SEGURIDAD INFORMÁTICA.

1. **Concepto de Seguridad Informática. Principios de la Seguridad.**
2. **Seguridad Activa y Pasiva**
3. **Seguridad Física y Lógica. Medidas de seguridad lógica:**
    a. Control de Acceso
    b. Seguridad de contraseñas.
    c. Copias de seguridad, imágenes y restauración. Seguridad en redes inalámbricas.
    d. Criptografía. Firma digital y certificados digitales. Protocolos seguros.
    e. Cortafuegos.
    f. Servidor Proxy
4. **Amenazas y fraudes de los sistemas de información y a las personas**
    a. Software malicioso, herramientas antimalware y antivirus, protección y desinfección.
    b. Ingeniería Social: Phishing, Vishing, ...
5. **Legislación**
6. **Webs sobre seguridad**

1. CONCEPTO DE SEGURIDAD INFORMÁTICA. PRINCIPIOS DE SEGURIDAD.

La **seguridad informática** es el conjunto de medidas encaminadas a proteger el hardware, el software, la información y las personas. Se encarga de **proteger la integridad y la privacidad de la información** almacenada en un sistema **informático**.

La seguridad de la **información** es el **conjunto de medidas preventivas y reactivas** de las organizaciones y de los sistemas que permiten resguardar y proteger la **información** buscando mantener la confidencialidad, la **disponibilidad** e integridad de datos y de la misma.

La necesidad de seguridad es una constante que ha acompañado a la historia del ordenador. Es necesario asegurar tanto la máquina como la información que contiene, así como garantizar la seguridad de los usuarios ya que cualquier fallo en la seguridad puede tener consecuencias graves de tipo económico, social o personal.
La revolución de Internet y su continua evolución conllevan un cambio radical en la forma de entender los riesgos informáticos. La irrupción del **Big data** y el **Internet de las cosas** obligará a elaborar nuevas estrategias de seguridad.

La seguridad informática consiste en asegurar que los recursos de un sistema informático (datos, hardware y software) son bien utilizados y no pueden ser accedidos por personas no acreditadas.
Seguridad es un concepto asociado a la certeza, falta de riesgo o contingencia. No siendo posible la certeza absoluta, el elemento de riesgo está siempre presente, independientemente de las medidas que tomemos, por lo que debemos hablar de **niveles de seguridad**.
La seguridad absoluta no es posible, y en adelante entenderemos que la seguridad informática es un conjunto de técnicas encaminadas a obtener **altos niveles seguridad en los sistemas informáticos**.

Los principales **objetivos** de la seguridad informática son:

- **Detectar** los posibles **problemas y amenazas** a la seguridad, minimizando y gestionando los riesgos.
- Garantizar la adecuada utilización de los recursos y de las aplicaciones de los sistemas.
- Limitar las pérdidas y conseguir la adecuada recuperación del sistema en caso de un incidente de seguridad.
- Cumplir con el marco legal y con los requisitos impuestos a nivel organizativo.

Un **sistema seguro** consiste en garantizar los **principios de seguridad** informática son:

- **Confidencialidad:** garantizar que la información solamente será accesible al personal autorizado.
- **Integridad***:* propiedad que busca mantener los datos libres de actualizaciones no autorizadas.
- **Disponibilidad:** la información debe encontrarse accesible a quien debe acceder a ella.
- **Autenticación**: confirmación de la identidad de un usuario, comprobando que es quien dice ser.
- **No repudio:** permite comprobar la participación de las partes en una comunicación, de tal forma que ni el emisor ni el receptor puedan negar su participación en la comunicación.

ALTA DISPONIBILIDAD: se refiere a la capacidad de que aplicaciones y datos se encuentren operativos para los usuarios autorizados en todo momento y sin interrupciones, debido a su carácter crítico. El objetivo es mantener el sistema funcionando las 24 horas del día, 7 días a la semana, 365 días al año, manteniéndolo a salvo de interrupciones previstas (paralizamos el sistema para realizar cambios o mejoras) o imprevistas (apagón, error del hw/sw, problemas de seguridad, desastres naturales, virus , accidentes, caída involuntaria del sistema).

Las métricas para medir la disponibilidad y fiabilidad de un sistema son:

- El **tiempo medio entre fallos**, que mide el tiempo medio transcurrido hasta que un dispositivo falla.
- El **tiempo medio de recuperación**, que mide el tiempo medio tomado en restablecerse la situación normal una vez que se ha producido el fallo.

2. SEGURIDAD ACTIVA Y PASIVA.

La seguridad activa es el conjunto de acciones encaminadas a proteger el ordenador y su contenido (contraseñas seguras, antivirus actualizados…). Se trata de **reducir las vulnerabilidades** todo lo posible, prevenir ataques o errores, es **preventiva**.

Son medidas de Seguridad Activa:

- **Contraseñas seguras**
- **Analizar** con **Antivirus** el sistema periódicamente en busca de malware.
- **Criptografía**: encriptación de datos.
- **Cortafuegos** (firewall) y **Proxi**
- Hacer **imágenes de disco**
- Hacer **copias de seguridad** de los datos

La seguridad pasiva es la que intenta minimizar el impacto y los efectos causados por un posible daño, accidentes (hacer copias de seguridad de los datos, SAI frente a cortes de luz…). Es decir, se consideran **acciones posteriores a un ataque o incidente** (es **paliativa**). Comprende:

- Restauración de copias de seguridad.
- Restauración de Imágenes del sistema o disco
- Seguridad física y ambiental, como sistemas de alimentación ininterrumpida (SAI)
- Comprobar si el antivirus funciona correctamente cuando hay una infección por un virus

3. SEGURIDAD FÍSICA Y LÓGICA

3.1. SEGURIDAD FÍSICA

La **Seguridad Física** está enfocada a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el sistema.

Cuando hablamos de *seguridad física* nos referimos a todos aquellos mecanismos --generalmente de prevención y detección-- destinados a proteger físicamente cualquier recurso hardware del sistema (desde un simple teclado hasta una cinta de backup con toda la información que hay en el sistema, pasando por los servidores o la propia CPU de la máquina)

Las **principales amenazas** que se prevén son:

- **Desastres naturales, incendios** accidentales y cualquier variación producida por las condiciones ambientales. Inundaciones….
- Amenazas ocasionadas por el hombre: **robos o sabotajes.**
- Disturbios internos y externos deliberados.

Tener controlado el ambiente y acceso físico permite disminuir **siniestros** y tener los medios para luchar contra accidentes.

Los **mecanismos para asegurar la seguridad física** son**:**

- **Recinto cerrado: CPD (**Centro de Proceso de datos) con control de acceso físico, suelo y techo técnicos, refrigeración, sistemas antiincendios…
- **Control de acceso físico a personas:** (prevención y detección) puertas blindadas, **biometría**, verificación automática de firmas, detector de metales, laser detector, tarjetas de identificación, biometría, videocámaras, vigilante jurado…Políticas de control de acceso.
- **Medidas contra inundaciones**
- **Detector de incendios, extintores, regaderas, detector de humos…**
- **Videovigilancia y medidas antirrobo**
- **Controlar picos corriente y apagones: SAI**
- **Control de la temperatura: refrigeración**
- **Control de ruido eléctrico y campos eléctricos.**
- **Control de backups o copias de seguridad**
- **Protección del cableado**

BIOMETRÍA: estudio para el reconocimiento inequívoco de personas basado en uno o más rasgos físicos intrínsecos.

- **Reconocimiento de la Huella dactilar**
- **Métricas de la mano**
- **Reconocimiento del iris o de la Retina**
- **Reconocimiento de voz**
- **Reconocimiento de la forma de la Palma de la mano**
- **Reconocimiento Dinámica de Firma**
- **Reconocimiento de rostros**

Electricidad

Quizás los problemas derivados del entorno de trabajo más frecuentes son los relacionados con el sistema eléctrico que alimenta nuestros equipos; cortocircuitos, picos de tensión, cortes de flujo ... Para corregir los problemas con las subidas de tensión podremos instalar tomas de tierra o filtros reguladores de tensión.

Para los cortes podemos emplear ***Sistemas de Alimentación Ininterrumpida*** **(SAI)**, que además de proteger ante cortes mantienen el flujo de corriente constante, evitando las subidas y bajadas de tensión. Estos equipos disponen de baterías que permiten mantener varios minutos los aparatos conectados a ellos, permitiendo que los sistemas se apaguen de forma ordenada (generalmente disponen de algún mecanísmo para comunicarse con los servidores y avisarlos de que ha caído la línea o de que se ha restaurado después de una caida).

Por último indicar que además de los problemas del sistema eléctrico también debemos preocuparnos de **la corriente estática**, que puede dañar los equipos. Para evitar problemas se pueden emplear esprais antiestáticos o ionizadores y tener cuidado de no tocar componentes metálicos, evitar que el ambiente esté excesivamente seco, etc.

Protección del hardware

El *hardware* es frecuentemente el elemento más caro de todo sistema informático y por tanto las medidas encaminadas a asegurar su integridad son una parte importante de la seguridad física de cualquier organización.

Problemas a los que nos enfrentamos:

- Acceso físico
- Desastres naturales
- Alteraciones del entorno

Copias de seguridad

Es necesario establecer una **política adecuada de copias de seguridad periódicas** en cualquier organización; al igual que sucede con el resto de equipos y sistemas, los medios donde residen estas copias tendrán que estar protegidos físicamente; de hecho quizás deberíamos de emplear medidas más fuertes, ya que en realidad es fácil que en una sola cinta haya copias de la información contenida en varios servidores.

Lo primero que debemos pensar es dónde se almacenan los dispositivos donde se realizan las copias. Un error muy habitual es almacenarlos en lugares muy cercanos a la sala de operaciones, cuando no en la misma sala; esto, que en principio puede parecer correcto (y cómodo si necesitamos restaurar unos archivos) puede convertirse en un problema serio si se produce cualquier tipo de desastre (como p. ej. un incendio). Hay que pensar que en general el *hardware* se puede volver a comprar, pero una pérdida de información puede ser ireemplazable.

Así pues, lo más recomendable es guardar las copias en una zona alejada de la sala de operaciones; lo que se suele recomendar es disponer de varios niveles de copia, una que se almacena en una caja de seguridad en un lugar alejado y que se renueva con una periodicidad alta y otras de uso frecuente que se almacenan en lugares más próximos (aunque a poder ser lejos de la sala donde se encuentran los equipos copiados).

Para proteger más aun la información copiada se pueden emplear **mecanismos de cifrado**, de modo que la copia que guardamos no sirva de nada si no disponemos de la clave para recuperar los datos almacenados.

3.2. SEGURIDAD LÓGICA

La Seguridad Lógica es el conjunto de medidas destinadas a la **protección de datos y aplicaciones** informáticas, así como a **garantizar el acceso a la información únicamente a las personas autorizadas** .

La seguridad lógica consiste en la **aplicación de barreras y procedimientos que** resguarden el acceso a los datos, que solo se permita acceder a ellos a las personas autorizadas para hacerlo.

La seguridad lógica la lleva a cabo el **administrador** o administradores del sistema y se basa, en gran medida, en la efectiva **administración de los permisos y el control de acceso** a los recursos informáticos, basados en la identificación, autenticación y autorización de los accesos.

Algunas **medidas de seguridad lógica** son:

- **Política de Seguridad** de la empresa: es una serie de normas, protocolos, reglamentos, convenciones… en las que se fijarán los mecanismos de seguridad que se emplearán en dicha empresa.
- **Control de acceso lógico**: consiste en controlar el acceso mediante *login-password* al sistema a varios niveles: a nivel de BIOS, sistema operativo y aplicaciones.
- **Política de contraseñas**.: para que las contraseñas sean robustas deberán tener una longitud superior a 8 caracteres e incluir letras mayúsculas, minúsculas, números y signos de puntuación.
- **Política de usuarios y grupos** del Sistema Operativo en red.
- **Permisos** de los archivos y carpetas
- **Criptografía: firma y certificado digital. Protocolos seguros**: HTTPS, IPSec, TSL, SSL.

- **Actualización** de sistemas operativos y aplicaciones software. Los ciberdelicuentes se aprovechan de las vulnerabilidades de seguridad de los sistemas. Los fabricantes de software actualizan sus sistemas cada vez que encuentran agujeros de seguridad.
- **Antivirus** y suites de seguridad integrada.
- **Firewall** o Cortafuegos: control del tráfico de red.
- **Proxy**
- **Mantenerse informado** sobre amenazas: INCIBE, OSI.

CONTROL DE ACCESO LÓGICO

Es la principal defensa de los sistemas, permiten prevenir el acceso a personas no autorizadas y al ingreso de la información de los mismos.
Se pueden implementar directamente en la BIOS, en el sistema operativo, sobre los sistemas de aplicación, en un paquete específico de seguridad y en cualquier otra aplicación.

Se emplean 2 procesos para la tarea de controlar el acceso:
- **Identificación**: Cuando el usuario se da a conocer al sistema
- **Autenticación**: La verificación del sistema a la identificación del usuario

Existen 4 tipos que permitan realizar la autenticación de la identificación del usuario, las cuales pueden ser utilizadas:
- Algo que el usuario solamente conozca (una clave, un pin…)
- Algo que la persona posee (tarjeta...)
- Algo que el individuo es (huella digital, voz…)
- Algo que el individuo es capaz de hacer (patrones de escritura)

Los sistemas de control de acceso protegidos con contraseña, suelen ser un punto crítico de la seguridad y por ello suelen recibir distintos tipos de ataques, los más comunes:
- **Ataque de fuerza bruta**: Se intenta obtener la clave realizando todas las combinaciones posibles hasta encontrar la correcta, es aún más sencillo si la clave es corta.
- **Ataque de diccionario:** Obtienen la clave probando todas las palabras del diccionario o palabras comunes del usuario (nombres de familiares, mascotas…)
  Una forma sencilla de evitar este tipo de ataques se establece un número máximo de tentativas, de esta manera se bloquea el sistema automáticamente después de exceder este número máximo.
  La seguridad se basa en gran medida en la efectiva administración de los permisos de acceso a los recursos informáticos.
- **Roles**: En este caso los derechos de acceso y políticas de seguridad, pueden agruparse de acuerdo con el rol de los usuarios. Pueden controlarse a tares de la función, perfil o rol del usuario que requiere dicho acceso.
- **Limitaciones a los servicios:** Se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema.
- **Modalidad de acceso:** Se refiere al modo de acceso que se le permite al usuario los recursos y la información. Ejemplo: lectura, escritura, ejecución borrado, todas las anteriores.
- **Ubicación y horario:** Permite limitar el acceso de los usuarios a determinadas horas del día o a determinados días de la semana.
- **Administración:** Ya planteado los controles de accesos se deben tener una excelente administración de los mismos, involucrando la implementación, seguimientos, pruebas y modificaciones sobre los accesos de los usuarios al sistema. También requiere determinar cuál será el nivel de seguridad en los datos, se debe clasificar la información para los diferentes usuarios que accederán al sistema los cuales requieren también distintas medidas y niveles de seguridad.
- Administración del personal y usuarios

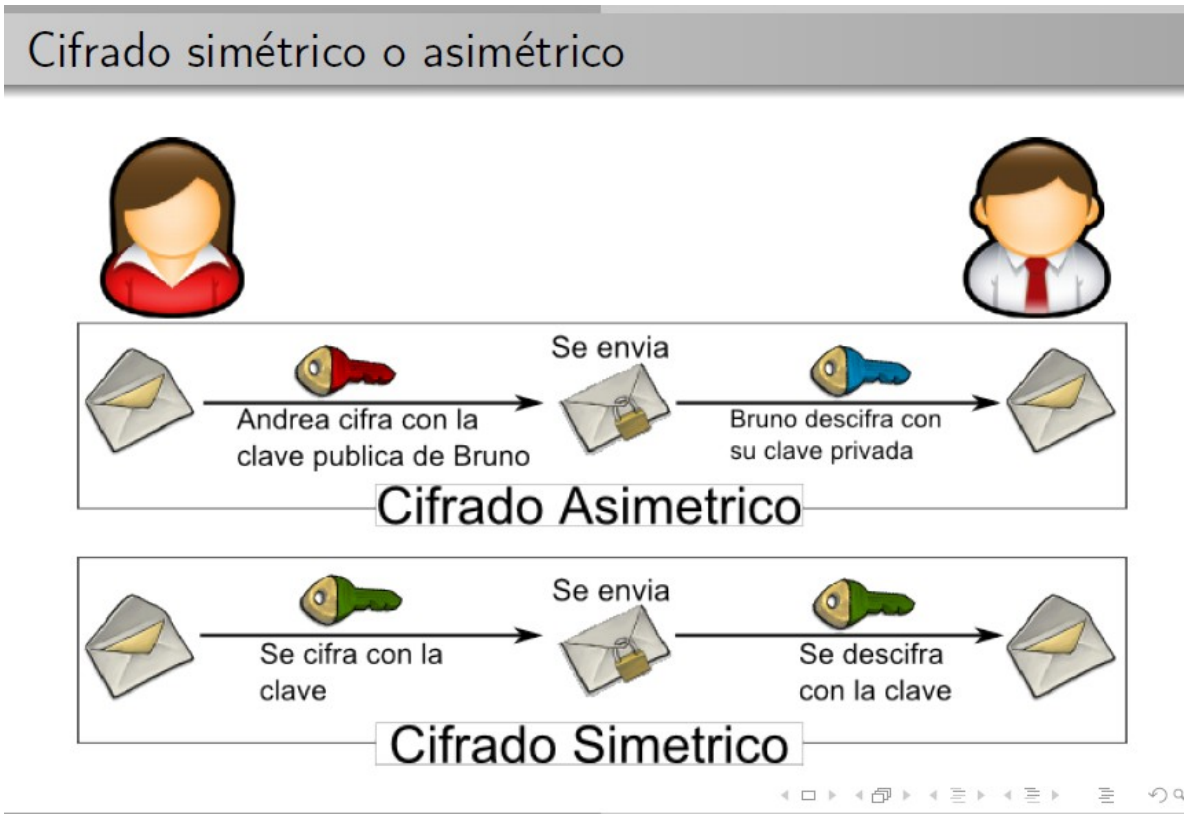
CRIPTOGRAFÍA

La **criptografía** es un conjunto de técnicas matemáticas que permiten el enmascaramiento o encriptado de mensajes de tal forma que sólo el destino de una comunicación podrá interpretarlo.

Para encriptar el mensaje se emplea una **clave** o llave que puede ser un número o una secuencia de letras y números.

Existen dos métodos de criptografía:

- **CRIPTOGRAFÍA SIMÉTRICA**: se emplea la misma clave para encriptar y desencriptar el mensaje.
- **CRIPTOGRAFÍA ASIMÉTRICA:** se emplean dos claves distintas. Asigna a cada extremo de la comunicación **un par de llaves:**
    - **Clave pública,** la emplea el emisor para cifrar el mensaje.
    - **Clave privada,** la emplea el receptor para descifrar el mensaje.



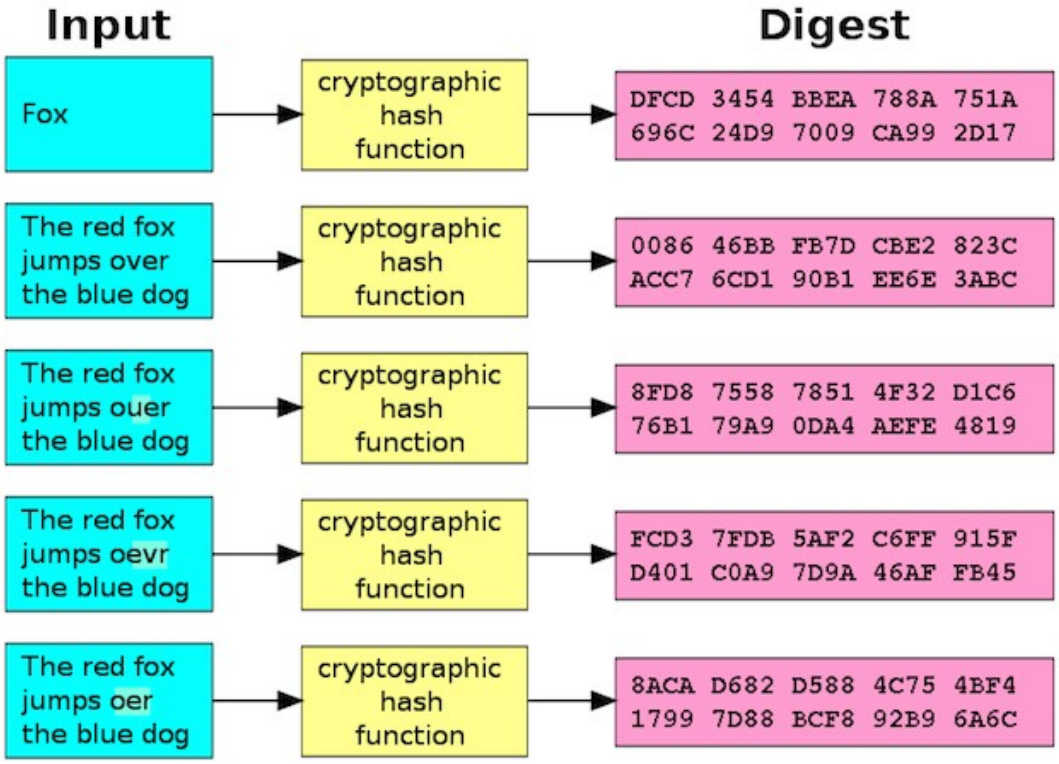
ALGORITMO CRIPTOGRÁFICO: es *una función matemática usada en los procesos de encriptación y desencriptación*. El algoritmo se sirve de una **clave** para encriptar y desencriptar datos. Algunos algoritmos de uso frecuente son **RSA, DES, RC5, IDEA**, **Diffie-Hellman…**

FUNCIÓN HASH

Una función criptográfica **hash**- usualmente conocida como "hash"- es un algoritmo matemático que **transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija**. Independientemente de la longitud de los datos de entrada, **el valor hash de salida tendrá siempre la misma longitud.** El Hash sirve para **autenticar** datos: comprobar que el archivo origen y el recibido son el mismo. Estrictamente hablando, el hash no es una forma de cifrado, aunque usa

criptografía (funciones hash). Entonces, se toma datos y se crea un hash fuera de él, una cadena de datos con tres propiedades importantes:

(1) los mismos datos siempre producirán el mismo hash,
(2) **es imposible revertirlo a los datos originales**, dado el conocimiento del hash,
(3) es inviable crear otra cadena de datos que creará el mismo hash (llamado "**colisión**" en el lenguaje criptográfico).



Un ejemplo de función hash es el código **MD5**, una secuencia de letras y números que descargamos junto a un archivo para garantizar que el archivo se descargó correctamente. Ejemplo de código MD5: ec5c4971bece420b2584766d675b426a.

Estos sistemas de cifrado se basan en funciones resumen o funciones hash de un solo sentido, que aprovechan propiedades particulares, por ejemplo, los números primos. Una función en un solo sentido es aquella cuya computación es fácil, mientras que su inversión resulta extraordinariamente difícil. Por ejemplo, es fácil multiplicar dos números primos juntos para obtener un compuesto, pero es difícil factorizar uno compuesto en sus componentes primos. Algunos algoritmos empleados como funciones hash son MD5 y SHA.
Puedes leer más sobre hashing en:

https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/

EL CERTIFICADO DIGITAL

Es un método de cifrado de **clave asimétrica.**

El Certificado Digital es el único medio que permite garantizar técnica y legalmente la identidad de una persona en Internet.

Se trata de un requisito indispensable para que las instituciones puedan ofrecer servicios seguros a través de Internet (protocolos HTTPS y *SSL : Secure Socket Layer,* que emplea un certificado digital)

El Certificado Digital es un **documento digital** que contiene la **clave pública** junto con los datos del titular, todo ello firmado electrónicamente por una **Autoridad de Certificación**, que es una tercera entidad de confianza que asegura que la clave pública se corresponde con los datos del titular .

Una **Entidad de Certificación** es una entidad de confianza que asegura que la clave pública se corresponde con los datos del titular. En España son ENAC: Entidad Nacional de Certificación, Fabrica Nacional de Moneda y timbre (FNMT.es) , AENOR...

El certificado digital permite **la firma electrónica de documentos.**

LA FIRMA ELECTRÓNICA

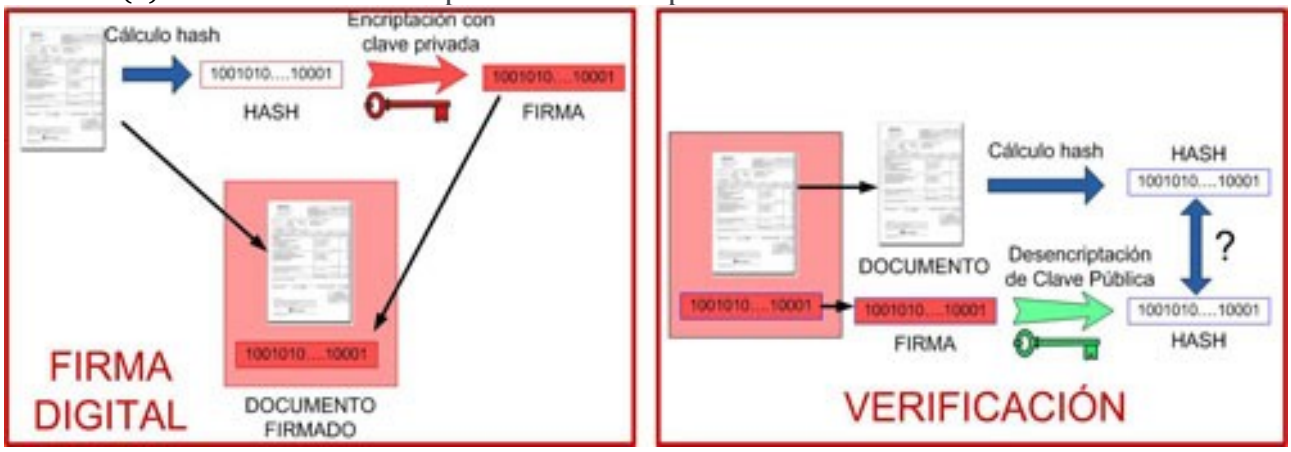
La **Firma Digital** es un método criptográfico que asocia la identidad de una persona o de un equipo informático al mensaje o documento. En función del tipo de firma, puede, además, asegurar la integridad del documento o mensaje.

La firma digital sirve para:

- identificar al autor,
- para señalar conformidad (o disconformidad) con el contenido,
- para indicar que se ha leído o, según el tipo de firma,
- garantizar que no se pueda modificar su contenido.
- Otorga al documento validez jurídica

El procedimiento de firma digital de documentos incluye dos fases:

(1) Se genera un hash del documento original con una función hash.
(2) El resultado se encripta con la clave pública del emisor.

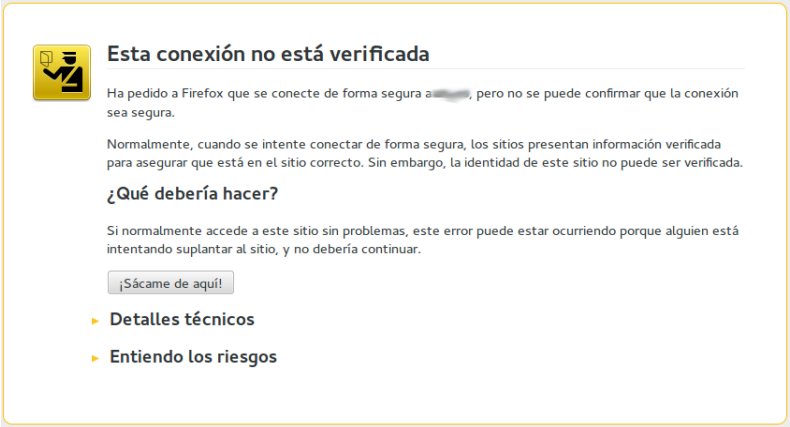


CERTIFICADOS DIGITALES EN SITIOS WEB

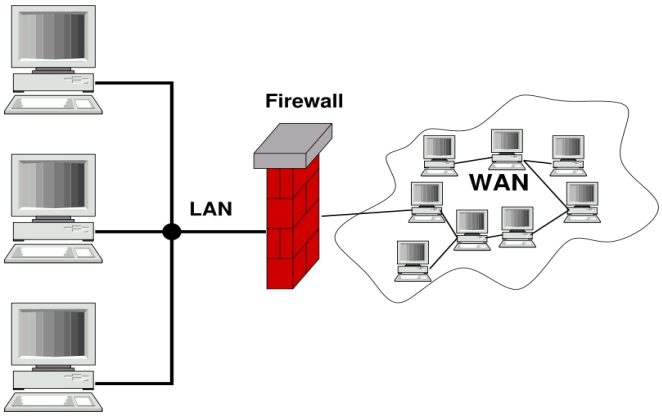
Garantizar la seguridad de un sitio web es sinónimo de implementar **SSL** (Secure Socket Layer) y para ello es imprescindible disponer de un **certificado digital** e instalarlo en nuestro sitio web.

Existen distintos tipos de certificados:

- EMITIDO POR UNA ENTIDAD CERTIFICADORA
- NO EMITIDO POR UNA ENTIDAD CERTIFICADORA: en este caso el navegador nos avisa de que el sitio no es confiable.



EL CORTAFUEGOS: FIREWALL



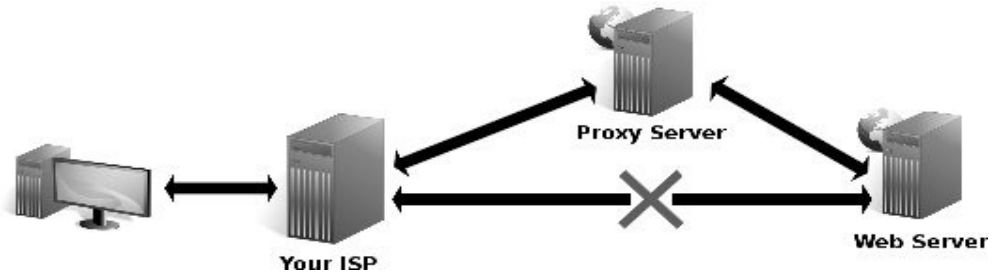
Un **cortafuegos** (***firewall***) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar o descifrar el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Los cortafuegos pueden ser implementados en hardware o software, o en una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados.

SERVIDOR PROXY

Un servidor proxy es un servidor que actúa como **intermediario entre un cliente y un servidor web** para que la empresa pueda garantizar el servicio de seguridad, control administrativo y almacenamiento en caché. Mediante el uso del servidor proxy puede ocultar y hacer que su identificación de red sea anónima **ocultando su dirección IP**.



Esta situación estratégica de punto intermedio le permite al proxy ofrecer diversas funcionalidades:

- Caché web.
- Control de acceso,
- Registro del tráfico,
- Restricción a determinados tipos de tráfico, mejora de rendimiento,
- Anonimato de la comunicación

4. AMENAZAS Y FRAUDES DE LOS SISTEMAS DE INFORMACIÓN Y A LAS PERSONAS

a. Software malicioso, herramientas antimalware y antivirus.

El término *malware* viene de las palabras inglesas *malicious software*.

Se refiere al tipo de **programas o códigos** informáticos que fueron creados con el propósito de infiltrarse en una computadora, sin consentimiento de su usuario.

- **VIRUS :** programa que infecta a otros archivos del sistema incrustando su código malicioso en el interior del archivo víctima (suele ser un ejecutable que al ejecutarse infecta otros archivos…). Los virus **no se pueden propagar sin intervención humana**, como cuando ejecutamos un programa infectado. Los usuarios propagan un virus informático, casi siempre de manera involuntaria, compartiendo archivos infectados o enviando mensajes de correo electrónico con virus en archivos adjuntos.
- **TROYANOS:** Un troyano no es un virus, sino un programa destructivo que se hace pasar por una aplicación auténtica, y engaña a la víctima para que lo instale en su ordenador. A diferencia de los virus, los troyanos no se replican, pero pueden ser igual de dañinos. Además, algunos troyanos abren una puerta trasera en el equipo que facilita a usuario atacante y programas maliciosos el acceso al sistema para robar información personal y confidencial.
- **GUSANOS O WORMS:** Los gusanos se propagan de ordenador en ordenador pero, a diferencia de los virus, tienen la capacidad de **desplazarse sin intervención humana**. El mayor peligro de un gusano es su **capacidad de replicarse en su sistema.** Es decir, en lugar de enviar un solo gusano, su equipo puede enviar centenares o miles de copias de sí mismo, lo que puede tener consecuencias devastadoras.
- **Backdoor.-** Impide que el sistema de la computadora se cierre totalmente, para que los ciberdelincuentes puedan usar los recursos de esa computadora. Es común entre las computadoras conectadas en red. Control remoto del ordenador.

- **Rootkits.-** Crean un programa fantasma, que evita que el malware sea detectado o incluso borrado. Consume la memoria RAM.
- **Adware**.- Abren ventanas emergentes sin haberlas solicitado, para volver molesto el trabajo.
- **Spyware.-** Recopilan la actividad de un computador, mediante barras de herramientas instalables o cookies, para enviarla a agencias de publicidad.
- **Hijackers**: secuestran funciones del navegador, como modificar la pagina de inicio. Otros redireccionan los resultados de las búsquedas hacia anuncios de pago o phishing bancario.
- **Keylogger.-** Monitorizan y almacenan la actividad del teclado, para enviar esa información a otras organizaciones. Es muy común para cometer delitos de banca electrónica.

- **BOTNET: REDES ZOMBI:** El PC se infecta con un virus capaz de controlar tu ordenador de forma remota. Esto quiere decir que alguien puede manejarlo a su antojo remotamente. Un conjunto o red de robots informáticos o bots, que se ejecutan de manera autónoma y automática. El artífice de la botnet puede controlar todos los ordenadores/servidores infectados de forma remota.

- **RAMSOMWARE**: secuestran los datos del disco. Introducen un código de bloqueo en la computadora, cuyo autor ofrece retirarlo a cambio de un pago.

ANTIVIRUS Y SUITES DE SEGURIDAD INTEGRADA CONTRA EL MALWARE

Un Antivirus es un programa que identifica y elimina virus informáticos y otros programas maliciosos como Worms, Trojans, Rootkit, Spyware… de una computadora infectada.
También protege a la computadora de ataques de virus adicionales. Previene infecciones .
Tienen una **base de datos de virus** que hay que mantenerla actualizada.
Cuando un antivirus detecta un virus puede hacer dos cosas con el archivo:

- Borrar el archivo
- Poner el archivo en cuarentena: eliminar el archivo de su localización original, **y lo convierte en un archivo que no puede ejecutarse como programa**, y a su vez lo esconde en una carpeta oculta que no puede ser vista ni accedida.

Una **suite de seguridad integrada** es la suma de varios programas de seguridad, un "Todo en uno". :

- **Antivirus,**
- **Anti-spyware,**
- **Firewall,**
- **Antirootkit,**
- **Antiphishing, etc.**

b. INGENIERÍA SOCIAL: PHISHING, VISHING, …

La **ingeniería social** consiste en obtener información confidencial a través de la manipulación de usuarios legítimos. Explota el principio : "los usuarios son el eslabón débil".

Es una técnica que pueden usar ciertas personas, tales como investigadores privados, criminales, o delincuentes informáticos, para obtener información en S.I. que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgo o abusos. Se suele emplear email o teléfono. Algunas técnicas de ingeniería social son:

- **PHISHING** : Ataque que se inicia enviando a la víctima un **e-mail suplantando a una entidad conocida**, te piden que hagas clic en un enlace, descargues un fichero o envíes información sensible. **Estafa, obtener información confidencial** de forma fraudulenta, como contraseñas, nº de tarjeta de crédito...

  El estafador, conocido como **phisher,** se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo general un **correo electrónico**, o algún sistema de mensajería instantánea, redes sociales SMS/MMS, a raíz de un malware o incluso utilizando también llamadas telefónicas.

- **VISHING: Phishing por teléfono. C**onsiste en realizar **llamadas telefónicas** encubiertas bajo **encuestas** con las que también se podría sacar información personal de forma que la víctima no sospeche.

- **BAITING:** se utiliza un **USB infectado** con un software malicioso, dejándolo en un lugar en el cual sea fácil de encontrar (baños públicos, ascensores, aceras, etc.). Cuando la víctima lo introduzca en su ordenador, el software se instalará y permitirá que el hacker obtenga todos los datos personales del usuario.

- **QUID PRO QUO:** El atacante llama a números aleatorios en una empresa, alegando estar llamando de nuevo desde el **soporte técnico**. Esta persona informará a alguien de un problema legítimo y se ofrecerá a ayudarle, durante el proceso conseguirá los datos de acceso y lanzará un malware. Suelen ofrecer un **regalo.**

5. LEGISLACIóN SOBRE PRIVACIDAD Y SEGURIDAD

Las leyes que nos protegen frente a los ciberataques en España son:

- **LOPD**: Ley Orgánica de Protección de Datos de carácter Personal. (AEPD)
- **LSSICE**: Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- **Ley de la Propiedad Intelectual**
- La Directiva 1999/93/CE de la Unión Europea sienta un marco común para la firma electrónica en la zona Euro. La transposición de dicha Directiva en España corresponde a la **Ley 59/2003, de Firma electrónica**,

La **Agencia Española de Protección de Datos** (AEPD) es la autoridad pública independiente encargada de velar por la privacidad y la protección de datos de los ciudadanos y por el cumplimiento de la Ley Orgánica de Protección de Datos de Carácter Personal en España.

Su objetivo de este espacio es, por un lado, fomentar que los ciudadanos conozcan sus derechos y las posibilidades que la Agencia les ofrece para ejercerlos y, por otro, que los sujetos obligados tengan a su disposición un instrumento ágil que les facilite el cumplimiento de la normativa.

Es un ente de derecho público con personalidad jurídica propia y plena capacidad pública y privada que actúa con independencia de la Administración pública en el ejercicio de sus funciones. Su principal misión es velar por el cumplimiento de la legislación de protección de datos por parte de los responsables de los ficheros (entidades públicas, empresas privadas, asociaciones, etc.) y controlar su aplicación a fin de garantizar el derecho fundamental a la protección de datos personales de los ciudadanos. La AEPD lleva a cabo sus potestades de investigación fundamentalmente a instancias de los ciudadanos, aunque también está facultada para actuar de oficio. La Agencia es estatutaria y jerárquicamente independiente y se relaciona con el Gobierno a través del Ministerio de Justicia.

https://www.agpd.es

6. WEBS SOBRE SEGURIDAD INFORMÁTICA:

- INSTITUTO DE CIBERSEGURIDAD: www.incibe.es
- OFICINA DE SEGURIDAD DEL INTERNAUTA: www.osi.es
- CENTRO CRIPTOLOGICO NACIONAL: https://www.ccn.cni.es/index.php
- SOBRE CRIPTOGRAFIA: https://esgeeks.com/guia-para-principiantes-de-criptografia
- SOBRE CERTIFICADO DIGITAL: http://www.upv.es/contenidos/CD/info/711545normalc.html http://cefire.edu.gva.es/file.php/1/Comunicacion_y_apertura/B1_Navegacion_Internet/certificados.html
- SOBRE FIRMA DIGITAL: https://firmaelectronica.gob.es/ https://www.upv.es/contenidos/CD/info/711250normalc.html
- SEGURIDAD EN REDES SOCIALES: https://ignaciosantiago.com/consejos-seguridad-redes-sociales/
- GUIA BASICA DE PRIVACIDAD Y SEGURIDAD: https://esgeeks.com/guia-basica-seguridad-y-privacidad/