UD10: Seguridad en SI

Sistemas Informáticos

Objetivos de la seguridad informática

Se basa en 3 principios:

CONFIDENCIALIDAD

INTEGRIDAD

DISPONIBILIDAD

Y dos secundarios:

AUTENTICIDAD Y NO REPUDIO

Objetivos de la seguridad informática:
CONFIDENCIALIDAD

Solo se permite el acceso a la información, a los sistemas y a los recursos a aquellos usuarios o procesos autorizados.

"La confidencialidad es la capacidad de garantizar que la información, almacenada en el sistema informático o transmitida por la red, solamente va a estar disponible para aquellas personas autorizadas a acceder a dicha información, es decir, que si los contenidos fueran sustraídos (por ejemplo, robo de un portátil de la empresa), estos no podrán ser interpretados."

¿Cómo garantizar la confidencialidad?

- Restringiendo el acceso a la información, mediante software (autenticación al entrar) o mediante seguridad física (guarda en un Centro de Procesamiento de Datos).
- Criptografía en la transmisión de datos o en el almacenamiento.

Objetivos de la seguridad informática:Integridad

La modificación de la información o recursos debe realizarse por procesos o usuarios autorizados.

"La integridad es la capacidad de garantizar que los datos no serán alterados sin autorización. Por ejemplo, en una transmisión de información por red (transacción bancaria, compra online, etc.), los datos enviados en el origen, deberán ser los mismo que los recibidos en el destino."

¿Cómo garantizar la integridad?

- Evitar las modificaciones (y pérdidas) accidentales. Uso de RAID
- Asegurar que la información es realmente la que debe ser y que no ha sido modificada por usuarios no autorizados. CRC (verificación por redundancia cíclica) y criptografía.
- Subsanar las modificaciones no intencionadas que pueden ser realizadas por usuarios autorizados, sea por error o por desconocimiento. Copias de seguridad

Objetivos de la seguridad informática: disponibilidad

La información debe estar en el lugar, momento y forma requeridos por cualquier usuario autorizado.

"La disponibilidad es la capacidad de garantizar que tanto el sistema como los datos van a estar disponibles en todo momento para los usuarios autorizados. Esto será muy importante, por ejemplo, para las empresas que dan servicios online."

¿Cómo garantizar la disponibilidad?

- Redundancia de la información
- Distribución de la información

Objetivos de la seguridad informática:
AUTENTICIDAD Y NO REPUDIO

Confirmar la identidad del emisor y/o el receptor

*"**La autenticación** y el control de acceso que permite verificar la identidad de quien accede a un recurso y se le permite o no el acceso según dicha identidad."*

*"**El no repudio** permite probar la participación de las partes en una comunicación permitiendo por tanto la auditoría de la información". En toda comunicación, existe un emisor y un receptor, por lo que podemos distinguir dos tipos de no repudio:*

No repudio en origen: el emisor no puede negar el envío. La prueba la crea el propio emisor y la recibe el destinatario.

No repudio en destino: el receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción. En este caso la prueba irrefutable la crea el receptor y la recibe el emisor.

¿Cómo los garantizo ?

- Autenticación web
  - Proceso inicial de usuario y contraseña
- Autenticación de un documento
  - Firma electrónica (autenticidad y fecha de última modificación)
- Autenticación biométrica
  - Huella dactilar, reconocimiento facial, reconocimiento ocular, reconocimiento de voz…

Políticas de Seguridad

Para alcanzar **los objetivos** se deben establecer unas políticas de seguridad a partir de planes de contingencia y seguridad basándose en los elementos a proteger.
Para ello, periódicamente es necesario un análisis de riesgos: evaluar recursos, infraestructuras de red y los sistemas, estableciendo sus puntos débiles para definir planes de contingencia y seguridad, con los criterios y métodos para abordar la seguridad.

Aspectos sobre las políticas anteriores:

- Empleo de contraseñas robustas y su actualización periódica
- Uso de aplicaciones conocidas y actualizadas
- No difusión de cuentas y contraseñas a terceros
- Actualización del sistema operativo
- Creación y mantenimiento de las copias de seguridad
- Protección antimalware
- Control de acceso físico a los sistemas y medios de red
- Configuración segura de las redes inalámbricas

Políticas de Seguridad

Autenticación, que permite identificar al emisor de un mensaje, al creador de un documento o al equipo que se conecta a una red o a un servicio.

Autorización, que controla el acceso de los usuarios a zonas restringidas, a distintos equipos y servicios después de haber superado el proceso de autenticación.

Auditoría, que verifica el correcto funcionamiento de las políticas o medidas de seguridad tomadas.

Encriptación, que ayuda a ocultar la información transmitida por la red o almacenada en los equipos.

Realización de **copias de seguridad** e **imágenes de respaldo**, para que en caso de fallos nos permita la recuperación de la información perdida o dañada.

Antivirus, como su nombre indica, consiste en un programa que nos permite estar protegido contra las amenazas de los virus.

Cortafuegos o firewall, programa que audita y evita los intentos de conexión no deseados en ambos sentidos, desde los equipos hacia la red y viceversa.

Servidores proxys, los cuales hacen de intermediario entre la red interna de una empresa y una red externa, como puede ser Internet. Estos servidores, entre otras acciones, auditan y autorizan los accesos de los usuarios a distintos tipos de servicios como el de FTP (transferencia de ficheros), o el Web (acceso a páginas de Internet).

Utilización de **firma electrónica o certificado digital**, son mecanismos que garantizan la identidad de una persona o entidad, consiguiendo el objetivo del no repudio en las comunicaciones. También se utilizan mucho hoy en día para establecer comunicaciones seguras entre el PC del usuario y los servidores de Internet como las páginas Web de los bancos.

Conjunto de **leyes** encaminadas a la protección de datos personales que obligan a las empresas a asegurar su confidencialidad.

Clasificación de la seguridad

Se pueden hacer diversas clasificaciones de la seguridad informática en función de distintos criterios:

Según el activo a proteger

- **Lógica**
- **Física**

según se actúe antes de producirse el percance evitando los daños o después del percance minimizando los efectos dañinos

- **Activa**
- **Pasiva**

Seguridad física y lógica

La seguridad física es aquella que trata de proteger al hardware (los equipos informáticos, el cableado, etc.) de los posibles desastres naturales (terremotos, huracanes, etc.), de incendios, inundaciones, sobrecargas eléctricas, de robos y un sinfín de amenazas más.

Amenazas	Mecanismos de defensa
Incendios	• El mobiliario de los centros de datos debe ser ignífugo. • Evitar la localización del CPD cerca de zonas donde se manejen o almacenen sustancias inflamables o explosivos • Deben existir sistemas anti-incendios, detectores de humos, extintores... para sofocar el incendio en el menor tiempo posible y evitar que se propague.
Inundaciones	• Evitar la ubicación de los centros de cálculo en las plantas bajas de los edificios para protegerse de la entrada de aguas superficiales. • Impermeabilizar paredes y techos del Centro de Cálculo.
Robos	• Proteger los centros de cálculo mediante accesos con medidas biométricas, cámaras de seguridad, vigilantes para evitar la entrada de personal no autorizado.
Señales Electromagnéticas	• Evitar la ubicación de los centros de cálculo próximos a lugares con gran radiación de señales electromagnéticas, pues pueden interferir en el correcto funcionamiento de los equipos informáticos del cableado de red. • En caso de no poder evitar estas ubicaciones, proteger el centro mediante el uso de filtros o de cableado especial, o si es posible, utilizar fibra óptica.
Apagones	• Utilizar sistemas de alimentación ininterrumpida (SAI). Que proporcionan corriente eléctrica durante un periodo de tiempo suficiente.
Sobrecargas eléctricas	• Además de proporcionar alimentación, los SAI profesionales incorporan filtros para evitar picos de tensión, y así, estabilizar la señal eléctrica.
Desastres naturales	• Estar en continuo contacto con el Instituto Geográfico Nacional y de Meteorología, organismos que informan sobre los movimientos sísmicos y meteorológicos en España.

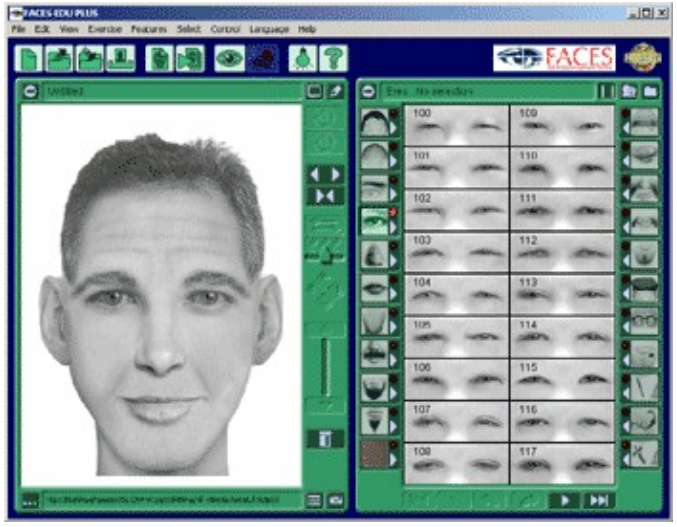
Seguridad física y lógica

Sistemas biométricos

Los sistemas biométricos consisten en la utilización de sistemas automáticos para la clasificación y/o reconocimiento de rasgos personales de identificación. Se clasifican en los siguientes tipos:

- Rasgos fisiológicos: huellas dactilares, geometría de la mano/dedo, iris, ADN, etc
- Rasgos del comportamiento: voz, firma, modo de teclear, modo de andar, etc.

El principal riesgo que se deriva de los sistemas biométricos es la suplantación de identidad mediante la imitación (voz, cara) o la reproducción (huella, iris) del rasgo a reconocer.



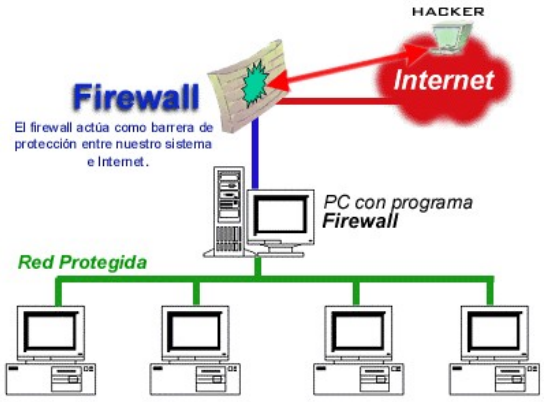
Seguridad física y lógica

La seguridad lógica complementa a la seguridad física, protegiendo el software de los equipos informáticos (aplicaciones y datos) de usuarios, de robos, de pérdidas de datos, de entrada de virus informáticos, de modificaciones no autorizadas, de ataques desde la red, etc.

Amenazas	Mecanismos de defensa
Robos	• Cifrar la información almacenada en los soportes para que en caso de robo no sea legible. • Utilizar contraseñas para evitar el acceso a la información. • Sistemas biométricos (uso de huella dactilar, tarjetas identificadoras, ...)
Pérdida de información	• Realizar copias de seguridad para poder restaurar la información perdida. • Uso de sistemas tolerantes a fallos, elección del sistema de ficheros del sistema operativo adecuado. • Uso de conjunto de discos redundantes, protege contra la pérdida de datos y proporciona la recuperación de los datos en tiempo real.
Pérdida de integridad de la información	• Uso de programas de chequeo del equipo, SiSoft Sandra 2000, TuneUp... • Mediante la firma digital en el envío de información a través de mensajes enviados por la red. • Uso de la instrucción del SO Windows, sfc (System file checker).
Entrada de Virus	• Uso de Antivirus, que evite que se infecten los equipos con programas malintencionados.
Ataques desde la red	• Firewall, autorizando y auditando las conexiones permitidas. • Programas de monitorización. • Servidores Proxys, autorizando y auditando las conexiones permitidas.
Modificaciones no autorizadas	• Uso de contraseñas que no permitan el acceso a la información. • Uso de listas de control de acceso. • Cifrar documentos.

Seguridad activa y pasiva

La **seguridad activa** la podemos definir como el conjunto de medidas que previenen e intentan evitar los daños en los sistemas informáticos.



Técnicas	¿qué previene?
Uso de contraseña	• El acceso a recursos por parte de personas no autorizadas.
Listas de control de acceso	• El acceso a los ficheros por parte de personas no autorizadas.
Encriptación	• Evitan que personas sin autorización puedan interpretar la información.
Uso de software de seguridad informática	• Virus informáticos y entradas indeseadas al sistema informático.
Firmas y certificados digitales	• Permite comprobar la procedencia, autenticidad e integridad d ellos mensajes.
Sistemas de ficheros con tolerancia a fallos	• Fallos de integridad en caso de apagones de sincronización o comunicación.
Cuotas de disco	• Qué ciertos usuarios hagan un uso indebido de la capacidad de disco.

Seguridad activa y pasiva

La **seguridad pasiva** complementa a la seguridad activa y se encarga de minimizar los efectos que haya ocasionado algún percance.

Técnicas	¿Cómo minimiza?
Conjunto de discos redundantes	Podemos restaurar información que no es válida ni consistente.
SAI	Una vez que la corriente se pierde, las baterías del SAI se ponen en funcionamiento proporcionando la corriente necesaria para mantener los equipos encendidos el tiempo necesario para guardar la información una vez que se ha producido el desastre (el apagón de luz).
Realización de copias de seguridad	A partir de las copias realizadas, podemos recuperar información en caso de pérdida de datos.

Amenazas

Las amenazas a un sistema informático pueden provenir desde un hacker remoto que entra en nuestro sistema con un troyano, pasando por un programa descargado gratuitamente que nos ayuda a gestionar nuestras fotos pero que supone una puerta trasera a nuestro sistema permitiendo la entrada a espías, hasta la entrada no deseada al sistema mediante contraseñas de bajo nivel de seguridad.

El objetivo final de la seguridad es proteger lo que la empresa posee. Todo aquello que es propiedad de la empresa se denomina **activo**. Un activo puede ser:

- el mobiliario de la oficina (sillas, mesas, estanterías, etc.)
- los equipos informáticos (servidores, ordenadores, impresoras, etc.)
- los datos que se manejan (datos de clientes, facturas, personal, etc.).

Cualquier daño que se produzca sobre estos activos tendrá un impacto en la empresa y supone una amenaza.

La seguridad de un sistema real nunca será completa, pero el uso de buenas políticas de seguridad es imprescindible para evitar y minimizar los daños.

Amenazas: Vulnerabilidades

Una **vulnerabilidad** es cualquier fallo que compromete la seguridad del sistema, y un **riesgo** es la posibilidad de que se produzca un impacto negativo para la empresa aprovechando alguna de sus vulnerabilidades. Son una puerta abierta para posibles ataques, de ahí que sea tan importante tenerlas en cuenta pues en cualquier momento podrían ser aprovechadas.

Los pasos a seguir para mejorar la seguridad son los siguientes:

- **Identificar los activos**, es decir, los elementos que la empresa quiere proteger.
- **Evitar los riesgos**, considerando el impacto que puede tener la perdida de los datos sobre los activos del sistema.
- **Diseñar el plan de actuación**, que debe incluir:
  - Las medidas que traten de minimizar el impacto de los daños ya producidos (seguridad pasiva)
  - Las medidas que traten de prevenir los daños minimizando la existencia de vulnerabilidades (seguridad activa)
  - Revisar periódicamente las medidas de seguridad adoptadas.

Amenazas: Vulnerabilidades

Podemos diferenciar tres tipos de vulnerabilidades según cómo afectan a nuestro sistema:

Vulnerabilidades ya conocidas sobre aplicaciones o sistemas instalados. Son vulnerabilidades de las que ya tienen conocimiento las empresas que desarrollan el programa o sistema al que afecta, y para las cuales, ya existe una solución, que se publica en forma de parche o actualización explícita.

Vulnerabilidades conocidas sobre aplicaciones no instaladas. Estas vulnerabilidades también son conocidas por las empresas desarrolladoras de la aplicación, pero puesto que nosotros no tenemos dicha aplicación instalada no tendremos que actuar.

Vulnerabilidades aún no conocidas. Estas vulnerabilidades aún no han sido detectadas por la empresa que ha desarrollado el programa que podemos tener instalado, por lo que, si otra persona ajena a dicha empresa detectara alguna, podría utilizarla contra todos los equipos que tienen instalado ese software.

Amenazas: Vulnerabilidades

Lograr que los sistemas y redes operen con seguridad resulta primordial para cualquier empresa y organismo. Esto ha llevado a que empresas como Microsoft dispongan de departamentos dedicados exclusivamente a la seguridad, como es **Microsoft Security Response Center (MSRC)**. Sus funciones son, entre otras, evaluar los informes que los clientes proporcionan sobre posibles vulnerabilidades en sus productos, y preparar y divulgar revisiones y boletines de seguridad que respondan a estos informes. Para ello **clasifica** las vulnerabilidades **en función de su gravedad**, lo que nos da una idea de los efectos que pueden tener en los sistemas.

Codificación	Definición
Crítica	Vulnerabilidad que puede permitir la propagación de una amenaza de Internet sin la acción del usuario.
Importante	Vulnerabilidad que puede poner en peligro la confidencialidad, integridad o disponibilidad de los datos de los usuarios, o bien, la integridad o disponibilidad de los recursos de procesamiento.
Moderada	El impacto se puede reducir en gran medida a partir de factores como configuraciones predeterminadas, auditorías o la dificultad intrínseca en sacar partido a la vulnerabilidad.
Baja	Vulnerabilidad muy difícil de aprovechar o cuyo impacto es mínimo.

Amenazas: Vulnerabilidades. Auditoría

Una auditoría de seguridad informática o auditoría de seguridad de sistemas de información es **el estudio** que comprende el análisis y gestión de sistemas para **identificar** y posteriormente **corregir** las diversas **vulnerabilidades** que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servidores.

Los resultados, se detallan, archivan y reportan a los responsables

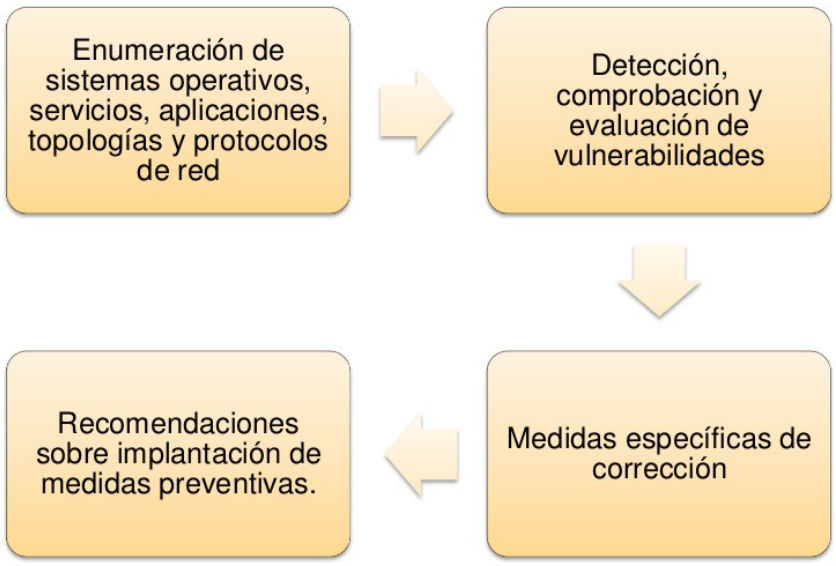
establecer medidas preventivas de refuerzo, aprendiendo de los errores cometidos con anterioridad.

Los objetivos:

- Revisar la seguridad de los entornos y sistemas.
- Verificar el cumplimiento de la normativa y legislación vigentes.
- Elaborar un informe independiente.

Amenazas: Vulnerabilidades. Auditoría

Constan de las siguientes fases:



Auditoría de seguridad interna: se contrasta el nivel de seguridad de las redes locales y corporativas de carácter interno.

Auditoría de seguridad perimetral: se estudia el perímetro de la red local o corporativa, conectado a redes públicas.

Test de intrusión: se intenta acceder a los sistemas, para comprobar el nivel de resistencia a la intrusión no deseada.

Análisis forense: análisis posterior de incidentes (recogida de evidencias del sistema de información), mediante el cual se trata de reconstruir cómo se ha penetrado en el sistema, a la par que se valoran los daños ocasionados. Si los daños han provocado la inoperatividad del sistema, se denomina análisis post-mórtem

Amenazas: Ataques

Un **ataque** es una acción ofensiva y deliberada con el objetivo de alterar el funcionamiento del sistema, provocar daños en éste o sustraer información sensible. Pueden ser:

- **Activos**: ocasionan cambios en la información o los recursos
- **Pasivos**: monitorizan, registran o acceden a los recursos, sin alterarlos

Podemos clasificar también estos ataques por:

- El tipo de atacante
- Cómo actúa el atacante

Ataques más usuales

- Reconocimiento y detección de vulnerabilidades en los sistemas: tratan de obtener información del sistema, sin provocar daño alguno, de vulnerabilidades para su posterior explotación
- Interceptación de información, vulnerando la confidencialidad
- Modificación de información, reenviando documentos alterados previamente interceptados.
- Suplantación de identidad
    - Capturas de cuentas de usuario y contraseña
    - IP spoofing, DNS spoofing, SMTP spoofing

Amenazas: Ataques

Según el tipo de atacante

Tipo	Definición
Hackers	Expertos informáticos con una gran curiosidad por descubrir las vulnerabilidades de los sistemas pero sin motivación económica o dañina.
Crackers	Hackers con intención maliciosa, cuando rompe la seguridad de un sistema lo hace o bien para dañar o para obtener un beneficio económico.
Phreakers	Crackers telefónicos, que sabotean redes de telefonía para conseguir llamadas gratuitas.
Sniffers	Expertos en redes que analizan el tráfico para obtener información de los paquetes que se transmiten por la red.
Lammers	Sin grandes conocimientos de informática pero se consideran Hackers y alardean de ello.
Newbie	Hacker novato.
Ciber terrorista	Expertos en informática e intrusiones en la red que trabajan para países y organizaciones como espías y saboteadores informáticos.
Programador de virus	Expertos en programación, redes y sistemas que crean programas dañinos que producen efectos no deseados en los sistemas o aplicaciones.
Carders	Personas que se dedican al ataque de los sistemas de tarjetas, como los cajeros automáticos.

Según cómo actúa el atacante

Tipos	Definición
Spoofing	Suplanta la identidad de un PC o algún dato del mismo (como su dirección MAC)
Sniffing	Monitoriza y analiza el tráfico de la red para hacerse con información.
Conexión no autorizada	Se buscan agujeros de la seguridad de un equipo o un servidor, y cuando se descubren, se realiza una conexión no autorizada a los mismos.
Malware	Se introducen programas malintencionados (virus, troyanos o gusanos) en nuestro equipo, dañando el sistema de múltiples formas.
Keyloggers	Se utiliza una herramienta que permite conocer todo lo que el usuario envía a través del teclado, e incluso puede realizar capturas de pantalla.
Denegación de servicio	Interrumpen el servicio que se está ofreciendo en servidores o en redes de ordenadores. También denominado DoS (denial of service)
Ingeniería social	Se obtiene información confidencial de una persona u organismo para utilizarla con fines maliciosos. (Phising y Spam)
Phising	Se engaña al usuario para obtener su información confidencial suplantando la identidad de un organismo o páginas Web de Internet.
Spam	Correo o mensaje basura, no solicitado, no deseados o de remitente no conocido.
Pharming	Redirigir un nombre de dominio a otra máquina distinta falsificada y fraudulenta.
Pasword cracking	Descifrar contraseñas de sistemas y comunicaciones. Los métodos más comunes son mediante Sniffing, observando directamente la introducción de credenciales (shoulder surfing), ataque por fuerza bruta.
Botnet	Conjunto de robots informáticos o bots, que se ejecutan de manera autónoma en multitud de host, para controlarlos de forma remota.

Amenazas: Mecanismos de seguridad

- **Cortafuegos o firewall**: filtros que gestionan, restringen y limitan el tráfico de paquetes entrante y saliente de una red
- **Redes virtuales o VPN**: creación de una extensión de red local a través de una red pública (como Internet), con el objetivo de tener una conexión virtual segura punto a punto. Entre sus usos:

Navegar de forma anónima **Descargas P2P** **Comunicaciones seguras** **Teletrabajo**

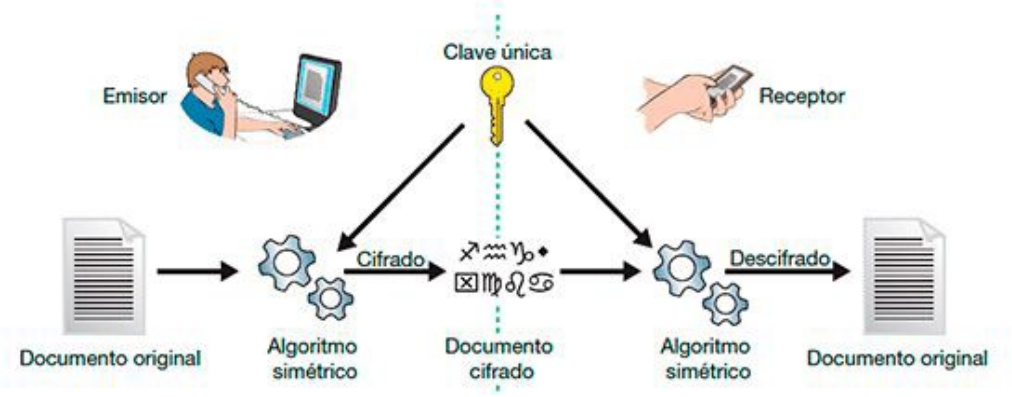
- **Software antimalware**
- **Herramientas de cifrado**: consiste en aplicar un algoritmo que transforme un mensaje a partir de una clave. 2 tipos de cifrado:

  Cifrado simétrico: una clave para cifrar y descifrar

  Cifrado asimétrico: se emplean dos claves, una privada y otra pública. La clave pública cifra el mensaje que solo la clave privada descifra.

Ejemplos de **protocolos seguros**, como SSL/TLS, OpenSSL, HTTPS, SFTP

Amenazas: Mecanismos de seguridad



Alta disponibilidad

Capacidad de que aplicaciones y datos **se encuentren operativos** para los usuarios autorizados **en todo momento** y sin interrupciones, debido principalmente a su **carácter crítico**.
las 24 horas del día, 7 días a la semana, 365 días al año

Las interrupciones previstas,paralizamos el sistema para realizar cambios o mejoras en nuestro hardware o software.

Las interrupciones imprevistas, que suceden por acontecimientos como un apagón, un error del hardware o del software, problemas de seguridad, un desastre natural, virus, accidentes, caídas involuntarias del sistema, etc.

Como ejemplos de sistemas y servicios de alta disponibilidad podemos mencionar los sistemas sanitarios, de control aéreo, de comercio electrónico, bancarios, de transporte marítimo, militares, etc., donde la pérdida o interrupción de conectividad pueden suponer graves consecuencias personales y/o económicas.

Alta disponibilidad

Las métricas para medir la disponibilidad y fiabilidad de un sistema son el tiempo medio entre fallos o **MTTF** (Mean Time To Failure) que mide el tiempo medio transcurrido hasta que un dispositivo falla, y el tiempo medio de recuperación o **MTTR** (Mean Time To Recover) que mide el tiempo medio tomado en restablecerse la situación normal una vez que se ha producido el fallo.

El tiempo de no disponibilidad del servicio, se mide a menudo como el cociente **MTTR / MTTF**. Lógicamente, nuestro principal objetivo es **aumentar** el **MTTF** y **reducir** el **MTTR** de forma que minimicemos el tiempo de no disponibilidad del servicio.

Existen distintos niveles de disponibilidad del sistema, y según el tiempo aproximado de inactividad por año se determina el porcentaje de disponibilidad. El mayor nivel de exigencia de alta disponibilidad acepta 5 minutos de inactividad al año, con lo que se obtiene una disponibilidad de 5 nueves: 99,999%.