

Trabajar de forma segura con Windows XP (II)

Introducción

✔ Le será de suma utilidad la revisión de la [primera parte](#) de este informe antes de comenzar la lectura de este documento

En un segmento anterior tratamos de analizar Windows XP y de averiguar qué medidas generales y sencillas se deben tomar para que este sistema operativo sea más seguro solamente con una personalización del sistema, una configuración adecuada y un comportamiento prudente, adecuado e informado.

Esto significa no tener que recurrir a programas externos o herramientas de terceros, es decir, utilizar solamente aquellos disponibles de manera inmediata en el propio sistema operativo Windows.

En este segmento, analizaremos cómo mejorar aún más la seguridad de Windows implementando aplicaciones comerciales y gratuitas de terceros, disponibles en la actualidad en Internet.

Protéjase con un programa antivirus

Creemos que, no por sabido, deja de ser necesario decir enfáticamente que se debe utilizar programas antivirus actualizados para verificar archivos, mensajes de correo electrónico y cualquier elemento que envíe o reciba a través de Internet y, de esa forma, controlar la presencia de virus.

Además, es necesario advertir a los usuarios para que no abran documentos, archivos ejecutables, programas salvapantallas, video, fotografías o publicidad en boletines recibidos de fuentes desconocidas o sospechosas.

Pero, sin embargo, muchas personas desestiman estas advertencias y, por consiguiente, infectan sus ordenadores con toda clase de programas maliciosos y peligrosos.

Donde, para los usuarios más cautelosos existe un claro indicio de una posible infección, para los menos cautelosos existe únicamente la posibilidad de algo interesante adjunto y una correspondencia no solicitada que en realidad no contiene nada, salvo una carga maliciosa incluida.

Existen algunos detalles a considerar acerca del uso de programas antivirus:

1. Si ya sabe o sospecha que un archivo o carpeta podría contener un virus, realice un análisis de ese objeto antes de tratar de abrirlo.
2. Bajo ninguna circunstancia trate de ejecutar un programa recibido de fuentes dudosas sin asegurarse, previamente, que no contiene virus.

La mayoría de los programas antivirus actuales contienen dos módulos de verificación de virus, cómo mínimo:

- Un módulo a petición del usuario que se puede utilizar para analizar archivos o carpetas seleccionadas en un ordenador.
- Otro módulo es un monitor de actividad de virus en tiempo real, que funciona de forma permanente y que asegura que ningún archivo que contenga un virus se abrirá de forma accidental.

De forma adicional, algunas soluciones antivirus de última generación, poseen módulos adicionales y específicos para mejorar la prevención y seguridad en objetos determinados, como podrían ser: documentos de Microsoft Office y clientes de correo electrónico, entre otras posibilidades.

El módulo a petición, según como esté diseñada la solución antivirus, podrá servir sólo para verificar aquello que el usuario desea analizar en un momento específico o, también, pudiera ser incluido como una línea de defensa adicional al ejecutarse periódicamente en el ordenador, verificando si se hubieran vulnerado todas las líneas de defensa y el sistema se encontrase infectado.

Algunos antivirus, de última generación, son capaces de analizar e interceptar los virus en el momento en que acceden al ordenador a través del sistema específico de conexión Winsock, y mediante filtros selectivos de revisión, mientras que otros, menos desarrollados, sólo cuentan con la capacidad de interceptación del módulo monitor.

Mientras que el módulo a petición es ejecutado por el usuario cada vez que este lo desea (a excepción de aquellos que permiten utilizarlo también para la revisión periódica del sistema) el módulo residente o monitor, se encuentra en ejecución y alerta, desde el mismo momento en que el sistema se inicia y, en última instancia, será el encargado de la última línea de defensa, ya que analizará el posible riesgo de un archivo al ser éste seleccionado o, en soluciones avanzadas, al detectarse la actividad del mismo.

Soluciones antivirus más desarrolladas tendrán además, varias líneas de defensa intermedias según sea el tipo de aplicación y actividad involucrada.

Pero lo que sí debe quedar en claro, es que cuanto antes (y más alejado de dejar toda la responsabilidad en el módulo monitor) se pueda interceptar un virus, mejores condiciones de seguridad se obtendrá en el ordenador.

Adicionalmente, tenga en cuenta que los programas antivirus tienen dos formas básicas de detectar la presencia de virus, y la capacidad de análisis e interceptación no son iguales para todos los productos actuales:

- **Firmas o definiciones de virus**

Son las equivalentes informáticas de las huellas dactilares humanas utilizadas para identificar un virus.

En la mayoría de las soluciones antivirus cualquier pequeña desviación de la definición brindada y el programa antivirus no tendrá ninguna forma de detectar los virus más modernos o creados recientemente.

Por lo tanto, en estos casos, existe una brecha clara entre el instante en que un nuevo virus se dispersa y el momento en que la correspondiente definición que describe al virus es incorporada por los proveedores de programas antivirus.

Dado que esta brecha puede oscilar entre una hora y algunos días, siempre habrá momentos en los cuales no exista una definición del nuevo virus y por consiguiente los programas verificadores no los podrán detectar. Ese tiempo es el más destructivo y es cuando el virus que logra infectar un ordenador realiza los estragos más grandes: una brecha que las compañías antivirus se esfuerzan por minimizar.

Sin embargo, coincidente con una nueva tendencia, algunos productos de última generación han incorporado firmas genéricas que les permite detectar esas desviaciones e interceptar variantes, que anteriormente no era posible individualizar.

- **Análisis heurístico**

Algunas soluciones antivirus de última generación, han desarrollado sistemas de detección, muy sofisticados, en base a comportamientos presuntos y puntos específicos de verificación que permiten interceptar un nuevo virus antes que el mismo haya sido clasificado e incorporado a la base de firmas, disminuyendo la brecha entre la primer diseminación y la incorporación a las definiciones de virus.

Ultimamente, las soluciones antivirus más desarrolladas han comenzado a incorporar definiciones de firmas para código malicioso en general, mucho más allá de sólo interceptar virus de distinto tipo sino, que también, intentando detectar distintos tipos de amenazas.

En cualquiera de estos casos, no todas las soluciones antivirus son iguales ni tienen el mismo poder de detección. Se puede encontrar una buena referencia para analizar la calidad de un producto antivirus, consultando las estadísticas de una publicación independiente como [Virus Bulletin](#), que periódicamente efectúa análisis comparativos entre distintos programas disponibles, otorgando sus premios VB 100% a aquellos que logran cumplir con las exigentes pruebas.

Para utilizar su programa antivirus de forma más eficiente y maximizar el índice de captura de virus, no olvide habilitar la opción de análisis heurístico y seleccionar, cómo mínimo, las siguientes carpetas sobre las que deberá prestarse especial atención:

- Donde se ha instalado Windows
- Archivos de Programas
- Documents & Settings (Documentos y configuración)
- Archivos temporales de Internet

Es conveniente verificar periódicamente los registros de análisis para verificar que todo funciona como se ha configurado y, además, verificar las posibles infecciones.

Cierre las puertas de la red con un cortafuegos

Como empresa que desarrolla su propio cortafuegos, la lista de posibilidades que podemos citar, ofrecida por esta tecnología, es realmente vasta.

Pero los principios esenciales detrás de cada cortafuegos eficiente son:

- Filtrado de paquetes (tráfico global y datos por procesos)
- Vigilancia de puertos
- Defensa contra ataques de piratas
- Protección de la privacidad del usuario

Un **cortafuegos** es como un escudo que protege las comunicaciones de datos entre su ordenador y el resto de los equipos con los que se encuentra conectado, ya sea por medio de la red de área local o Internet.

Protege los paquetes que ingresan y salen de su ordenador para asegurarse que solamente los datos legítimos puedan ingresar y, que se descarte el resto de manera efectiva.

Sin la protección de un cortafuegos, cualquier programa que se instale en un ordenador ya sea de forma conciente o no, podría conectarse a cualquier dirección remota y cargar o descargar la información que desee (que podría ser información privada del usuario que debe mantenerse de forma segura).

Podría prácticamente abrir un programa en un ordenador cualquiera, enteramente a su discreción.

Con un cortafuegos puede definir explícitamente cuáles serán las funciones que realizará cada programa, con quién se conectará y qué tipo de libertad de comunicación podrá tener.

Un cortafuegos es en cierta forma un “mentor de la red” que siempre está vigilando las conexiones de los ordenadores y protegiendo la seguridad del usuario en línea.

A continuación se encuentra una lista de los peligros contra los que puede proteger un cortafuegos, para que pueda discernir si debe instalar uno:

- Protección contra ataques pirata, bloqueo de gusanos y programas espía impidiendo la divulgación de datos confidenciales.
- Permite ocultar la presencia del ordenador en la red para que el mismo no sea susceptible de ataques a través de Internet.
- Puede denegar la actividad de programas ilegales, brindando registros de los eventos que suceden en un ordenador.
- Es capaz de mantener en privado la actividad de navegación en Internet, lo que facilita el bloqueo de contenido inapropiado.
- Puede llevar registros, en tiempo real, de todas las conexiones de red.

Windows XP SP2 incluye un cortafuegos integrado, pero no brinda ni la mitad de las funciones mencionadas anteriormente, por consiguiente, no es el más apropiado y no puede competir contra programas cortafuegos comerciales independientes y de amplia trayectoria, entre los que **Outpost Firewall PRO** se ubica en el primer lugar.

🔗 Consulte la [comparativa](#) entre las prestaciones de ambos cortafuegos para obtener información más precisa.

Erradique programas espía y diversas aplicaciones no deseadas

Por lo menos, se recomienda la existencia de una aplicación contra programas espía, para que se limpie del ordenador lo que el programa antivirus podría haber dejado sin verificar, es decir, diferentes formas de programas espía que no entran en la definición de un virus de ordenador y, por consiguiente, no puede ser eliminado con técnicas de antivirus convencionales.

Un cortafuegos puro cerrará el camino que el programa espía utiliza para “llamar a casa”, pero para erradicarlo del ordenador por completo, se requiere un programa de búsqueda y eliminación de aplicaciones contra programas espía.

El problema con los programas espía en general, radica en su definición.

No existe consenso absoluto acerca de cuál programa debería considerarse como espía y, por consiguiente, ser eliminado de los ordenadores de los usuarios.

Sin embargo, un buen explorador de programas espía, debe brindar una opción para que el usuario seleccione los tipos de programas a eliminar junto con consejos acerca de programas espía específicos y conocidos.

Desde la versión 3.0 de Outpost Firewall Pro se ha incorporado una herramienta específica contra programas espía.

Elimine correo no deseado de forma automática

Todo el mundo sabe que el correo no deseado, es muy invasivo, persistente y bastante engañoso.

Sin embargo, muchas personas eligen combatirlo manualmente y eliminarlo de sus casillas de correo todos los días mientras intercambian correo electrónico.

No obstante, este proceso se puede automatizar con un programa confiable contra el correo no deseado que analice el texto en el cuerpo de un mensaje no solicitado, y juzgue de manera adecuada si es válido.

El programa protege su estado financiero y la seguridad de su ordenador al no permitir que cargas maliciosas como *Phishing* o *gusanos* de ordenadores enviados junto con el mensaje de correo no deseado lleguen a usted.

Al utilizar un programa para filtrar correo no deseado, desde el comienzo deberá "enseñarle" al mismo a identificar el correo legítimo del que no lo es, pero después de un tiempo, su tarea se reducirá sensiblemente y podrá minimizar los errores o falsos positivos.

Conclusión

Por supuesto, las recomendaciones brindadas en este material no garantizan por sí solas que su ordenador estará completamente seguro.

Nada en la vida es absoluto. Pero estas recomendaciones contribuirán en gran medida a proteger su ordenador al máximo posible.