SEGU-INFO.COM.AR
SEGURIDAD DE LA INFORMACION
- Jueves 20 de octubre de 2005 -

Panorama actual de los distintos antivirus*

-Guía básica-

http://www.segu-info.com.ar/terceros/panorama_antivirus.zip

Por Arnoldo Moreno Pérez**

"Es mejor saber después de haber pensado y discutido que aceptar los saberes que nadie discute para no tener que pensar." Fernando Savater.

"Saber no es suficiente, debemos aplicar. Desear no es suficiente, debemos hacer." Johann W. von Goethe."

"La clave está en las actualizaciones: un antivirus sin soporte no sirve más que un reloj sin manecillas (o sin baterías si es electrónico)." José Anaya***.

En la actualidad no es difícil suponer que cada vez hay más personas que están conscientes de la necesidad de hacer uso de algún antivirus -y también antiespías, cortafuegos y antispam, en ocasiones- como medida de protección básica para sus equipos de cómputo. No obstante, en principio lo deseable sería poder tener un panorama de los distintos productos que existen y con ello, una guía inicial para proceder a evaluarlos. El objetivo de este trabajo, es facilitar -en primera instancia- dicha tarea.

Los distintos antivirus:

ARCAVIR
http://www.arcabit.pl/
http://www.arcabit.com/index.html

ANTIGEN
http://www.sybari.com/
http://www.sybari.com/portal/alias__es/lang__es/Default.aspx?init
Microsoft anunció el 21 de junio de 2005 la adquisición del proveedor de seguridad empresarial Sybari Software, como puede verse en:
http://www.microsoft.com/latam/prensa/2005/junio/sybari.asp

ANTIVIR (E+BEDV)
http://www.antivir.de/de/
http://www.antivir.de/en/
http://www.antivir.de/es/
http://www.antivir.de/fr/index.html
http://www.antivir.de/it/

ANTIVIR PERSONAL EDITION CLASSIC
http://www.free-av.de/
http://www.free-av.com/

ANTIVIRUS UNA (THE UKRAINIAN NATIONAL ANTIVIRUS)
http://www2.una.ua/index_e.html
http://www.unasoft.com.ua/eng/news.php

AVAST! ANTIVIRUS
http://www.avast.com/
http://www.auditoria.com.mx/productos/av/avast/avast.htm
http://www.globaltecsa.com/productos/avast.html

AVG ANTI-VIRUS
http://www.grisoft.com/doc/1
http://www.grisoft.com/doc/1/lng/br-pt/tpl/tpl01
http://www.one.net.mx/AVG_antivirus_ONE.htm

AVIRA ANTIVIRUS
http://www.avira.com/
http://www.avira.com/es/pages/index.html

BITDEFENDER
http://www.bitdefender.ro/bd/site/page.php?country_id=98
http://www.bitdefender.com/
http://www.bitdefender-es.com/index.php
http://www.bitdefender.com.mx/index.php

BULLGUARD ANTIVIRUS
http://www.bullguard.com/
http://www.dbnet.dk/1061.aspx

CLAMAV
http://www.clamav.net/
http://www.sosdg.org/clamav-win32/index.php

COMMAND ANTIVIRUS CON F-PROT
http://www.authentium.com/
http://www.commandcom.com/

http://www.antivirusmex.com/
http://www.antivirus1.com/

DOCTOR WEB (DR. WEB)
http://www.drweb.com/
http://www.drweb-usa.com/
http://old.antivir.ru/english/dsav_toolkit/drweb32.htm
http://www.drwebfrance.com/
http://www.vsantivirus.com/drweb.htm

EMERGENCY RESPONSE ANTIVIRUS (PAL ANTIVIRUS)
http://www.palsol.com/index.html

ESAFE
http://www.aladdin.com/esafe/default.asp
http://www.interbel.es/noticias/desglosarnoticia.cfm?id=70
http://www.hardlock.com.mx/
http://www.advantage-security.com/soluciones/esafe.html

ESCAN
http://www.mspl.net/
http://www.mwti.net/
http://www.microworld.de/

ETRUSTANTIVIRUS
http://www.ca.com/
http://www.ca.com/es/
http://www.ca.com/mx/

FORTIGUARD ANTIVIRUS
http://www.fortinet.com/
http://www.dacas.com/website/argentina/productos/marcas/
http://www.tso.cl/

F-PROT ANTIVIRUS
http://www.f-prot.com/
http://www.vsantivirus.com/f-prot.htm

FREEDOM ANTI-VIRUS
http://www.freedom.net/viruscenter/index.html

F-SECURE ANTIVIRUS
http://www.f-secure.com/
http://www.microasist.com.mx/
http://www.codine.es/001/producto_fsecure.php

IKARUS MANAGED SECURITY SERVICES
http://www.ikarus-software.at/portal/index.php
http://www.ikarus-software.at/portal/index.php?newlang=english
http://www.mymailwall.com/

KASPERSKY ANTIVIRUS (AVP)
http://www.kaspersky.ru/
http://www.kaspersky.com/
http://www.kaspersky.com.mx/kasperwww/index.php
http://www.avp-es.com/
http://www.kaspersky.net.ar/
http://www.kaspersky.cl/
http://www.segurmatica.com/gruporedes/sociedad.jsp
http://www.codine.es/001/producto_kaspersky.php
http://www.vsantivirus.com/avp.htm

MCAFEE VIRUSSCAN ANTIVIRUS
http://www.mcafee.com/us/
http://www.mcafee.com/es/
http://www.mcafee.com/uk/
http://www.mcafee.com/mx/
http://www.vsantivirus.com/virscan.htm

NOD32 ANTIVIRUS SYSTEM
http://www.nod32.com/home/home.htm
http://www.nod32.com.mx/home/home.php
http://www.nod32-a.com/
http://www.nod32-es.com/home/home.htm
http://www.nod32-la.com/home/home.htm
http://www.viruscenter.com.ar/
http://www.nod32.videosoft.net.uy/
http://www.vsantivirus.com/nod32.htm

NORMAN VIRUS CONTROL
http://www.norman.com/
http://www.norman.com/es
http://www.norman.com/Product/Home_Home_office/NVC/en
http://ns.abaco.net.mx/

NORTON ANTIVIRUS
http://www.symantec.com/index.htm
http://www.symantec.com/region/mx/
http://www.symantec.com/region/es/
http://www.vsantivirus.com/norton.htm#des

PANDA ANTIVIRUS
http://www.pandasoftware.es/

http://www.pandasoftware.com/
http://www.pandasoftware.es/com/ar/
http://www.pandasoftware.es/com/cr/
http://www.pandasoftware.es/com/mx/
http://www.pandasoftware.com.pe/
http://www.pandasoftware.es/com/uy/

PC-CILLIN
http://es.trendmicro-europe.com/
http://www.trendmicro.com/la/home/enterprise.htm
http://www.smartekh.com/index.html

PER ANTIVIRUS
http://www.persystems.net/

PROTECTOR PLUS
http://www.pspl.com/

QUICK HEAL
http://www.quickheal.co.in/
http://www.intelliplans.net/quickheal/

RAV ANTIVIRUS
http://www.rav.ro/
http://www.ravantivirus.com
Microsoft se propuso adquirir la tecnología de este antivirus, anunciándolo el 10 de junio de 2003, como puede constatarse en las referencias:
http://www.microsoft.com/latam/prensa/2003/jun/GeCADSoftware.asp
http://www.rav.ro/pages/shownews.php?i=153

SECURITY BUNDLE
http://www.freedom.net/

SOLO ANTIVIRUS
http://www.antivirus-download.com/

SOPHOS ANTI-VIRUS
http://www.sophos.com/
http://esp.sophos.com/
http://www.vsantivirus.com/sophos.htm

SUPERLITE ANTIDOTE
http://www.vintage-solutions.com/indexeng.html

THE HACKER ANTIVIRUS
http://www.hacksoft.com.pe

THE SHIELD PRO
http://www.pcsecurityshield.com/webApp/90023e.asp
http://www.pcsecurityshield.com/webApp/90023d.asp

VBA32 ANTIVIRUS
http://www.anti-virus.by/./en/
http://www.anti-virus.by/
http://www.meteor-pc.de/
http://www.virusblokada.ru/

VEXIRA ANTIVIRUS
http://www.centralcommand.com/index.html

VIROBOT EXPERT
http://www.globalhauri.com/html/
http://www.haurilatin.com/
http://www.hauri-europe.com/
http://www.dric.com.mx/hauri/hauri.html
http://www.scsi.com.mx/Final/Nueva%20Pagina%20SCSI/hauri.htm
http://www.mayfra.com/productos_haury_4.html
http://www.alpha21.cl/esp/productos/productos_hauri.htm
http://www.ipuntorp.com.mx/

ZONDEX GUARD
http://www.zondex.com/

Esta sin duda no es una lista completa y difícilmente podría serlo. Corresponde exclusivamente al grupo de antivirus con los cuales he tenido cierta experiencia en los últimos años y por ende recomiendo por lo menos una vez en la vida tomarse la molestia de conocerlos y evaluarlos. Todo esto en la medida que el interés por el tema sea lo suficientemente grande.

Tratando de ir a lo fundamental, se tienen comúnmente dos distintos enfoques:

1. El del administrador de una empresa corporativa que desea prioritariamente tener resuelto el problema de administración centralizada. Es decir desea un antivirus que posea una consola que permita la instalación remota tanto en una red LAN como en una WAN y no verse obligado a instalar el producto a pie en cada una de las estaciones de trabajo. La experiencia ha demostrado que por lo regular cuando esto se logra, no siempre hay la garantía de que la calidad en la detección y la limpieza sea de lo mejor.

2. El del usuario final al cual lo que le interesa es no infectarse por ningún motivo y que la protección en memoria del producto sea de lo más eficaz, tanto para detectar y remover cualquier virus que pueda presentarse. Pero cuando esto se da, también suele suceder que las prestaciones de dicho antivirus para administrarlo lleguen a ser muy limitadas.

Tal parece que lo ideal para una empresa es tener bien estructurado un equipo de personas que procuren entender responsablemente ambos enfoques. Ningún producto en el mercado puede garantizar que se tendrán eficientemente el total de todas las prestaciones deseables. Por ello, más que procurarse el mejor antivirus lo que se necesita es diseñar las mejores estrategias de seguridad acordes a la problemática que se tenga. A veces no basta con una sola elección.

En virtud de lo anterior, al hacer una evaluación es importante tratar de verificar hasta qué punto los diversos antivirus que vayamos a considerar cumplen con las siguientes características:

I. Deben actualizar los patrones o firmas diariamente, o de no ser así poseer un buen motor heurístico.

II. La empresa que los promueve debe contar con un equipo de soporte técnico con acceso a un laboratorio especializado en códigos maliciosos y un tiempo de respuesta no mayor a 24 horas, el cual pueda orientar al usuario en su idioma, en caso de que contraiga una infección o tenga dificultades con el producto.

III. Deben contar con distintos métodos de verificación y análisis de posibles códigos maliciosos, incluyendo el heurístico, el cual no se basa en firmas vírales sino en el comportamiento de un archivo. Y así poder detener amenazas, incluso de posibles virus nuevos.

IV. Deben poderse adaptar a las necesidades de diferentes usuarios.

V. Deben poder realizar la instalación remota tanto en una red LAN como en una WAN.

VI. Deben constar de alguna consola central en donde se puedan recibir reportes de virus, mandar actualizaciones y personalizar a distintos usuarios. Todo esto, siempre y cuando se garantice que no se compromete de manera alguna la seguridad debido a vulnerabilidades no contempladas.

VII. Deben ser verdaderamente efectivos para efectos de detección y eliminación correcta y exacta de los distintos virus que puedan amenazar a los sistemas.

VIII. Deben de permitir la creación de discos de emergencia o de rescate de una manera clara y satisfactoria.

IX. No deben afectar el rendimiento o desempeño normal de los equipos. De preferencia lo que se desea es que su residente en memoria sea de lo más pequeño. También se espera que su motor de búsqueda sea rápido y eficiente.

X. El número de falsos positivos que se den tanto en el rastreo normal como en el heurístico debe ser el mínimo posible. La empresa debe de corregir en poco tiempo los “bugs” y los falsos positivos que se le reporten.

XI. Su mecanismo de auto-protección debe poder alertar sobre una posible infección a través de las distintas vías de entrada, ya sea Internet, correo electrónico, red, USB´s o discos flexibles, etc.

XII. Deben tener posibilidad de inspeccionar el arranque, así como los posibles cambios en el registro de las aplicaciones.

Con todas estas pautas anteriores, consideramos que se pueden tener los elementos suficientes que nos permitan ponerlos a prueba y de acuerdo con nuestras prioridades poder establecer nuestras propias conclusiones.

ANTIVIRUS EN LÍNEA

Un antivirus en línea, es un programa antivirus que se ofrece, por lo general, de forma gratuita para “escanear” y en algunos casos desinfectar los archivos infectados por virus. La característica principal de este tipo de programa es que se distribuyen a través de Internet, basta con tener un navegador Web (Internet Explorer) y acceso a la red para poder utilizarlo.

A pesar de que el uso de este tipo de programas es una gran ventaja, hay que tomar en cuenta algunas consideraciones:

i) La mayoría de los rastreadores en línea, en realidad no son tan en línea. De hecho instalan el rastreador en la máquina del cliente, de manera más o menos permanente. Lo hacen así porque realizar el rastreo desde una máquina remota sería extremadamente lento. Lo que ocurre es que no instalan el "exe", sino solo los DLLs y las definiciones; la orden de ejecutar el rastreo es lo único que viene del servidor Web una vez que se instaló el rastreador en el equipo del usuario (esto quiere decir algo interesante: cuando se hace un rastreo en línea, generalmente el producto se queda en la máquina del cliente y puede usarse sin tener que comprarlo, siempre que se sepa cómo activarlo sin ir a la página del fabricante). Algunos “escaners” tienen la decencia de incluir un desinstalador, mientras otros dejan allí su basura; y otros más, los que sí “escanean” desde el servidor, tienen la limitación de que hay que subir los archivos a “escanear”, lo que prácticamente anula su utilidad para la mayoría de las situaciones.

ii) El uso de la tecnología ActiveX, excluye a usuarios que usen otros navegadores como Netscape u Opera.

iii) En ocasiones, sólo van a ser útiles para detectar el tipo de virus que infecta al equipo. Por lo que se sugiere informarse si es necesario ocupar algún procedimiento especial de desinfección.

No obstante, existe una ventaja que a veces se pasa por alto: muchos virus y gusanos desactivan los antivirus para evitar ser detectados, pero a menudo sólo desactivan los antivirus que el autor del virus conoce, lo que excluye a las versiones "en línea", así que no es raro que algunos antivirus no puedan detectar virus que su “escáner” en línea sí encuentra.

A continuación tenemos algunos de los antivirus –la lista no es completa, para no quitarle al lector el encanto de buscar cuántos más existen- que hay disponibles en línea:

BITDEFENDER
http://www.bitdefender-es.com/scan/licence.html

COMMAND ANTIVIRUS CON F-PROT
http://www.antivirusmex.com/COD/scan.htm
Authentium tiene ahora una página para Command on Demand, el scanner en línea. El URL es http://www.commandondemand.com/. Ya no venden el producto, por eso lo quitaron de la página institucional, pero lo siguen regalando o incluyendo con una suite para ISPs, que es donde ellos piensan que el producto puede tener mercado.
La página de antivirusmex.com (de México) sigue ofreciendo este servicio gratuito y actualizado en la dirección http://www.antivirusmex.com/COD/scan.htm

DOCTOR WEB (DR. WEB)
http://old.antivir.ru/english/www_av/

ETRUSTANTIVIRUS
http://www3.ca.com/securityadvisor/virusinfo/scan.aspx

FORTIGUARD ANTIVIRUS
http://www.fortinet.com/FortiGuardCenter/virus_scanner.html

FREEDOM ANTI-VIRUS (SECURITY BUNDLE)
http://www.freedom.net/viruscenter/onlineviruscheck.html

KASPERSKY ANTIVIRUS (AVP)
http://www.kaspersky.com/virusscanner

MCAFEE VIRUSSCAN ANTIVIRUS
http://www.mcafee.com/myapps/mfs/default.asp
http://es.mcafee.com/root/mfs/default.asp

NORTON ANTIVIRUS
http://security2.norton.com/ssc/lunavbrk.asp?j=1&scantype=2&plfid=22&langid=us&venid=sym&pkj=WZLPJUIYCZRWEJGSSKE

http://security.symantec.com/sscv6/vc_scan.asp?langid=ie&venid=sym&plfid=23&pkj=CWEDYNBRFNJSVSTIVVB&vc_scanstate=2
Si se desea además buscar agujeros de seguridad, esto se puede hacer en: http://security.symantec.com/sscv6/sc_scan.asp?langid=ie&venid=sym&plfid=23&pkj=MRCDVYRMHCGVRVRMNRY&scanstate=2

OPEN ANTIVIRUS
http://www.openantivirus.org/
OpenAntivirus es el proyecto de desarrollo para un antivirus de código abierto, con licencia GNU, como Linux. Uno de sus componentes, VirusHammer (http://www.openantivirus.org/virushammer.php) es un antivirus de escritorio. Desarrollado en Java, debe funcionar en cualquier ordenador con JRE 1.3. La forma más sencilla de usarlo es en línea, para lo cual necesita descargar Java WebStart (http://java.sun.com/products/javawebstart/downloads/index.html). Aún está en fase de desarrollo y los patrones de virus no se actualizan con demasiada frecuencia.

Es interesante considerar lo expresado por Bernardo Quintero de Hispasec en:

OpenAntivirus, crónica de una muerte anunciada
(16/12/2003)
http://www.hispasec.com/unaaldia/1878

PANDA ANTIVIRUS
http://www.pandasoftware.es/productos/activescan/es/activescan_principal.htm
Tutorial: http://www.zonavirus.com/datos/manuales/4/Panda_Software_OnLine.asp

PC-CILLIN
http://housecall.antivirus.com/

PC PITSTOP (BASADO EN PANDA ANTIVIRUS)
http://pcpitstop.com/antivirus/default.asp

RAV ANTIVIRUS
http://www.ravantivirus.com/scan/

VIROBOT EXPERT
http://www2.globalhauri.com/html/onlineservice/livecall_service.html

Existe también el servicio **Jotti´s Malware Scan** para el “escaneo” completo de algún archivo a través de varios antivirus (AntiVir, ArcaVir, Avast, AVG Antivirus, Bitdefender, ClamAV, Dr. Web, F-Prot Antivirus, Fortinet, Kaspersky Anti-Virus, Nod32, Norman Virus Control, UNA y VBA32), que al final arroja un cuadro con el resultado.
http://virusscan.jotti.org/

De manera muy especial, nos referimos ahora a:
VIRUS TOTAL
http://www.virustotal.com/flash/index_es.html

Virus Total es un servicio desarrollado por:

Hispasec Sistemas
http://www.hispasec.com

Este es un laboratorio independiente de Seguridad Informática, que utiliza las versiones de línea de comando de varios motores antivirus (Avast! Antivirus, AVIRA Desktop, Quick Heal, ClamWin, Iris&Vet, Dr. Web, Nod32, Fortinet, F-Prot, AVG, AntiVir, The Hacker, Ikarus, AVP (KAV), VirusScan, Norman Antivirus, Panda Platinum, BitDefender, SAV, Antigen, Norton Antivirus y VBA32), actualizados puntualmente con las firmas oficiales publicadas por sus desarrolladores.

Este servicio permite enviar una muestra para que sea analizada por todos los antivirus ya mencionados y emite un cuadro de resumen.

Consideramos que un servicio tan valioso debiera abiertamente ser apoyado –respetando su independencia- por todas las empresas antivirus que tengan ya conocimiento de su existencia (por muchas razones a todas les conviene). Existen antivirus que no forman parte de esta lista y se echa de menos su presencia, por ejemplo:

a) F-Secure. Que aunque incluya con su tecnología “countersign” a los motores AVP y F-Prot, puede que no necesariamente signifique que se cuente con el uso de ambos motores a su máxima eficiencia, eso habría que constatarlo.

b) Command Antivirus con F-Prot. Aunque su motor de búsqueda sea el mismo que el de F-Prot y sus firmas sean compatibles, lo que no es igual es el interceptor de tiempo real (ni otros componentes gráficos, de instalación, etc.).
El interceptor de Command (llamado DVP) detecta y elimina los virus al vuelo, el de Frisk sólo detecta y detiene, pero requiere de un rastreo manual para eliminar.
Pese a estas diferencias, al parecer no tan importantes, habría que valorar las posibles ventajas de incluirlo en vez del F-Prot.

c) ViRobot de HAURI Inc. Quizá no les interese colaborar o no posean una buena versión para línea de comandos que soporte todas las propiedades necesarias.

En fin, sería bueno que al menos los antivirus mencionados en este artículo colaboraran con Virus Total. De esta manera, serían las empresas mismas las que

nos permitieran como usuarios conocer los distintos antivirus.

Adicionalmente, es recomendable conocer alguna página donde se pueda hacer algún análisis de vulnerabilidades en puertos, se recomiendan:

NEWORDER
http://neworder.box.sk/
Donde frecuentemente quedan en evidencia algunas empresas antivirus por los boquetes de seguridad que sus productos suelen abrir a cambio de ciertas "ventajas" de administración centralizada que ofrecen (la comodidad o aparente funcionalidad no necesariamente garantizan una buena seguridad).

Y la clásica:

BLACK ICE
http://www.blackcode.com/scan/

Aunado a esto, dado que la seguridad frente a códigos maliciosos, va de la mano con los problemas de Spyware (Los programas espía o spyware son aplicaciones que recopilan información sobre una persona u organización sin su conocimiento. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas, pero también se han empleado en círculos legales para recopilar información contra sospechosos de delitos. Además pueden servir para enviar a los usuarios a sitios de Internet que tienen la imagen corporativa de otros, con el objetivo de obtener información importante). Recomendamos:

AHNLAB SPYZERO (AHNLAB)
http://info.ahnlab.com/english/product/02_6_run.html

FREE ONLINE SPYWARE REMOVAL UTILITY (TREND MICRO)
http://www.trendmicro.com/spyware-scan/

ONLINE SPYWARE DETECTOR (PEST-PATROL)
http://home.ca.com/dr/v2/ec_main.entry25?page=PestScan1&client=ComputerAssociates&sid=35715&CID=190323

No olvidando:

DOXDESK (PARASITES, OR UNSOLICITED COMMERCIAL SOFTWARE)
http://www.doxdesk.com/parasite/
Que corresponde a un detector en línea de parásitos alojados en el registro.

Claramente, tratar con el Spyware no es un asunto trivial. Antes de hacer uso de

cualquier Anti Spyware que nos encontremos “regalado” en la Web, conviene que reflexionemos con calma el contenido de:

Anti Spywares sospechosos o no confiables
José Luis López
http://www.vsantivirus.com/lista-nospyware.htm

La delgada barrera que separa los códigos maliciosos ilegales de los legales (Adware y Spyware)
http://www.enciclopediavirus.com/enciclopedia/articulo.php?id=564

VIRUS PARA LOS CUALES NO HAY ANTIVIRUS (VIRUS FALSOS, RUMORES, ETC.)

Haciendo primero hincapié en:

VMYTHS.COM
http://www.vmyths.com/
Página que incluye la documentación más completa y la más antigua conocida sobre hoaxes y leyendas urbanas.

Recomendamos aquí algunos artículos relativos a los famosos bulos o falsas alarmas:

El verdadero peligro de los hoax
Nuria Cordón Villapalos
http://alerta-antivirus.red.es/virus/ver_pag.html?tema=V&articulo=6&pagina=12

"La ciencia del rumor"
Vicente Coll
(Escrito por primera vez el 2/10/2002)
(Revisado el 9/5/2003)
http://www.enciclopediavirus.com/enciclopedia/articulo.php?id=125

Las más peligrosas alimañas informáticas: los virus manuales
Ignacio M. Sbampato (17/05/2001)
http://www.vsantivirus.com/sbam-virus-manuales.htm
http://diariored.com/analisis/2001_05_18_19_28_47.html

Ahora bien, si lo que se desea es tener un buen conocimiento de los alcances –reales- y las certificaciones de los distintos productos del mercado, no basta conocer lo más básico e inmediato del tema, que es lo que se encuentra plasmado en páginas de Internet tales como:

About.com
http://antivirus.about.com/

AV-Test.org
http://www.av-test.org/index.php3?lang=en

ICSA Labs
http://www.icsa.net/

HackFix
http://www.hackfix.org/

Virus Bulletin
http://www.virusbtn.com/
En relación a esta página hay un verdadero problema, que ya no es de acceso gratuito, para ver las comparativas hay que pagar. Es difícil interesarse por información (aunque sea buena) que solamente unos cuantos puedan ver.
Es una lástima, pues de otra manera, el lector podría cotejar directamente lo dicho en artículos tales como:

¿Porque fallan los antivirus?
http://www.noticiasdot.com/publicaciones/2005/0405/2604/noticias/noticias_260405-14.htm

NOD32 y otros antivirus
http://www.nod32.com.mx/compare/Files/NOD32yotrosantivirus.pdf

"Colby-Sawyer College."
http://www.eset.com/resources/Colby_Sawyer_white_paper.pdf

"Frost & Sullivan."
http://www.nod32.com/resources/Frost-Sullivan%20White%20Paper%20-%20Evolving%20Threats.pdf

Virus Research Unit
http://www.uta.fi/laitokset/virus/

Virus Test Center
http://agn-www.informatik.uni-hamburg.de/vtc/naveng.htm

West Coast Labs
http://www.westcoastlabs.org/

WildList Organization
http://www.wildlist.org/

Es recomendable, recurrir a comparativas más imparciales para tener un poco de más de luz sobre el tema. Se tienen -por ejemplo- las de Hispasec:

Comparativa del 2001
http://www.hispasec.com/directorio/laboratorio/articulos/Comparativa2001

Comparativa del 2000
http://www.hispasec.com/directorio/laboratorio/articulos/Comparativa2000

Comparativa del 1999
http://www.hispasec.com/directorio/laboratorio/articulos/Comparativa1999

U otras, también interesantes:

Análisis comparativo de los principales sistemas antivirus
Luis Armas Montesino (20/07/2003)
http://bvs.sld.cu/revistas/aci/vol11_5_03/aci05503.htm

¿Cuál antivirus elegir?
José Luis López (Agosto de 2000)
http://www.vsantivirus.com/comparativa.htm

Si de certificaciones se trata, es bastante interesante leer:

Las certificaciones antivirus I, II y III
Informe de Ignacio M. Sbampato
Vicepresidente de ESET para Latinoamérica
http://www.segu-info.com.ar/terceros/ISbampato_LasCertificacionesAntivirus_I.htm
http://www.segu-info.com.ar/terceros/ISbampato_LasCertificacionesAntivirus_II.htm
http://www.segu-info.com.ar/terceros/ISbampato_LasCertificacionesAntivirus_III.htm

Comparativas y certificaciones antivirus: la necesidad de un nuevo modelo
Bernardo Quintero (21/07/2004)
http://www.hispasec.com/unaaldia/2096

Los mitos del British Standard 7799 y el ISO 17799
Andrés Velásquez (06/05/2004)

http://www.netmedia.info/bsecure/articulos.php?id_sec=52&id_art=4743
http://www.netmedia.info/bsecure/articulos.php?id_sec=52&id_art=4743&num_page=20389

Comparativas y certificaciones antivirus
Bernardo Quintero (22/07/2003)
http://www.hispasec.com/unaaldia/1731

ISO 17799: LA GESTIÓN DE LA SEGURIDAD
D. Daniel Cruz Allende (Julio De 2003)
http://www.virusprot.com/Art41.htm

CERTIFICACIONES EN SEGURIDAD INFORMÁTICA. CONCEPTOS Y REFLEXIONES
D. Jeimy J. Cano (Abril de 2003)
http://www.virusprot.com/Art38.html

Certificaciones de productos, ¿garantía de seguridad o marketing?
Bernardo Quintero (11/11/2002)
http://www.hispasec.com/unaaldia/1478

Certificaciones antivirus obsoletas
Bernardo Quintero (24/07/2002)
http://www.hispasec.com/unaaldia/1368

¿Cuán creíbles pueden ser las comparativas de antivirus?
José Luis López (04/06/2002)
http://www.vsantivirus.com/04-06-02.htm

Personalmente puntualizamos lo siguiente:

1).- El enfoque de crítica a las certificaciones no es preciso del todo. Pues Virus Bulletin, ICSA Labs, se aplican de manera muy explícita a los especimenes que pueden ser considerados como virus en todo el sentido de la palabra y cuya peligrosidad ya sea grande o relativa no está puesta a duda, no se enfocan tan fuertemente al problema de gusanos, troyanos, backdoors, –a menos que su difusión constituya en el mundo una amenaza clara-; y demás variantes de malware (código malicioso), pues este no es su objetivo ni tampoco es sencillo agotar el tema. Los antivirus no son un software "anti-lo-que-sea".

2).- Con las certificaciones más comunes, se ha analizado la eficacia relativa sin llegar al fondo de la calidad relativa de la limpieza de cada producto y por lo regular no suelen enfocarse por igual a arrojar análisis en todas y en cada una de las plataformas, como sería lo deseable.

3).- Irnos por el lado de ISO (certificación de calidad total), nos daría garantía de que como empresa certifican que tienen cierta calidad en sus procesos y los documentan. Esto es más bien garantía de seriedad y cumplimiento de estándares

comúnmente aceptados, pero esto por sí solo no acredita holgadamente la eficacia ni la eficiencia. El caso de los antivirus, tanto como producto así como servicio suele ser más delicado. Una empresa antivirus que tenga ISO, no por ello ya "la hizo".

4).- Más que las certificaciones y las comparativas, lo ideal sería poder evaluar y comparar la velocidad real de los laboratorios de las empresas antivirus ante una amenaza real, cómo responden, a qué velocidad y que tan sólida o buena suele ser su respuesta. Un ejemplo de ello se puede ver en los interesantísimos artículos de José Luis López, en relación a un virus específico, a saber:

Crónica de un virus (Nueva versión del Frethem)
(15/07/2002)
http://www.vsantivirus.com/15-07-02.htm

Crónica de un virus (II) (Nueva versión del Frethem)
(16/07/2002)
http://www.vsantivirus.com/16-07-02.htm

5).- De las comparativas que se pueden hallar en:
http://webs.ono.com/usr009/Coburn44/testAV.htm
(un sitio que reúne varias comparativas)

Solamente la de HISPASEC es la que se puede considerar con más seriedad e independencia, por la honestidad y el rigor de Bernardo Quintero. No es perfecta, pero estoy seguro que Bernardo es de los pocos especialistas en el mundo que si se le cuestiona o se le refuta con bases sólidas lo que dice, no solamente contesta sino que es capaz de hacer público que los que los discrepan con sus apreciaciones también pueden tener razón. Además de que procura hacer su trabajo de la manera más imparcial y objetiva.

En torno a esto, quedan abiertas –como una invitación a la reflexión- algunas preguntas a las cuales se les da una respuesta inicial o tentativa:

¿Es o no importante que alguien pueda finalmente certificar la calidad de respuesta de los laboratorios de las empresas antivirus ante una nueva amenaza?
- Desde luego que no sólo es importante, sino crucial. Eso pondría a cada quién en su lugar. Porque de esa manera, los antivirus con una buena heurística quedarían muy por encima de otros que sin definiciones dejan pasar todos los nuevos virus en las primeras horas de difusión.

¿Es importante o no que alguien pueda certificar que las bases de los antivirus no incluyan a virus que no son tales?

- Sólo por razones de eficiencia, no de eficacia. Se puede vivir con eso mientras no repercuta sensiblemente en el desempeño del sistema, pues con los virus que hay ya es suficiente. Este problema va de la mano de la pregunta anterior, los antivirus con buena heurística no se ven afectados por una base de datos inflada artificialmente, porque sólo recurren a ella cuando ya se confirmó la presencia de un intruso. En cambio los antivirus que están atados a la base de datos, como sucede con algunos de los más comerciales, sí llegan a impactar el desempeño. Hay que reconocer que de todos modos, estos no siempre tienen la reputación de inflar sus bases de datos.

¿Qué aspectos en los antivirus son importantes y hasta la fecha nadie los contempla en las certificaciones?

- La velocidad de respuesta ante un nuevo espécimen que les es enviado para análisis. También la capacidad de reacción ante nuevas tecnologías virales que no pueden atacarse con sólo la actualización de definiciones. De nuevo, este es un talón de Aquiles de ciertos antivirus apoyados bastante por el "marketing", pues el usuario tiene que esperar hasta que sale la nueva versión del programa o conformarse con una solución ad-hoc que es inadmisible en el contexto corporativo, donde no se puede pretender que se descontaminen a mano 3,000 o más equipos. La capacidad de actualizar componentes y no sólo definiciones, a menudo no es ponderada con la seriedad debida y puede más una marca o un anuncio que los méritos tecnológicos del producto. Esto se debe en buena parte a que los evaluadores corporativos aplican los mismos parámetros para seleccionar la suite de Office que un antivirus.

Procedamos a concluir este artículo, estableciendo una serie de referencias para posteriormente poder entrar bastante en detalle:

En lo que concierne a los diversos criterios para conocer algo sólido acerca de los antivirus (y temas bastante relacionados), siempre y cuando se tenga la suficiente motivación, adicionando a ello opiniones verdaderamente calificadas (las cuales nos permitirán obtener los elementos básicos para cuestionar el tema de manera crítica en torno a sus diferentes sutilezas), nos atrevemos a recomendar los siguientes artículos:

Amenazas contra el aparato financiero I y II
Informe de Ignacio M. Sbampato
Vicepresidente de ESET para Latinoamérica
http://www.segu-info.com.ar/terceros/ISbampato_AmenazasContraElAparatoFinanciero_I.htm
http://www.segu-info.com.ar/terceros/ISbampato_AmenazasContraElAparatoFinanciero_II.htm

Los virus de 2004. Incidencia y tendencias. Previsión para 2005
http://www.alerta-antivirus.es/docs/seguridad_empresas.pdf

CÓMO COMPRAR UN SOFTWARE DE SEGURIDAD
José de Jesús Ángel (septiembre de 2003)

http://www.virusprot.com/Art44.html

VIRUS INFORMÁTICOS Y OTROS BITCHOS
Juan José Nombela Pérez (Mayo de 2002)
http://www.virusprot.com/Art26.html

Firmas antivirus más allá del malware tradicional
Bernardo Quintero (24/05/2005)
http://www.hispasec.com/unaaldia/2404

Virus Bulletin: Reflexiones sobre detección heurística
(22/10/2004)
Información publicada con autorización de Virus Bulletin
Autor: Andrew Lee. Eset LLC, USA.
Traducción y adaptación al español: Ontinet.com, S.L.
http://www.vsantivirus.com/heuristica-comparativas.htm

Vulnerabilidad en múltiples antivirus con archivos ZIP
Ángela Ruiz (20/10/2004)
http://www.vsantivirus.com/20-10-04.htm

No hay antivirus contra la curiosidad
José Luis López (04/08/2004)
http://www.vsantivirus.com/04-08-04.htm

Indicador del tiempo de reacción antivirus
Bernardo Quintero (28/07/2004)
http://www.hispasec.com/unaaldia/2103

Flecos de las soluciones antivirus
Bernardo Quintero (26/03/2004)
http://www.hispasec.com/unaaldia/1979

El Futuro de los Antivirus
Arnoldo Moreno Pérez (24/02/2004)
http://www.vsantivirus.com/am-futuro-av.htm

Virus dañados e inofensivos
Bernardo Quintero (08/01/2004)
http://www.hispasec.com/unaaldia/1901

Gusano invisible a filtros y antivirus perimetrales
Bernardo Quintero (01/12/2003)
http://www.hispasec.com/unaaldia/1863

El software antivirus actual no es suficiente
Fernando de la Cuadra (14/11/2003)

http://www.vsantivirus.com/fdc-nosuficiente.htm

Cuando un antivirus es peor que la enfermedad
Ángela Ruiz (31/08/2003)
http://www.vsantivirus.com/ar31-08-03.htm

Seguridad Informática: Peligros Ocultos
Por Juan Carlos. Zampatti Maida (20/08/2003)
http://www.vsantivirus.com/zma-peligros.htm

La importancia de los parches en la defensa contra los virus
Ignacio M. Sbampato (11/07/2003)
http://virusattack.virusattack.com.ar/articulos/VerArticulo.php3?idarticulo=61

Advertencia del CERT sobre virus y antivirus
Redacción VSAntivirus (07/07/2003)
http://www.vsantivirus.com/cert-in-2003-01.htm

Microsoft, punto de inflexión para la industria antivirus
Ángela Ruiz (21/06/2003)
http://www.vsantivirus.com/21-06-03.htm

Microsoft y el mercado antivirus
Bernardo Quintero (13/06/2003)
http://www.hispasec.com/unaaldia/1692

Funcionamiento de un programa antivirus
Fernando de la Cuadra (09/05/2003)
http://www.vsantivirus.com/fdc-funcionamiento-antivirus.htm

Virus, antivirus, y sensacionalismo mediático
Bernardo Quintero (28/04/2003)
http://www.hispasec.com/unaaldia/1646

Antivirus: ¿Incluir o no incluir? Ésa es la cuestión
Ignacio M. Sbampato (10/04/2003)
http://www.vsantivirus.com/sbam-incluir.htm
http://diariored.com/blog/ana/archivo/000300.html
http://www.kriptopolis.com/more.php?id=57_0_1_0_M

Tests antivirus para comprobar la protección del e-mail
Bernardo Quintero (01/04/2003)
http://www.hispasec.com/unaaldia/1619

Antivirus: ¿especialización o navaja suiza?
Bernardo Quintero (28/03/2003)
http://www.hispasec.com/unaaldia/1615

Office 2003 puede poner en aprietos a los antivirus
Redacción VSAntivirus (23/03/2003)
http://www.vsantivirus.com/23-03-03.htm

Desarrollador antivirus pide que Internet sea regulada por los gobiernos
Bernardo Quintero (19/03/2003)
http://www.hispasec.com/unaaldia/1606

Antivirus: el efecto "zoo"
Bernardo Quintero (03/02/2003)
http://www.hispasec.com/unaaldia/1562

La problemática del SPAM desde un ángulo distinto
Ignacio M. Sbampato (21/01/2003)
http://diariored.com/blog/ana/archivo/000091.html

Bautizar un virus
Bernardo Quintero (26/12/2002)
http://www.hispasec.com/unaaldia/1523

Comentarios sobre los antivirus perimetrales
Bernardo Quintero (31/10/2002)
http://www.hispasec.com/unaaldia/1467

Antivirus corporativo: dos (diferentes) mejor que uno
Bernardo Quintero (13/08/2002)
http://www.hispasec.com/unaaldia/1388
http://virusattack.virusattack.com.ar/articulos/VerArticulo.php3?idarticulo=46

Mitos y verdades en la seguridad de los antivirus
Marcos Rico (09/07/2002)
http://www.vsantivirus.com/mr-mitos.htm

Antivirus que no son tales
DareDeviL (09/05/2002)
http://www.vsantivirus.com/sol-antivirusno.htm

¡Pruebe si su antivirus lo está realmente protegiendo!
José Luis López (07/04/2002)
http://www.vsantivirus.com/eicar-test.htm

FBI y puertas traseras en los antivirus
Bernardo Quintero (12/12/2001)
http://www.hispasec.com/unaaldia/1144

Debilidades en los antivirus

Ignacio M. Sbampato (25/02/2001)
http://www.vsantivirus.com/sbam-debilidades.htm

Virus "in the wild": ¿cuál es la formula?
Giorgio Talvanti (23/02/2000)
http://www.hispasec.com/unaaldia/484

---

[*] Este artículo constituye la nueva versión de:

Conozca los distintos antivirus
VSantivirus No. 436 - Año 5 - Lunes 17 de septiembre de 2001
http://www.vsantivirus.com/am-conozcaav.htm

Más que una actualización de este trabajo, se procuró adicionar algunas cuantas precisiones sobre el tema.

El autor desea manifestar todo su reconocimiento, respeto y agradecimiento a:

Dr. José Enrique Villa Rivera
Instituto Politécnico Nacional
http://www.ipn.mx/comunicacionsocial/director/docts/DirectorGeneral.pdf

Profa. Alba Martínez Olivé
Dirección General de Formación Continua de Maestros en Servicio de la Secretaría de Educación Pública.

Dr. Salvador A. Sánchez de la Peña, Dra. Guadalupe Paz Peralta y Naim Emmanuel Mena Ramírez. Laboratorio de Cronobiología Médica de la Sección de Estudios de Posgrado e Investigación (SEPI) de la Escuela Nacional de Medicina y Homeopatía (ENMH) del Instituto Politécnico Nacional (IPN).

Dra. Flavia Becerril Chávez
Clínica de Acupuntura de la ENMH del IPN

Lic. Ana Luisa Calvillo Vázquez. Facultad de Ciencias Políticas y Sociales de la Universidad Nacional Autónoma de México.

[**] Mexicano. Consultor Independiente en Temas de Seguridad Informática (miru@prodigy.net.mx). Colaborador en varios medios digitales.

[***] El autor agradece la generosidad y los comentarios puntuales hechos por José Anaya (de la empresa CIBERSEL) a la versión preliminar de este artículo. Sobre todo en lo que respecta a la parte de Antivirus en Línea y la sección de preguntas y respuestas, estas últimas le corresponden íntegramente a él salvo muy ligeras modificaciones.