

## **Guía de protección de su ordenador**

*Por Leonardo Donaire Perales (Dr. Software)*

En primer lugar debemos tener conciencia que nuestra seguridad no la resuelve un solo programa por sofisticado y completo que nos parezca.

También debemos ser concientes que la seguridad es algo que no sólo depende de los programas sino también de nosotros mismos y de nuestro criterio.

Señalare algunos programas que deberíamos tener instalados en nuestro ordenador para estar mucho más seguros.

### **1.- Un antivirus. (pero actualizado)**

Es nuestra primera línea de defensa contra virus, gusanos, troyanos y otras amenazas. Un ordenador sin antivirus o con uno no actualizado, está expuesto a todo tipo de ataques lo cual nos puede producir desde la pérdida de datos vitales hasta el espionaje de todo lo que hacemos con él.

Hoy día la gama de antivirus es muy variada, no es fácil decidirse entre el Nod32. el Kaspersky y el Security Essentials.

No estaremos más seguros si instalamos dos antivirus, en muchos lugares he visto esto, lo cual es ilógico y es mas no se toman en cuenta las incompatibilidades de algunas marcas con otras.

Como regla de oro sólo un antivirus puede estar monitoreando.

Nunca falta el tonto que pregunta por que ingreso a su PC un virus, si tiene instalado un buen antivirus... Yo les pregunto, ¿si hubiera un solo antivirus que funciona 100% perfecto, usted compraría a otra empresa?, la obvia respuesta es no... nadie en su sano juicio pagaría por algo que no es bueno, de alli la competencia entre las compañías.

Otro si digo... la mayoria de los que se quejan tienen antivirus pirata... de Ripley!

### **2.- Un antipestes**

Muchas veces instalamos un antivirus y damos por sentado que la maquina esta protegida, pero existen programas que sin caer en la categoría de virus pueden causarnos molestias y/o perdida de información, a estos agentes se les conoce como "Pestes".

En esta categoría caen:

**Spyware.-** Son programas que pueden recabar información de nuestros hábitos de navegación para elaborar complejas estadísticas de consumo y perfiles de nuestras preferencias. Las razones suelen ser comerciales.

**Keyloggers.-** Son programas que monitorean lo que ingresamos por nuestro teclado para ver con quien nos comunicamos, que decimos, robar contraseñas, etc.

**AddWares.-** Son programas que nos muestran propaganda, vale decir hacen dinero a costa de nosotros.

**Spam.-** Es el llamado “correo basura” mayormente se dedica al envío de publicidad.

Aunque la mayoría de antivirus modernos ya incorpora el antipestes.

También debemos usar el HiJack, el CWS shredder.exe que nos permite eliminar el CoolWebSearch, el programa Spybot Search & Destroy y el programa EliStarA.exe.

### **3.- Usar cortafuegos y bloqueadores de puertos.**

La tercera línea defensiva de un ordenador es el cortafuegos o firewall. Muchos aún no entienden el concepto en el que se basan estos programas.

Cuando un ordenador accede a Internet se comunica mediante unos puertos de conexión. Existen 65.535 canales (independientemente de los protocolos que aceptan) por donde los datos pueden salir o entrar en nuestro ordenador.

Alguien puede intentar una intrusión por cualquiera de esos puertos. Windows abre por defecto varios puertos que dejan nuestros ordenadores muy vulnerables.

Se recomienda utilizar el ZoneAlarm, el pblocki.exe de la casa analogX y los productos de McAfee

También es bueno señalar que es conveniente utilizar un scaneador de puertos.

### **4.- Un programa para eliminar huellas en Internet**

Debemos ocultar nuestro IP, lugares visitados, nuestro correo electrónico, limpiar los cookies.

Es conveniente utilizar un proxy y usar un programa como el Anonymizer (<http://www.anonymizer.com/>).

### **5.- Un programa de encriptación segura:**

Que sucedería si enviáramos cartas sin el sobre cerrado.... que mucha gente podría leerlas.

Es recomendable utilizar programas de cifrado o utilizar estenografía, dependiendo del grado de seguridad que desee brindar a su comunicación, en mi sitio web hay varias herramientas de ese tipo.

#### **6.- Un programa para realmente borrar y/o proteger los archivos.**

Muchos borramos un archivo y pensamos que ya nadie puede leerlo, otros “mas vivos”, saben que el archivo aun esta en la papelera de reciclaje y lo elimina de allí, ahora si que esta seguro... FALSO!

Los archivos aun están allí, hay diversos programas que permiten la recuperación de datos, así que es recomendable utilizar un programa llamado “Shredder” sobre todo si sobrepasa los estándares del DOD de USA.

No debemos confiarnos en la falsa seguridad que nos brinda programas como los de Microsoft cuyas claves pueden ser eliminadas con seguridad.

#### **7.- Tener a mano un programa para recuperar información.**

Aún con las precauciones expuestas líneas arriba, podemos ser víctimas de un peligroso virus que nos borre documentos vitales de nuestro ordenador.

Podemos citar pro ejemplo FileRestore, Magic Recovery, Ontrack EasyRecovery y Lost and Found

#### **8.- Capacitar a los usuarios acerca de la necesidad del uso de estos programas.**

Como señalaba al principio, de nada nos vale tener todos los programas señalados si estos están desactualizados o no son utilizados, tan importante como tener los programas, es saber su utilización y tener conciencia de la necesidad de proteger nuestra información.

La primera línea de defensa somos nosotros mismos y nuestro sentido común.