Métodos de protección contra virus.

- **Antivirus**: los llamados programas antivirus tratan de descubrir las trazas que ha dejado un software malicioso, para detectarlo y eliminarlo, y en algunos casos contener o parar la contaminación. Tratan de tener controlado el sistema mientras funciona parando las vías conocidas de infección y notificando al usuario de posibles incidencias de seguridad. **ES VITAL MANTENER EL ANTIVIRUS ACTUALIZADO Y ANALIZAR EL EQUIPO PERIODICAMENTE**.

- **Filtros de ficheros**: consiste en generar filtros de ficheros dañinos si el ordenador está conectado a una red. Estos filtros pueden usarse, por ejemplo, en el sistema de correos o usando técnicas de **firewall.** En general, este sistema proporciona una seguridad donde no se requiere la intervención del usuario, puede ser muy eficaz, y permitir emplear únicamente recursos de forma más selectiva. **EL FIREWALL DE WINDOWS DEBE ESTAR ACTIVADO.**
- **Copias de seguridad**: Mantener una política de copias de seguridad garantiza la **recuperación de los datos** y una solución **cuando nada de lo anterior ha funcionado**.

- **Estudiar**: Aprender cómo es el software de nuestra computadora, buscando y buscando información, en sitios en los que se pueda confiar, sobre software dañino, para así evitarlo.
- **Desconfiar**: Si no conocemos algo o no sabemos lo que hace, será mejor tenerle respeto y no tocarlo hasta aclarar nuestra duda, (en el uso de esta regla es recomendable **no abrir archivos de correos de los que se desconoce el remitente, o se sospecha de que pueda contener código malicioso, o que no pidió usted. Aun así, si es de entera confianza, analice siempre con un antivirus el archivo antes de abrirlo**). Es aconsejable complementar esta manera de proceder aplicando una **política de contraseñas y de seguridad más seguras** a su red local o a los parámetros de acceso a Internet. Lo que muchos creadores de virus desean es la sensación de vulnerabilidad al provocar las condiciones de contagio idóneas que permitan una infección del virus a nivel mundial y causar daños sin dejar rastro de su presencia. En algunos casos los virus de correo pueden ser predichos debido al asunto del mensaje, por ejemplo la mayoría de estos virus se predicen a partir de asuntos perfectamente escritos o en otros idiomas. **NO UTILICE LA OPCIÓN DE RECORDAR CONTRASEÑAS EN SU NAVEGADOR**

- **Hacer reenvíos seguros de email**: Cuando recibamos un mensaje de correo electrónico sospechoso de contener virus o que hable de algo que desconocemos conviene consultar su posible infección o veracidad (por ejemplo a partir de buscadores de la www). Sólo si estamos seguros de la ausencia de virus del mensaje o de que lo que dice es cierto e importante, de ser conocido por nuestros contactos, lo reenviaremos, teniendo cuidado de poner las direcciones de correo electrónico de los destinatarios en la casilla CCO. Así evitaremos la propagación de mensajes con virus, así como la del spam y la de aquellos mensajes con phishing u hoax. **Lea el siguiente documento antes de acceder, o a la hora de configurar su correo.**

- **Informar a nuestros contactos**: Conviene que hagamos saber lo mencionado en el punto anterior a nuestros contactos en cuanto nos reenvían mensajes con virus o contenido falso o sin utilizar la casilla CCO.

- **Limpiar y eliminar el virus**: En el caso de que nuestra máquina resulte infectada debemos proceder **a su desconexión inmediata de la red, ya sea local o Internet** (esto se hace para evitar contagios a otras máquinas) y, **una vez aislada, aplicar un programa Antivirus actualizado para tomar la acción que se corresponda.**

(Extraído de http://es.wikipedia.com) **Más información en: http://alerta-antivirus.red.es/**