SEGURIDAD EN INFORMÁTICA

LA SEGURIDAD Y SUS IMPLICACIONES

Características principales de la seguridad en Internet:

• **Confidencialidad.** Sólo deben tener acceso a aquellas personas autorizadas para ello.
• **Autentificación y gestión de claves.** Se ha de confirmar que tanto el origen como el destino son verdaderamente quienes dicen ser.
• **Autorización.** El acceso a los diferentes servicios debe estar condicionado por la identidad del usuario.
• **Integridad.** Los datos enviados deben ser los mismos que los recibidos, evitando la manipulación o corrupción de los mismos durante el camino.
• **Imposibilidad de repudio.** El emisor no puede negar haber enviado un mensaje.

CLASIFICACIÓN DE LA SEGURIDAD

• **Seguridad física.** Se entiende como el conjunto de medidas y protocolos para controlar el acceso físico a un elemento. A nivel general lo forman las puertas, cerraduras, rejas y paredes. En el caso concreto aplicado a la seguridad informática lo constituyen las medidas para evitar que personas no autorizadas puedan alcanzar un terminal o dispositivo concreto.

• **Seguridad lógica.** Son los diferentes protocolos, algoritmos y programas que pueden manipular directamente la información controlando el acceso a la misma desde terceras partes. Las contraseñas, cifrados y códigos son parte de la seguridad lógica.

• **Seguridad programable.** Son los diferentes programas antivirus, Proxy, cortafuegos que podemos tener para evitar la entrada de virus en nuestro equipo. También se consideran los diferentes usuarios de un mismo ordenador, o las categorías de los mismos.

• **Seguridad humana.** Es la que reside en el propio usuario que maneja la información. Es la responsabilidad que éste toma sobre la información y las medidas y protocolos de conducta que lleva a cabo para gestionarla adecuadamente. La elección de contraseñas seguras, no divulgación de claves y el uso de herramientas de seguridad son seguridad humana.

SEGURIDAD LÓGICA.

Protección de datos: la criptografía

El cifrado de mensajes es sin duda uno de los sistemas más antiguos para proteger las comunicaciones. Diferentes sistemas de codificación han ido evolucionando a lo largo de la historia, pero ha sido con la aplicación de máquinas y ordenadores a la criptografía cuando los algoritmos han conseguido verdadera complejidad. Este cifrado es transparente al usuario, que no participa en el proceso.

Protección de datos: Funciones hash

Son funciones, llamadas de **reducción criptográfica,** que tienen carácter irreversible.

Estas funciones operan sobre los datos obteniendo de ellos una clave que los representa de manera casi unívoca.

Protección de datos. La esteganografía

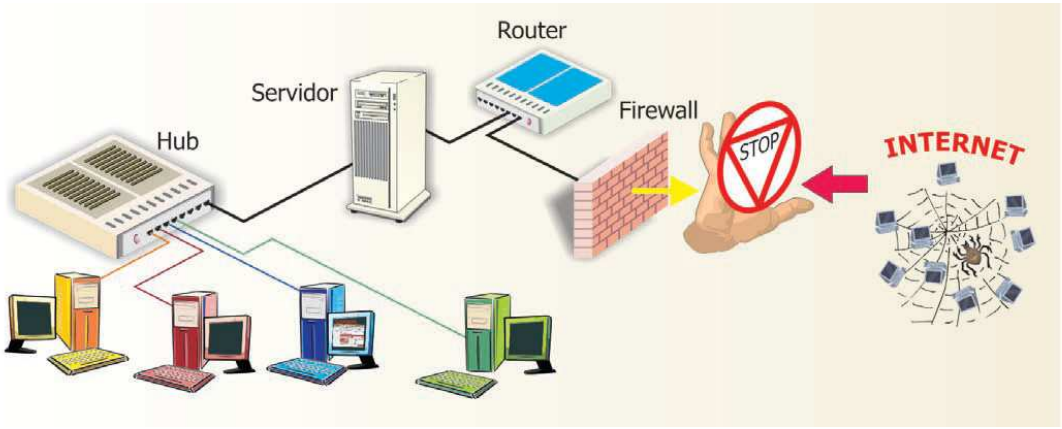
Es un conjunto de métodos y técnicas para ocultar mensajes u objetos dentro de otros, de modo que no se perciba la existencia de los primeros. Un mensaje oculto formado por la primera letra de cada frase de un texto es una forma de esteganografía.

Existen programas capaces de introducir datos en imágenes o archivos de música aprovechando las limitaciones de los sentidos humanos, bien en forma de frecuencias inaudibles en un archivo de audio o pequeñas «imperfecciones» en una imagen.

SEGURIDAD PROGRAMABLE.

Protección de las comunicaciones. Los cortafuegos

Un **cortafuegos** o **firewall** es un elemento encargado de controlar y filtrar las conexiones a red de una máquina o conjunto de máquinas. Se trata de un mecanismo básico de prevención contra amenazas de intrusión externa. Supone la barrera de protección entre un equipo o red privada y el mundo exterior. Controla el acceso de entrada y salida al exterior, filtra las comunicaciones, registra los eventos y genera alarmas.



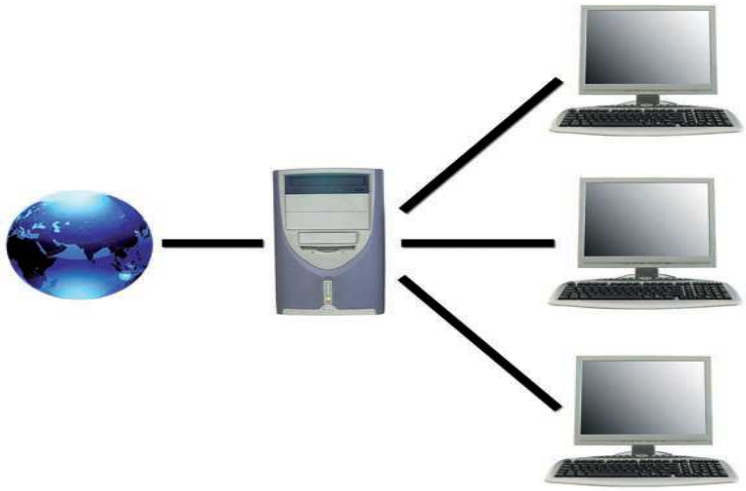
Protección de las comunicaciones. Los servidores proxy

Un Proxy es un ordenador que hace de intermediario entre un cliente y un destino. Cuando un cliente desea una información, conecta con el servidor Proxy en lugar de hacerlo con el servidor de destino.

El servidor proxy contacta con el servidor de destino como si fuese el propio cliente y, una vez obtenida la información, se la envía al ordenador que inició la petición.

En una red local, un servidor proxy puede dar este servicio a todos los ordenadores, de forma que las comunicaciones no se realizan con el exterior, sino únicamente con el servidor proxy.

Por otro lado, este servidor es el único que accede e intercambia datos con la red externa.



Protección de las comunicaciones. Seguridad de la red Wi-Fi

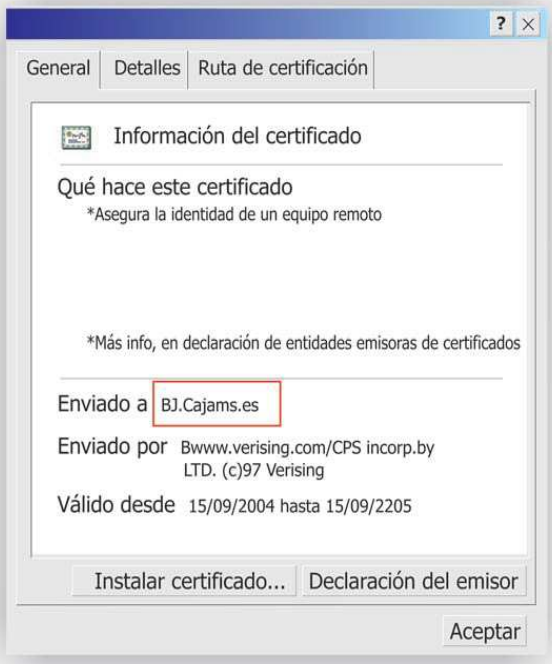
Cuando la información viaja por ondas de radio, éstas son accesibles para cualquier receptor que se encuentre dentro del área que abarcan, esté autorizado o no.
Con la proliferación de este tipo de redes es bastante frecuente encontrar que un mismo terminal recibe señales de diversas redes colindantes. Es importante entonces proteger las comunicaciones Wi-Fi de posibles intrusos.
Existe un doble motivo para ello. En primer lugar, para asegurar la **confidencialidad de las comunicaciones** de una red. En segundo, para evitar que un **intruso pueda** utilizar la red para llevar a cabo acciones ilegales que acabarán siendo imputadas al dueño de la misma.

Navegación segura. Protocolo https

Este protocolo de comunicación Web cifrado es una versión segura del protocolo **http** de Web, y es común en las comunicaciones con entidades bancarias, tiendas en línea y servicios privados. Cuando se accede a una página que requiere este protocolo, el navegador del cliente y el servidor se ponen de acuerdo en realizar una comunicación cifrada. Es frecuente que algunos navegadores indiquen el acceso a este servicio utilizando un icono en forma de candado.
La navegación por estas páginas está garantizada, tanto a nivel de ausencia de virus, como a nivel de cualquier otro tipo de malware.

Navegación segura. Protocolo certificado digital.

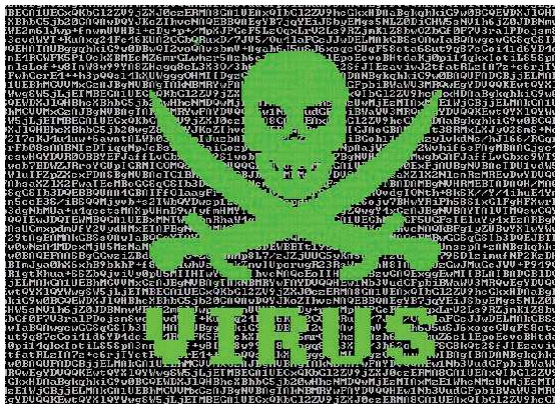
Se trata de un documento digital mediante el cual una autoridad de certificación garantiza la autenticidad de una entidad y su vinculación con su clave pública. De ese modo, un certificado digital asegura que la entidad a la que el usuario se conecta es quien dice ser, es auténtica, y ofrece una clave con la que iniciar una comunicación cifrada segura. Un ejemplo de ello es el DNI electrónico, que actúa como un certificado de nuestra identidad.
Es habitual que el uso del certificado digital se encuentre vinculado al del protocolo **https.**



SEGURIDAD PROGRAMABLE.

Definición de malware.

Malware (software malicioso).
Se denomina malware al programa cuya finalidad es infiltrarse o dañar un ordenador sin el conocimiento del dueño. Son programas «disfrazados» con el objetivo de engañar al usuario. Los virus informáticos son el tipo más común de malware, por lo que es habitual ese nombre para denominar a todos los tipos de programas hostiles.



Clasificación de los virus o malware.

1. Virus
Son **programas** de tamaño muy reducido, que pasan desapercibidos, y su función es la de reproducirse.

Suelen ir ocultos dentro de otro programa, llamado **programa infectado** y, una vez que se ejecuta el programa infectado, el virus pasa a la memoria y se queda en ella residente hasta que se apague el ordenador. Una vez en memoria, sus primeras acciones suelen ser implantarse en el sistema, infectando programas que se ejecutan al arrancar el ordenador para que, de este modo, pueda estar siempre presente. Una vez implantado en el sistema trata de propagarse, generalmente infectando a otros programas y confiando en que éstos puedan ser copiados y ejecutados en más ordenadores.

2. Gusanos

Su comportamiento es muy similar al de un **virus,** pero no se reproduce infectando a otros programas. Su método de **expandirse** es utilizar la red para enviarse a otros ordenadores, generalmente usando el correo electrónico y autoenviándose a los integrantes de la agenda de contactos del usuario. Se extienden con gran velocidad, hasta el punto de llegar a saturar las redes en poco tiempo.

3. Troyanos

Son programas que disfrazan y esconden una función no deseada en un programa aparentemente inofensivo.

- **Puertas traseras o backdoors.** Modifican el sistema para permitir una puerta oculta de acceso al mismo.
- **Keyloggers.** Almacenan, de forma que no pueda advertirlo el usuario, todas las pulsaciones de teclado que éste efectúa. Por tanto, registran nuestras contraseñas.
- **Software espía o spyware.** Una vez instalado, envía al exterior información proveniente del ordenador del usuario de forma automática. Registra las páginas Web que visitamos y en lo que estamos interesados. Suelen venir incrustados en archivos o canciones “gratuitas” o en programillas que descargan juegos o demos gratis.
- **Adware.** Son programas de publicidad que muestran anuncios, generalmente mediante ventanas emergentes o páginas del navegador. Suelen ir conectados a un Spyware y nos mandan información justo de cosas en las que hemos investigado recientemente.

Sistemas de protección contra virus y troyanos

Antivirus

Son programas diseñados para detectar y eliminar el software dañino. Tienen dos mecanismos básicos de detección de amenazas:

1.º Comparación, buscando entre los programas el patrón de código que coincida con los almacenados en una biblioteca de patrones de virus conocidos.

2.º Detección de programas hostiles basados en su comportamiento. El antivirus conoce una serie de comportamientos sospechosos y estudia a los programas que, por su código, estén preparados para llevarlos a cabo.

Antispyware

Son programas específicos para detectar el spyware, que complementan la actividad del antivirus.

SEGURIDAD HUMANA: SENTIDO COMÚN.
El usuario es a veces el eslabón más débil

• **Una contraseña segura**. No compartirla ni escribirla al lado del nombre de la cuenta de correo. Utilizar una mezcla de números y letras.

• **No dejar pistas.** Cerrar siempre la sesión en ordenadores compartidos. No activar en nuestro explorador la opción “recordar contraseñas”, tener un correo para trabajar o/y para los amigos y otro para registrarse en páginas y no configurar nunca el Outlook con éste último.

• **Visitar páginas seguras o comprobadas.** Desconfiar de las páginas que nos den cosas gratis, especialmente si son cosas ilegales como música o libros. Si necesitamos un archivo, driver o programa, elegir la página del fabricante en lugar de otras que ofrecen lo mismo a cambio de nada.

• **Desinfectar los lápices USB y tener copias de seguridad.** Si utilizamos nuestro USB en varios equipos, es muy importante pasarle el antivirus a menudo, porque es un dispositivo muy sensible a los virus.
Por si acaso se infecta y hay que formatearlo, es conveniente tener copia de seguridad de su contenido. Si no podemos tenerla en otro ordenador, podemos enviarnos los archivos importantes por correo electrónico a nosotros mismos.

• **No dejarse engañar.** La mejor manera de protegerse de los programas hostiles es ser consciente de su existencia y hacer un uso de la red y del software que minimice el riesgo de que puedan entrar en el sistema. La prudencia es la principal herramienta y se ha de extremar la cautela a la hora de enfrentarse a un programa desconocido. No todos los programas que se reciben por correo o se descargan gratuitos de la red están limpios de amenazas. Es importante comprobar y pensar antes de ejecutar.