

Guía N° 16	Antivirus
-------------------	------------------

Introducción :	Esta guía aborda el tema de los virus y antivirus, y como lidiar con ellos en los computadores que se utilizan.
-----------------------	---

Objetivos :	<ul style="list-style-type: none"> - Diferenciar conceptos: virus y antivirus - Identificar la importancia de actualizar frecuentemente el antivirus - Lograr autonomía en la actualización de antivirus.
--------------------	--

Material de Apoyo

16.1 Definiciones previas

Programa o Aplicación	Un conjunto de rutinas y subrutinas, desarrolladas en un lenguaje de programación, que se unen para desarrollar una tarea en común.
Virus	Desde un punto de vista formal es, en esencia, una aplicación como muchas otras, pero su objetivo, por lo general, es destructivo, dañino o molesto.
Antivirus	Un antivirus es otra aplicación que detecta a los virus y los elimina o los desinfecta del sistema.
Boot o Sector de Arranque	Un sector reservado de la información que se guarda en el disco duro cuya finalidad es almacenar parte de un sistema operativo.

16.2 Recursos necesarios

<p>Archivo Estándar EICAR (European Institute for Computer Antivirus Research). El archivo EICAR es un archivo de texto (con extensión COM) y que contiene una secuencia de caracteres los cuales son reconocidos, por el antivirus, como un virus.</p> <p>Este archivo contiene 68 caracteres, cuya secuencia es:</p> <p style="text-align: center;">X5O!P%@AP[4\PZX54(P^)7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H*</p>

16.3 Definir el concepto de virus y antivirus

<p>Un virus es una aplicación o programa, que tiene como objetivo generalmente destruir o dañar información del computador o, sencillamente, molestar.</p> <p>Los antivirus son programas creados por empresas especializadas que tienen por misión inspeccionar un computador en busca de virus y, una vez encontrado algún programa de este tipo, eliminarlo definitivamente del sistema.</p>

16.4 Tipos de virus

Tipo	Descripción
------	-------------

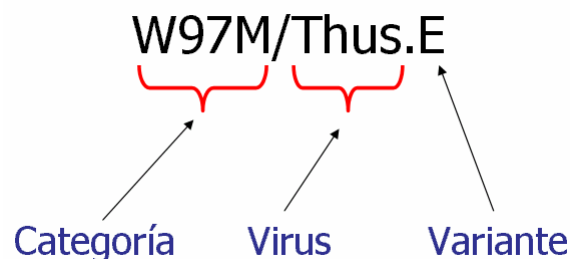
Virus de Fichero	Este tipo de virus se encarga de infectar programas o archivos ejecutables (archivos con extensiones EXE o COM). Al realizar la ejecución de uno de estos programas, de forma directa o indirecta, el virus se activa produciendo los efectos dañinos que le caractericen en cada caso.
Virus de Boot	Este virus infecta el sector Boot del disco. El término Boot representa lo que se denomina "sector de arranque". Se trata de una sección muy importante en un disco (disquete o disco duro), en la cual se guarda la información sobre las características de ese disco, además de incluir un programa que permite arrancar el ordenador con ese disco, determinando previamente si existe sistema operativo en el mismo. Este tipo de virus de Boot, no afectan a los archivos por lo que el contenido del disco no estará en peligro a no ser que se intente arrancar el ordenador con dicho disco, con lo cual se ejecuta en virus.
Virus de Macro	Estos virus realizan infecciones sobre los archivos (documentos, libros, presentaciones y/o bases de datos) que se han creado con determinadas aplicaciones o programas. Cada uno de estos tipos de ficheros puede tener adicionalmente unos pequeños programas, denominados macros. Una macro es un micro-programa que el usuario asocia al fichero que ha creado con determinadas aplicaciones. Al abrir un documento que contenga macros, éstas se cargarán de forma automática (ejecutándose o esperando que el usuario decida ejecutarlas). En ese instante o posteriormente, el virus actuará realizando cualquier tipo de operación perjudicial. Por otra parte, estos virus pueden infectar las plantillas genéricas o globales (a través de las macros) que las herramientas (procesadores de texto, hojas de cálculo,...) utilizan. Al abrir un documento, hoja de cálculo o base de datos con la plantilla infectada, éstos se infectarán. Este es el método más habitual que emplean los virus de macro para extender sus infecciones.
Gusanos	Los gusanos no intentan infectar otros ficheros. Su único objetivo es propagarse o expandirse a otros computadores de la forma más rápida posible. Por otra parte, emplean técnicas para replicarse (propagarse). En realidad su objetivo es crear copias de sí mismos y con ellas realizar infecciones en otros computadores. Las infecciones producidas que éstos realizan casi siempre son a través de medios como: el correo electrónico, las redes de ordenadores y los canales de IRC en Internet, entre los que podemos mencionar. También es posible que se repliquen dentro de la memoria del computador.
Caballos de Troya	Los troyanos no se pueden considerar virus como tales. Recogen su nombre de la mitología, utilizando esa estrategia para ingresar a los computadores. Llegan al computador por cualquier medio, cuando se ejecuta el programa, se instala en nuestro computador otro programa que podrá producir efectos destructivos. En un principio, el troyano podría no activar sus efectos. De todas formas, cuando esto ocurra (cuando se cumple la condición de activación), se podrán eliminar archivos, perder la información del disco duro, o abrirse los posibles huecos de seguridad a modo de puertas traseras (backdoor) por las que nuestro equipo podría ser

	atacado.
Hoaxes	Los Hoaxes son mensajes tremendistas de alerta o advertencia relacionada con virus desconocidos de diversos tipos. Estos mensajes informan que ha aparecido una nueva especie viral, la misma que "se está propagando a través de los canales de Internet para destruir la información o afectar a los sistemas de los computadores". Estos mensajes deliberadamente falsos, son creados con la intención de provocar pánico. Los usuarios ingenuos, caen en la trampa y siguiendo las instrucciones, empiezan a re-transmitirlos, ocasionando la saturación de los buzones de correo y la consiguiente congestión de las conexiones en Internet.

16.5 Clasificación

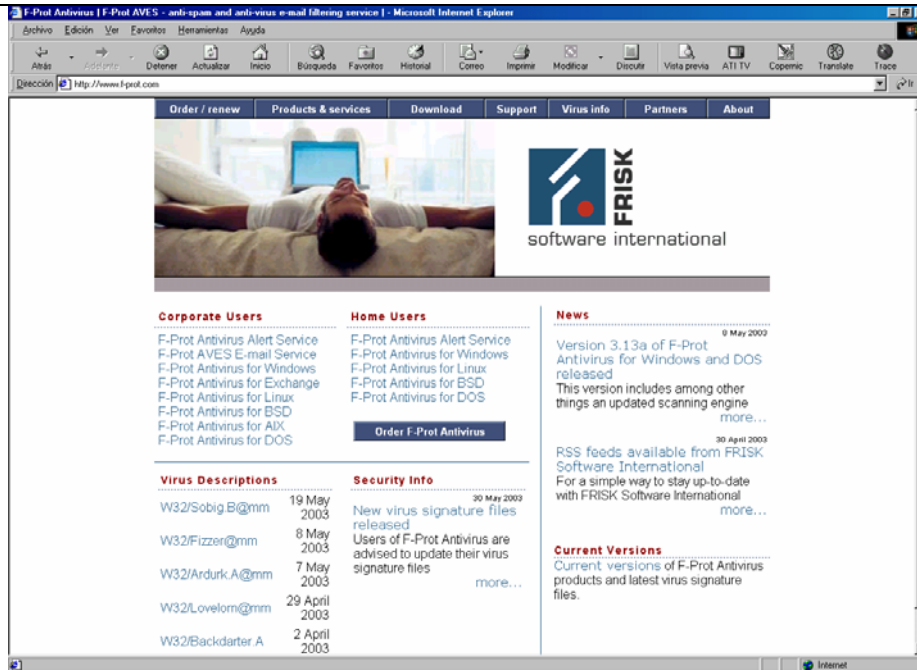
Los virus se pueden clasificar en tres tipos:

- **Categoría:** Los virus se clasifican en varios tipos, dependiendo de sus formatos de archivo y sus rutinas para infectar, indicadas anteriormente. Para distinguirlos se les antepone un prefijo que puede ser W97M, W32, etc, esto según el tipo de virus que sea.
- **Virus:** es el nombre en si de un virus.
- **Variante:** para un virus pueden existir muchas variantes del mismo, por eso se determina esta especificación. Las variantes son distintas versiones del mismo virus que varían levemente, por ejemplo la fecha de activación.

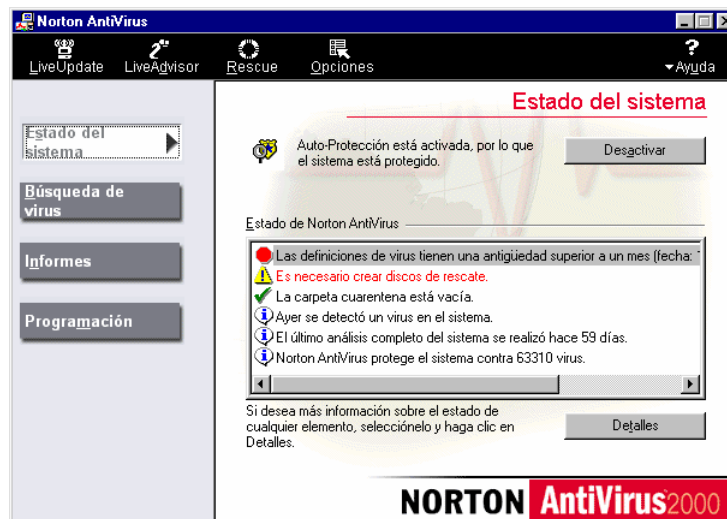


16.6 Manejo de Antivirus

Existen muchas empresas de antivirus, los establecimientos de Enlaces han recibido los Antivirus McAfee y Norton. También es una buena opción utilizar antivirus que se pueden bajar gratis de Internet, un buen ejemplo de esto es el antivirus F-PROT, el cual se puede bajar de www.f-prot.com.



Los antivirus como Norton y McAfee actúan en el sistema, protegiéndolo según como se programe. Se caracterizan por tener una interfaz amigable (diferente dependiendo de la versión del antivirus), desde la cual se acceden a todas sus opciones, por ejemplo, Norton Antivirus utiliza la siguiente interfaz:



Para que los antivirus mantengan protegido al computador de los virus, deben actualizarse su definición de virus de manera periódica (semanal o quincenalmente). En el caso de tener un antivirus registrado como Norton o McAfee, ellos traen una opción de actualización automática, con el cual se conecta directamente la empresa y actualiza la definición de virus. La definición de virus es el registro de todos los virus que el antivirus reconoce y puede, no siempre, desinfectar; por lo que resulta importante siempre mantenerla actualizada para que nuestro antivirus pueda reconocer los virus más recientes.

Específicamente F-PROT, por ser un antivirus manual (no actúa en el sistema en forma automática, debe ser ejecutado por el usuario), se debe actualizar directamente desde su página en Internet.

16.7 Síntomas para detectar la posibilidad de un virus en el sistema

Los siguientes síntomas pueden ser evidencias de la presencia de algún virus, pero no necesariamente:

- Lentitud en la ejecución de programas o el sistema operativo.
- Mayores tiempos de carga o la no ejecución de los programas, por ejemplo Word.
- Desaparición de archivos o carpetas.
- Imposibilidad de acceso al contenido de los archivos.
- Mensajes de errores inesperados y no habituales.
- Disminución del espacio de memoria y disco duro.
- Errores del sistema operativo.
- Archivos renombrados o duplicados.
- Alteración de las propiedades de los archivos.
- El teclado o ratón no funciona correctamente.

16.8 Prevención de virus

Para prevenir el “contagio” de virus en el computador, podemos tener en cuenta sencillos pasos de precaución:

- Cada vez que se necesite utilizar un disquete que se halla utilizado en otro computador o se desconozca su procedencia, hay que revisarlo con el antivirus que se tenga instalado.
- Revisar todo lo que descarga desde Internet con nuestro antivirus antes de utilizarlo.
- Revisar todos los documentos que se adjuntan en los correos electrónicos antes de abrirlos.
- Es de vital importancia tener un antivirus instalado en el equipo, al cual se le deben actualizar sus definiciones de virus periódicamente.
- Si se desea utilizar un CD no original, debe ser escaneado por el antivirus, porque puede tener virus.

16.9 Descargar definiciones de virus por Internet

Páginas de descarga de las definiciones de virus de distintos fabricantes de antivirus, como Norton Antivirus, McAfee, F-Secure y F-PROT:

<http://download.mcafee.com/default.asp>
<http://www.symantec.com/avcenter/download.html>
<http://www.f-secure.com/download-purchase/>
<http://www.f-prot.com/>