BREVE INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

Miércoles 24 de agosto de 2016

Por el Trad. Públ. Héctor A. Gomá.

Palabras clave: Seguridad, Software

Uno de los aspectos que más desvela a los usuarios de tecnología es la seguridad informática. Muchos la asimilan con la protección contra virus y otro tipo de programas maliciosos, pero veremos que esta disciplina abarca mucho más que eso.

Para resumir, podemos afirmar que la seguridad informática consiste en aquellas prácticas que se realizan dentro de un determinado sistema con un objetivo doble: proteger el funcionamiento y salvaguardar los datos almacenados.

Los **riesgos** se componen de **amenazas**, que comprende a toda acción que resulta en un peligro cierto para equipos o archivos como podría ser un intento de intrusión a nuestro dispositivo (PC, celular o tableta) y **vulnerabilidades**, que expresan el grado de exposición, muchas veces involuntario, al que están sometidos los sistemas informáticos. El ejemplo más claro es el de un programa con un error interno que facilita accesos no deseados a nuestra información.

Ahora bien, ¿de dónde provienen las mayores amenazas para un sistema? La respuesta puede ser obvia para algunos y antipática para casi todos: los **usuarios**. Son (somos) ellos los que, a través de acciones premeditadas o no, permiten que un sistema resulte vulnerado. Los ejemplos abundan: la descarga de archivos peligrosos, la instalación de programas maliciosos, muchas veces disfrazados de utilidades y la entrega de datos a terceros que los solicitan mediante subterfugios variopintos.

Ante este panorama, dentro del espacio acotado con el que contamos, intentaremos dejar unas breves indicaciones y opciones informáticas para robustecer la seguridad de nuestros datos.

Antivirus y antimalware: semejanzas y diferencias

Son dos programas que cumplen funciones similares, pero con ciertas diferencias que hacen que los clasifiquemos en categorías independientes, si bien en muchas ocasiones suelen detectar y neutralizar amenazas de índole parecida.

Primero, es necesario definir y contrastar dos términos muy usados: virus y malware.

Los virus son programas creados para infectar sistemas y otros programas. El objetivo es causar daños a los datos y, en general, afectar el funcionamiento de las computadoras contagiadas.

Malware es la abreviatura de *malicious software* (*software* malicioso), que engloba a todo tipo de programa o código informático que tenga como objeto dañar un sistema o afectar su funcionamiento. Este término comprende a los troyanos, gusanos, *spyware*, *adware*, *rootkits*, *hijackers*, *keyloggers*, etc.

Si el malware es el género y el virus la especie, entonces ¿por qué hay programas específicos para detectar *malwares* y otros para eliminar virus?

Un antimalware y un antivirus no son lo mismo ya que el primero está orientado a todo tipo de *malware*, salvo los virus, debido a que históricamente ya los antivirus desempeñaban esta función. Sin embargo, el avance tecnológico hizo que cada vez existieran más programas maliciosos con características más refinadas que un simple virus, hecho que condujo a la implementación de los antimalware.

Antivirus

Este es el programa básico para proteger nuestros archivos. Por tratarse de un componente del que nadie puede prescindir, la oferta es extensa y variada. Muchos programas ofrecen versiones gratuitas, en general pensadas para el uso hogareño que suelen sacrificar ciertas características avanzadas que solo ofrecen las versiones pagas. Naturalmente, siempre es mejor adquirir una licencia paga, pero eso no significa que un programa gratuito no logre resguardarnos, aunque es lógico que debamos ser algo más cuidadosos para suplir las opciones de las que no dispondremos.

¿Cuál debemos elegir? Es una pregunta para la que no existe una respuesta definitiva. Cada antivirus tiene puntos débiles y fuerte y la experiencia suele variar según el usuario.

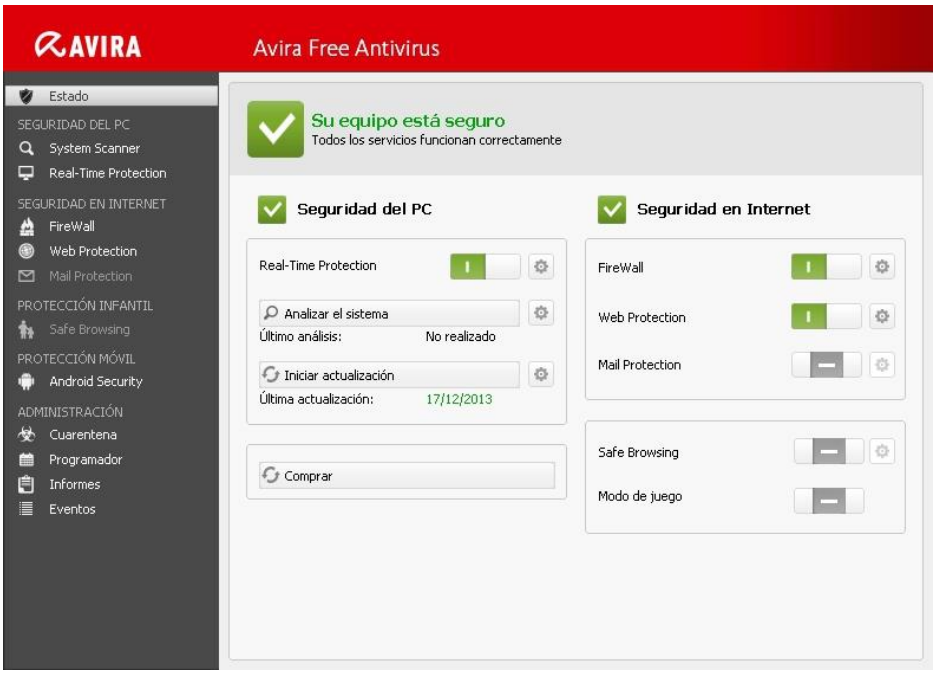
Entonces, presentaremos aquí algunos ejemplos que han funcionado bien en nuestros equipos, sin que ello constituya un impedimento para que el lector pruebe otras soluciones.

Avast

Muy difundido y de eficacia comprobada, ofrece, además de eficacia alta en la detección de virus, uno de los mejores desempeños en el bloqueo de sitios y aplicaciones maliciosas. Tiene varias opciones de configuración, lo que le confiere una flexibilidad notable para este tipo de programas.

Enlace de descarga: https://www.avast.com/index

Avira



Un poderoso y difundido antivirus, que siempre está en el podio de los mejores. Usa el mismo motor que la versión comercial, lo que garantiza resultados óptimos. Por si fuera poco, también protege contra todo tipo de *malware*. Para los usuarios más aviesos, posee herramientas extra listas para instalar si así lo deseamos.

Enlace de descarga: https://www.avira.com/es/download/product/avira-free-antivirus

BitDefender Free

BitDefender es, quizás, el programa que menos necesita de nosotros para realizar su tarea. Una vez instalado, ya no requiere configuración alguna y se limita a ofrecernos una interfaz espartana que es posible activar mediante un simple clic. No cuenta con publicidad y consume pocos recursos. Una opción más que válida, aunque aquellos usuarios que deseen mayor control sobre las aplicaciones, quizás echen en falta más opciones. Funciona con Windows 7, 8 y, según el desarrollador, ya es totalmente compatible con Windows 10.

Enlace de descarga: http://www.bitdefender.com/solutions/free.html

Antimalware

Malwarebytes Anti-Malware

Aquí la elección apunta a un programa en particular: Malwarebytes Anti-Malware. Si bien muchos antivirus ofrecen protección contra troyanos y otro tipo de código malicioso, pocos pueden competir con la potencia de esta aplicación. La versión gratuita no detecta amenazas en tiempo real (salvo los primeros 14 días, luego de lo cual esta característica se desactiva), por lo que

recomendamos **analizar la computadora periódicamente o si sospechamos de la presencia de un programa malicioso**.

Enlace de descarga: https://www.malwarebytes.com/mwb-download/

Otras recomendaciones

Algunas o quizás todas, parezcan obvias. No por ello están de más y siempre es bueno recordarlas. La seguridad informática, como ya hemos visto, no se limita a la búsqueda de amenazas, sino que también comprende seguir una serie de prácticas para minimizar los riesgos.

- Evitar bajar archivos y programas de proveniencia sospechosa. Es posible que este sea e consejo menos original de todos, pero no deja ser el más importante. Desde imágenes "gratuitas" para adornar los mensajes de Skype, hasta supuestos optimizadores del desempeño de la computadora, cualquier anzuelo es bueno para aprovecharse de un usuario desprevenido. Ni hablemos de los portales que ofrecen copias pirata que suelen ser la puerta principal para los virus y códigos maliciosos más dañinos.
- No acceder a sitios web de reputación dudosa. Esta sugerencia está vinculada con la anterior. En muchas ocasiones, un sitio en apariencia inocuo, como puede ser un *hosting* de imágenes puede conducir a la instalación subrepticia de aplicaciones de publicidad no deseada o algo peor.
- Actualizar el software periódicamente. Siempre es prudente mantener nuestros programas actualizados y no nos referimos solo al sistema operativo. Navegadores, herramientas de traducción y cualquier otro tipo de programa son, en general, más seguros cuando están al día, no solo porque incorporan mejoras, sino que los desarrolladores suelen remediar cualquier posible vulnerabilidad que se haya pasado por alto en versiones iniciales.
- Evitar proporcionar cualquier tipo de datos personales a través de formularios o correos electrónicos. En este caso se aconseja extrema prudencia al enviar datos personales, en especial ante pedidos de contraseñas u otro tipo de información confidencial a través de correos de «soporte técnico» o similares.
- Contar con contraseñas fuertes. Correo, wifi hogareño, claves de banca electrónica son objetivos tentadores para cualquier pirata informático. Por ello, es imperativo elegir contraseñas que no remitan a obviedades (fechas de cumpleaños, nombres de familiares, etc.) para no facilitar la tarea de ajenos inescrupulosos.

Esperamos que este artículo conciso sea de ayuda para los colegas preocupados por la protección de sus equipos y datos.