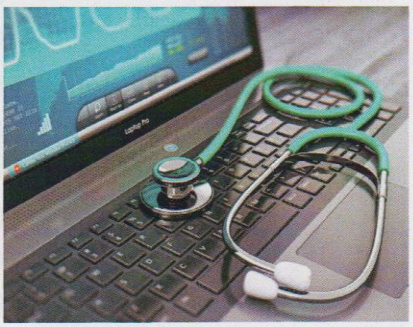
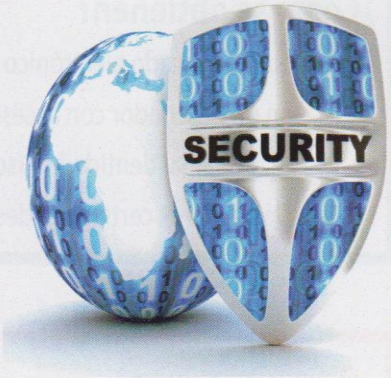
4. Seguridad activa



La seguridad activa consiste en identificar qué partes del sistema son vulnerables y establecer medidas que minimicen el riesgo. Mantener al día la seguridad de nuestro equipo es una labor fundamental para evitar ataques al mismo y pérdidas de información.

El software y los elementos de prevención del equipo son:

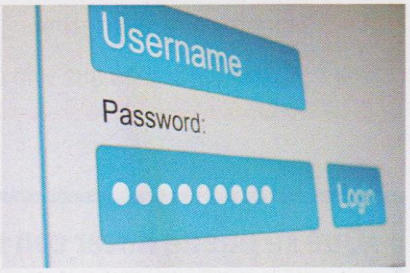
- **Antivirus**. Un antivirus es un **programa** que analiza las distintas unidades y dispositivos, así como el flujo de datos entrantes y salientes, revisando el código de los archivos y buscando fragmentos de caracteres. Utiliza una base de datos con cadenas de caracteres características de distintos virus. El antivirus puede detectar virus y sólo a veces identificarlos. Aunque la creación de virus es rápida y siempre va a ir por delante de la protección de los fabricantes de antivirus, podemos estar tranquilos si tenemos uno instalado y actualizado. En realidad, los antivirus protegen contra virus, troyanos y gusanos, y la mayor parte contienen también antispyware e incluso filtros antispam.
- **Cortafuegos** o **firewall**. Se trata de un sistema de defensa que **controla y filtra el tráfico** de entrada y salida a una red. El cortafuegos se configura para que controle el tráfico de los puertos (las conexiones de nuestro ordenador se hacen a través de ellos) y nos muestre alertas para pedir confirmación de cualquier programa que utilice la conexión a Internet. Por ello, es muy importante realizar esta configuración con criterio. Normalmente están incorporados en los sistemas operativos y existen además otros de software libre o de pago.



- **Proxy**. Es un **software** instalado en el PC que funciona como puerta de entrada; se puede configurar como cortafuegos o como limitador de páginas web.
- **Contraseñas**. Pueden ayudar a proteger la seguridad en un archivo, una carpeta o un ordenador dentro de una red local o en Internet. Se recomienda que tengan entre seis y ocho caracteres para que no se puedan vulnerar fácilmente, aunque el nivel de seguridad será distinto en nuestra clave de usuario del ordenador que en un router Wi-Fi, por ejemplo.

Consejos para crear una contraseña segura

- Alternar mayúsculas y minúsculas
- Utilizar números y caracteres no alfabéticos
- Que se pueda teclear rápidamente
- Que no esté contenida en un diccionario
- Que no se relacione con datos personales (DNI, apellido, etc.)



- **Criptografía**. Es el cifrado de información para proteger archivos, comunicaciones y claves. La necesidad de proteger mensajes ha existido desde la antigüedad. Al haber cada vez más posibilidades de almacenamiento de información y más medios y dispositivos de comunicación, se hace más necesaria la criptografía.

5. Seguridad pasiva

La **seguridad pasiva** consiste en minimizar el impacto de un posible daño informático, asumiendo que, por mucho que pongamos en funcionamiento la seguridad activa, cualquier sistema es vulnerable. En este caso, se trata de disminuir las consecuencias de ataques, pérdidas de información involuntarias, accidentes, descuidos, etc.

Los principales mecanismos de actuación pasivos son:

- **Sistemas de alimentación ininterrumpida (SAI)**. El ordenador toma la corriente eléctrica de estos dispositivos en lugar de conectarse a la red directamente. Protegen a los equipos frente a apagones y también frente a picos o caídas de tensión que podrían estropear el sistema. Cuando se produce un corte de suministro eléctrico, el SAI proporciona el tiempo suficiente al usuario para guardar la información que esté generando o utilizando y apagar correctamente el equipo.

SAI.

- **Dispositivos NAS** (*network area storage*, sistemas de almacenamiento en red). Son dispositivos de almacenamiento específicos a los que se accede a través de una red, por lo que suelen ir conectados a un router. Permiten sistemas de almacenamiento **en espejo**, es decir, con dos discos duros que se copian de forma automática, lo que facilita la recuperación de la información en caso de rotura de uno de los discos.

NAS.

- **Política de copias de seguridad** (o **backups**). Permiten restaurar sistemas o datos si es necesario. Es importante planificar en qué soporte se realizan, con qué periodicidad y de qué elementos del sistema. Por ejemplo, en el sistema operativo Windows se llama **copia de seguridad completa** a la que se realiza con aplicaciones y datos, y **copia de archivos** a aquella en que sólo se copian datos.

Recomendaciones de Microsoft para las copias de seguridad

- No haga la copia de seguridad de sus archivos en el mismo disco duro en el que está instalado Windows.
- Almacene siempre los medios usados para las copias de seguridad (discos duros externos, DVDs o CDs) en un lugar seguro para impedir el acceso de usuarios no autorizados a los archivos; recomendamos usar una ubicación ignífuga independiente del equipo. También dispone de la opción de cifrar los datos de la copia de seguridad.

A veces es difícil distinguir si nuestro ordenador está siendo atacado o bien está funcionando mal por otros motivos. A continuación se recogen los síntomas que nos pueden indicar si está sufriendo algún ataque, así como una serie de pautas para prevenirlo.

¿Cómo saber si nuestro PC ha sido atacado?

Los síntomas de que nuestro nuestro PC ha sido atacado pueden ser:

1. El ordenador trabaja con una ralentización exagerada de los procesos o la conexión a la Red.
2. Disminuye el espacio disponible en el disco (salen avisos de que no hay espacio suficiente).
3. Aparecen programas desconocidos, se abren páginas de inicio nuevas en el navegador o se añaden elementos que no se pueden eliminar.
4. Aparecen iconos desconocidos en el escritorio (a veces no se pueden eliminar).
5. El teclado y/o el ratón hacen cosas extrañas.

Seguridad activa y pasiva

Como en tantos otros aspectos de la vida, la mayor seguridad es la **prevención**. Unas sencillas medidas de prevención serán suficientes para utilizar con seguridad nuestro equipo de uso educativo o doméstico, eso sí, teniendo en cuenta que no existe la seguridad absoluta. Es aconsejable:

1. Realizar periódicamente **copias de seguridad** (o **backups**) del sistema que permitan restaurarlo si es necesario.
2. Utilizar **contraseñas seguras** en todos los dispositivos y aplicaciones.
3. Usar solamente **redes Wi-Fi abiertas** que sean de confianza para intercambiar datos privados.
4. Tener instalado y actualizado un programa **antivirus** (y conocer sus **funciones y limitaciones**).
5. Tener actualizado el **sistema operativo**.
6. Revisar sistemáticamente los **dispositivos** introducidos en el equipo.
7. Llevar cuidado con las **descargas de archivos** con programas del tipo P2P o *peer to peer* (eMule, Ares, BitTorrent, etc.), que son una vía de entrada de archivos desconocidos que pueden contener virus.
8. Tener cuidado a la hora de configurar el **cortafuegos** para permitir la comunicación de estos programas.
9. Prestar atención a las **descargas gratuitas** de programas.