Publicación quincenal editada por el Departamento de Telecomunicaciones y Telemática del Instituto Superior Politécnico José Antonio Echeverría
Auspiciada por el Ministerio de la Informática y las Comunicaciones

Año VII No. 7

ISSN: 1729-3804

Telem@tica

Junio 3, 2008
"Año 50 de la Revolución"

REVISTA DIGITAL DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

FRASE DE LA SEMANA

"El amor es un fruto que madura en todas las estaciones y que se encuentra al alcance de todas las manos."

Teresa de Calcuta

SUMARIO

Contáctenos

REVISTA TELEM@TICA
Departamento de Telemática
Facultad de Ingeniería Eléctrica

Instituto Superior Politécnico
José Antonio Echeverría

Calle 114, No. 11901, entre 119 y 127, Municipio Marianao, Habana,Cuba

Teléfono:
+53 (7) 2606279 / 2679880

Fax:
+53 (7) 2671576

Telematica@revistas.cujae.edu.cu

Sitio Web:
http://www.cujae.edu.cu/revistas/telematica

IR al SUMARIO

NOTA DEL EDITOR

Estimado lector:

La selección del antivirus para proteger nuestra información se ha convertido en una polémica tan antigua como los propios programas malignos. Diversas son las opiniones, y múltiples las comparativas y las anécdotas al respecto.

El artículo que se presenta hoy en Telem@tica ofrece un análisis acerca del complejo tema de los productos antivirus y aborda qué aspectos deben tenerse en cuenta, en nuestro entorno informático, para elegir uno apropiado.

Sin pretender tener una respuesta final categórica (como procuran muchos acalorados “entendidos”), en este número encontraremos algunas ideas, expuestas por un verdadero especialista en la materia, que nos resultarán muy útiles a la hora de seleccionar el producto antivirus que protegerá nuestros archivos, mensajes de correo y otros.

Esperamos que lo disfruten.

Nos encontraremos nuevamente en el próximo número.

Los Editores.

TÉCNICAMENTE HABLANDO

Actualización: Conjunto de ficheros a descargar e instalar por el software antivirus, emitidos de manera regular por su fabricante, que contienen las bases de definiciones de programas malignos o bases antivirus, a partir de los cuales el producto puede identificar y descontaminar los códigos malignos descritos en estas.

Antivirus: Software capaz de detectar y prevenir el accionar de los programas malignos o, en su defecto, combatirlos o minimizar su impacto.

Licencia: Fichero suministrado por el fabricante antivirus al cliente contratado y que necesita incorporarse en el producto para que este pueda actualizar las bases antivirus y funcionar de acuerdo con su manual de operación.

Protección permanente: Módulo del antivirus que, al estar activado, previene el accionar de los códigos malignos reconocidos mediante el bloqueo de la ejecución de los ficheros infectados que detecta.

Programa maligno: Programa que afecta el normal funcionamiento del sistema operativo de una computadora y puede propagarse, al infectar otros programas y ficheros del mismo sistema o mediante las vías de conexión de las redes de computadoras, para así afectar otros sistemas. Las categorías más comunes son virus, gusano y Caballo de Troya.

ARTÍCULO

La selección del antivirus: ¿comodidad o estrategia informática?

Alejandro Enrique Monett Díaz
Ingeniero en Telecomunicaciones y Master en Ciencias. Empresa de Consultoría y Seguridad Informática, SEGURMATICA.
Amonett@segurmatica.cu

INTRODUCCIÓN

Ante la masiva aparición de programas malignos en el mundo informático de hoy, toda computadora, para cumplir su función cabalmente, requiere de una protección efectiva. Se necesita un software que monitorice el sistema operativo en busca de infecciones y que sea capaz de prevenirlas o, una vez detectadas, neutralizarlas y restablecer las condiciones normales de operación, a la vez que se actualice de manera automática y no monopolice los recursos del sistema[1,2].

Los productos antivirus surgieron inicialmente para contrarrestar la acción de los virus informáticos y se han utilizado para combatir los restantes tipos de programas malignos, entre los que sobresalen gusanos, caballos de Troya (por comodidad llamados troyanos), chistes, bombas de tiempo, los más recientes como *spyware* y *rootkits*, y sus posibles combinaciones, hasta el conocido *spam* que puede incluir cualquiera de las categorías anteriores[3].

PRODUCTOS ANTIVIRUS EN CUBA

Basta con analizar cuántos códigos malignos distintos agrega en el día un fabricante de productos antivirus a sus bases de definiciones, comúnmente bases antivirus, para comprender la proliferación de los mismos en los sistemas informáticos actuales. Ya desde principios del 2007 los fabricantes antivirus de mayor renombre reportaban cantidades promedio diarias entre 200 y 300 programas malignos nuevos incorporados a sus bases. Esta tendencia se ha mantenido hasta el año 2008 a nivel internacional, donde han prevalecido las categorías de troyanos y las nuevas variantes de una misma familia de códigos[4]. Como era de esperar, también en Cuba se han reportado incidencias de programas malignos por lo que la protección de sus sistemas informáticos ha estado constantemente a prueba.

La Empresa de Consultoría y Seguridad Informática (Segurmatica), perteneciente al Ministerio de la Informática y las Comunicaciones, surgió en 1995 para institucionalizar la labor precedente del Grupo Nacional de Expertos creado en 1988[5], cuando se detectó en el país el primer código maligno, y posteriormente el trabajo del Laboratorio Latinoamericano para la Protección contra los Virus Informáticos[6], inaugurado en 1993 con el auspicio de la UNESCO. En Segurmatica se continuó, además, el desarrollo de productos antivirus, únicos de factura nacional y cuyo inicio databa de 1988.

Segurmatica es reconocida, principalmente, por la efectividad de su producto antivirus ante la aparición de programas malignos de producción nacional. La política de la empresa ha sido desarrollar un software antivirus para enfrentar, en primera línea, las amenazas que representan los códigos malignos hechos para Cuba, los que sean reportados nacionalmente antes de que exista una respuesta a nivel internacional, los que tengan un alto nivel de propagación o puedan representar un peligro mayor para los sistemas informáticos. Los frutos de esta estrategia son halagüeños: La calidad del producto antivirus nacional se puede medir por su eficacia en la descontaminación de los códigos malignos reportados en el país, a la vez que previene la propagación de otros de mayor incidencia internacional.

Es conocido que los fabricantes de antivirus enfocan el análisis de muestras de códigos malignos en la identificación o detección más que en la descontaminación y dejan al producto antivirus la solución del problema. Para ello es necesario que el producto se mantenga actualizado y que el mecanismo de prevención (comúnmente residente, monitor, protección en tiempo real, protección permanente, entre otros términos) se encargue de detectar cualquier actividad asociada al código maligno, impida su acción mediante el bloqueo al acceso del objeto infectado y lo elimine del sistema. En otras palabras, la eficacia del producto recae en la potencialidad de su prevención[7].

La razón de este enfoque es sencilla: consume mucho menos tiempo analizar qué es lo que identifica o distingue a un código maligno del resto si se compara con la investigación asociada y la programación de las acciones que debe llevar a cabo el antivirus para restablecer los daños ocasionados, lo que se conoce como descontaminación, tarea más compleja en programas malignos diferentes de la categoría virus.

Mientras el programa maligno sea un virus y pueda ser identificado será efectiva la descontaminación, la cual eliminará la parte infectada del fichero asociado al mismo. Pero si pertenece a cualquiera de las restantes categorías, entonces fallará la descontaminación y se podrá borrar el fichero infectado del sistema si así se define como acción secundaria por el módulo de prevención. En este caso, si ya el sistema estaba infectado, los restantes y posibles efectos de la infección, como llaves de registro dañadas o mal configuradas, quedarían intactos y, en consecuencia, el sistema operativo no sería restablecido a sus condiciones normales de operación[3].

El análisis en Segurmatica de los códigos malignos reportados en Cuba, a partir de las muestras obtenidas de los clientes, permite la posterior emisión de actualizaciones antivirus que no solo incorporan la identificación sino también la descontaminación, siempre que sea posible[8]. Aquí reviste especial importancia el producto antivirus nacional, a pesar de que la competencia que crean los propios usuarios se basa, generalmente, en la cantidad de códigos detectados por un antivirus o si tal antivirus detecta lo que otro no.

Como no existe una solución única para todos los problemas ocasionados por los programas malignos, en aras de aumentar el nivel de seguridad informática de las entidades cubanas con la presencia de un producto antivirus de prestigio internacional, en el año 2003 Segurmatica realizó una alianza con la empresa rusa Kaspersky Labs, fabricante de productos antivirus, de la cual se convirtió en su distribuidor oficial a nivel nacional. Esta alianza, lejos de abrir una fuerte competencia de los productos de Kaspersky con sus homólogos de Segurmatica, inició una línea de trabajo en el desarrollo de software antivirus cuyo ejemplo a seguir son los productos del mundialmente reconocido fabricante.

A partir de esta relación, Segurmatica comenzó el desarrollo de un software que integra el motor antivirus de Kaspersky en el producto cubano, denominado Segurmatica Antivirus Edición Kaspersky, cuya primera versión pública ya está disponible. Con ello, se puede decir que, en el momento de confección de este artículo, hay tres productos antivirus cuyas licencias se pueden obtener de manera oficial en Cuba.

EL RIESGO DE USAR PRODUCTOS ANTIVIRUS NO OFICIALES

¿Por qué no valorar las ofertas de otros fabricantes antivirus cuando sus productos también son excelentes? La respuesta es simple, aunque es lamentable que todavía no sea conocida por todos los directivos, informáticos y, en general, usuarios de todo el país: Porque esos fabricantes “no le venden a Cuba”. Asimismo, lo publican en sus sitios Web o en las condiciones del acuerdo de licencia de sus productos. Para ello utilizan términos, basados en el genocida bloqueo contra la Isla del cual la venta de software no escapa, los que se enmascaran con artificios legales como “Prohibida su exportación o reexportación a los países catalogados por el Gobierno de los Estados Unidos como terroristas o que se encuentren en la lista del Embargo (…)”, entre otros, pero cuya idea final es impedir al nacional obtener ese producto tan necesario o deseado. De esta única razón se derivan ciertas limitaciones, unas explícitas y fáciles de evaluar por el experto informático, otras con consecuencias difíciles de probar pero perfectamente posibles de ocurrir.

Los principales fabricantes antivirus del orbe, que adquieren su fama no solo por la efectividad de sus productos sino también por la globalización de su uso, están asentados en los Estados Unidos o se relacionan, de alguna forma, con empresas de ese país, por lo que tal prohibición se extiende públicamente entre todos y el producto no está disponible. Ante esa situación, es inapropiado utilizar un producto de este tipo y, sobre todo, más inseguro.

Las limitaciones fundamentales que se derivan de usar productos antivirus distintos a los oficialmente comercializados en Cuba se explican a continuación[8]:

La licencia de operación no sería la otorgada por el fabricante antivirus a la entidad, sino obtenida de forma gratis pero desde cualquiera de los sitios maliciosos de Internet que publican ya sea licencias robadas de otras entidades, licencias piratas que confunden al producto antivirus y son aceptadas como válidas o bien programas para su generación pirata aleatoria.

Por lo general, estas licencias piratas son para tipos y versiones de productos cuya funcionalidad es específica y no contemplan toda la variedad que puede brindar el fabricante, para los cuales rara vez se encuentra una licencia pirata útil. Aún cuando se permita el uso ilegal del software más usado de un fabricante antivirus, típicamente para una estación de trabajo, se pierde la opción de contar con licencias para emplear en otros productos y así establecer una defensa en profundidad que abarque todos los frentes o servicios de red y que constituyen las vías de propagación de los códigos malignos.

El tema de la licencia constituye, además, una espada de Damocles, ya que obliga a buscar una nueva cuando está próximo a expirar el tiempo de utilización de la licencia actual – comúnmente por un año– y no siempre se encuentra donde mismo se consiguió aquella.

A lo anterior se suma la posibilidad del fabricante de incorporar, en una suerte de lista negra de su sitio Web o en el propio producto, aquellas licencias detectadas como piratas por su uso y ubicación geográfica y que invalidan la actualización de las bases antivirus del producto, al estilo del mecanismo de verificación de autenticidad que emplea Microsoft para la actualización de los sistemas Windows.

Para los productos no oficiales tampoco existe el soporte técnico, hoy catalogado como un valor tan o más importante que el propio software antivirus pues garantiza la continuidad de su funcionamiento y la solución de problemas comunes, entre los que se incluyen la instalación in situ del producto – a realizar por especialistas experimentados y por ende, más eficiente y eficaz que si fuera llevada a cabo por la propia entidad– y el enfrentamiento de códigos malignos de nueva aparición. Por tal motivo, se considera al soporte técnico como un valor agregado, un producto más, por el cual se esmera cada fabricante de antivirus en que sea de excelencia y así se mantenga la preferencia del cliente.

Por último, y a consideración del autor constituye la principal limitación, no existe la garantía de que cada actualización de las bases antivirus que se descargue del sitio oficial sea verídica o confiable. El fabricante puede establecer en su sitio Web un mecanismo automático que detecte el origen de la computadora que intenta actualizar el producto y, si es de Cuba (fácilmente reconocible por bloques bien definidos de direcciones IP asignados al país), prohibir la descarga e incluso implementar mecanismos solapados que brinden una falsa sensación de protección.

La falsa protección que se crea es difícil de comprobar pues se necesita actualizar el mismo producto antivirus desde dos fuentes distintas, léase instalarlo en dos computadoras y que una de ellas no acceda al sitio Web oficial directamente desde una dirección pública cubana y después comparar la cantidad de códigos distintos que se detectan con cada actualización; aunque para mayor confiabilidad se debiera intentar la descontaminación de un sistema infectado con ambas actualizaciones y comprobar su efectividad. Segurmatica ha encontrado casos con diferencias en ese sentido, donde la actualización descargada desde una dirección IP de Cuba no ha sido más eficaz que la obtenida en el mismo momento por otra vía.

Problemas de índole similar pero más grave se han detectado en un ámbito más amplio. Existen reportes internacionales que han comprobado puertas traseras en productos de Microsoft y de otras compañías con el objetivo de acceder a la información de la computadora cliente. Y si nos remontamos en el tiempo vale recordar que en la década de 1980 el sistema computadorizado adquirido por la URSS a los EEUU para controlar un importante oleoducto siberiano estuvo infectado, desde sus inicios, por un programa troyano implantado por los EEUU, que al cabo del tiempo inutilizó todo el sistema y originó una explosión catastrófica. Claro está, ambos ejemplos preocupan mucho más por cuanto están relacionados con productos comprados oficialmente, pero ¿qué no podría ocurrir con productos pirateados?

La confiabilidad se pierde cuando no se conoce lo que está descargando el antivirus. El usuario cree que el producto está actualizado y confía en la seguridad del sistema pero no hay garantía en ello. Lo mismo puede descargar, sin su consentimiento pues el antivirus lo hace de manera automática, programas malignos orientados al robo de información o pensar que la actualización identifica o descontamina un código nuevo cuando en realidad no es así. Todo ello implica un daño potencial difícil de evitar o muy complicado de evaluar sus consecuencias. Mucho menos responsabilidad podría tener el fabricante antivirus para generar una actualización que resuelva en tiempo y forma el problema ocasionado por un programa maligno desarrollado en o para Cuba.

Si lo anterior no lo hacen hoy la mayoría de los fabricantes de seguro están por hacerlo en cualquier momento. De todos modos, lo hagan o no, nunca se conocerá todo lo que se descarga.

Los productos antivirus disponibles como gratis en Internet y los de código abierto, en cualquier caso aquellos cuyo paquete de instalación no requiere un fichero de licencia para su uso y puede actualizar las bases antivirus libremente desde su sitio oficial, no están exentos de este análisis. A pesar de no requerir trámites oficiales o de contratación para su uso también caen en la duda de confiar en su actualización antivirus. De todos modos, la ventaja para un posible uso futuro la tienen los antivirus de código abierto, pertenecientes al conocido software libre, al cual no ha estado ajeno el país pues ya se observan estrategias para su implementación paulatina a nivel nacional.
Los riesgos de utilizar productos antivirus no oficiales son evidentes, sobre todo los desarrollados por fabricantes que expresamente publican la prohibición de su venta a Cuba. En algo tan importante como la actualización antivirus, que casi todos los fabricantes emiten diariamente y en algunos casos cada una hora para combatir los programas malignos de nueva aparición, no existe garantía en su efectividad si el producto no es oficial.

LA SELECCIÓN DEL ANTIVIRUS APROPIADO

En agosto de 2007 la Gaceta Oficial de Cuba publicó la Resolución 127/07 que define el "Reglamento de seguridad para las tecnologías de las información"[9]. En la "Sección Sexta: Seguridad ante programas malignos" se indica que se "utilizarán los programas antivirus de producción nacional u otros autorizados oficialmente para su uso en el país, debidamente actualizados". Esta indicación constituye un importante paso de avance y establece una línea a seguir para las entidades cubanas.
Entonces, ¿cuál antivirus seleccionar? Retomemos el análisis inicial y valoremos las limitaciones de los productos pirateados. Si contamos con los mencionados productos que de manera oficial se comercializan en el país (de Segurmatica, de Kaspersky y la integración Segurmatica Antivirus Edición Kaspersky), la selección debe valorar, en primer lugar, los riesgos o amenazas inherentes a los activos informáticos a proteger. En otras palabras, se debe analizar lo que se quiere proteger y de qué se quiere proteger y entonces aplicar el producto más apropiado. Para ello se deben considerar las posibles vías de entradas de programas malignos, entre las que se encuentran la navegación por Internet, los mensajes de correo electrónico y el acceso a los ficheros locales y compartidos en red, por solo citar las más comunes, y ubicar en cada una el producto adecuado.
En la selección debe influir el nivel de complejidad del producto a utilizar y la preparación técnica del especialista informático que se encargará de su despliegue y mantenimiento, sin olvidar la aceptación del usuario final, que en definitiva es quien "convivirá" con el producto.
Asimismo, la compatibilidad con sistemas operativos y aplicaciones afines puede marcar la diferencia. Aquí se deben valorar los requerimientos de instalación y funcionamiento de cada producto y revisar su cumplimiento en cada sistema informático.
Se debe considerar, además, el precio de la licencia a comprar. Si existe un "empate" en los aspectos anteriores el factor determinante pudiera ser el precio, pues los productos de alguna forma relacionados con Kaspersky Labs incluyen, como es lógico, una componente de moneda libremente convertible y la consiguiente erogación de divisas del país. La renovación de la licencia de cada producto contratado será a través del mismo mecanismo utilizado cuando se contrató por vez primera y con una frecuencia anual.
De manera excepcional se pudiera contar con más de un producto antivirus instalado en el mismo sistema operativo, en cuyo caso se recomienda mantener habilitada la protección permanente de uno solo para no afectar el buen desempeño del sistema. De todos modos, existen productos que comprueban en el momento de su instalación la existencia de otro antivirus y, en consecuencia, no la efectúan.
Llegado a este punto del análisis, el controvertido tema de la actualización se despeja al estar garantizada su disponibilidad, confiabilidad y veracidad con cualquiera de estos tres productos oficiales. La licencia contratada posibilita que el antivirus pueda actualizarse de verdad y cuando se desee, siempre que se sigan las instrucciones de su manual de operación. Las actualizaciones de Kaspersky se ubican en su sitio Web oficial[1] mientras que las de Segurmatica Antivirus y de Segurmatica Antivirus Edición Kaspersky están disponibles en el sitio Web de Segurmatica[2].

EL ANTIVIRUS NO LO PUEDE RESOLVER TODO

De nada sirve utilizar un producto antivirus contratado oficialmente si no se establece una configuración aceptable o no se actualiza de manera frecuente, de acuerdo con lo recomendado en su manual de operación. El riesgo de infección aumenta si, por ejemplo, se deshabilita la protección permanente del producto o este se actualiza con una frecuencia semanal.

IR al SUMARIO

Incluso un antivirus bien configurado y actualizado no puede resolver los problemas que se deriven de[8]:

- La falta de actualizaciones de seguridad para los sistemas operativos y aplicaciones afines, emitidas por los correspondientes fabricantes.
- La ausencia de medidas prácticas y técnicas para regular el uso de los recursos y servicios de la red, que incluyen: el filtrado de adjuntos ejecutables en el servicio de correo electrónico, la configuración segura del cliente de correo y del navegador de Internet y la desactivación de la reproducción automática para los dispositivos de almacenamiento extraíbles, esta última catalogada de imprescindible desde principios de 2007 hasta la fecha.
- La deficiente preparación, en cuanto a la seguridad informática, de los administradores de la red y sus usuarios.
- La incorrecta arquitectura de cortafuego empleada.
- La poca aplicación o desuso del plan de seguridad informática de la entidad.

Cualquiera de estas deficiencias u otras de seguridad informática puede propiciar la propagación de un programa maligno, tanto peor si es de nueva aparición, a lo cual siempre estará expuesto el producto antivirus. En cuanto a este, es responsabilidad del especialista informático de la entidad garantizar su constante monitorización para que funcione de acuerdo con lo recomendado en su manual de operación.

IR al SUMARIO

CONCLUSIONES

La inmunidad absoluta no existe, los riesgos por infección se suceden de manera vertiginosa, y lleva tiempo y recursos proteger los sistemas informáticos. La clave del éxito está en minimizar, en lo posible, las consecuencias dañinas del accionar de los programas malignos por medio de una solución que combine la implementación de medidas de seguridad correctas, que eviten las mencionadas deficiencias u otras similares con el uso de un producto antivirus apropiado, sobre la base de que la seguridad informática es un proceso constante.
El presente análisis no pretende favorecer un producto específico con el simple descarte del resto. No se trata de mercadotecnia para mantener clientes actuales o ganar nuevos, sino de exponer la mejor solución antivirus para nuestras computadoras. La selección del antivirus no se debe regir por la arbitrariedad, pues requiere de una estrategia bien definida que garantice la continuidad de los sistemas computacionales. Está en juego la seguridad informática del país.

REFERENCIAS

1. **KASPERSKY LABS:** Sitio Web oficial, disponible en: http://www.kaspersky.com.

2. **SEGURMATICA:** Sitio Web oficial, disponible en: http://www.segurmatica.cu.

3. **GIL HERNÁNDEZ, ELIZABETH:** "Sistema de Gestión de Información de programas malignos", *Tesis de Lic. en Ciencia de la Computación*, Universidad de La Habana, La Habana, Cuba, 2005.

4. **RAIU, COSTIN:** "Situación internacional de los programas malignos", Conferencia presentada en *XII Convención Informática 2007*, La Habana, Cuba, 2007.

5. **BIDOT PELÁEZ, JOSÉ:** "Un Laboratorio Latinoamericano para la Protección contra los Virus Informáticos", Metánica, Año 0, Número 0, pp 33-34, La Habana, Cuba, 1994.

6. **QUINTERO, BERNARDO:** "Antivirus: Rendimiento vs. Protección", Hispasec Una al día, disponible en: http://www.hispasec.com/unaaldia/3210, 2007.

7. **SEGURMATICA:** Documentación de los Grupos de Laboratorio Antivirus y Soporte Técnico.

8. **GACETA OFICIAL:** "Reglamento de seguridad para las tecnologías de las información", Resolución 127/07, Sección Sexta, La Habana, Cuba, 2007.

IR al SUMARIO

EVENTOS

Estimado(a) colega:

El Departamento de Telecomunicaciones y Telemática del Instituto Superior Politécnico José Antonio Echeverría, CUJAE, tiene el agrado de invitarle al V Congreso Internacional de Telemática y Telecomunicaciones CITTEL´08. Esta quinta convocatoria se desarrollará del 1 al 5 de diciembre del actual año en el marco de la XIV Convención Científica de Ingeniería y Arquitectura (CCIA 14) en La Habana, Cuba, la cual tendrá como sede el Palacio de las Convenciones de esta capital.

El evento tiene como Tema central “La Telemática y las Telecomunicaciones: protagonistas en el camino hacia la independencia tecnológica”

Las temáticas a abordar en el Congreso son:

1. Gestión de Redes
2. Seguridad de Redes y Sistemas
3. Sistemas Informativos
4. Comunicaciones Móviles e Inalámbricas
5. Servicios Telemáticos
6. Computación Distribuida y Paralela
7. Redes de Próxima Generación (NGN - Next Generation Networks)
8. Redes de Telecomunicaciones
9. Enseñanza de la Telemática

El programa del evento incluye conferencias magistrales, mesas redondas, paneles, seminarios, presentación de ponencias y cursos tutoriales.

Ccleaner 1.14.072

Por:

Ing. Julio Cesar Camps

Email: camps@tesla.cujae.edu.cu

Ficha Técnica	
Fecha:	Octubre 7/2004
Nombre:	CCleaner
Propiedad:	CCleaner.com
Versiones:	CCleaner 1.14.072
Tamaño:	306.86 KB
Plataformas	Microsoft Windows 95, 98, ME, XP, NT, 2000, 2003.
Idiomas	Inglés
Clasificación	CNET > Downloads > Windows > Internet >Online Privacy>
URL	http://www.ccleaner.com/
Descripción	CCleaner (Crap Cleaner) es una herramienta gratis de optimización del sistema. Permite la eliminación de los ficheros temporales y no usados, permitiendo que el sistema operativo se ejecute de una forma más rápida, más eficiente, y a la vez liberar una mayor cantidad de espacio de disco duro. La mejor parte, es que !Es muy rápido!
Observaciones	Elimina: • Caché del Internet Explorer, historial, cookies, index.dat, la papelera de reciclaje, ficheros temporales y ficheros de log. • Urls recientemente visitadas y ficheros. • ficheros temporales y ficheros recientemente usados de terceras aplicaciones (Media Player, eMule, Kazaa, Google Toolbar, NetsCape, Office XP, Nero, Adobe Acrobat, Winrar, Winace, Winzip y más.). • Scanner avanzado de registros, y limpiador para eliminar entradas viejas y sin usar. • Incluyendo ficheros de extensiones, controles de activex, ClassIDs, ProgIDs, desinstaladores, DLLs compartidas, ficheros de fuentes(letras), ficheros de ayuda, iconos, accesos directos inválidos.
Calificación	Excelente según opiniones y análisis @ @ @ @ @ 91%

Resumen

Aunque es aplicación, no posee algunas de las características de otras de su misma rama (borrado seguro, entre otras), ofrece las suficientes como para constituir por si misma, una opción recomendable. CCleaner , inclusive, puede realizar un backup del registro de windows, antes de realizar cualquier cambio, para prevenir que un borrado accidental pueda colapsar el sistema; además incluye la posibilidad de desinstalar cualquier programa. Debido a todo lo antes expuesto, podemos, sin ningun tipo de problemas ni reservas, recomendar este software para cualquier usuario que necesite un poco más de privacidad, mediante la eliminación de datos sensitivos.

NOTICIAS

SEGURIDAD

Sitio web falso regala solución antispyware 30/05/2008

IronPort Systems detectó la aparición de un sitio web falso que ofrece una solución antispyware gratuita.Se trata de un envío aleatorio de mensajes que invita al usuario a instalar una solución antispyware gratuita para proteger la PC. Cuando es abierto el sitio web falso gratuito automáticamente se activa la descarga de un troyano malicioso. La aparición del archivo en PDF muestra el virus troyano y ofrece más información sobre su detección y proliferación.

Fuente: http://www.diarioti.com

TECNOLOGIA

Sony lleva el concepto de “pantalla plana" a una nueva dimensión 02/06/2008

El presidente de Sony, Howard Stringer, presentó la nueva novedad en el ámbito de las pantallas ultraplanas. El anuncio fue hecho durante la conferencia D6; es decir, la sexta edición de la conferencia que Wall Street Journal denomina "D" (All Things Digital). La pantalla OLED tiene un espesor de solo 0,3 mm; es decir, más delgada que una tarjeta de crédito. La pantalla tiene una superficie útil de 11 pulgadas y una resolución de 960x540 píxeles. Sony está además abocada al desarrollo de una versión de 27 pulgadas de la pantalla, que dado su espesor funcionará prácticamente como un autoadhesivo. A mediano plazo, OLED competirá con LCD por las preferencias de los usuarios para televisores. El mayor inconveniente de la tecnología OLED es su elevado precio.

Fuente: http://www.diarioti.com

IR al SUMARIO

SEGURIDAD

Vulnerabilidad en Adobe Flash distribuye malware 30/05/2008

Los ciberdelincuentes están distribuyendo archivos con extensión .swf (la extensión de los archivos de Flash) modificados para aprovechar esta nueva vulnerabilidad en Adobe Flash de dos maneras distintas. En algunos casos, cuando un usuario visita una página web que contiene uno de estos archivos modificados, su navegador interpreta el código incluido en los mismos como una orden para descargar un ejemplar de malware determinado. En otros casos, el código incluido en el archivo Flash lo que hace es redirigir la navegación en segundo plano -es decir, sin que el usuario se percate de ello- a una página maliciosa desde la que se lanzan nuevos ataques contra el sistema, con el fin de introducir malware en el mismo.Un dato interesante es que los ciberdelincuentes han creado códigos para afectar a distintos navegadores.

Fuente: http://www.diarioti.com

HARDWARE

Acer presenta nueva línea de PCs para jugadores 02/06/2008

Acer presenta la nueva computadora de escritorio Aspire Predator. Con un +diseño original y agresivo del chasis alberga las tecnologías de más reciente generación que los gamers exigen. Aspire Predator se presenta con una cubierta en color cobre metálico, la parte frontal del cuerpo puede elevarse, acompañado del primer mecanismo de bahía óptica que revela un lector de DVD y Blu-ray Disk. Los puertos USB y de audio de fácil acceso en la parte superior se complementan con un lector de tarjetas montado al frente. Rayos azules de luz emanan del botón de encendido y de la puerta frontal de la unidad de disco duro. Una de las características de Predator es el hecho que se puede tener acceso a los Discos Duros a través de una puerta especial ubicada al frente de la parte inferior del chasis: la solución estándar Acer Easy-swap Hard Drive permite sacar los 4 discos duros removibles de alta capacidad Serial ATA 3 Gb/s incluso cuando la PC está encendida y en uso.

Fuente: http://www.diarioti.com

IR al SUMARIO

SOFTWARE

Adobe presenta Acrobat 9

03/06/2008

Adobe Systems anunció el software Adobe Acrobat 9, una importante actualización que transformará el proceso de creación e intercambio de documentos electrónicos.Acrobat 9 ofrece soporte nativo para la tecnología Adobe Flash, la habilidad de unificar una gama de contenido en PDF Portfolios interactivos y acceso a capacidades en tiempo real para co-navegar un documento PDF. Por primera vez, Acrobat 9 ofrece un soporte para la tecnología Adobe Flash, lo que permite a los usuarios incluir video y archivos de aplicación compatibles con Adobe Flash Player en documentos PDF. Los destinatarios solo necesitan el software gratuito Adobe Reader 9 para poder tener acceso al contenido. Además, la solución ofrece acceso a capacidades para colaboración en vivo dentro de un mismo documento PDF, mediante el uso de Acrobat.com, una nueva suite de servicios hospedados de Adobe (anunciada en versión beta).

Fuente: http://www.diarioti.com

TELEM@TICA

PARA INSCRIBIRSE EN LA REVISTA:

Enviar un mensaje a:

revistatelematica-subscribe@cujae.edu.cu

PARA ANULAR SU INSCRIPCIÓN EN LA REVISTA:

Enviar un mensaje a:

revistatelematica-unsubscribe@cujae.edu.cu

PARA AUTORES QUE DESEEN PUBLICAR EN TELEM@TICA

Para la publicación en nuestra revista los interesados deberán enviar su propuesta escrita indicando claramente: Título del artículo, glosario de términos (No más de media cuartilla), imágenes referenciadas (No más de 200Kb), nombre de los autores, sus fotografías y la institución a la que pertenecen, así como alguna forma de comunicación (teléfono, Fax o correo electrónico). Para una guía más detallada descargue el formato de publicación de la dirección: http://www.cujae.edu.cu/revistas/telematica/Soporte_Tecnico/formato.doc
Su artículo se someterá a revisión por un comité de árbitros que decidirá sobre la publicación del mismo. Deberán acompañar igualmente (en no más de media cuartilla) un glosario, de los términos más importantes utilizados en el artículo. Puede contactarnos a través de nuestro email telematica@revistas.cujae.edu.cu