SEGURIDAD INFORMÁTICA

Tema 6

Seguridad informática

SEGURIDAD INFORMÁTICA

Índice

SEGURIDAD INFORMÁTICA

Índice

SEGURIDAD INFORMÁTICA

Introducción

SEGURIDAD INFORMÁTICA

- Se entiende por **seguridad informática** el conjunto de normas, procedimientos y herramientas, que tienen como objetivo garantizar la disponibilidad, integridad, confidencialidad y buen uso de la información que reside en un sistema de información.

SEGURIDAD INFORMÁTICA

La seguridad informática

SEGURIDAD INFORMÁTICA

- Se entiende por **seguridad informática** el conjunto de normas, procedimientos y herramientas, que tienen como objetivo garantizar la disponibilidad, integridad, confidencialidad y buen uso de la información que reside en un sistema de información.

SEGURIDAD INFORMÁTICA

- Se entiende por **seguridad informática** el conjunto de normas, procedimientos y herramientas, que tienen como objetivo garantizar la disponibilidad, integridad, confidencialidad y buen uso de la información que reside en un sistema de información.

- El objetivo de la seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

SEGURIDAD INFORMÁTICA

- El objetivo de la seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

SEGURIDAD INFORMÁTICA

- Para que un sistema informático pueda considerarse seguro debe garantizar los principios de confidencialidad, integridad y disponibilidad.

- Principios de seguridad informática:
  - Confidencialidad.
  - Integridad.
  - Disponibilidad.

SEGURIDAD INFORMÁTICA

- Principios de seguridad informática:
  - **Confidencialidad**: La confidencialidad hace referencia a la privacidad de los elementos de información almacenados y procesados en un sistema informático.
  - Basándose en este principio, las herramientas de seguridad informática deben proteger el sistema de invasiones y accesos por parte de personas o programas no autorizados.
  - Este principio es particularmente importante en sistemas distribuidos (aquellos en los que los usuarios, computadores y datos residen en lugares diferentes, pero están física y lógicamente interconectados).

SEGURIDAD INFORMÁTICA

- Principios de seguridad informática:
  - **Integridad**: La integridad hace referencia a la validez y consistencia de los elementos de información almacenados y procesados en un sistema informático.
  - Basándose en este principio, las herramientas de seguridad informática deben asegurar que los procesos de actualización estén bien sincronizados y no se dupliquen, de forma que todos los elementos del sistema manipulen adecuadamente los mismos datos.
  - Este principio es importante en sistemas descentralizados (aquellos en los que diferentes usuarios, computadores y procesos comparten la misma información).

SEGURIDAD INFORMÁTICA

- Principios de seguridad informática:
  - **Disponibilidad**: La disponibilidad hace referencia a la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático.
  - Basándose en este principio, las herramientas de seguridad informática deber reforzar la permanencia del sistema informático, en condiciones de actividad adecuadas para que los usuarios accedan a los datos con la frecuencia y dedicación que requieran. Este principio es importante en sistemas informáticos cuyo compromiso con el usuario, es prestar un servicio permanente.
  - El concepto de disponibilidad hace referencia a la posibilidad de que un sistema sea accesible y esté disponible para ser utilizado.

SEGURIDAD INFORMÁTICA

- Las principales amenazas de un sistema informático son: los usuarios, los intrusos, el software malicioso o malware y los accidentes, averías y siniestros (incendios, inundaciones, etc.).

- Principales amenazas:
  - Los usuarios.
  - Los intrusos.
  - El software malicioso (malware).
  - Los accidentes, averías y siniestros (incendios, inundaciones, etc.).

SEGURIDAD INFORMÁTICA

- Principales amenazas:
  - **Los usuarios**: que, a menudo, con sus acciones (descargar archivos, abrir correos sospechosos, borrar archivos del sistema, etc.), premeditadas o no, desencadenan episodios de vulnerabilidad del sistema.
  - Los intrusos.
  - El software malicioso (malware).
  - Los accidentes, averías y siniestros (incendios, inundaciones, etc.).

SEGURIDAD INFORMÁTICA

- Principales amenazas:
  - Los usuarios.
  - **Los intrusos**: que ingresan al sistema sin autorización con propósitos perjudiciales.
  - El software malicioso (malware).
  - Los accidentes, averías y siniestros (incendios, inundaciones, etc.).

SEGURIDAD INFORMÁTICA

- Principales amenazas:
  - Los usuarios.
  - Los intrusos.
  - **El software malicioso (malware)**: se trata de software creado para instalarse en un ordenador ajeno sin el conocimiento del usuario. Su finalidad consiste en obtener información y en ralentizar el funcionamiento o destruir archivos.
  - Los accidentes, averías y siniestros (incendios, inundaciones, etc.).

SEGURIDAD INFORMÁTICA

- Principales amenazas:
  - Los usuarios.
  - Los intrusos.
  - El software malicioso (malware).
  - **Los accidentes, averías y siniestros (incendios, inundaciones, etc.)**: que tienen un efecto devastador para cualquier sistema informático.

SEGURIDAD INFORMÁTICA

- Se entiende por **seguridad informática** el conjunto de normas, procedimientos y herramientas, que tienen como objetivo garantizar la disponibilidad, integridad, confidencialidad y buen uso de la información que reside en un sistema de información.

- La seguridad informática utiliza un sinfín de recursos para paliar los efectos de las amenazas y los riesgos: realización de copias de seguridad, instalación de programas antivirus, encriptación de datos, cortafuegos, etc.

SEGURIDAD INFORMÁTICA

Seguridad activa y pasiva

SEGURIDAD INFORMÁTICA

- Se entiende por **seguridad informática** el conjunto de normas, procedimientos y herramientas, que tienen como objetivo garantizar la disponibilidad, integridad, confidencialidad y buen uso de la información que reside en un sistema de información.

- Desde el punto de vista del activo a proteger:
  - Seguridad física.
  - Seguridad lógica.

SEGURIDAD INFORMÁTICA

- Se entiende por seguridad informática el conjunto de normas, procedimientos y herramientas, que tienen como objetivo garantizar la disponibilidad, integridad, confidencialidad y buen uso de la información que reside en un sistema de información..

- Desde el punto de vista del activo a proteger:
  - **Seguridad física**: es aquella que trata de proteger el hardware (los equipos informáticos, el cableado, etc.) de los posibles desastres naturales (terremotos, tifones, etc.), incendios, inundaciones, sobrecargas eléctricas, robos y un sinfín de amenazas más.
  - Seguridad lógica.

SEGURIDAD INFORMÁTICA

- Se entiende por seguridad informática el conjunto de normas, procedimientos y herramientas, que tienen como objetivo garantizar la disponibilidad, integridad, confidencialidad y buen uso de la información que reside en un sistema de información.

- Desde el punto de vista del activo a proteger:
  - Seguridad física.
  - **Seguridad lógica**: complementa a la seguridad física, protegiendo el software de los equipos informáticos (es decir, las aplicaciones y los datos de los usuarios) de robos, pérdida de datos, entrada de virus informáticos, modificaciones no autorizadas de los datos, ataques desde la red, etc.

SEGURIDAD INFORMÁTICA

- Se entiende por seguridad informática el conjunto de normas, procedimientos y herramientas, que tienen como objetivo garantizar la disponibilidad, integridad, confidencialidad y buen uso de la información que reside en un sistema de información.

- Desde el punto de vista del momento preciso de actuación:
  - Seguridad activa.
  - Seguridad pasiva.

SEGURIDAD INFORMÁTICA

- Desde el punto de vista del momento preciso de actuación:
  - **Seguridad activa**: interviene antes de producirse el percance, de tal manera que se eviten los daños en el sistema. La seguridad activa la podemos definir como el conjunto de medidas que previenen e intentan evitar los daños en los sistemas informáticos.
  - Seguridad pasiva.

SEGURIDAD INFORMÁTICA

- Desde el punto de vista del momento preciso de actuación:
  - Seguridad activa.
  - **Seguridad pasiva**: actúa después del percance, minimizando los efectos ocasionados por el mismo. La seguridad pasiva complementa a la seguridad activa y se encarga de minimizar los efectos que haya ocasionado algún percance.

SEGURIDAD INFORMÁTICA

- Se entiende por seguridad informática el conjunto de normas, procedimientos y herramientas, que tienen como objetivo garantizar la disponibilidad, integridad, confidencialidad y buen uso de la información que reside en un sistema de información.

- Técnicas de seguridad activa:
  - Empleo de contraseñas seguras.
  - Encriptación de datos.
  - Uso de software de seguridad informática.
  - Firmas y certificados.
  - Cortafuegos (firewall).

SEGURIDAD INFORMÁTICA

- Se entiende por seguridad informática el conjunto de normas, procedimientos y herramientas, que tienen como objetivo garantizar la disponibilidad, integridad, confidencialidad y buen uso de la información que reside en un sistema de información..

- Técnicas de seguridad pasiva:
  - Uso de hardware y dispositivos físicos de protección adecuados.
  - Realización de copias de seguridad.
  - Particiones del disco duro.
  - Conjunto de discos redundantes.

SEGURIDAD INFORMÁTICA

- Técnicas de seguridad activa:
  - Empleo de contraseñas seguras.
  - Encriptación de datos.
  - Uso de software de seguridad informática.
  - Firmas y certificados.
  - Cortafuegos (firewall).
- Técnicas de seguridad pasiva:
  - Uso de hardware y dispositivos físicos de protección adecuados.
  - Realización de copias de seguridad.
  - Particiones del disco duro.
  - Conjunto de discos redundantes.

SEGURIDAD INFORMÁTICA

Seguridad activa

SEGURIDAD INFORMÁTICA

- Se entiende por seguridad informática el conjunto de normas, procedimientos y herramientas, que tienen como objetivo garantizar la disponibilidad, integridad, confidencialidad y buen uso de la información que reside en un sistema de información..

- Desde el punto de vista del momento preciso de actuación:
  - Seguridad activa.
  - Seguridad pasiva.

SEGURIDAD INFORMÁTICA

- Se entiende por seguridad informática el conjunto de normas, procedimientos y herramientas, que tienen como objetivo garantizar la disponibilidad, integridad, confidencialidad y buen uso de la información que reside en un sistema de información..

- Desde el punto de vista del momento preciso de actuación:
  - **Seguridad activa**: interviene antes de producirse el percance, de tal manera que se eviten los daños en el sistema. La seguridad activa la podemos definir como el conjunto de medidas que previenen e intentan evitar los daños en los sistemas informáticos.

SEGURIDAD INFORMÁTICA

- Se entiende por seguridad informática el conjunto de normas, procedimientos y herramientas, que tienen como objetivo garantizar la disponibilidad, integridad, confidencialidad y buen uso de la información que reside en un sistema de información..

- Técnicas de seguridad activa:
  - Empleo de contraseñas seguras.
  - Encriptación de datos.
  - Uso de software de seguridad informática.
  - Firmas y certificados.
  - Cortafuegos (firewall).

SEGURIDAD INFORMÁTICA

Seguridad activa

Las contraseñas

SEGURIDAD INFORMÁTICA

- Las contraseñas
  - Las **contraseñas (passwords)** son las herramientas más utilizadas para restringir el acceso a los sistemas informáticos. Su misión es prevenir el acceso a los recursos por parte de personas no autorizadas. Sin embargo, sólo son efectivas si se escogen con cuidado y se cambian periódicamente.
  - Es muy importante cambiar periódicamente las contraseñas. En los sistemas informáticos, mantener una buena política de seguridad de creación, mantenimiento y recambio de claves es un punto crítico para salvaguardar la seguridad y privacidad.

SEGURIDAD INFORMÁTICA

- Criterios para elegir una buena contraseña (I):
  - No utilizar contraseñas que sean palabras (aunque sean extranjeras) o nombres (el del usuario, miembros de la familia, mascotas, personajes de ficción, marcas, ciudades, etc.).
  - No usar contraseñas completamente numéricas con algún significado (número de teléfono, D.N.I., fecha de nacimiento, etc.).
  - No utilizar terminología técnica conocida.

SEGURIDAD INFORMÁTICA

- Criterios para elegir una buena contraseña (II):
  - Elegir una contraseña que mezcle caracteres alfabéticos (mayúsculas y minúsculas) y numéricos. Combine letras, números y símbolos. Cuanto más diversos sean los tipos de caracteres de la contraseña, más difícil será adivinarla.
  - Deben ser largas (de 8 caracteres o más).
  - Tener contraseñas diferentes en máquinas diferentes y sistemas diferentes. Es posible usar una contraseña base y ciertas variaciones lógicas de la misma para distintas máquinas. Esto permite que si una password de un sistema cae no caigan todos los

SEGURIDAD INFORMÁTICA

- Criterios para elegir una buena contraseña (III):
  - Deben ser fáciles de recordar para no verse obligado a escribirlas. Algunos ejemplos son:
    - Combinar palabras cortas con algún número o carácter de puntuación: soy2_yo3
    - Usar un acrónimo de alguna frase fácil de recordar: A río Revuelto Ganancia de Pescadores: ArRGdP.
    - Añadir un número al acrónimo para mayor seguridad: A9r7R5G3d1P.
    - Mejor incluso si la frase no es conocida: Hasta Ahora no he Olvidado mi Contraseña: aHoeIlo.
    - Elegir una palabra sin sentido, aunque pronunciable: taChunda72, AtajulH, Wen2Mar.
    - Realizar reemplazos de letras por signos o números: En Seguridad Más Vale Prevenir que Curar.

SEGURIDAD INFORMÁTICA

- Algunos consejos (I):
  - No permitir ninguna cuenta sin contraseña. Si se es administrador del sistema, repasar este hecho periódicamente (auditoría).
  - No mantener las contraseñas por defecto del sistema. Por ejemplo, cambiar las cuentas de Administrador, Root, System, Invitado, Guest, etc.
  - Nunca compartir con nadie la contraseña. Si se hace, cambiarla inmediatamente.
  - No escribir la contraseña en ningún sitio. Si se escribe, no debe identificarse como tal y no debe identificarse al propietario en el mismo lugar.

SEGURIDAD INFORMÁTICA

- Algunos consejos (II):
  - No teclear la contraseña si hay alguien observando. Es una norma tácita de buen usuario no mirar el teclado mientras alguien teclea su contraseña
  - No enviar la contraseña por correo electrónico ni mencionarla en una conversación. Si es necesario mencionarla, no hacerlo explícitamente diciendo: "mi contraseña es...".
  - No mantener una contraseña indefinidamente. Cambiarla regularmente. Se puede disponer de una lista de contraseñas que pueden usarse cíclicamente (por lo menos 5).

SEGURIDAD INFORMÁTICA

- Ejercicio:
  - Accede a la página:

    https://password.es/comprobador/

    y comprueba la seguridad de tus contraseñas.

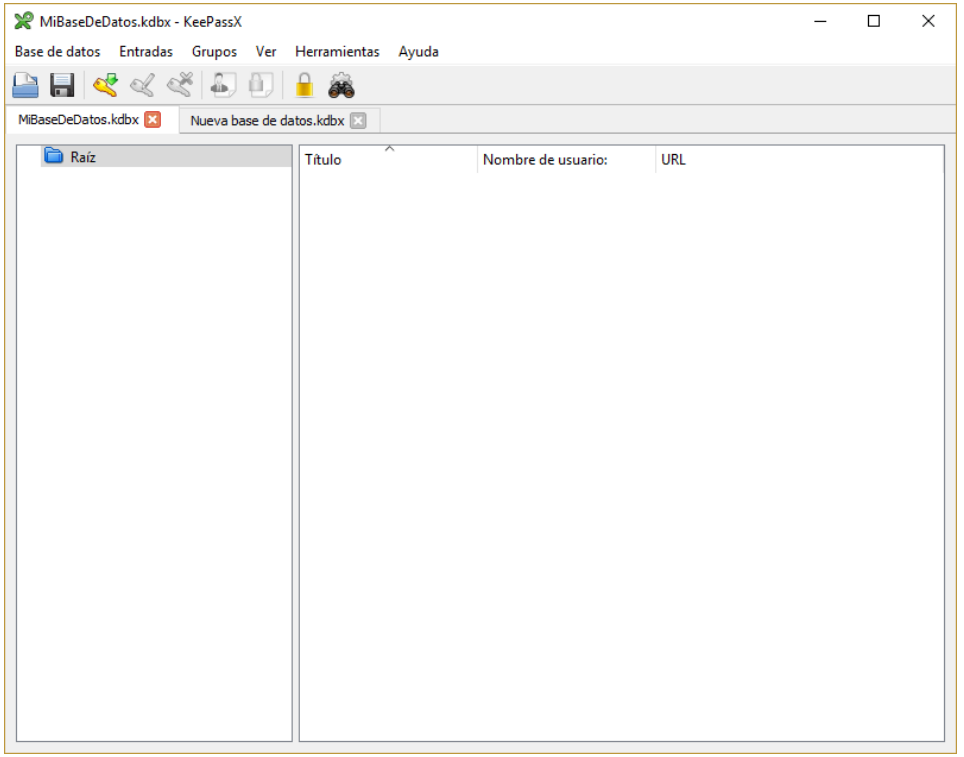
  - Intenta conseguir una contraseña con seguridad 100% y que sea fácil de recordar.

SEGURIDAD INFORMÁTICA

- Ejercicios:
  - Ejercicio KeePassX.

https://www.keepassx.org/

https://www.keepassx.org/downloads



SEGURIDAD INFORMÁTICA

Seguridad activa

Encriptación de datos

SEGURIDAD INFORMÁTICA

- Encriptación de datos
  - Las **encriptación** (una posible traducción al castellano sería cifrado) es el proceso mediante el cual cierta información o texto sin formato es transformada en un código ilegible a menos que se conozcan los datos necesarios para su interpretación.
  - La encriptación es una medida de seguridad utilizada para que, al almacenar o transmitir información sensible, ésta no pueda ser interpretada por personas no autorizadas.

SEGURIDAD INFORMÁTICA

- Encriptación de datos (Funcionamiento de un sistema criptográfico)
  - Un sistema criptográfico moderno se basa en un determinado algoritmo de encriptación o de cifrado que realiza unas transformaciones sobre el texto original (texto claro), para obtener un texto modificado (texto cifrado).

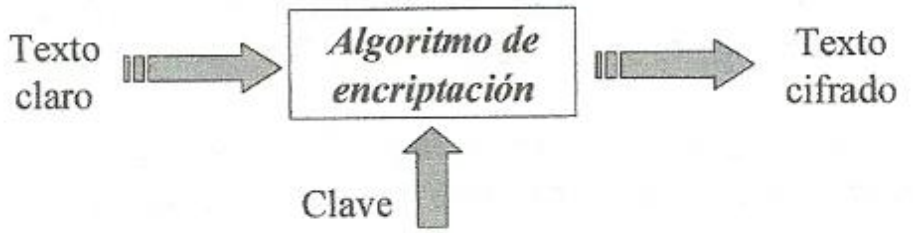
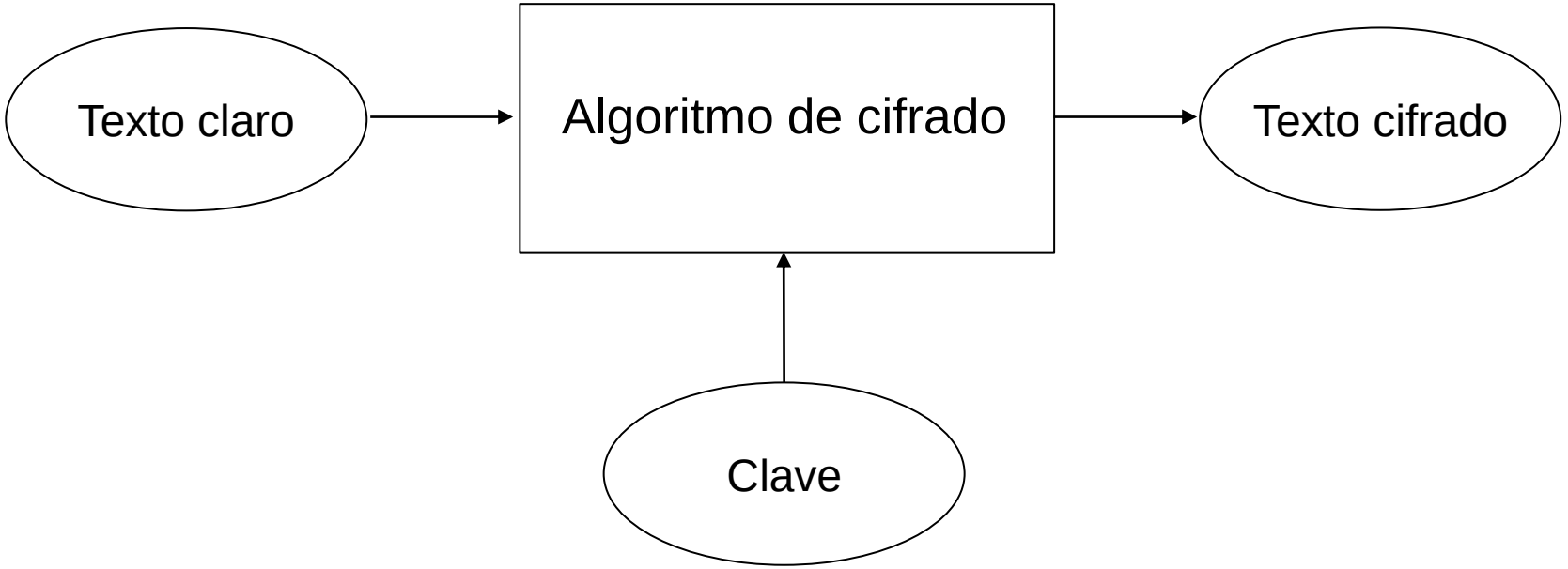


Figura 1.1. Esquema del proceso de cifrado

SEGURIDAD INFORMÁTICA

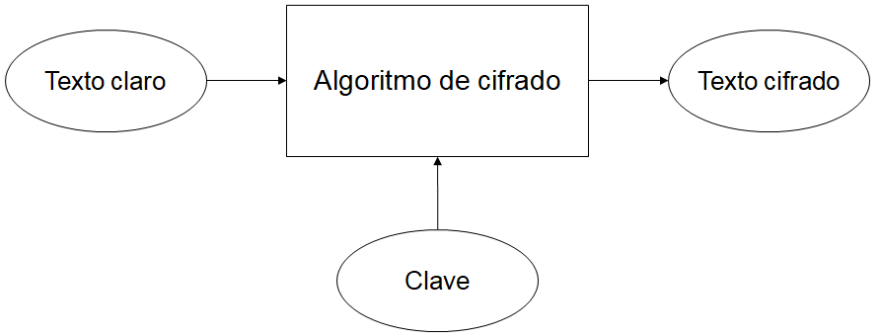
- Encriptación de datos (Funcionamiento de un sistema criptográfico):



Esquema del proceso de cifrado

SEGURIDAD INFORMÁTICA

- Encriptación de datos (Funcionamiento de un sistema criptográfico):
  - Un sistema criptográfico moderno se basa en un determinado algoritmo de encriptación o de cifrado que realiza unas transformaciones sobre el texto original (texto claro), para obtener un texto modificado (texto cifrado).



Esquema del proceso de cifrado

SEGURIDAD INFORMÁTICA

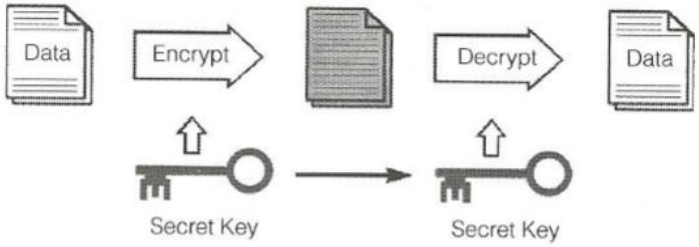
- Encriptación de datos
  - Algunos de los usos mas comunes de la encriptación son el almacenamiento y transmisión de información sensible como contraseñas, números de identificación legal, números de tarjetas crédito, informes contables y conversaciones privadas, entre otros.

SEGURIDAD INFORMÁTICA

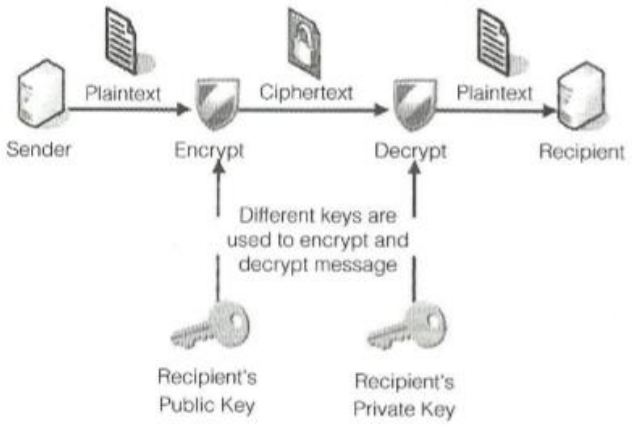
- Encriptación de datos
  - En criptografía, la encriptación es un procedimiento que utiliza un algoritmo de cifrado con cierta clave (clave de cifrado) para transformar un mensaje, de tal forma que sea incomprensible a toda persona que no tenga la clave secreta (clave de descifrado) del algoritmo.
  - Las claves de cifrado y de descifrado pueden ser iguales (criptografía simétrica) o distintas (criptografía asimétrica).

SEGURIDAD INFORMÁTICA

- Tipos de cifrado:
  - **Simétrico**: se utiliza la misma clave para cifrar y descifrar.
  - **Asimétrico**: se utilizan claves distintas para cifrar y descifrar.



Ejemplo de clave privada/simétrica.

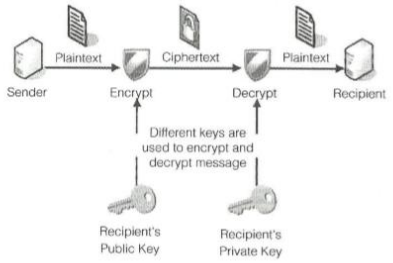


Ejemplo de clave pública/asimétrica.

SEGURIDAD INFORMÁTICA

- Tipos de cifrado:
  - **Simétrico**: se utiliza la misma clave para cifrar y descifrar.
  - **Asimétrico**: se utilizan claves distintas para cifrar y descifrar.

Ejemplo de clave privada/simétrica.



Ejemplo de clave pública/asimétrica.

El proceso de encriptación se puede llevar a cabo utilizando diferentes tipos de algoritmos: algoritmos hash, algoritmos simétricos y algoritmos asimétricos.

SEGURIDAD INFORMÁTICA

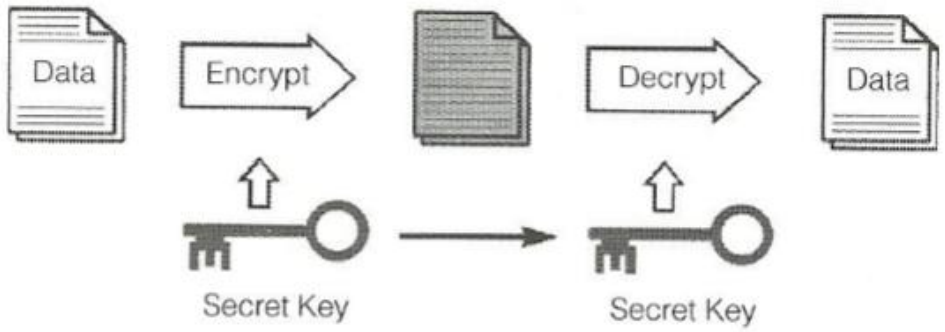
- Tipos de cifrado:
  - **Simétrico**: En los sistemas criptográficos simétricos se emplea la misma clave para realizar tanto el cifrado como el descifrado del texto original.

Figura 1.7. Cifrado mediante un algoritmo simétrico

Figura 1.8. Descifrado mediante un algoritmo simétrico

SEGURIDAD INFORMÁTICA

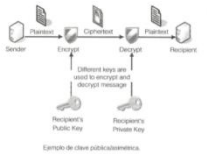
- Tipos de cifrado:
  - **Simétrico**: En los sistemas criptográficos simétricos se emplea la misma clave para realizar tanto el cifrado como el descifrado del texto original.



Ejemplo de clave privada/simétrica.

SEGURIDAD INFORMÁTICA

- Tipos de cifrado:
  - **Asimétrico**: se utilizan claves distintas para cifrar y descifrar.



  - El funcionamiento es el siguiente:
    - Un determinado usuario B genera dos claves. Una de estas claves se hace pública (es la clave que otros usuarios del sistema tendrán que utilizar para para cifrar los datos enviados a B)
    - Si el usuario A tiene que enviar datos de forma confidencial a B, debe proceder a su cifrado utilizando la clave pública de B.
    - El texto cifrado obtenido a partir de la clave pública de B sólo puede ser descifrado utilizando la clave privada de B.

SEGURIDAD INFORMÁTICA

- Tipos de cifrado:
  - **Asimétrico**: se utilizan claves distintas para cifrar y descifrar.

El funcionamiento es el siguiente:

- Un determinado usuario B genera dos claves. Una de estas claves se hace pública (es la clave que otros usuarios del sistema tendrán que utilizar para para cifrar los datos enviados a B)
- Si el usuario A tiene que enviar datos de forma confidencial a B, debe proceder a su cifrado utilizando la clave pública de B.
- El texto cifrado obtenido a partir de la clave pública de B sólo puede ser descifrado utilizando la clave privada de B.

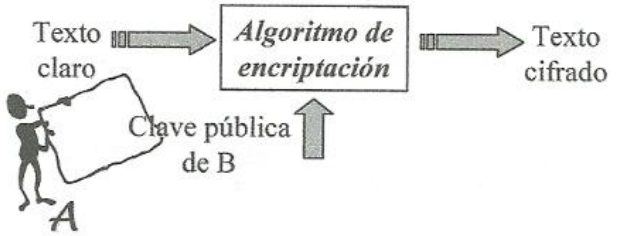


Figura 1.12. Cifrado mediante un algoritmo asimétrico

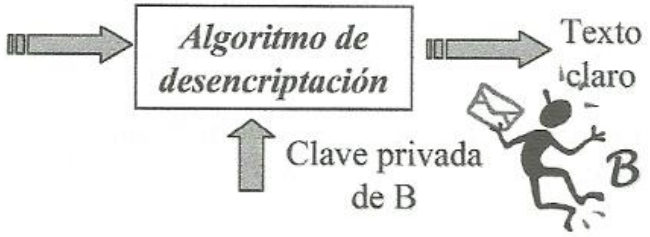
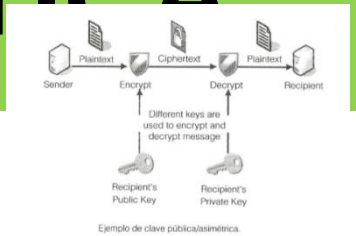


Figura 1.13. Descifrado mediante un algoritmo asimétrico

SEGURIDAD INFORMÁTICA

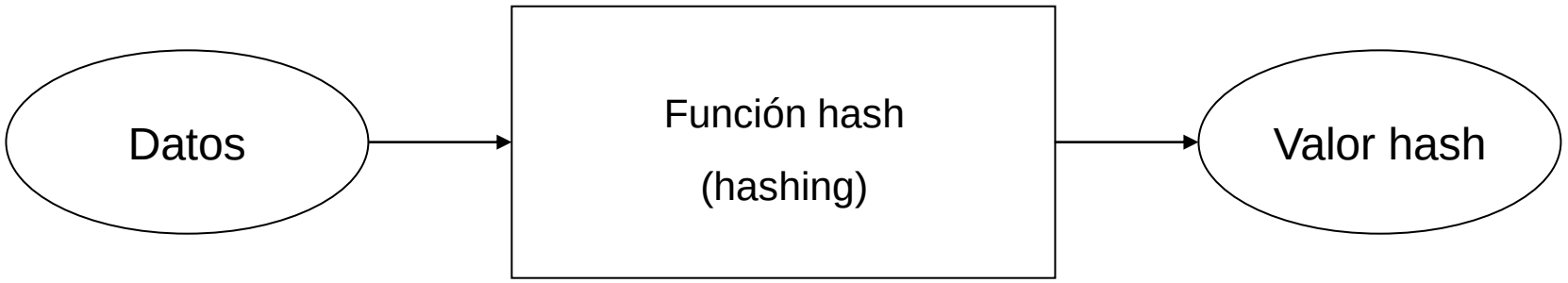


Ejemplo de clave pública/asimétrica.

- Tipos de cifrado:
  - **Asimétrico**: se utilizan claves distintas para cifrar y descifrar.
  - Por lo tanto, en los sistemas criptográficos asimétricos o sistemas de clave pública, cada usuario posee una pareja de claves: su clave privada (se debe guardar en secreto y se utiliza para descifrar) y su clave pública (que será conocida y que otros utilizan para cifrar).

SEGURIDAD INFORMÁTICA

- Algoritmos hash:
  - Un **algoritmo hash** efectúa un cálculo matemático sobre los datos que constituyen el documento y da como resultado un número llamado valor hash. Un mismo documento dará siempre un mismo valor hash.



SEGURIDAD INFORMÁTICA

- Algoritmos hash:
  - Un **algoritmo hash** efectúa un cálculo matemático sobre los datos que constituyen el documento y da como resultado un número llamado valor hash. Un mismo documento dará siempre un mismo valor hash.

SEGURIDAD INFORMÁTICA

- Ejercicio:
  1. Busca algún ejemplo de algoritmo simétrico.
  2. Busca algún ejemplo de algoritmo asimétrico.
  3. Busca algún ejemplo de algoritmo hash.

SEGURIDAD INFORMÁTICA

- Ejercicio:
  - Descifra el siguiente mensaje sabiendo que ha sido cifrado utilizando un cifrado tipo César :

Ñ	D	Y	L	G	D	H	V	O	D	U	D	Y	L	Ñ	Ñ	R	V	D

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z

D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

L	A	V	I	D	A	E	S	M	A	R	A	V	I	L	L	O	S	A

SEGURIDAD INFORMÁTICA

Seguridad activa

Uso de software de seguridad informática

SEGURIDAD INFORMÁTICA

- Uso de software de seguridad informática:
  - El objetivo del software de seguridad informática es prevenir contra virus informáticos y entradas indeseadas al sistema.
- Se denomina **malware** (software malicioso) al software específicamente diseñado para llevar a cabo acciones no deseadas (como infiltrase o dañar un ordenador o sistema informático) sin el consentimiento explicito del usuario.

SEGURIDAD INFORMÁTICA

- Uso de software de seguridad informática:
  - Existen muchos tipos de malware: virus, gusanos, troyanos, adware, keyloggers, dialers, rootkits, spyware, ransomware, rogueware, etc. que se diseñan con diferentes fines.
  - Algunos tipos de malware se diseñan con ánimo de lucro, otros son destructivos y su misión es alterar programas y archivos, otros hacen que un equipo sea controlado y explotado con fines ilícitos (envío de correo electrónico, almacenar pornografía, ataques a otros equipos o almacenar datos de actividades ilegales), etc.

SEGURIDAD INFORMÁTICA

- Uso de software de seguridad informática:
  - Dentro del software de seguridad informática, se pueden citar:
    - Los antivirus.
    - Los antiespías.
    - Etc.

SEGURIDAD INFORMÁTICA

- Uso de software de seguridad informática:
  - Los **antivirus** son programas que ayudan a proteger el equipo contra virus y otras amenazas a la seguridad.
  - Los **programas antiespía** impiden que se instalen en nuestro ordenador determinados programas cuyo objetivo es alterar su correcto funcionamiento (impiden acceder a determinadas páginas Web, muestran continuamente ventanas emergentes en nuestro navegador, etc.) o recopilar información del usuario.

SEGURIDAD INFORMÁTICA

Seguridad activa

Firmas y certificados

SEGURIDAD INFORMÁTICA

- Firmas y certificados (¿Qué es la firma digital?):
  - La firma digital es fundamental para posibilitar el desarrollo del comercio electrónico y los servicios digitales de forma segura a través de Internet.
  - La **firma digital** son los datos añadidos a un conjunto de datos que permiten al receptor probar el origen y la integridad de los mismos, así como protegerlos contra falsificaciones.
  - La firma digital de un mensaje o transacción permite garantizar la integridad, la autenticación y la no repudiación en un sistema informático.

SEGURIDAD INFORMÁTICA

- Firmas y certificados (¿Qué es la firma digital?):
  - La firma digital es fundamental para posibilitar el desarrollo del comercio electrónico y los servicios digitales de forma segura a través de Internet.
- La **firma digital** son los datos añadidos a un conjunto de datos que permiten al receptor probar el origen y la integridad de los mismos, así como protegerlos contra falsificaciones.
  - La firma digital de un mensaje o transacción permite garantizar la integridad, la autenticación y la no repudiación en un sistema informático.

SEGURIDAD INFORMÁTICA

- Firmas y certificados (¿Qué es la firma digital?):
  - La firma digital son los datos añadidos a un conjunto de datos que permiten al receptor probar el origen y la integridad de los mismos, así como protegerlos contra falsificaciones.

Figura 1.18. Obtención de la firma electrónica o digital de un mensaje

  - La firma digital de un mensaje o transacción permite garantizar la integridad, la autenticación y la no repudiación en un sistema informático.

SEGURIDAD INFORMÁTICA

- Firmas y certificados (¿Qué es la firma digital?):
  - Obtención de la firma digital:
    - El creador del mensaje debe cifrar la huella digital del mensaje con su clave privada y enviarla al destinatario acompañando al mensaje cifrado. El cifrado asimétrico se aplica sobre la huella digital del mensaje y no sobre el propio mensaje, debido al elevado coste computacional que supondría el cifrado de todo el mensaje (sería una alternativa mucho más lenta y compleja.

Figura 1.18. Obtención de la firma electrónica o digital de un mensaje

SEGURIDAD INFORMÁTICA

- Firmas y certificados (¿Qué es la firma digital?):
  - Obtención de la firma digital:

Figura 1.18. Obtención de la firma electrónica o digital de un mensaje

SEGURIDAD INFORMÁTICA

- Firmas y certificados (¿Qué es la firma digital?):
  - Procedimiento seguido por un usuario A para enviar un mensaje cifrado a otro usuario B acompañado de su correspondiente firma digital:

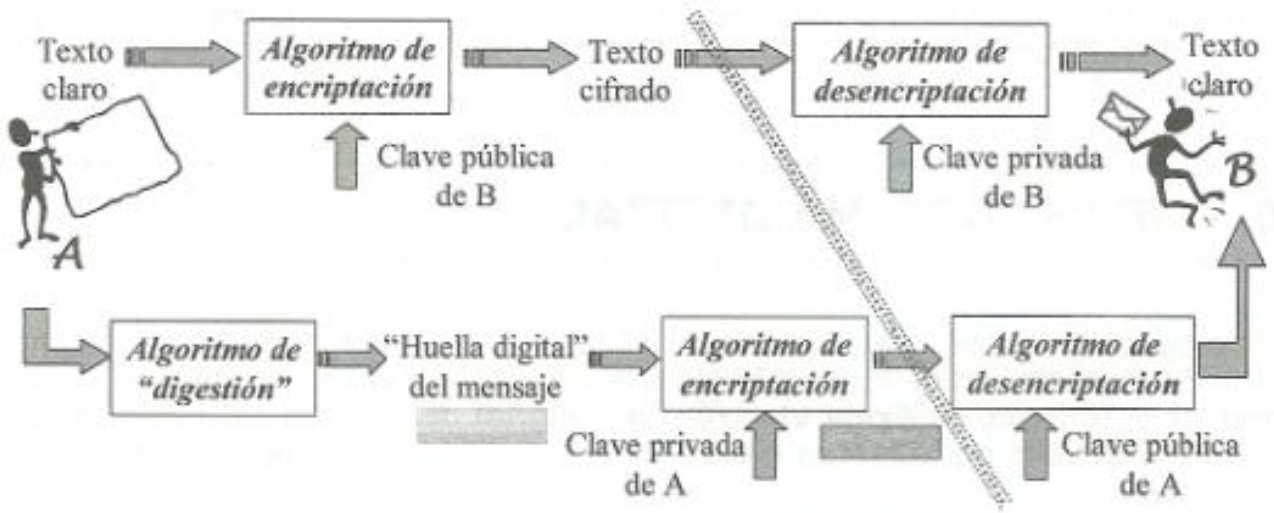


Figura 1.19. Utilización de la firma electrónica o digital (I)

SEGURIDAD INFORMÁTICA

- Firmas y certificados (¿Qué es la firma digital?):
  - Procedimiento seguido por un usuario B para comprobar la autenticidad e integridad del mensaje:
    - Recupera el mensaje original descifrando el texto cifrado con su clave privada. Como sólo el conoce esta clave, se garantiza la confidencialidad en la red informática.
    - Aplica un algoritmo de digestión (algoritmo hash) para generar la huella digital del mensaje que acaba de recibir.
    - Utiliza la clave pública de A para descifrar la huella digital del mensaje original. Esta huella digital ha sido cifrada por el usuario A con su clave privada (constituía la firma digital de A sobre el mesaje original).
    - Compara la huella digital descifrada con la que acaba de generar a partir del mensaje recibido y, si ambas coinciden, podrá estar seguro de que el mensaje es auténtico y se ha respetado su integridad.

SEGURIDAD INFORMÁTICA

- Firmas y certificados (¿Qué es la firma digital?):
  - Procedimiento seguido por un usuario B para comprobar la autenticidad e integridad del mensaje:

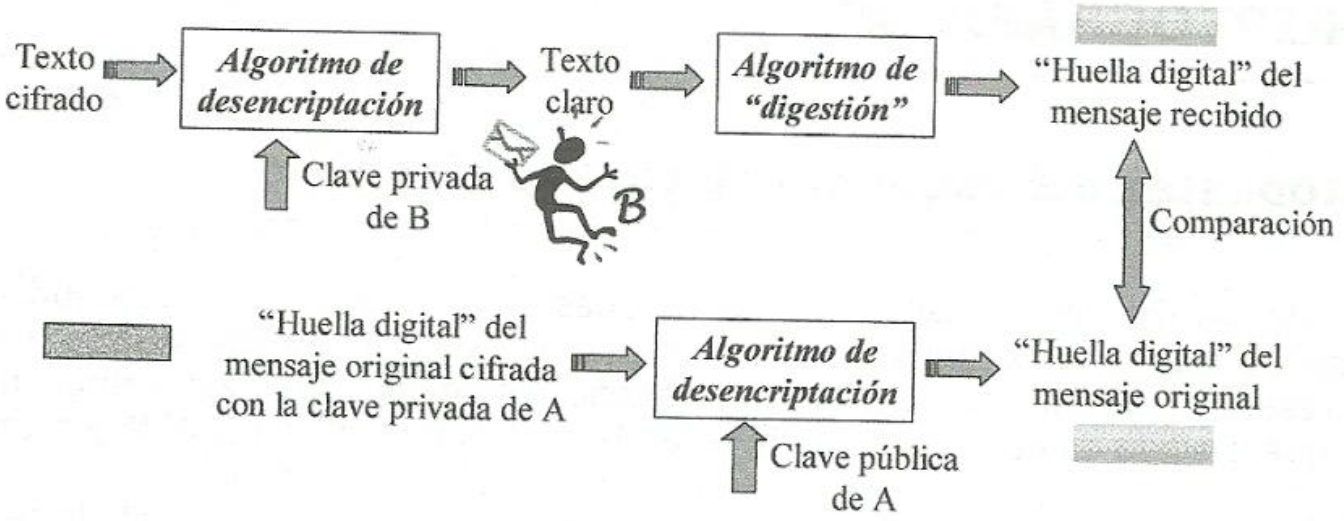


Figura 1.20. Utilización de la firma electrónica o digital (II)

SEGURIDAD INFORMÁTICA

- Firmas y certificados (¿Qué es la firma digital?):
  - Con el esquema propuesto, basado en un sistema criptográfico y la firma digital, se consigue garantizar la confidencialidad, la integridad y la autenticación de los mensajes transmitidos:

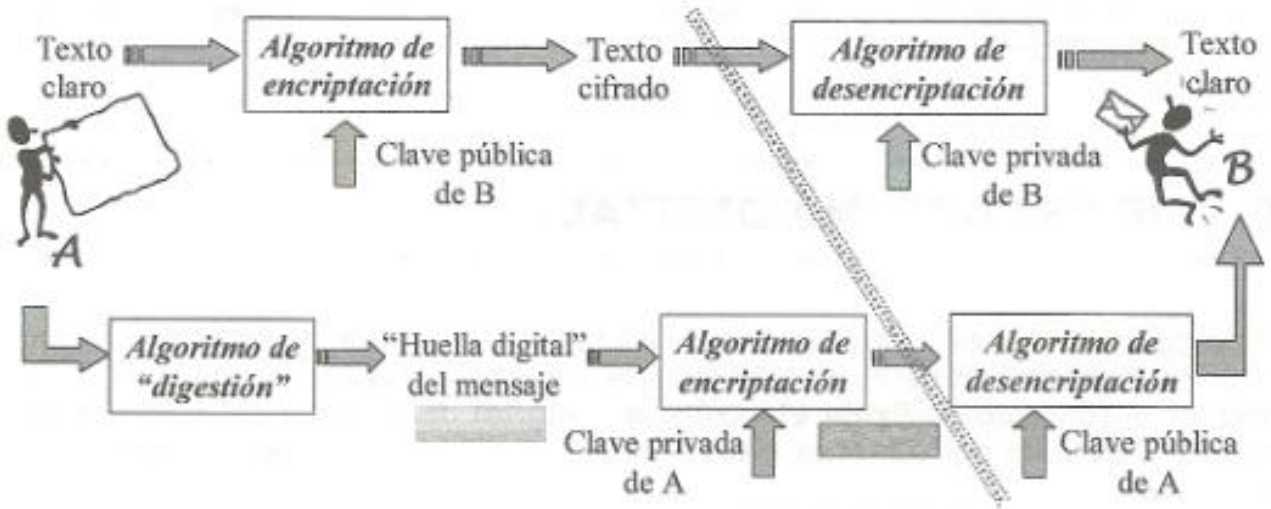
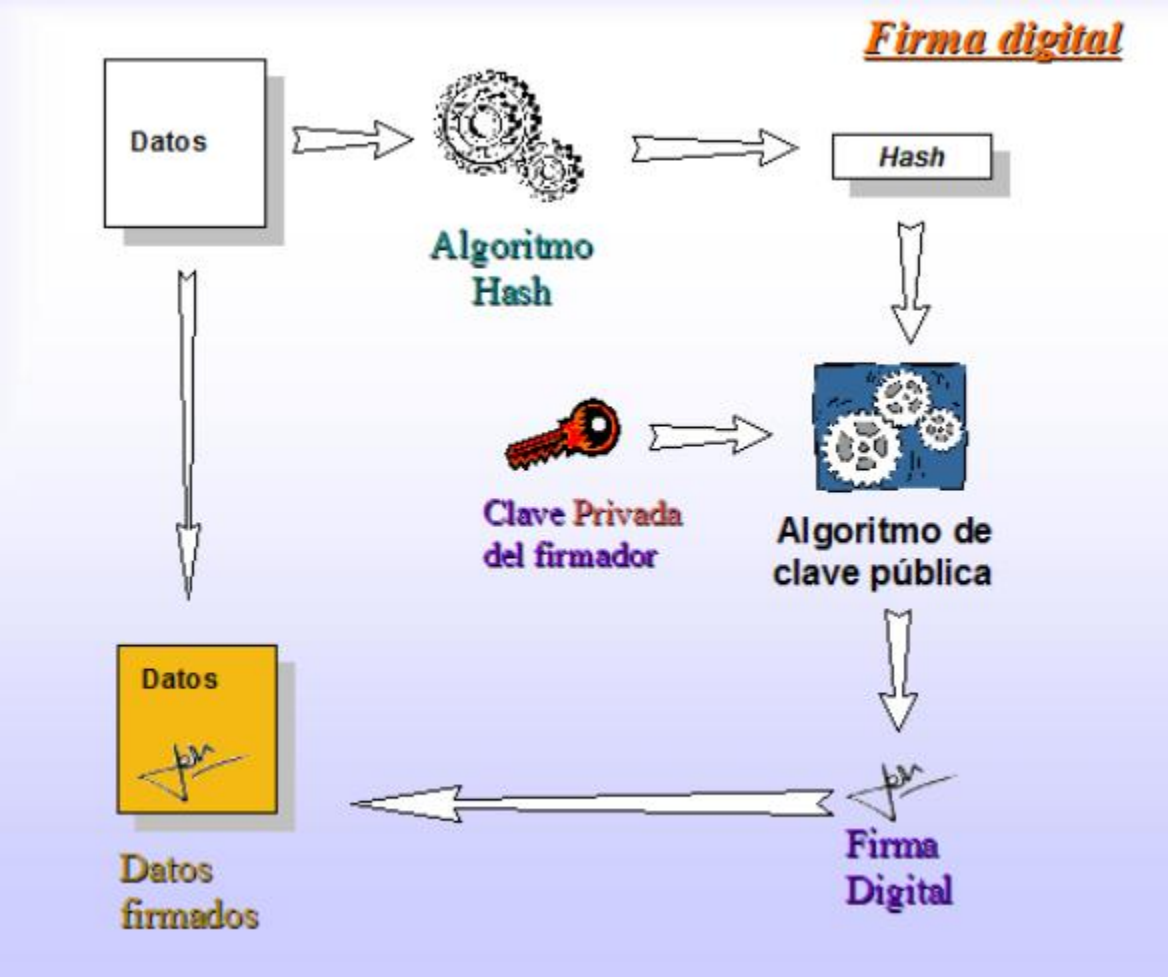


Figura 1.19. Utilización de la firma electrónica o digital (I)

SEGURIDAD INFORMÁTICA

- Firmas y certificados (¿Qué es la firma digital?):
  - Principales características de la firma digital:
    - Es personal, ya que sólo el legítimo propietario la puede generar. La firma digital asocia al firmante con un determinado documento y prueba su participación en el acto de la firma.
    - Se puede considerar que es prácticamente infalsificable.
    - Es fácil de autenticar.
    - Es fácil de generar.
    - Es no repudiable.
    - Además de depender del autor (garantizando de este modo la autenticidad), también depende del mensaje que se firma (garantizando así también su integridad, es decir, la validez del contenido firmado).

SEGURIDAD INFORMÁTICA



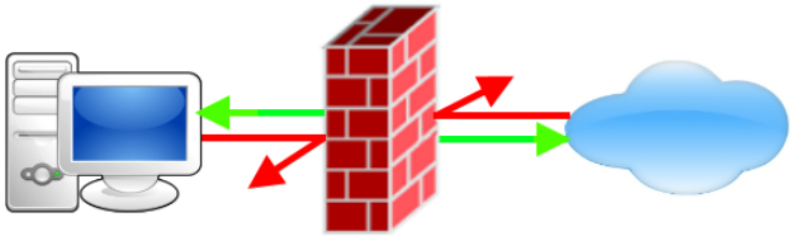
SEGURIDAD INFORMÁTICA

Seguridad activa

Cortafuegos

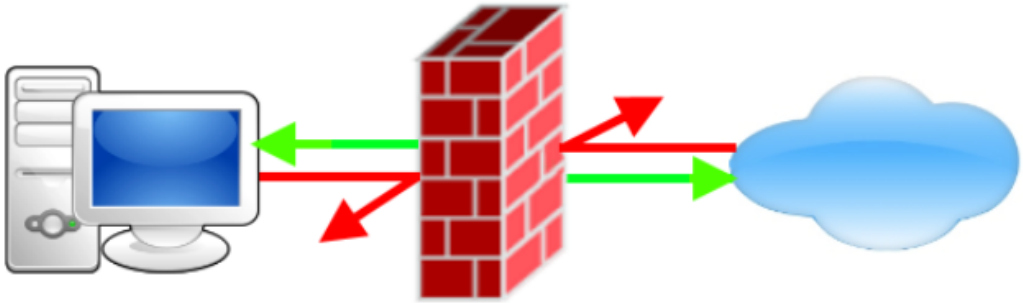
SEGURIDAD INFORMÁTICA

- Cortafuegos:
  - Los cortafuegos (Firewalls) están diseñados para proteger una red interna contra los accesos no autorizados.
  - Un cortafuegos es un gateway (puerta de enlace) con un bloqueo que sólo deja pasar los paquetes de información que pasan una o varias inspecciones de seguridad.



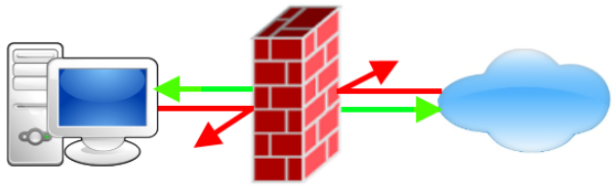
SEGURIDAD INFORMÁTICA

- Cortafuegos:
  - Aunque los cortafuegos (firewalls) son las herramientas o elementos más utilizadas a la hora de establecer seguridad, estos aparatos sólo son utilizados por las grandes organizaciones.



SEGURIDAD INFORMÁTICA

- Cortafuegos:
  - Como ya hemos dicho, un cortafuegos es el mecanismo encargado de proteger una red confiable de una que no lo es (por ejemplo Internet).
  - Un cortafuegos puede consistir en distintos dispositivos, tendientes a los siguientes objetivos:
    - Todo el tráfico desde dentro hacia fuera, y viceversa, debe pasar a través de él.
    - Sólo el tráfico autorizado, definido por la política local de seguridad, es permitido.



SEGURIDAD INFORMÁTICA

- Cortafuegos:
  - Algunos cortafuegos aprovechan esta capacidad de que toda la información entrante y saliente debe pasar a través de ellos para proveer servicios de seguridad adicionales como la encriptación del tráfico de la red.

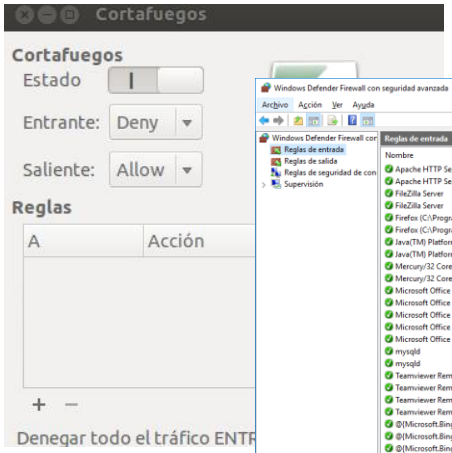
SEGURIDAD INFORMÁTICA

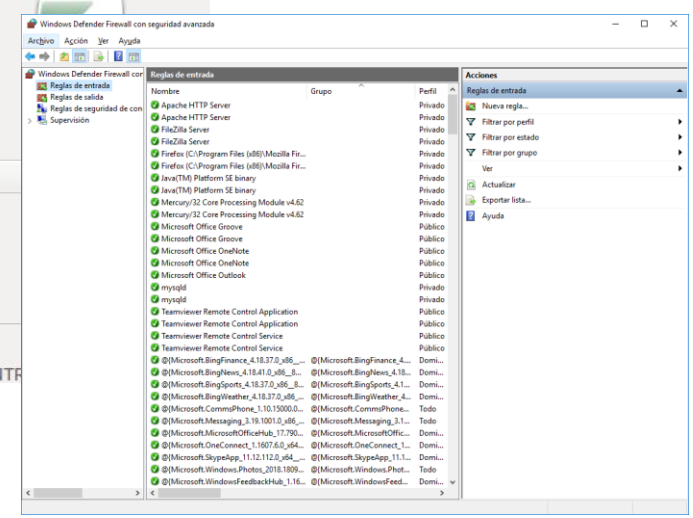
- Cortafuegos:

  - Como puede observarse, los cortafuegos, sólo sirven de defensa perimetral de las redes, no defienden de ataques o errores provenientes del interior, así como tampoco pueden ofrecer protección una vez que el intruso lo traspasa. Por eso, es conveniente, complementar el trabajo del cortafuegos con una defensa interna.
  - El cortafuegos tampoco provee de herramientas contra la filtración de software o archivos infectados con virus, aunque es posible dotar, a la máquina donde se aloja el cortafuegos, de antivirus apropiados.

SEGURIDAD INFORMÁTICA

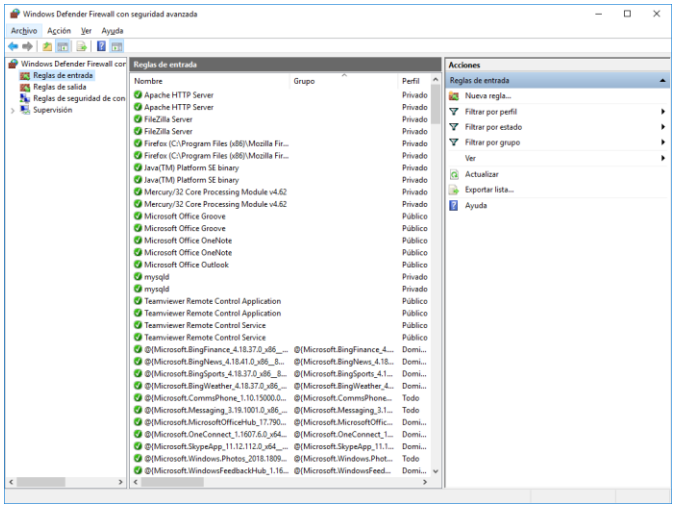
- Cortafuegos:
  - Importante: Aunque se ha hablado de los cortafuegos dentro del apartado del software de seguridad informática, hay que decir que, los cortafuegos pueden ser soluciones hardware o software.





SEGURIDAD INFORMÁTICA

- Ejercicios:
  - Ejercicio cortafuegos windows.
  - Ejercicio cortafuegos iptables.



SEGURIDAD INFORMÁTICA

Seguridad pasiva

SEGURIDAD INFORMÁTICA

- Se entiende por seguridad informática el conjunto de normas, procedimientos y herramientas, que tienen como objetivo garantizar la disponibilidad, integridad, confidencialidad y buen uso de la información que reside en un sistema de información..

- Desde el punto de vista del momento preciso de actuación:
  - Seguridad activa.
  - Seguridad pasiva.

SEGURIDAD INFORMÁTICA

- Se entiende por seguridad informática el conjunto de normas, procedimientos y herramientas, que tienen como objetivo garantizar la disponibilidad, integridad, confidencialidad y buen uso de la información que reside en un sistema de información.

- Desde el punto de vista del momento preciso de actuación:
  - Seguridad activa.
  - **Seguridad pasiva**: actúa después del percance, minimizando los efectos ocasionados por el mismo. La seguridad pasiva complementa a la seguridad activa y se encarga de minimizar los efectos que haya ocasionado algún percance.

SEGURIDAD INFORMÁTICA

- Se entiende por seguridad informática el conjunto de normas, procedimientos y herramientas, que tienen como objetivo garantizar la disponibilidad, integridad, confidencialidad y buen uso de la información que reside en un sistema de información..

- Técnicas de seguridad pasiva:
  - Uso de hardware y dispositivos físicos de protección adecuados.
  - Realización de copias de seguridad.
  - Particiones del disco duro.
  - Conjunto de discos redundantes.

SEGURIDAD INFORMÁTICA

Seguridad pasiva

Uso de hardware y dispositivos físicos de protección adecuados

SEGURIDAD INFORMÁTICA

- Uso de hardware y dispositivos físicos de protección adecuados:
  - Ningún sistema de seguridad, ni siquiera el más sofisticado, puede garantizar al cien por ciento una protección completa de los datos.
  - Un pico o una caída de tensión pueden limpiar en un instante hasta el dato más cuidadosamente guardado. Entre los dispositivos físicos que se pueden utilizar para aumentar la seguridad se pueden citar:
    - Sistemas de alimentación ininterrumpida (SAI).
    - Protectores de sobrecarga.

SEGURIDAD INFORMÁTICA

- Uso de hardware y dispositivos físicos de protección adecuados:
  - Entre los dispositivos físicos que se pueden utilizar para aumentar la seguridad se pueden citar:
    - **Sistemas de alimentación ininterrumpida (SAI)**: Un SAI se utiliza para proteger a los ordenadores contra la perdida de datos durante una caída de tensión.
    - **Protectores de sobrecarga**: Los protectores de sobrecarga protegen los equipos contra los dañinos picos de tensión, evitando así costosas reparaciones posteriores.

SEGURIDAD INFORMÁTICA

- Sistemas de alimentación ininterrumpida (SAI):
  - Un **sistema de alimentación ininterrumpida** (SAI) es un dispositivo que gracias a sus baterías u otros elementos almacenadores de energía, puede proporcionar energía eléctrica por un tiempo limitado y durante un apagón eléctrico a todos los dispositivos que tenga conectados.

SEGURIDAD INFORMÁTICA

- Sistemas de alimentación ininterrumpida (SAI):
  - Una vez que la corriente se pierde, las baterías del SAI se ponen en funcionamiento proporcionando la corriente necesaria para el correcto funcionamiento del sistema.
  - Otras de las funciones que se pueden adicionar a estos equipos es la de mejorar la calidad de la energía eléctrica que llega a las cargas, filtrando subidas y bajadas de tensión y eliminando armónicos de la red en el caso de usar corriente alterna.

SEGURIDAD INFORMÁTICA

- Protectores de sobrecarga:
  - Los protectores de sobrecarga, aunque no sirven durante un apagón, protegen los equipos contra los dañinos picos de tensión, evitando así costosas reparaciones posteriores.

SEGURIDAD INFORMÁTICA

Seguridad pasiva

Realización de copias de seguridad

SEGURIDAD INFORMÁTICA

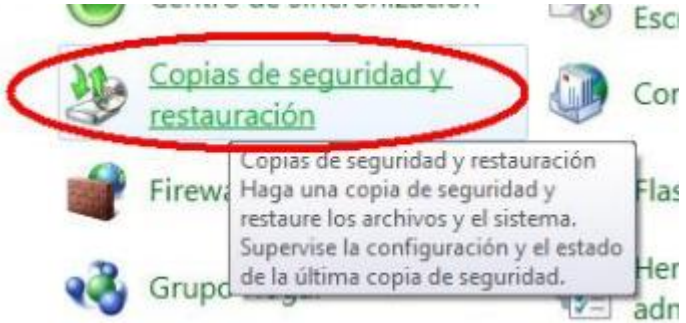
- Realización de copias de seguridad (backup):
  - Ningún sistema de seguridad puede garantizar al cien por ciento una protección completa de los datos.
  - Cualquier sistema de seguridad completo debe incluir un plan de recuperación en el caso de producirse un desastre. La técnica más utilizada es llevar a cabo copias de seguridad regulares.
  - Las copias de seguridad son una manera de proteger la inversión realizada en los datos. La pérdida de información no es tan importante si existen varias copias resguardadas.

SEGURIDAD INFORMÁTICA

- ¿Por qué son útiles las copias de seguridad?:
  - Para restaurar un ordenador a un estado operacional después de un desastre (copias de seguridad del sistema)
  - Para restaurar un pequeño número de ficheros después de que hayan sido borrados o dañados accidentalmente (copias de seguridad de datos).
  - En el mundo de la empresa, además es útil y obligatorio, para evitar ser sancionado por los órganos de control en materia de protección de datos.

SEGURIDAD INFORMÁTICA

- Realización de copias de seguridad (backup):
  - Normalmente las copias de seguridad se suelen hacer en cintas magnéticas, aunque dependiendo de la cantidad y tipo de información también pueden utilizarse disquetes, CD, DVD, Discos Zip, Jaz o magnéticos-ópticos, pendrivers o pueden realizarse sobre un centro de respaldo remoto propio o vía Internet.



SEGURIDAD INFORMÁTICA

- Realización de copias de seguridad (backup):
  - Las copias de seguridad en un sistema informático tienen por objetivo el mantener cierta capacidad de recuperación de la información ante posibles pérdidas.
  - Las copias de seguridad suelen ser utilizadas como la última línea de defensa contra pérdida de datos, y se convierten por lo tanto en el último recurso a utilizar.

SEGURIDAD INFORMÁTICA

Seguridad pasiva

Particiones del disco duro

SEGURIDAD INFORMÁTICA

- Particiones del disco duro:
  - Una **partición de disco**, en mantenimiento, es el nombre genérico que recibe cada división presente en una sola unidad física de almacenamiento de datos.
  - Toda partición tiene su propio sistema de archivos (formato) y generalmente, casi cualquier sistema operativo interpreta, utiliza y manipula cada partición como un disco físico independiente, a pesar de que dichas particiones estén en un solo disco físico.

SEGURIDAD INFORMÁTICA

- Particiones del disco duro:
  - Las razones principales para tener más de una partición de disco suelen ser:
    - Tener más de un sistema operativo en el ordenador.
    - Conseguir una mejor distribución del contenido (normalmente con una partición para el sistema operativo y las aplicaciones y otra para los documentos y archivos del usuario).

SEGURIDAD INFORMÁTICA

- Ventajas del uso de particiones:
  - Generalmente, en una de las particiones se mantiene el sistema operativo y en la otra los archivos del usuario (documentos, correos electrónicos, etc.).
  - La principal ventaja del uso de particiones es que si se necesita formatear e instalar de cero el sistema por cualquier inconveniente, simplemente se procede a formatear la partición que contiene el sistema operativo, dejando intacta la otra.

SEGURIDAD INFORMÁTICA

- Dado que si se rompe el disco duro pueden verse afectadas las dos particiones, no suele ser buena idea utilizar una partición como respaldo. Siempre es conveniente utilizar como respaldo otra unidad de almacenamiento.

SEGURIDAD INFORMÁTICA

Seguridad pasiva

Conjunto de discos redundantes

SEGURIDAD INFORMÁTICA

- Conjunto de discos redundantes:
  - La utilización de un conjunto de discos redundantes permite restaurar la información que no es válida ni consistente.
  - Los sistemas más comúnmente utilizados son los sistemas RAID (Matriz redundante de discos independientes). Se trata a grandes rasgos de almacenar simultáneamente la información en varios de estos discos a la vez con el objeto de que en caso de que se produzca un fallo se pueda utilizar alguno de los discos donde se guardo la información.

SEGURIDAD INFORMÁTICA

Actividades

SEGURIDAD INFORMÁTICA

FIN

Muchas gracias por su atención