ACIMED
ISSN 1024-9435 *versión impresa*

ACIMED v.11 n.5 Ciudad de La Habana sep.-oct. 2003

Como citar este artículo

Análisis comparativo de los principales sistemas antivirus

Lic. Luis Armas Montesino1

Resumen

Con el objetivo de comprender los virus informáticos, así como de analizar y comparar los principales sistemas antivirus existentes, se procedió a revisar algunas de las comparativas principales publicadas en sitios y fuentes de reconocido prestigio en este tema. Se trató un grupo de elementos teóricos sobre los virus y los sistemas antivirus: definiciones, clasificaciones, características, estructura, etcétera. Se analizó y comparó un conjunto de sistemas antivirus, ubicados entre los más poderosos y populares en la literatura consultada: Norton Antivirus, McAfee VirusScan, Sophos, Norman Virus Control 5.0, Panda Platinum 6.22, F-Secure, PC-Cillin 7.5 y AVP. Para el trabajo en redes, se recomienda el uso de F-Secure, PC-Cillin, y el Norman Antivirus. Para usuarios independientes, Norton Antivirus, McAfee VirusScan, AVP y Panda. Ningún sistema antivirus ofrece una protección completa, pero el uso correcto de estas herramientas produce una sensible reducción de los daños y pérdidas provocadas por este flagelo en la red.

Clasificación: Artículo docente

Descriptores (DeCS): SEGURIDAD COMPUTACIONAL
Descriptores (DeCI): VIRUS INFORMATICO/evolución; CRIMEN INFORMATICO; PROGRAMAS ANTIVIRUS/ventajas; SEGURIDAD COMPUTACIONAL

Abstract

Aimed at understanding informatic viruses, and analyzing and comparing the main antivirus systems avalilable a review of some comparative analysis published in sites and services of recognized prestige in this subject was carried out. A group of theorical elements on virus and antivirus systems: definitions, classification, features, structure was studied. A set of antivirus systems was analyzed and compared located among the most powerful and used in the reviewed literature: Norton Antivirus, McAfee VirusScan, Sophos, Norman Virus Control 5.0, Panda Platinum 6.22, F-Secure, PC-Cillin 7.5 and AVP. We recommend the use of F-Secure, PC-Cillin and Norman Antivirus to work in networks. For independent users, Norton Antivirus, McAfee VirusScan, AVP and Panda are the best choice. Although any antivirus system offers a complete protection we recommend the correct use of these tools to achieve a sensible reduction of the damages and losses caused by this flagellum in the network.

Classification: Learning article

Subject headings (DeCS): COMPUTER SECURITY
Subject headings (DeCI): COMPUTER VIRUS/evolution; COMPUTER CRIME; ANTIVIRUS PROGRAMS/advantages; COMPUTER SECURITY

En los años 50, los especialistas del área de la computación discutieron, por primera vez, la posibilidad de

generar un programa capaz de duplicarse y extenderse entre las computadoras. Pero, no fue hasta 1983, que se creó un software de virus real, cuando un estudiante en la Universidad de California, *Fred Cohen*, elaboró una tesis de doctorado sobre el tema.

Hace algunos años cuando se hablaba de las infecciones por virus, algunas empresas argumentaban que ellas no presentaban ese problema; consideraban que al extraer las torres de discos de las estaciones de trabajo de sus usuarios, evitarían que ellos invadieran su red de computadoras. Hoy, todos saben muy bien que el problema de los virus no se resuelve tan simplemente, porque dichos usuarios disponen, además, de acceso a Internet y a correo electrónico. Un usuario puede recibir un correo infectado con un virus desde cualquier parte del mundo, y en pocos minutos, su red estará totalmente infectada.1

Normalmente las empresas piden a los administradores de redes que comparen los antivirus existentes para determinar cuáles son capaces de reconocer y eliminar la mayor cantidad de virus posibles.2 Cada día crece el número de virus informáticos que circulan por las redes, fundamentalmente mediante el correo electrónico y desde Internet. Crece, por lo tanto, la necesidad de proteger los recursos de software y en especial la información.

El objetivo del presente trabajo es revisar los sistemas antivirus más empleados a escala mundial con el objetivo de determinar cuál o cuáles son los más convenientes para la protección de los recursos de información de una organización o empresa de acuerdo con las características particulares de cada una de ellas.

MARCO TEÓRICO

¿Qué es un virus?

Un virus es un pequeño programa capaz instalarse en la computadora de un usuario sin su conocimiento o permiso. Se dice que es un programa parásito porque ataca a los archivos o sectores de "booteo" y se replica para continuar su esparcimiento.3

Algunos se limitan solamente a replicarse, mientras que otros pueden producir serios daños a los sistemas. Nunca se puede asumir que un virus es inofensivo y dejarlo "flotando" en el sistema. Ellos tienen diferentes finalidades. Algunos sólo 'infectan', otros alteran datos, otros los eliminan, algunos sólo muestran mensajes. Pero el fin último de todos ellos es el mismo: propagarse.

Clasificación general de los virus

Existen diferentes tipos de virus:1

- Virus de macros/código fuente. Se adjuntan a los programas fuente de los usuarios y a las macros utilizadas por: procesadores de palabras (Word, Works, WordPerfect), hojas de cálculo (Excell, Quattro, Lotus), etcétera.
- Virus mutantes. Son los que, al infectar, realizan modificaciones a su código, para evitar su de detección o eliminación (NATAS o SATÁN, Miguel Angel, por mencionar algunos).
- Gusanos. Son programas que se reproducen y no requieren de un anfitrión, porque se "arrastran" por todo el sistema sin necesidad de un programa que los transporte.
  Los gusanos se cargan en la memoria y se ubican en una determinada dirección, luego se copian a otro lugar y se borran del que ocupaban y así sucesivamente. Borran los programas o la información que encuentran a su paso por la memoria, causan problemas de operación o pérdida de datos.
- Caballos de Troya. Son aquellos que se introducen al sistema bajo una apariencia totalmente diferente a la de su objetivo final; esto es, que se presentan como información perdida o "basura", sin ningún sentido. Pero al cabo de algún tiempo, y de acuerdo con una indicación programada, "despiertan" y comienzan a ejecutarse y a mostrar sus verdaderas intenciones.
- Bombas de tiempo. Son los programas ocultos en la memoria del sistema, en los discos o en los archivos de programas ejecutables con tipo COM o EXE, que esperan una fecha o una hora determinada para "explotar". Algunos de estos virus no son destructivos y solo exhiben mensajes en las pantallas al momento de la "explosión". Llegado el momento, se activan cuando se ejecuta el programa que los contiene.

- Autorreplicables. Son los virus que realizan las funciones mas parecidas a los virus biológicos, se autorreproducen e infectan los programas ejecutables que se encuentran en el disco. Se activan en una fecha u hora programada o cada determinado tiempo, a partir de su última ejecución, o simplemente al "sentir" que se les trata de detectar. Un ejemplo de estos es el virus llamado Viernes 13, que se ejecuta en esa fecha y se borra (junto con los programas infectados), para evitar que lo detecten.
- Infectores del área de carga inicial. Infectan los disquetes o el disco duro, se alojan inmediatamente en el área de carga. Toman el control cuando se enciende la computadora y lo conservan todo el tiempo.
- Infectores del sistema. Se introducen en los programas del sistema, por ejemplo COMMAND.COM y otros que se alojan como residentes en memoria. Los comandos del sistema operativo, como COPY, DIR o DEL, son programas que se introducen en la memoria al cargar el sistema operativo y es así como el virus adquiere el control para infectar todo disco que se introduzca a la unidad con la finalidad de copiarlo o simplemente para revisar sus carpetas.
- Infectores de programas ejecutables. Estos son los virus más peligrosos, porque se diseminan fácilmente hacia cualquier programa como hojas de cálculo, juegos, procesadores de palabras.

La infección se realiza al ejecutar el programa que contiene al virus, que, en ese momento, se sitúa en la memoria de la computadora y, a partir de entonces, infectará todos los programas cuyo tipo sea EXE o COM, en el instante de ejecutarlos, para invadirlos mediante su autocopia.

Aunque la mayoría de estos virus ejecutables "marcan" con un byte especial los programas infectados --para no volver a realizar el proceso en el mismo disco--, algunos de ellos, como el de Jerusalén, se duplican tantas veces en el mismo programa y en el mismo disco, que llegan a saturar su capacidad de almacenamiento.

Clasificación por el modo en que actúan

En la literatura revisada, se encontraron distintas clasificaciones según el modo en que los virus infectan:3

- Programa: Infectan archivos ejecutables como .com / .exe / .ovl / .drv / .sys / .bin
- Boot: Infectan los sectores Boot Record, Master Boot, FAT y la tabla de partición.
- Múltiples: Infectan programas y sectores de "booteo".
- Bios: Atacan al Bios para desde allí reescribir los discos duros.
- Hoax: Se distribuyen por correo y la única forma de eliminarlos es el uso del sentido común. Al respecto, se trata de virus que no existen y que se utilizan para aterrar a los novatos especialmente en Internet a pesar que los rumores lo muestran como algo muy serio y, a veces, la prensa especializada toma la información. Por lo general, como se expresó, la difusión se hace por cadenas de correo con terribles e inopinadas advertencias. En realidad el único virus es el mensaje. A continuación se relacionan una serie de supuestos "virus", por lo que es aconsejable ignorar los mensajes que aparecen y no ayudar a replicarlos para continuar con la cadena, porque se crearon precisamente para producir congestionamiento en Internet.

Los virus stealth (invisibles) engañan a los software antivirus. Esencialmente, un virus de este tipo conserva información sobre los archivos que ha infectado y después espera en memoria e intercepta cualquier programa antivirus que busque archivos modificados y le ofrece la información antigua en lugar de la nueva.

Los virus polimórficos se alteran sólo cuando se duplican, de modo que el software antivirus que busca comportamientos específicos no encontrará todas las apariciones de los virus; los que sobreviven pueden seguir duplicándose.

La función de un programa antivirus es detectar, de alguna manera, la presencia o el accionar de un virus informático en una computadora. Este es el aspecto más importante de un antivirus, independientemente de las prestaciones adicionales que pueda ofrecer, porque el hecho de detectar la posible presencia de un virus informático, detener el trabajo y tomar las medidas necesarias, es suficiente para eliminar un buen porcentaje de los daños posibles. Adicionalmente, un antivirus puede dar la opción de erradicar un virus informático de una entidad infectada.3

Técnicas para la detección de virus informáticos

Existen diferentes técnicas para la detección de los virus informáticos.3

1. Scanning o rastreo: Fue la primera técnica que se popularizó para la detección de virus informáticos, y que todavía se utiliza -aunque cada vez con menos eficiencia. Consiste en revisar el código de todos los archivos ubicados en la unidad de almacenamiento - fundamentalmente los archivos ejecutables - en busca de pequeñas porciones de código que puedan pertenecer a un virus informático.

   La primera debilidad de este sistema radica en que al detectarse un nuevo virus, este debe aislarse por el usuario y enviarse al fabricante de antivirus, la solución siempre será a posteriori: es necesario que un virus informático se disperse considerablemente para que se envíe a los fabricantes de antivirus. Estos lo analizarán, extraerán el trozo de código que lo identifica y lo incluirán en la próxima versión de su programa antivirus. Este proceso puede demorar meses a partir del momento en que el virus comienza a tener una gran dispersión, lapso en el que puede causar graves daños sin que pueda identificarse.

   Otro problema es que los sistemas antivirus deben actualizarse periódicamente debido a la aparición de nuevos virus. Sin embargo, esta técnica permite identificar rápidamente la presencia de los virus más conocidos y, al ser estos los de mayor dispersión, posibilita un alto índice de soluciones.

2. Comprobación de suma o CRC (Ciclyc Redundant Check): Es otro método de detección de virus. Mediante una operación matemática que abarca a cada byte del archivo, generan un número (de 16 ó 32 bytes) para cada archivo. Una vez obtenido este número, las posibilidades de que una modificación del archivo alcance el mismo número son muy pocas. Por eso, es un método tradicionalmente muy utilizado por los sistemas antivirus. En esta técnica, se guarda, para cada directorio, un archivo con los CRC de cada archivo y se comprueba periódicamente o al ejecutar cada programa. Los programas de comprobación de suma, sin embargo, sólo pueden detectar una infección después de que se produzca. Además, los virus más modernos, para ocultarse, buscan los ficheros que generan los programas antivirus con estos cálculos de tamaño. Una vez encontrados, los borran o modifican su información.
3. Programas de vigilancia: Ellos detectan actividades que podrían realizarse típicamente por un virus, como la sobreescritura de ficheros o el formateo del disco duro del sistema. En esta técnica, se establecen capas por las que debe pasar cualquier orden de ejecución de un programa. Dentro del caparazón de integridad, se efectúa automáticamente una comprobación de suma y, si se detectan programas infectados, no se permite que se ejecuten.
4. Búsqueda heurística: Es otra técnica antivirus que evita la búsqueda de cadenas. Con ella, se desensambla el programa y se ejecuta paso a paso, a veces mediante la propia CPU. De ese modo, el programa antivirus averigua qué hace exactamente el programa en estudio y realiza las acciones oportunas. En general, es una buena técnica si se implementa bien, aunque el defecto más importante es la generación de falsas alarmas, que no se tiene la certeza de que un programa sea un virus en función de su comportamiento. La mayoría de los virus nuevos evitan directamente la búsqueda heurística modificando los algoritmos, hasta que el programa antivirus no es capaz de identificarlos.

A pesar de utilizar estas cuatro técnicas, ningún programa puede asegurar la detección del ciento por ciento de los virus.

La calidad de un programa antivirus no sólo se demuestra por el número de virus que es capaz de detectar, sino también por el número de falsas alarmas que produce, es decir, cuando el programa antivirus estima que ha localizado un virus y en realidad se trata de un fichero sano (falso positivo). Puede ocurrir que un fichero presente una combinación de bytes idéntica a la de un virus, y el programa antivirus indicaría que ha detectado un virus y trataría de borrarlo o de modificarlo.

Programas antivirus

Estructura de un programa antivirus

Un programa antivirus está compuesto por 2 módulos principales: el primero denominado de control y el

segundo de respuesta. A su vez, cada uno de ellos se divide en varias partes:3

1. Módulo de control: posee la técnica para la verificación de integridad que posibilita el hallazgo de cambios en los archivos ejecutables y las zonas críticas de un disco rígido, así como la identificación de los virus. Comprende diversas técnicas para la detección de virus informáticos y de códigos dañinos: En caso necesario, busca instrucciones peligrosas incluidas en programas para garantizar la integridad de la información del disco rígido. Esto implica descompilar (o desensamblar) en forma automática los archivos almacenados y tratar de ubicar sentencias o grupos de instrucciones peligrosas. Finalmente, el módulo de control también efectúa un monitoreo de las rutinas mediante las que se accede al hardware de la computadora (acceso a disco, etc.). Al restringir el uso de estos recursos, -por ejemplo, cuando se impide el acceso a la escritura de zonas críticas del disco o se evita que se ejecuten funciones para su formateo-, se limita la acción de un programa.
2. Módulo de respuesta: la función alarma se encuentra incluida en todos los programas antivirus y consiste en detener la acción del sistema ante la sospecha de la presencia de un virus informático. Se informa la situación mediante un aviso en pantalla. Algunos programas antivirus ofrecen, una vez detectado un virus informático, la posibilidad de erradicarlo.

Características que debe poseer un sistema antivirus

La expresión "cuál es el mejor antivirus", puede variar de un usuario a otro. Es evidente que para un usuario inexperto el término define casi con seguridad al software que es más fácil de instalar y utilizar, algo totalmente intranscendente para usuarios expertos, administradores de redes, etc.4

No se puede afirmar que exista un solo sistema antivirus que presente todas las características necesarias para la protección total de las computadoras; algunos fallan en unos aspectos, otros tienen determinados problemas o carecen de ciertas facilidades. De acuerdo con los diferentes autores consultados, las características esenciales son las siguientes:5,6

1. Gran capacidad de detección y de reacción ante un nuevo virus.
2. Actualización sistemática.
3. Detección mínima de falsos positivos o falsos virus.
4. Respeto por el rendimiento o desempeño normal de los equipos.
5. Integración perfecta con el programa de correo electrónico.
6. Alerta sobre una posible infección por las distintas vías de entrada (Internet, correo electrónico, red o discos flexibles).
7. Gran capacidad de desinfección.
8. Presencia de distintos métodos de detección y análisis.
9. Chequeo del arranque y posibles cambios en el registro de las aplicaciones.
10. Creación de discos de emergencia o de rescate.
11. Disposición de un equipo de soporte técnico capaz de responder en un tiempo mínimo (ejemplo 48 horas) para orientar al usuario en caso de infección.

Existen sistemas antivirus que tienen además, la característica de trabajar directamente en redes LAN y WAN, así como en servidores proxy.

Ante la masiva proliferación, tanto de virus como de productos dirigidos a su tratamiento, existe la necesidad de que algún organismo reconocido de carácter internacional certifique los productos antivirus y asegure su correcto rendimiento. En un antivirus lo más importante es la detección del virus y, al estudio de tal fin se dedican asociaciones como la ICSA (International Computer Security Association) - anteriormente la NCSA - y la Checkmark. Ambas siguen procedimientos similares. En concreto, para que la ICSA certifique un producto antivirus, ha de ser capaz de detectar el 100 % de los virus incluidos en la Wildlist (lista de virus considerados en circulación) y, al menos, un 90 % de la Zoolist -una colección de varios miles de virus no tan difundidos. La certificación de un producto se realiza cuatro veces al año, sin el conocimiento del fabricante y con una versión totalmente comercial, con lo que se asegura que la versión que se certifica es la que recibe directamente el usuario y no una especialmente preparada para la prueba.

MÉTODOS

Existen distintos estudios comparativos sobre el tema, realizados por organizaciones competentes no vinculadas a ningún productor de antivirus.

Se revisaron fundamentalmente los siguientes estudios comparativos:

1. *Hispasec*, editado por la revista especializada PC Actual, de gran prestigio y seriedad.4
2. *Vsantirus*, de VideoSoft BBS.
3. Dos comparaciones publicadas por la revista especializada PC World, también de gran renombre mundial.
4. Un artículo publicado sobre el tema y disponible en el sitio www.monografías.com, algo antiguo, pero con datos muy interesantes sobre los diferentes sistemas antivirus.3

Además, se consultaron las siguientes:5

Comparación de HISPASEC
www.hispasec.com

SECUSYS, Tests des Anti-Virus
www.secusys.com/laboratoire.htm

Comparación de VIRUSPROT
www.virusprot.com

Vsantivirus de VideoSoft BBS
www.vsantivirus.com/comparativa.htm

En las comparaciones analizadas, pudo apreciarse resultados contradictorios con respecto a un sistema antivirus específico. Por ello, se revisaron cuidadosamente los resultados de cada uno de los estudios con respecto a cada uno de los diferentes sistemas evaluados con el objetivo de validarlos.

Los softwares antivirus analizados en este trabajo fueron certificados por la ICSA.
Los sitios de los antivirus estudiados se encuentran referidos al final del artículo (anexo).

Valoración de los diferentes sistemas antivirus

- **NORTON ANTIVIRUS**

Según la comparación publicada M Mansón,3 este antivirus posee una protección automática en segundo plano. Detiene prácticamente todos los virus conocidos y desconocidos, mediante una tecnología propia, denominada NOVI, que implica el control de las actividades típicas de un virus. Protege la integridad del sistema, actúa antes de que causen algún daño o pérdida de información, con una amplia línea de defensa, que combina búsqueda, detección de virus e inoculación. Utiliza diagnósticos propios para prevenir infecciones en sus propios archivos y de archivos comprimidos. El rastreo puede realizarse manual o automáticamente a partir de la planificación de la fecha y la hora. También, posibilita reparar los archivos infectados por virus desconocidos. Incluye información sobre muchos de los virus que detecta y permite establecer una contraseña para aumentar así la seguridad.

La lista de virus conocidos puede actualizarse periódicamente (sin cargo) mediante servicios en línea como Internet, América On Line, Compuserve, The Microsoft Network o el BBS propio de Symantec, entre otros.

Según la comparación de Hispasec,7 entre las características destacables del Norton Antivirus se encuentra la opción LiveUpdate que automatiza la actualización del motor y de las nuevas definiciones de virus de forma simultánea por Internet. Con la compra del producto, se obtiene Soporte Gold durante un año, que integra línea gratuita de soporte help-desk y actualizaciones de firmas.

El menú principal se divide en estado del sistema, estado de correo electrónico, búsqueda de virus, un apartado de informes y un módulo de programación para planificar tareas. Cabe destacar la existencia de un módulo para el análisis de los correo que entran, así como las opciones *cuarentena* y *soporte* de muestras sospechosas con el mismo programa.

En las pruebas, Norton se ha mostrado débil en la detección de *troyanos* y *backdoors*, indicador que aun se agrava más en el apartado de muestras de la colección Internet. En el resto de las pruebas, aparece en un nivel medio, que decae de nuevo en el apartado de formatos de compresión o en la prueba de instalación en

un sistema con virus. Destaca de forma especial en la prueba de detección en correo, donde es la mejor solución de las probadas. En un producto tan integrado en Internet, resulta atrayente la falta de una protección específica a nivel del navegador.

Los resultados de este análisis con respecto al Norton Antivirus presentan algunas contradicciones con los publicados en otro por la revista PC World (www.pcworld.com).8 Según esta última, Norton es el que mejores resultados ha ofrecido en las pruebas. Tal vez, demora algo más en completar el proceso de análisis, pero detectó el 100 % de los virus utilizados, con un porcentaje muy bajo de falsos positivos.

La interfaz de usuario es muy buena, muy sencilla y fácil de utilizar. Desde un único programa se controlan todas las funciones, sin escatimar información. Aunque se puede llamar independientemente al módulo de actualización de nuevas versiones, también puede hacerse desde un icono en la pantalla principal.

Después de un proceso de instalación algo tedioso, y que realiza un primer análisis exhaustivo de todos los ficheros, el sistema queda configurado con todas las opciones de análisis activadas. Además de mantener activado el análisis heurístico, también queda activado el escáner manual sobre todo tipo de ficheros, y es precisamente esta la causa de la tardanza en el análisis inicial.

Según este estudio, Norton Antivirus resultó el mejor en la comparación.

El número de opciones que pueden configurarse es muy elevado, y el proceso es simple. El centro de desinfección de Symantec, llamado SARC (Symantec AntiVirus Research Center), recibe los ficheros infectados y, según los distribuidores, es cuestión de horas, obtener una respuesta con un fichero limpio y una nueva actualización.

Por otra parte, Norton Antivirus reconoce perfectamente las cuentas de correo que se utilizan y permite protegerlas individualmente. Además, pueden configurarse alertas para enviar un mensaje a otras cuentas de correo o a otro usuario de la red.

Finalmente, la actualización de nuevas versiones es un claro ejemplo de simplicidad. No hace falta conectarse a un sitio web y seleccionar cómo queremos actualizar el producto. Lo único que se debe hacer es clic sobre el icono de LiveUpdate y el programa se conecta a Internet y se actualiza automáticamente. Además, la licencia no está limitada en tiempo. Symantec ofrece actualizaciones de por vida (anexo).

- **McAFEE VIRUSSCAN**

Según *M. Mansón*,3 el antivirus de McAfee Associates es uno de los más famosos. Trabaja por el sistema de escaneo descrito anteriormente, y es el mejor en su estilo. Para escanear, hace uso de dos técnicas propias: CMS (Code Matrix Scanning, Escaneo de Matriz de Código) y CTS (Code Trace Scanning, Escaneo de Seguimiento de Código).

Una de las principales ventajas de este antivirus es que la actualización de las bases de datos de *strings* es muy fácil de realizar. Ello, sumado a su condición de programa shareware, lo coloca al alcance de cualquier usuario. Es bastante flexible en cuanto a la configuración de cómo detectar, reportar y eliminar virus.

En la comparación de Hispasec,7 publicada por la revista PC Actual, en abril del 2001, McAfee VirusScan es uno de los clásicos entre los productos antivirus y según ella, suele ocupar siempre los puestos punteros en sus estudios. La compañía Network Associates adquirió McAfee y el doctor Solomons integró este producto con nuevas tecnologías para analizar los protocolos de Internet, de forma que el módulo VShield permite analizar el tráfico con los navegadores Netscape Navigator e Internet Explorer, así como con los clientes de Outlook Express, Eudora, Netscape Mail, Microsoft Exchange, Outlook y Lotus cc:Mail. El producto incluye 90 días de asistencia telefónica y actualizaciones gratuitas durante un año.

VirusScan se presenta actualmente con una nueva interfaz algo más futurista, con una imagen que huye de las típicas aplicaciones Windows, donde, sin embargo falta la extrema sencillez y claridad de la anterior interfaz minimalista, basada en pestañas. En lo que a opciones se refiere, además del menú de exploración, se encuentra un planificador de tareas y una sección de cuarentena que permite aislar los archivos infectados y sospechosos y enviarlos de forma automática a los laboratorios AVERT para su análisis.

En las pruebas, sin llegar a destacarse de forma especial, se comporta de forma adecuada, tanto a nivel de detección como heurístico, y en el resto de pruebas se sitúa en un punto intermedio. No se ha encontrado mejora significativa alguna en el motor con respecto a otros años, sigue entre los antivirus que menos formatos de compresión soporta. En definitiva, nueva cara para VirusScan y opciones adicionales, si bien se encuentra algo estancado en la tecnología de su motor antivirus donde otros productos han realizado avances significativos.

Según la comparación de PC World,8 McAfee VirusScan es el antivirus más extendido mundialmente. Anuncia en su publicidad que se han vendido más de 70 millones de copias, seguido del Norton Antivirus. Es, curiosamente, el programa antivirus seleccionado por Microsoft para utilizarlo dentro de su webmail: hotmail.com.

En su nueva versión ofrece una interfaz nada convencional; sin embargo, incluye los controles en el menú del botón derecho del ratón, para seleccionar los ficheros que se desean revisar. También mantiene dos iconos pequeños en la esquina derecha de la barra de tareas.

La interfaz de usuario no se ajusta a los estándares actuales de ventanas, produce cierta confusión en su uso.

Los resultados de las pruebas no fueron muy buenos. Fue capaz de detectar el 94 % de los virus y sólo presentó un 3 % de falsos positivos. En los virus del tipo macro, la desinfección fue muy satisfactoria, al conservarse las macros operativas.

El factor más desfavorable en su evaluación fue en la detección en correo. En algunos casos, cuando se adjuntó un fichero infectado con virus a un mensaje, el programa lo detectó hasta que se guardó en el disco.

La documentación sobre los virus no se encuentra en el CD, sino que es necesario estar conectado a Internet para poder acceder a ella. Esto supone un problema para cualquier usuario de un equipo que no esté conectado a Internet.

Por otra parte, McAfee ofrece un servicio de desinfección para nuevos virus, también a partir de una conexión a Internet. Puede enviarse un fichero en formato comprimido y McAfee se compromete a limpiarlo y devolverlo en cuestión de horas desde los laboratorios AVERT Labs. Mientras tanto, puede colocarse en cuarentena, para evitar su difusión a otros equipos.

Las actualizaciones del escáner y del fichero de patrones se hacen también por Internet. Se puede configurar la interfaz para arrancar una actualización al hacer clic con el botón derecho del ratón. Las actualizaciones pueden hacerse de por vida. El resto de los servicios son de carácter indefinido. Es el programa más económico de la esta comparación.

- **SOPHOS**

Sophos, con centro en Reino Unido, es uno de los fabricantes de antivirus que más se destaca por su especialización en entornos corporativos y por la cantidad de plataformas que soporta. Junto con el software, el usuario adquiere el servicio de actualizaciones periódicas, alertas y emergencias técnicas vía correo electrónico y soporte por teléfono e Internet. Nada más activar Sophos, se accede a una sencilla interfaz. Mediante tres pestañas, puede accederse a la exploración inmediata, a la agenda para planificar tareas y, por último, a la configuración de InterCheck, el módulo residente. En la barra de herramientas, pueden iniciarse las exploraciones o detenerlas, entrar en el apartado de configuración, alarmas y diccionario de virus. Incluye una relación de todos los virus detectados, con sus propiedades.7

Según el estudio de Hispasec,7 si bien este software ofrece un nivel de soporte alto, se trata sin duda del peor producto antivirus de los evaluados en el aspecto técnico. Además de ser uno de los productos que obtiene los índices más bajos de detección, es el único que no es capaz de desinfectar ejecutables, una opción que hoy por hoy no se concibe en antivirus profesionales. En su lugar, este antivirus recomienda que se eliminen los ficheros afectados y que se reemplace por una copia limpia.

Según la comparación de PC World,8 la interfaz de usuario no es intuitiva, el simple hecho de analizar un directorio obliga a adentrarse en la opción de configuración, y marcar exactamente los tipos de fichero que

se desea analizar, porque las opciones de análisis de ficheros comprimidos aparecen deshabilitadas.

La configuración del escáner es compleja, obliga a editar un fichero de configuración, algo que nunca podrá hacer un usuario "no experto". Sin embargo, en las pruebas, ha obtenido resultados muy buenos.

Sólo necesita 3 MB de espacio en disco, porque el resto de la documentación la mantiene en el CD.
Las funciones de soporte de programas de correo son escasas y el servicio de actualización no está integrado en el programa.
La principal ventaja de Sophos es su capacidad para trabajar en distintos entornos, como Lotus Notes, Exchange, Novell, etc. Esto lo convierte en una seria opción para sistemas hetereogéneos.

- **NORMAN VIRUS CONTROL 5.0**

Norman Data Defense es su productora. Hace unos años se integró con ThunderByte, uno de los antivirus míticos de la época MS-Dos por el uso de técnicas heurísticas.

En Norman Virus Control 5.0, la interfaz se renovó completamente, con una filosofía basada en tareas, módulo de cuarentena y con la posibilidad de actualizar las firmas de virus desde el mismo programa por Internet, como mejoras más relevantes a primera vista en comparación con las versiones anteriores.

Según Hispasec,7 en las pruebas se ha comportado con un nivel medio en general. Se destacó en pruebas como la de soporte telefónico y obtuvo los peores resultados en la consulta por Internet. En la parte técnica, fue muy eficiente en la prueba de instalación en un sistema infectado, donde ha compartido el primer puesto junto con AVP. Sin embargo, carece de una heurística efectiva para los nuevos formatos y módulos de protección específicos para Internet y requiere mejoras en el soporte de formatos de compresión.

Según PC World,8 la interfaz de Norman es interesante. Permite una configuración muy extensa en cuanto a número de opciones. Esto es muy beneficioso para un usuario avanzado, pero puede resultar un poco confuso para un principiante. La versión que se comercializa actualmente se encuentra en inglés.

Al igual que ocurre con el programa de McAfee, se presenta un icono en la esquina derecha de la barra de tareas, con el que puede accederse a un menú desde el que es posible lanzar todas las funciones.

El producto ha obtenido un porcentaje de aciertos del 93 %, bastante elevado. El número de falsos positivos fue del 15 %, con el que clasifica en un lugar mucho más bajo que el resto de productos en este aspecto. Los mejores resultados de Norman fueron en el tratamiento y la detección de virus de tipo macro. El factor más negativo en la evaluación del producto es la falta de integración con Outlook, que obliga a escanear manualmente cada uno de los ficheros que se recibe.

El producto se divide en siete programas distintos. Esto dificulta sensiblemente su uso, porque el usuario tiene que saber para qué se utiliza cada uno y seleccionarlo cuando lo crea oportuno. No es fácil saber cuándo se está infectado y, por eso, tampoco lo es, decidir si utilizar un programa de análisis específico sobre un fichero.

El programa principal es el que se emplea para hacer el análisis manual de los ficheros. También se puede acceder desde este programa a la configuración de cada una de las opciones.

Existen otros programas, como Smart Behavior Blocker, cuya misión es la de analizar el comportamiento de algún programa posiblemente infectado. A nuestro juicio, este programa debería de integrarse en la interfaz principal, para que el usuario no se vea obligado a averiguar para qué sirve y cómo tiene que utilizarlo.

El sistema de ayuda también se encuentra íntegramente en Internet. De hecho, si se selecciona la opción de ayuda, se obtiene una página HTML desde la que es posible bajar de Internet todos los manuales del producto en formato PDF.

El control que ofrece Norman Virus Control es superior al resto de los programas probados. Además de permitir configurar el programa con una mayor cantidad de opciones, y de incluir programas específicos

para analizar virus de tipo Troyano, también puede incluso seleccionarse fragmentos de código que nos interese que el programa no entre a analizar.

El costo del programa es razonable, y su licencia se renueva anualmente. El laboratorio de desinfección está en Noruega y el envío del programa infectado también se realiza mediante la página web de Norman.

- **PANDA PLATINUM 6.22**

Panda Software, muy popular en España, lucha fuerte por imponerse a nivel internacional con un producto avanzado y una nueva concepción de servicios añadidos. Con la adquisición de su producto, el usuario obtiene durante un año soporte telefónico 24 horas x 365 días, servicio de desinfección de virus nuevos en 24 horas, actualizaciones diarias del fichero de firmas, así como del software de la aplicación.

A primera vista, Panda Platinum conserva la misma interfaz que se destaca por ser similar en su concepción a la de Outlook, sus componentes multimedia, y su integración en los clientes de correo. Uno de los cambios más significativos experimentados por ella no se puede observarse a simple vista, y se encuentra en un renovado interior para integrarse de lleno con las nuevas especificaciones de Windows 2000.

Según Hispasec,7 es la única solución con soporte telefónico real 24 x 365. En el resto de pruebas de soporte y respuesta ante un virus nuevo también destaca con respecto a la media obtenida por los productos evaluados. Si bien este año, en relación a comparaciones anteriores, lo más sorprendente son sus resultados en las pruebas de detección con unos indicadores, donde destaca, en especial, un primer puesto en la colección de troyanos y backdoors. También es una de las pocas soluciones que contempla módulos específicos para Internet con análisis a nivel de los diferentes protocolos, incluido el web, correo entrante y saliente, ftp y noticias. Sin embargo, se ha visto algo empañado en la prueba de correo al no soportar la desinfección en Outlook Express. Otro punto a mejorar es el soporte de compresores de ejecutables.

Según PC World,8 Panda es posiblemente el programa antivirus de mayor difusión en España, hecho perfectamente lógico, si se considera que es una empresa española, con una estructura comercial grande y con un servicio técnico en español.

Panda es uno de los programas más completos y que ha obtenido mejores resultados en esta comparación. El porcentaje de virus detectados fue el segundo más elevado, justo después del Norton Antivirus, y el número de falsos positivos fue el menor.

Llama la atención la presentación del producto, con más manuales muy bien editados y con mucha más información que el resto. Así, el usuario no depende tanto de una conexión a Internet para obtener ayuda, que por cierto es muy extensa y clara y, además, en el mismo paquete incluye una breve documentación de todos los virus que se conocen.

Evidentemente, para realizar actualizaciones del programa, es necesario conectarse a Internet, aunque también existe un servicio de actualizaciones por CD.

Panda también comercializa otros productos relacionados con Platinum 6.0, como el Seguro Antivirus Global, para Exchange, Lotus Notes, Firewall y proxy.

Cuando se instala el programa, la opción de análisis heurístico queda deshabilitada. Esto es un poco contradictorio, porque un usuario novato la mantendrá así indefinidamente y el programa no será capaz de ofrecer su máximo potencial de análisis.

La integración con Outlook es buena, así como con el software de transferencia de ficheros. El usuario puede configurar el producto para analizar los ficheros según se descarguen de Internet. De esta forma, ningún fichero se quedará en el disco duro sin analizarse.

Dentro de un único programa principal, puede seleccionarse la opción de planificación de actividades. En esta opción, puede indicarse cómo se desea que se realicen las actualizaciones del programa, o bien cuándo se quiere que se proceda con los análisis.

En los materiales utilizados para el manual y las fichas técnicas incluye un par de disquetes de emergencia, y el sistema de ayuda es mucho más extenso que el de otros antivirus estudiados.

- **F-SECURE**

Según Hispasec,7 es el detector por excelencia, es el único producto que integra varios motores antivirus de forma paralela, AVP y F-Prot, ambos de reconocido prestigio. Junto con el software, el usuario recibe tres meses de soporte técnico, actualizaciones de firmas vía Internet, y acceso al laboratorio para el envío y solución ante virus nuevos.

La interfaz de F-Secure se mantiene con respecto a años anteriores, basada en tareas predefinidas y en la posibilidad de añadir o editar nuevos trabajos de análisis, ello permite una distribución y gestión centralizada, especialmente útil para redes corporativas.

Una vez más, como es habitual, F-Secure obtuvo los mayores resultados en las pruebas de detección, fruto de sumar la potencia de AVP y F-Prot en sus análisis. Se ha apreciado una mejora en la velocidad a la hora de escanear grandes colecciones de virus, donde en comparaciones pasadas era particularmente lento. En el apartado de compresión recoge los frutos del motor de AVP que incorpora. No ha destacado en ninguna de las pruebas de soporte, no contempla la potencia heurística que llega a demostrar AVP en su producto, y llama la atención la ausencia de un módulo específico para Internet que hace que caiga en los resultados de este apartado.

Por ahora, sólo se ha traducido al idioma español el procedimiento de instalación del producto. Los manuales y la página web también se encuentran en inglés.

Según PC World,8 F-Secure es un antivirus con una gran experiencia. La nueva versión se ha simplificado sensiblemente en cuanto a la interfaz de usuario, pero ahora resulta poco intuitiva. Para encontrar la manera de configurar el producto no hay que acudir al menú de Inicio de Windows, sino que es necesario seleccionar el icono que se encuentra en la esquina derecha de la barra de tareas, y a continuación pinchar en el botón de Propiedades.

En F-Secure, la interfaz de usuario es excesivamente simple. No incluye un panel de control.

Desde el menú de inicio de Windows sólo pueden iniciarse los análisis del disco, de disquete o de un determinado directorio. Una vez comenzado el análisis, el usuario debe tomar una decisión sobre cada uno de los virus que encuentre. No puede seleccionarse una opción para continuar hasta el final sin arreglar los problemas, por que, si se escoge Cancelar, se detiene el proceso de análisis.

Desde las opciones, pueden seleccionarse los métodos de análisis a utilizar. Se combinaron distintas opciones y, aun así, se obtuvo un resultado algo inferior al resto de los programas analizados en el estudio. No obstante, el resultado es óptimo, y por eso es un producto certificado por ICSA, que asegura que es capaz de detectar más de un 95% de los virus de la Wild List.

El costo final del programa es algo elevado. Si se compara con el resto, puede llegar a valer el doble de cualquier otro sistema antivirus. Por ejemplo, en España en todos los casos, el costo de los sistemas es inferior a 10.000 pesetas, en el caso de F-Secure asciende a 24.900.

El soporte y la actualización de producto son muy buenos. Para actualizarlo, es necesario conectarse a Internet.

- **PC-CILLIN 7.5**

PC-Cillin es la solución para estaciones de trabajo Windows que propone Trend Micro, una multinacional conocida por la calidad de sus soluciones antivirus en el terreno de los servidores, toda una garantía para los usuarios domésticos. Junto con el software, el usuario accede al servicio de actualizaciones de patrones de virus y motor antivirus, puede inscribirse en un servicio de noticias sobre virus junto con un calendario mediante un Active Desktop que le mantendrá informado en todo momento.

El interfaz de PC-Cillin es similar a Outlook en su concepción, con una barra de botones vertical que permite acceder a las distintas opciones. Se destaca la posibilidad de poder enviar muestras sospechosas a partir de la misma aplicación y un módulo para chequear el correo entrante.

Según Hispasec,7 en las pruebas de detección PC-Cillin ha obtenido buenos resultados, como era de esperar en un producto que utiliza las bases de firmas de Trend Micro. Sin embargo, el resultado en el resto de pruebas fue discreto; quedó en los últimos lugares en la prueba de instalación en un sistema infectado, no consiguió detectar la muestra en el apartado de heurística, y se detectaron algunos problemas en el módulo de análisis por Internet, en especial cuando se realiza a través de un proxy por puertos no estándares.

Lo primero que llama la atención de este producto es la cantidad de versiones para distintos entornos incluidas en el mismo CD. Ofrece versiones para Solaris, Windows NT, Lotus Notes, Exchange, etc. Es un producto multiplataforma.

También dispone de diversos programas dentro de los CD de instalación. Por un lado, se instala el antivirus PC-Cillin, pero además se encuentran productos como ServerProtect, InterScan WebManager, ScanMail e InterScan VirusWall. Todos ellos ofrecen una solución conjunta para la seguridad de la red.

En PC World,8 después de realizar las pruebas, se obtuvo una respuesta alta en lo relativo al número de virus detectados. De la misma manera, el número de falsos positivos fue bastante bajo, y, en general, obtuvo una buena valoración en cuanto a fiabilidad.

La interfaz de usuario es muy amigable. Se parece un poco a Outlook, en cuanto al sistema de menús de la izquierda de la ventana, al presentar una barra de iconos grandes y distintas lengüetas para seleccionar las opciones.

El producto se integra muy bien con el cliente de correo. Después de la instalación, se activa la opción de análisis de los POP3 del equipo, por lo que se analizará todo mensaje que llegue a partir de ese momento, sin importar el cliente de correo que se emplee. En la versión de Exchange, la integración es todavía mayor, porque se analizan los ficheros adjuntos a los mensajes antes de que los reciba el usuario. Por otra parte, el Virus Wall es capaz de analizar en tiempo real el tráfico SMTP y FTP para buscar virus. Evidentemente, este análisis debe combinarse con el análisis heurístico durante el rastreo de un posible virus, pero, para entonces, no será necesario el análisis de patrones.

PC-Cillin es un producto a considerar cuando conviven equipos UNIX y Windows 2000 dentro de una empresa.

- **AVP**

Fabricado por Kaspersky Lab, el AVP, de origen ruso, es uno de los productos más apreciados entre los entendidos por la potencia de su motor antivirus en lo que toca a detección y desinfección. Junto con el software, se obtiene soporte técnico por correo electrónico y actualizaciones diarias de las bases de virus durante un año.

Según Hispasec,7 AVP se destaca por presentar una de las interfaces más sencillas y prácticas. A su ya conocida potencia como motor antivirus, se suman unos resultados excelentes a nivel de soporte, al ser el primero en aportar una solución para una infección por virus, así como ganar en la contestación a una consulta realizada mediante el correo, en ambos casos con tiempos de respuesta sorprendentes. Su peor resultado fue en el indicador de asistencia telefónica.

En el apartado técnico, AVP volvió a obtener buenos resultados en las pruebas de detección, tal y como ocurrió en comparaciones pasadas. Fue, junto con Norman, el primero en resolver con éxito la instalación en un sistema infectado. Su heurística también se ha mostrado acertada las veces que se ha puesto a prueba, y su dominio en el apartado de soporte de formatos de compresión es absoluto, muy por encima del resto en la prueba de compresores de ejecutables. Su sencillez y potencia tiene en contra un punto débil que este año quedó demostrada: la ausencia de módulos específicos para analizar las vías de entrada desde Internet, con el agravante de su conflicto con Outlook Express.

El estudio de PC World,8 no consideró en su análisis el AVP. Sin embargo, se incluyó en el presente trabajo, porque además de que los resultados obtenidos en Hispasec, fueron muy satisfactorios, se sabe que es un antivirus muy utilizado a escala mundial, como se ha constatado en la bibliografía consultada en Internet, y se encuentra muy difundido en Cuba, donde cuenta con la aceptación de muchos usuarios. Por ejemplo, en la comparación realizada por *Calzón Fiestero* en julio del 2002, basada en las opiniones de los usuarios, expresó "Si Kaspersky logra corregir de forma eficiente el problema de la demora que su antivirus provoca, probablemente vuelva a ser el líder indiscutible que para muchos fue su "anciano padre", el AVP Gold."9

Existen muchos otros sistemas antivirus, algunos de ellos de renombre internacional, como el Inoculate IT y AVG, pero al analizar la bibliografía consultada sobre ellos,4,7,10 no se consideró de importancia su inclusión en este trabajo por no estar a la altura de los comparados. Por ejemplo, del AVG se comenta lo siguiente: "En definitiva; un ágil y aceptable antivirus gratuito que poco tiene para envidiarle a otros que cobran por su licencia, aunque aún está algo lejos de los principales productos del género."9

Como resultado de la revisión efectuada con los estudios utilizados y otras páginas especializadas, se pudo constatar que:

- Los sistemas antivirus que mayor poder de detección han demostrado son: Norton Antivirus (100 %), AVP (más del 95 %), Panda (95 %), McAfee (94 %) y Norman AV (93 %).
- En cuanto a la detección de falsos positivos, los mejores fueron, el Norton que no mostró ninguno y el McAfee con un 3 %. Sin embargo, hay otros con un alto porcentaje, como el Norman AV que obtuvo un 15 %.
- En cuanto a la integración con el correo electrónico e Internet, se encuentra el Norton, McAfee, aunque presenta algunos errores en la detección por correo, el Panda, con módulos específicos para correo e Internet, aunque con algunos problemas de interacción con Outlook Express. Sin embargo, otros como el AVP, no presentan una buena integración con Outlook Express y para el análisis de las vías de entrada desde Internet; el PC- Cillin también presenta problemas con el módulo de análisis de Internet, el F-Secure no tiene módulo para el análisis de Internet y el Norman no tiene integración con el correo.

A continuación se resumen las características más significativas de los sistemas evaluados.

Sistema antivirus	Ventajas	Desventajas
Norton	1. Es el segundo más vendido en el mundo. 2. Mejor porcentaje de detección. 3. Interfaz sencilla. 4. Buena integración con el correo y los navegadores de Internet. 5. Licencia del producto de por vida. 6. Al instalarse queda con todas las opciones habilitadas. 7. Respuesta rápida ante nuevos virus.	1. Algo débil en la detección de troyanos y backdoors. 2. Problemas con la instalación en sistemas infectados.
McAfee	1. Es el primero en ventas en el mundo. 2. Alta detección de virus con un 94 % de la Wildlist. 3. Buena integración con el correo e Internet. 4. Rápida respuesta ante nuevos viru	1. Falta de sencillez en la interfaz, que puede confundir al usuario. 2. Presenta algunos fallos en la detección en correo

Sophos	1. Especializado en entornos corporativos. 2. Soporta varias plataformas 3. Interfaz sencilla.	1. Indice muy bajo de detección. 2. Es el único sistema que no es capaz de desinfectar ejecutables. 3. Interfaz de configuración compleja. 4. Funciones escasas de soporte por correo.
Norman AV	1. Se destaca en la instalación sobre un sistema infectado. 2. Detección aceptable (93 %). 3. Al presentar una gran cantidad de productos especializados permite un gran control cuando se utiliza por expertos.	1. Detectó un 15 % de falsos positivos. 2. Interfaz de configuración extensa y compleja. 3. Falta de integración al correo.
Panda	1. Alta detección de virus, (segundo después de Norton). 2. Módulos específicos para correo e Internet con buena detección. 3. Menor porcentaje de detección de falsos positivos.	1. Problemas con Outlook Express. 2. Al instalarse, la opción de análisis heurístico queda deshabilitada y debe ser el usuario quien la habilite.
F-Secure	1. Alta detección (> 95 %). 2. Util para redes corporativas, porque permite una distribución y gestión centralizada. 3. Interfaz muy simple, poco intuitiva.	1. No se destaca en diferentes plataformas. 2. No posee módulo específico para Internet. 3. El usuario debe tomar una decisión en cada virus encontrado. 4. El costo del producto es muy elevado y dobla el costo de casi todos los demás sistemas.
PC-Cillin	1. Alta detección y bajo por ciento de falsos positivos. 2. Existen diferentes versiones para distintos entornos (multiplataforma). 3. Buena integración con el correo. 4. Buenos resultados cuando se combina UNIX y Windows 2000 dentro de una empresa.	1. Problemas en su instalación en un sistema infectado. 2. Problemas en el módulo de análisis de Internet.
AVP (Karpesky)	1. Interfaz sencilla y práctica. 2. Alta detección de virus (más del 95 %). 3. Se destaca en la instalación sobre sistemas infectados. 4. Es altamente apreciado por la potencia de su motor de detección y desinfección. 5. Excelente nivel de respuesta	1. Ausencia de un módulo específico para analizar las vías de entrada desde Internet. 2. Conflictos con Outlook Express.

	y rapidez en la solución ante nuevos virus.	

Conclusiones

De acuerdo con el propósito de una empresa determinada en relación con la forma de trabajo de sus computadoras, es decir, el trabajo en redes o en estaciones de trabajo independientes, puede concluirse:

- Para el trabajo en redes, puede recomendarse el uso de los siguientes sistemas antivirus: F-Secure, PC-Cillin, y el Norman Antivirus.
- Para el uso de usuarios independientes, se recomienda: Norton Antivirus, McAfee VirusScan, AVP y Panda.
- No se recomienda el uso de Sophos por el bajo índice de detección con respecto a los demás sistemas evaluados. Además, no es capaz de desinfectar ficheros ejecutables, cualidades ambas de gran importancia en cualquier sistema antivirus.

Anexo. *Sitios de los fabricantes de los antivirus comparados el trabajo.*

1. AntiViral Toolkit Pro (AVP) [Sitio en Internet]. Disponible en: http://www.kaspersky.com
2. F-Secure Anti-Virus [Sitio en Internet]. Disponible en: http://www.f-secure.com
3. McAfee VirusScan [Sitio en Internet]. Disponible en: http://www.mcafee.com
4. Norman Virus Control [Sitio en Internet]. Disponible en: http://www.norman.no
5. Norton Antivirus [Sitio en Internet]. Disponible en: http://www.symantec.com
6. Panda Platinum [Sitio en Internet]. Disponible en: http://www.pandasoftware.es
7. PC-Cillin (Trend Micro) [Sitio en Internet]. Disponible en: http://www.trendmicro.com
8. Sophos Antivirus [Sitio en Internet]. Disponible en: http://www.sophos.com

Referencias bibliográficas

1. Pereira JE ¿Sabías qué es un virus? Disponible en: http://www.toptutoriales.com/underground/virus/virus2.htm# Acceso: 10 de enero del 2003.
2. Periodismo en Internet. Suplemento Informática 2.0. Disponible en: http://old.clarin.com/suplementos/informatica/2003/04/23/f-549045.htm Acceso: 10 de enero del 2003.
3. Mansón M. Estudio sobre virus informáticos. Disponible en: http: http://www.monografias.com/trabajos/estudiovirus/estudiovirus.shtml Acceso: 10 de enero del 2003.
4. López JL. ¿Cuál antivirus elegir? Disponible en: http://www.vsantivirus.com/comparativa.htm Acceso: 10 de enero del 2003.
5. Moreno Pérez A. Conozca los distintos antivirus. Disponible en: http://www.vsantivirus.com/am-conozcaav.htm Acceso: 10 de enero del 2003.
6. Programas antivirus McAfee VirusScan 95 v3, Norton Antivirus 4.0, Panda Antivirus 5.0, Antivirus Anyware, F-PROT Professional 3.01, ThunderByte Antivirus 8.03 y Dr. Solomon's Anti-Virus Toolkit. Disponible en: http://www.idg.es/pcworld/articulo.asp?id=46864 Acceso: 10 de enero del 2003.
7. Hispasec. Comparativa Antivirus 2001: Comparativa Antivirus Abril 2001. Disponible en: http://www.hispasec.com Acceso: 10 de enero del 2003.
8. Contreras Mejuto G. Antivirus: no salga a Internet sin ellos F-Secure Anti-Virus 5.0, McAfee VirusScan 5.15, Norman Virus Control 5.0, Panda Antivirus Platinum 6.0, Symantec Norton Antivirus 2001, Sophos Anti-Virus Febrero 2001 y Trend Micro PC-cillin 7.5. Disponible en: http://www.idg.es/pcworld/articulo.asp?id=119462 Acceso: 10 de enero del 2003.
9. Fiestero C. Comparativa antivirus para Space Saturn. Disponible en: http://www.terra.es/personal/spsaturn/pr-Cmp_Sp1.htm Acceso: 6 de febrero del 2003.
10. Comparativas software anti-virus. Diciembre 2002. Disponible en: http://www.virusprot.com/Companti.html#Diciembre2002 Acceso: 6 de febrero del 2003.
11. CIAO. Comparaciones. El mejor software anti-virus [Sitio en Internet] Disponible en:

http://www.ciao.es/ranking/El_Mejor_Software_Anti-Virus.html Acceso: 6 de febrero del 2003.
12. AVG Antivirus. Disponible en: http://ciudadfutura.com/mundopc/freeware/articulos/avg/avg1.htm Acceso: 2 de febrero del 2003.

Recibido: 7 de julio del 2003. Aprobado: 20 de julio del 2003
Lic. *Luis Armas Montesino*. Director Centro Territorial de Información de Ciencias Médicas, Artemisa, La Habana.
Hospital General Docente "Ciro Redondo" Calle 33 e/ 24 y 26, Artemisa, La Habana, Cuba.
Correo electrónico: cpicmar@infomed.sld.cu

1 Licenciado en Geografía. Profesor de Informática Médica. Director. Centro Territorial de Información de Ciencias Médicas Artemisa, La Habana.
