# Seguridad Informática

**Autor:** García Aparici, José Luis (Licenciado en Ciencias Físicas, Profesor de Informática en Educación Secundaria).
**Público:** 4º ESO. **Materia:** Tecnologías de la Información y Comunicación. **Idioma:** Español.

**Título:** Seguridad Informática.
**Resumen**
En todo sistema informático es necesario contemplar medidas de seguridad que protejan tanto su hardware como el software y la información que éste contiene. Deben tomarse medidas para impedir que tengan lugar riesgos informáticos y para recuperar el sistema si éste ha sufrido algún percance. Los usuarios deberán conocer el software necesario para proteger los equipos informáticos, los peligros de seguridad en Internet, cómo hacer compras con seguridad y manejarse con seguridad en una conexión WIFI.
**Palabras clave:** Seguridad, medidas de seguridad, riesgo informático.

**Title:** Computer security.
**Abstract**
In any computer system it is necessary to take security measures that protect its hardware and software and the information it contains. Measures should be taken to prevent computer risks from occurring and to recover the system if it has suffered an incident. Users should be aware of the software needed to protect computer equipment, security dangers on the Internet, how to shop safely and manage safely on a WIFI connection.
**Keywords:** Security, security measures, computer risk.

Recibido 2017-07-13; Aceptado 2017-07-25; Publicado 2017-08-25; Código PD: 086030

## 1. SEGURIDAD INFORMÁTICA ACTIVA Y PASIVA.

En todo sistema informático es necesario contemplar medidas de seguridad que protejan tanto su parte hardware como el software y la información que éste contiene. Hay dos tipos de seguridad informática: activa y pasiva.

### Seguridad Activa

Forman parte de la seguridad activa las medidas para **evitar o reducir los riesgos que amenazan al sistema informático.**

Ejemplos de seguridad activa serían:

- Introducción de nombres de usuario y con contraseña para acceder al sistema.
- Instalar un antivirus para evitar que un virus entre en el sistema.

### Seguridad Pasiva

Son las medidas encaminadas a **minimizar los efectos en el sistema una vez que ya se ha producido un incidente de seguridad y facilitar la recuperación del mismo.** Ejemplo: instalación de un SAI que suministre energía eléctrica al sistema en el caso de que haya un corte de luz.

## 2. SEGURIDAD ACTIVA

Vamos a profundizar en algunas medidas que forman parte de la seguridad activa.

### El uso de contraseñas robustas

Una contraseña robusta es aquella que es **difícil de de averiguar**. Una contraseña robusta:

- no debería ser una palabra del diccionario
- tendría que tener mezclados números, letras y símbolos
- debería mezclas letras mayúsculas con minúsculas
- no debería tener pocos caracteres. Se recomienda que al menos tengan 8 caracteres, aunque cuanto más larga mejor.

**Encriptación**

Se trata de usar las técnicas de encriptación para transformar mediante algoritmos la información en una estructura que resulta incompresible. Para ello la información se encripta de tal manera que sólo el usuario destinatario puede leerlo, ya que sólo él es capaz de descifrarlo.

El protocolo HTTPS que usa para conectar desde un navegador con páginas web aporta seguridad a la conexión ya que toda la información que viaja entre el navegador del usuario y el servidor va encriptada.

**Software de seguridad activa**

Hay diferentes programas que ayudan a mantener la seguridad informática activamente. Destacamos:

- **Los antivirus**: son programas cuyo objetivo principal es detectar y eliminar virus informáticos.
- **Software antispyware**: son programas cuyo objetivo es eliminar software espía (es un tipo de software que recopila información del sistema y la transmite sin que los usuarios del sistema lo perciban).
- **Cortafuegos (firewalls):** son programas diseñados para bloquear el acceso no autorizado a través de la red al sistema informático, permitiendo solo las comunicaciones autorizadas. Su misión es filtrar el tráfico de red que puede entrar o salir del equipo o sistema informático. Actualmente los sistemas con Windows llevan su propio cortafuegos.

**3. SEGURIDAD PASIVA**

Vamos a repasar las medidas principales que forman parte de la seguridad pasiva.

**Dispositivos físicos de protección**

Se trata de usar el hardware indicado para hacer frente a accidentes y averías.

Ejemplos:

- Uso de sistemas de refrigeración para que no se sobrecaliente
- Conexión de dispositivos SAI que protejan al sistema frente apagones eléctricos.

**Copias de seguridad**

Una copia de seguridad es una copia de los datos originales fuera de la infraestructura que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida. La copia de seguridad se guarda en dispositivos externos al sistema tales como discos duros externos, DVDs o espacios virtuales en Internet.

Para hacer la copia el administrador debe **configurarla.** Es decir, indicar al Sistema Operativo **dónde** lo queremos copiar, **qué** queremos copiar y con qué **periodicidad** se quiere realizar.

**Restaurar** una copia de seguridad significa volver a recuperar los archivos copiados tal y como eran y en la localización original que tenían en el sistema.

**Particiones del disco duro.**

Los discos duros son dispositivos de almacenamiento de información de gran capacidad. Es fácil encontrar actualmente equipos informáticos con discos duros de 1 TB o más. Los discos duros pueden ser divididos en lo que se llama **particiones** con el objeto de **separar el Sistema Operativo de los datos** (el sistema operativo en una partición y los datos en otra).

Es una buena práctica informática dividir el disco duro de nuestro equipo en dos particiones: en una tendremos instalado el Sistema Operativo y en otra guardaremos los datos. De esta manera, si debemos reinstalar el Sistema Operativo, los datos no se verán afectados.

## 4. RIESGOS EN EL USO DE EQUIPOS INFORMÁTICOS.

El riesgo de un equipo informático es la posibilidad de que ocurra algo dañino para el equipo aprovechando una debilidad del sistema. Para minimizar los riesgos deben aplicarse **medidas de seguridad.**

Ejemplos de riesgos son:

- Que los usuarios tengan excesivos privilegios como los del administrador.
- Que se extraiga información del sistema sin permiso.
- Recibir correo spam.
- Que el equipo se infecte con algún virus informático.
- Que se sufran ataques informáticos por la red para anular los servicios de un servidor.

## 5. LOS VIRUS (EL MALWARE)

Un virus es un software que tiene por objetivo alterar el funcionamiento normal del ordenador, sin el permiso o el conocimiento del usuario.

Existen dos grandes clases de propagación de los virus. En la primera, el usuario, en un momento dado, ejecuta o acepta de forma inadvertida la instalación del virus. En la segunda, el programa malicioso actúa replicándose a través de las redes, por ejemplo a través de una carpeta compartida en la red. En este caso se habla de gusanos.

Entre los **programas con códigos malignos** se incluyen:

- **Troyano**: es un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado.
- **Spyware**: es un malware que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador.
- **Gusano**: es un malware que tiene la propiedad de duplicarse a sí mismo, siendo su medio de propagación la red.
- **Hoax**: Son mensajes de contenido falso que animan al usuario a hacer copias y enviarla a sus contactos.
- **Adware:** software que muestra publicidad mientras se está utilizando una aplicación sin que el usuario haya consentido en la instalación de dicha publicidad.

## 6. SOFTWARE DE PROTECCIÓN DE EQUIPOS INFORMÁTICOS.

Los programas fundamentales que debe tener cualquier equipo informático conectado a la red son el antivirus y el cortafuegos.

**El programa antivirus** es un programa cuyo objetivo es detectar o eliminar virus informáticos. Para ello debe actualizarse constantemente, proteger el equipo en tiempo real y ser capaz de eliminar los virus detectados.

Un **cortafuegos** (***firewall***) es una parte de un sistema o una red que está diseñada para **bloquear el acceso por la red no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas**. Por ejemplo, se puede impedir que un determinado programa tenga acceso a Internet o que no se pueda acceder por la red a un equipo.

Por ejemplo, en un sistema con Windows , cuando instalamos un programa nuevo que utiliza funciones de red, el firewall nos preguntará si queremos que tenga acceso a la red.

**7. SEGURIDAD EN INTERNET.**

En informática, la **Ingeniería social** es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Por ejemplo, crear sitios web falsos para obtener información de los usuarios de un sitio web de confianza. Esta técnica de imitar la imagen corporativa de una entidad para estafar a sus usuarios recibe el nombre de **phising**.

El **spam o correo basura** es el envío en grandes cantidades de mensajes de correo electrónico que no ha sido solicitado por los remitentes con fin de sacar algún beneficio de los receptores de los correos. Por ejemplo, ofrecen productos estupendos a precios muy bajos. A pesar de que hay leyes, como la **ley LSSI** (Ley de Servicios de la Sociedad de la Información) en España que prohíben el spam, su difusión está muy extendida. Se ha llegado a calcular que el 80% de los correos que circulan en Internet son correo basura.

**8. SEGURIDAD DE LOS USUARIOS EN LAS COMPRAS EN INTERNET**

Internet también ofrece muchas posibilidades para realizar compras. Normalmente se necesita disponer de una **tarjeta de crédito** y además **c**onviene tomar algunas **precauciones:**

- Comprobar que se utiliza el protocolo de seguridad HTTPS en el navegador
- Comprobar que la empresa disponga de un **certificado digital**. Esto se pude ver haciendo doble clic en un pequeño icono, con **forma de candado,** que aparece al visualizar la página en el navegador.


**9. CONEXIÓN DE FORMA SEGURA A REDES WIFI.**

Debe tomarse una serie de precauciones de seguridad cuando se instala una red WIFI. Vamos a ver las más importantes.

**Medidas de Seguridad en redes WIFI**

**1) Cambiar los datos de acceso al router WIFI:** Los routers WIFI que se reciben cuando se contrata Internet con algún proveedor, suelen tener una **contraseña por defecto** para acceder a la administración y configuración del dispositivo. Esta contraseña **debe cambiarse cuanto antes por otra.**

**2) Ocultar el nombre (SSID) de la red WIFI**: Cuando alguien intenta conectarse a una red, **aparecerán todas las que se encuentran a su alrededor**. Para evitar esto al configurar el nombre de nuestra red inalámbrica en el router WIFI lo haremos **de forma que no se difunda el nombre de la red**. De esta manera si alguien quiere conectarse a ella, solo podrá hacerlo si previamente conoce el nombre de la red.

**3) Usar protocolos de seguridad y cambiar contraseña de acceso a la red:** Mediante protocolos de seguridad que permiten el **cifrado en función de una contraseña** conseguiremos proteger tanto el acceso a la red, como las comunicaciones entre dispositivos. El protocolo más seguro es el **WPA2**. Además, conviene cambiar la contraseña de acceso a la red WIFI que suele venir impresa en el exterior del router WIFI.

**Bibliografía**


- https://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica
- https://es.wikipedia.org/wiki/Cifrado_(criptograf%C3%ADa)
- https://es.wikipedia.org/wiki/Programa_esp%C3%ADa
- https://es.wikipedia.org/wiki/Sistema_de_alimentaci%C3%B3n_ininterrumpida
- https://es.wikipedia.org/wiki/Copia_de_seguridad
- https://es.wikipedia.org/wiki/An%C3%A1lisis_de_riesgo_inform%C3%A1tico
- https://es.wikipedia.org/wiki/Virus_inform%C3%A1tico
- https://es.wikipedia.org/wiki/Antivirus
- https://es.wikipedia.org/wiki/Ingenier%C3%ADa_social_(seguridad_inform%C3%A1tica)
- https://es.wikipedia.org/wiki/Seguridad_en_Internet
- https://es.wikipedia.org/wiki/Spam
- https://es.wikipedia.org/wiki/Troyano_(inform%C3%A1tica)
- https://es.wikipedia.org/wiki/Programa_esp%C3%ADa
- https://es.wikipedia.org/wiki/Gusano_inform%C3%A1tico
- https://es.wikipedia.org/wiki/Bulo
- https://es.wikipedia.org/wiki/Adware