se apaga con RESET, es decir, si tan solo se "resetea", probablemente el virus no sea eliminado, debido a que existen virus que contienen esas instrucciones de respaldo.

4.3.1.2.- Discos Magnéticos

Un método de prevención para evitar virus informáticos, es que al encender una máquina, se debe arrancar con un disco de sistema operativo libre de virus. Un método eficiente y que ha tenido gran validez, es vacunar un disco antes de meterlo a la computadora para que la vacuna revise si tiene o no virus y así poder eliminarlo y trabajar más cómodamente (con ausencia de virus).

Otro método más eficiente es proteger contra escritura un disco flexible para evitar que este sea contagiado en caso de que la máquina tenga virus en disco duro o en la memoria. En caso de que la memoria no tenga virus y tampoco el disco de arranque, pero si tiene virus el disco duro es necesario que se vacune y si no desaparece el virus es necesario formatearlo a bajo nivel con DEBUG o particionarlo nuevamente con FDISK y darle formato con FORMAT teniendo previo conocimiento de que la información que contenga ya no podrá recuperarse con UNDELETE. Pero si desea seguir trabajando desde la unidad "A" y el disco duro tiene virus es necesario que desactive el disco duro metiéndose al SETUP y así al ser desactivado el disco duro todo trabajo que realice desde la unidad "A" será libre de virus (si es que el disco desde "A" también está limpio de virus).

4.3.1.3.- Memoria Para Virus

En caso de que no se cuente con una vacuna eficiente y tengas un virus en el disco, entonces es necesario llevar a cabo este método que consiste en correr un programa que ocupe demasiada memoria y así con esto no dejar espacio para que el virus se active. Esto es porque como todo virus es un programa si no existe memoria suficiente para cargarlo entonces al no caber en memoria no ejecuta las tareas a realizar.

4.3.1.4.- En Caso De Infección

Algunas recomendaciones (medidas preventivas) para evitar al máximo un virus se debe:

- Apagar la máquina antes de usarla(si está encendida).
- Proteger los disco flexibles contra escritura.
- Arrancar la máquina con un disco limpio de virus.
- Revisar los discos con una o varias vacunas antes de empezar a operar en la computadora.
- Al hacer copia de un disco o un archivo verificar que el disco fuente esté libre de virus.
- Actualizar las vacunas que han caducado (expirado sus archivos de definición de virus).

4.3.2.- Reparación Del Software Contra Virus Informáticos

4.3.2.1.- Vitalidad De Las Vacunas

Una vacuna informática, es un programa que tiene una fecha de caducidad y al pasar de determinado tiempo ya no puede usarse esta vacuna de igual forma de eficiente que al principio, esto es debido a que cada vez existen virus nuevos y a su vez, vacunas nuevas.

4.3.2.2.- Uso De Las Vacunas

Una manera de utilizar una vacuna es la siguiente:

- 1.- Arrancar con un disco libre de virus
- 2.- Teclear el archivo ejecutable de la vacuna y a qué unidad se dirige y los parámetros existentes.
- 3.- Quitar la protección al disco que va a ser checado.
- 4.- Salir

4.3.2.3.- Infección Activa

En caso de que un virus exista en un disco y este virus no fue detectado por la vacuna se debe a los siguientes factores:

- 1.- Que esa vacuna no conoce al virus.
- 2.- Que esa vacuna no es la apropiada
- 3.- Que el virus es sólo un virus de memoria
- 4.- Que puede ser que el virus sea virtual

En caso de que un virus exista en un disco y este virus al ser detectado no fue limpiado se debe a:

- 1.- Que la vacuna ya caducó.
- 2.- Que el virus esta muy desarrollado.
- 3.- Que faltó especificar parámetros. para limpiar (como: CLEAN o /LIMPIA o /REPAIR etc.).
- 4.-Que el disco estaba protegido contra escritura.

Si a pesar de cumplir los requisitos anteriores el virus NO desaparece, entonces se recomienda que se evite usar al máximo el software con el que fue activado, ya que puede ocasionar perjuicios severos.

4.3.2.4.- Uso Del D.O.S. Y Utilerias.

En ocasiones, al eliminar un virus del disco, este virus afecta en el software, y tiende a deteriorar los sectores o pistas de un disco dejándolas defectuosas y en ocasiones el disco ya no puede ser utilizable con la misma capacidad que al principio; para ello existen algunos comandos o utilerias del D.O.S., de NORTON, y PC-TOOLS; los cuales contribuyen a librarnos de ese gran problema.

4.3.2.4.1.- Scandisk y Chkdsk

Scandisk y Chkdsk son comandos del DOS, que nos permiten reparar las pistas y sectores defectuosos en los discos.

Para usar CHKDSK se requiere:

* Tener un disco de sistema operativo con el archivo CHKDSK.COM.

* Desde raíz teclee, por ejemplo: CHKDSK [unidad] : /F /V

Donde :

- Unidad : Es la unidad donde se encuentra el disco a reparar.
- /F : Permite reparar los defectos en el disco.
- /V : Muestra el reporte del estado los archivos que contiene el disco.

NOTA: Si se omite el modificador /F no se podrá reparar ningún defecto en disco.

* Por ultimo presione ENTER.

Para usar SCANDISK se requiere:

* Tener un disco de sistema operativo con el archivo SCANDISK.EXE.

* Desde raíz teclee, por ejemplo: SCANDISK [unidad]:

Donde :

- Unidad : Es la unidad donde se encuentra el disco a reparar.
- Es más recomendable usar Scandisk ya que es un comando mucho mas potente que Chkdsk.

* Por ultimo presione ENTER.

4.3.2.4.2.- PC-TOOLS

En ocasiones algunos defectos ocasionados por un virus no se pueden corregir con SCANDISK ni con CHKDSK; entonces es mucho más eficiente usar PC-TOOLS utilerías.

Para usar PC-TOOLS se requiere:

- * Tener un disco de PC-TOOLS utilerías.
- * Desde raíz teclee : PC-TOOLS
- * Presione ENTER. Después saldrá un menú en donde por medio de una flecha se puede elegir el comando.
- * Elija el comando CHKDSK y presione ENTER.
- * Ya que salga el mensaje de solicitud de unidad, solicite la unidad a reparar y presione ENTER.
- * Por ultimo salga del menú seleccionando QUIT.

4.3.2.4.3.- Norton Disk Doctor

En ocasiones algunos virus al ser eliminados del disco tienden a ocasionar desperfectos a la tabla FAT del disco; por lo tanto si se intenta reparar con CHKDSK o SCANDISK se puede producir un error al leer el disco y ser imposible recuperar la información que se encuentra en el mismo. Tampoco se podrán reparar los desperfectos que haya en el disco ocasionado por el virus. En utilerías de NORTON existe un archivo llamado NDD.EXE el cual es mucho más potente que SCANDISK y CHKDSK.

Para usar NDD se requiere:

- * Tener un disco de utilerías NORTON con el archivo NDD.EXE.
- * Desde raíz teclee por ejemplo: NDD [unidad]:

Donde :

- Unidad : Es la unidad donde se encuentra el disco a reparar.

Conclusiones Preliminares

En algunas situaciones particulares, los virus informáticos producen daño a la información o software de las computadoras, teniendo en cuenta que uno de los factores de gran influencia de la existencia de los virus informáticos, es precisamente el bajo control que existe respecto a la protección de los derechos de autor del software creado por un programador. Esta situación obliga a los desarrolladores a incrustar condiciones en el software implementado, para garantizar que después de haber vencido la licencia de uso, este ya no pueda ser utilizado o plagiado. En esos términos, el desarrollador del software, puede proteger su creación, y ello da lugar a una gran variedad de negocios en la industria de software, porque ahora se tendrá que gastar en licencia de uso de software antivirus o vacunas. Es por ello, que en este proyecto se destacan algunos aspectos relevantes con información de virus informáticos (y vacunas); así como, algunos consejos para amortiguar el problema de la infección de este tipo de virus. Finalmente, teniendo en cuenta que este proyecto está orientado a plataformas Microsoft (DOS y/o Windows), es por ello que, como trabajo futuro, uno de los propósitos podría ser evaluar si en otras plataformas (como: MacOS o Linux) incurrir o no estas mismas problemáticas, y en qué dimensiones, pueden ser planteadas en comparación con las evaluadas en el presente trabajo.

Literatura Citada (Referencias)

- 1.- Ferreyra G.(1992). "Virus en las computadoras". Macrobit, México, D.F.
- 2.- Larry J. (1993).- "Los Virus". PH, México, D.F.
- 3.- Kazmier J. (1987). "Los virus en el sistema". McGH.