SEGURIDAD INFORMÁTICA

Índice

[Tema 1 1](#_Toc85646840)

[Conjunto de medidas y procedimientos: 1](#_Toc85646841)

[Tipos de seguridad: 1](#_Toc85646842)

[MAGERIT clasifica las amenazas de la siguiente manera: 2](#_Toc85646843)

[Principios de seguridad informática: 3](#_Toc85646844)

[Tema 2 6](#_Toc85646845)

[Tema 3 11](#_Toc85646846)

# Tema 1

## Conjunto de medidas y procedimientos:

* **Integridad**: certificar que toda la información y sus métodos de procesos son exactos y completos.
* **Confidencialidad**: asegurar que solo los usuarios autorizados pueden acceder a la información.
* **Disponibilidad**: permitir que la información esté disponible siempre que los usuarios lo necesiten.

## Tipos de seguridad:

* En función de lo que se quiere proteger:
  + **SEGURIDAD FÍSICA:** es la protección física del sistema ante inundaciones, incendios, robos, etc.
  + **SEGURIDAD LÓGICA:** mecanismos que protegen la parte lógica de un sistema informático.
* En función en que tiene lugar la protección:
  + **SEGURIDAD ACTIVA:** previene, detecta y evita cualquier incidente en el sistema informático antes de que se produzca, como contraseñas.
  + **SEGURIDAD PASIVA:** son las técnicas o procedimientos necesarios para minimizar las consecuencias de un incidente, como las copias de seguridad.
* Los activos son los recursos del sistema necesario para que la organización alcance los objetivos propuestos. Los principales activos son:
  + **Información:** elementos que contengan datos almacenados en cualquier tipo de soporte.
  + **Software:** programas o aplicaciones que utiliza la organización para su funcionamiento o automatizar los procesos de su negocio.
  + **Físicos:** es la infraestructura tecnológica utilizada para almacenar, procesar, gestionar o transmitir toda la información necesaria para el buen funcionamiento de la organización.
  + **Personal de la organización** que utilice la estructura tecnológica y de comunicación para el manejo de la información.
* **Vulnerabilidades:** cualquier debilidad que tiene un activo que puede repercutir en el funcionamiento del sistema informático.
* **Amenazas:** cualquier entidad o circunstancia que ponga en peligro el funcionamiento del sistema informático:
  + **Amenazas pasivas:** su objetivo es obtener información relativa a una comunicación.
  + **Amenazas activas:** su objetivo es realizar cualquier cambio no autorizado en el estado del sistema.

## MAGERIT clasifica las amenazas de la siguiente manera:

* **Desastres naturales:** fuegos, daños por agua, desastres naturales.
* **Desastres industriales:** fuego, daños por agua, desastres industriales, contaminación mecánica, contaminación electromagnética, etc.
* **Errores y fallos no intencionados:** errores de usuarios, errores de configuración, etc.
* **Ataques deliberados:** manipulación de la configuración, suplantación de la identidad del usuario, difusión del software dañino, etc.

**ATAQUES:** acción que aprovecha una vulnerabilidad de un sistema informático para provocar un impacto sobre él y/o tomar el control del mismo.

Fases de un ataque informático:

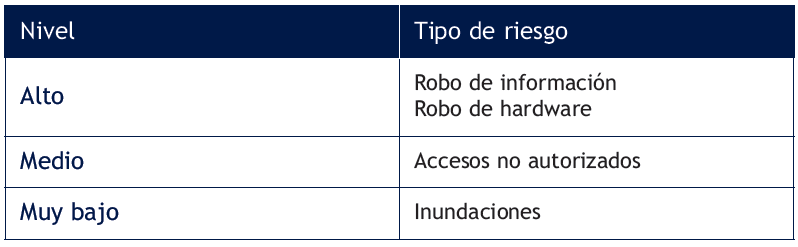
* **Reconocimiento:** se obtiene toda la información necesaria de la víctima, ya sea una persona u organización.
* **Exploración:** se consigue información sobre el sistema para atacar.
* **Obtención de acceso:** se intenta explotar alguna vulnerabilidad detectada en la víctima para realizar el ataque.
* **Mantener el acceso:** se busca la forma de implantar herramientas que permiten el acceso de nuevo al sistema en futuras ocasiones.
* **Borrar las huellas:** se intenta borrar las huellas que se hayan podido dejar durante el ataque para no ser detectado.

La ingeniería social consiste en obtener información confidencial y/o sensible de un usuario mediante métodos que son propios de la condición humana.

**RIESGO:** es una medida de la probabilidad de que se materialice una amenaza.

Para establecer métodos de seguridad hay que hacer un análisis de riesgos teniendo en cuenta qué activos hay que proteger, sus vulnerabilidades y amenazas, así como la probabilidad de que sucedan junto con lo que provocaría.

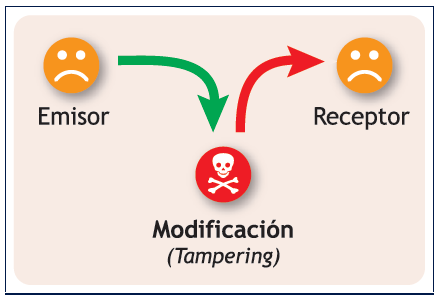
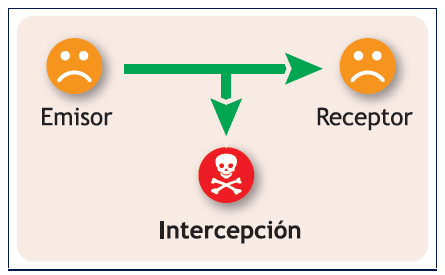
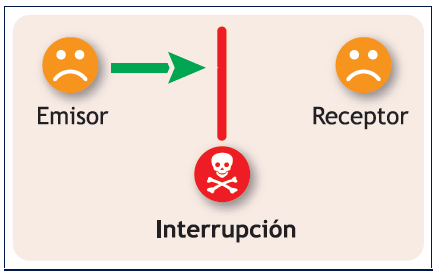
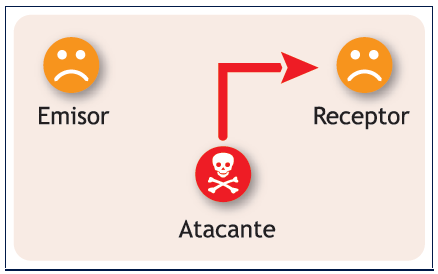
Niveles de riesgos:



**IMPACTO:** alcance producido o daño causado en caso de que una amenaza se materialice.

**DESASTRES:** es cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización. Las organizaciones tienen que prepararse ante cualquier desastre para reducir el impacto del desastre desarrollando planes de contingencia.

## Principios de seguridad informática:

* **Integridad**: garantiza que la información solo pueda ser alterada por personas autorizadas.
  + **Equipo de trabajo:** un usuario no autorizado modifica la información.
  + **Red de comunicaciones:** un atacante actúa de intermediario en una comunicación, recibe los datos enviados por un usuario, los modifica y los envía al receptor.
* **Confidencialidad**: garantiza que la información solo es accesible e interpretada por usuarios y temas autorizados
  + Equipo de trabajo: un atacante consigue acceso a un equipo sin autorización controlando sus recursos.
  + Red de comunicaciones: un atacante accede a los mensajes que circulan por la red sin tener autorización para ello.
* **Disponibilidad**: asegura que la información es accesible en el momento adecuado para los usuarios legítimos.
  + Equipos informáticos: los usuarios no tienen acceso al equipo.
  + Redes de comunicaciones: un recurso deja de estar disponible para otros usuarios que acceden a él a través de la red.
* **Otras** **características**:
  + No repudio: comprobación de la participación de ambas partes en una comunicación.
    - No repudio de origen: protege al destinatario del envío, probando que el emisor es quien dice ser.
    - No repudio de destino: protege al emisor del envío, ya que el destinatario no puede negar haber recibido el mensaje del emisor.
  + Autenticación: comprueba la identidad de los dos participantes en una comunicación y garantiza que son quienes dicen ser.

**Políticas de seguridad:** “es una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran.” Detallan una serie de normas y protocolos a seguir donde se definen las medidas a tomar para la protección de la seguridad del sistema, así como la definición de los mecanismos para controlar su correcto funcionamiento.

Elaborar políticas de seguridad:

* Elaborar reglas y procedimientos para los servicios críticos.
* Definir las acciones que habrá que ejecutar y el personal que deberá estar involucrado.
* Sensibilizar al personal del departamento encargado de la administración del sistema informático de los posibles problemas relacionados con la seguridad que pueden producirse.
* Establecer una clasificación de los activos a proteger en función de su nivel de criticidad, de forma que los sistemas vitales sean los más protegidos y no se gasten recursos en proteger aquellos activos con menor importancia.

**Planes de contingencia**: contemplan la parte de prevención de un sistema, teniendo en cuenta que, a pesar de las medidas tomadas, puede ocurrir un desastre. Contienen medidas detalladas para conseguir la recuperación del sistema.

Las fases que abarca son:

* **Evaluación**: se crea el grupo que desarrollará el plan identificando los elementos considerados como críticos para la organización, analizando el impacto que pueda producirse ante un desastre y definiendo cuáles deberán ser las soluciones alternativas los problemas que se puedan producir.
* **Planificación**: se documenta y se valida el plan de contingencia por parte de los responsables de las áreas involucradas de la organización. Ejecución del plan para comprobar que se asegurará la continuidad de las tareas críticas de la organización en caso de posible catástrofe.
* **Recuperación**: tras el incidente o ataque, deberá restablecerse el orden de la organización.

Para crear el plan de contingencia:

* **Tener redundancia:** tener un duplicado del hardware para el almacenamiento de la información, asegurando la continuidad de la actividad diaria en caso de problemas de dicho hardware.
* Tener la **información almacenada de manera distribuida**.
* Tener un **plan de recuperación** que contemple las medidas necesarias para restaurar el estado de los recursos tal y como estaban antes de la materialización de la amenaza.
* Tener a todo el **personal de la organización formado y preparado** ante cualquier situación de emergencia.

# Tema 2

**Importancia de la seguridad física:** el conjunto de medidas de prevención y detección destinadas a evitar los daños físicos a los sistemas informáticos y proteger los datos almacenados en ellos.

Medidas de seguridad:

* **Fenómenos naturales:** inundaciones, tormentas, terremotos. Hay medidas como instalación de equipos en ubicaciones adecuadas dotadas de las oportunas medidas de protección.
* **Riesgos humanos:** actos involuntarios, actos voluntarios, actos vandálicos y sabotajes. Hay medidas como control de acceso a recintos, elaboración de perfiles psicológicos de empleados con acceso a datos confidenciales, formación a usuarios en materia de seguridad…

**Protección física de los equipos:**

* **Entorno físico y temperatura del equipo:** Hay que tener en cuenta el espacio con una buena ventilación, una humedad del 50%, la luz solar no debe incidir en los equipos para evitar el sobrecalentamiento, una temperatura ambiente entre 15 y 35 ºC, limpieza de las partículas de polvo, evitar los campos magnéticos, los equipos deben estar alejados de aparatos que produzcan vibraciones y hay que poner suelos que eviten la electricidad estática.
* **Instalaciones:** 
  + Instalación eléctrica adecuada: los equipos informáticos, al funcionar con energía eléctrica, puede sufrir graves daños si la instalación eléctrica es defectuosa. Hay que tener en cuenta:
    - Protecciones eléctricas adecuadas, como enchufes con tomas de tierra y la corriente suministrada tiene que ser estable para evitar picos de tensión.
    - Mantenimiento del suministro eléctrico: la corriente eléctrica está sometida a anomalías como apagones, caídas de tensión etc, teniendo en cuenta esto, se desarrollaron los SAI (sistema de alimentación ininterrumpida.
  + Instalación de red adecuada: hay que proteger la red de accesos no deseados y tener en cuenta la exposición de los cables a la humedad, radiaciones electromagnéticas…
  + ***Control de acceso: establecimiento de claves.***
  + Protección frente a incendios:
    - ***Sistemas de prevención: instalación de detectores de humo y alarmas***, mantenimiento del orden y la limpieza para evitar la acumulación de materiales combustibles…
    - ***Sistemas de protección: colocación de barreras para aislar el incendio, la delimitación clara de las vías de evacuación y salidas de emergencia y la instalación de sistemas de extinción***.
* ***Sistemas de alimentación ininterrumpida:*** dispositivo cuya finalidad es proporcionar suministro eléctrico a los equipos conectados a él cuando se produce un corte de la corriente eléctrica.

***Tipos de SAI:***

* + ***Offline pasivos:*** Se activan cuando hay un fallo en la corriente eléctrica. Son los más habituales para ordenadores domésticos, televisores..
  + ***Offline interactivos:*** Están siempre activos y conectados a la corriente eléctrica. Tienen filtros activos que estabilizan la señal. Están destinados a equipos de pequeñas empresas.
  + ***Online:*** Se colocan entre el suministro normal de corriente y los equipos a proteger, cumpliendo con la función de estabilización y filtrado de señal. Sus baterías se cargan constantemente mientras suministra energía a los equipos, debido a esto sufren más deterioro sus baterías y hay que sustituirlos más a menudo.

Sus partes:

* + Batería y cargador.
  + Filtro: limpia la señal.
  + Conversor: es un transformador que convierte la tensión de 12 voltios de su batería en corriente continua.
  + Inversor: convierte la corriente continua en alterna a 220 voltios.
  + Conmutador: permite cambiar entre suministro proporcionado por la red eléctrica y el generado por la batería del SAI.

**Características del SAI:**

* + **Autonomía:**

Tiempo que el SAI puede seguir alimentando a un equipo en caso de fallo eléctrico. Se mide en minutos.

* + **Potencia:**

mide el consumo de energía en:

* + - ***Vatios (W):* potencia real consumida por el dispositivo.**
    - ***Voltamperios (VA):*** es la potencia aparente, se calcula multiplicando la tensión de la corriente en voltios por la intensidad de amperios.

Instalación y gestión de un SAI

* + *Búsqueda de una ubicación para el dispositivo que permita un funcionamiento óptimo como una base estable, con buena ventilación, sin objetos encima o alrededor…*
  + Conexión:
    - Conexión eléctrica: por un lado, tiene que estar conectado a la red eléctrica y por otro al equipo que va a proteger.
    - Conexión de datos: se conecta un cable de datos al sistema informático para poder gestionar el SAI de manera local o a través de una red.
      * Conexión Monopuesto local: solo se conecta a un equipo local.
      * Conexión de la batería del SAI a una LAN: a través de un switch se conecta a la red por TCP/IP y se gestiona mediante un servidor de la red o desde equipos remotos de internet.

**Controles de presencia y acceso:**

Métodos de control de acceso:

Se basan en 3 posibles métodos:

* Lo que soy: una clave
* Lo que tengo: tarjeta o dispositivo de acceso
* Lo que soy: características biométricas

Medidas de seguridad:

* Sistemas de vigilancia: personal de vigilancia que se encarga de evitar accesos no autorizados y alarmas y sistemas de detección de intrusos.
* Código de seguridad: los usuarios recuerdan un código numérico o contraseña de seguridad para acceder al recinto o al sistema.
* Acceso mediante dispositivos: se utilizan instrumentos de seguridad como llaves, tarjetas…
* Sistemas biométricos: se analizan ciertos rasgos físicos únicos del sujeto para identificarlo.

**Centro de proceso de datos (CPD):**

Es la ***INSTALACIÓN QUE CENTRALIZA LAS OPERACIONES Y LA INFRAESTRUCTURA DE TI DE UNA ORGANIZACIÓN***, en la que se almacenan, procesan, tratan y difunden datos y aplicaciones.

Centralizan bases de datos, servicios de correo electrónico, gestión de usuarios… y requieren servidores con varios procesadores y unidades de disco, sistemas de comunicaciones avanzados, equipos de alimentación redundantes, dispositivos para copias de seguridad… necesitan una temperatura ambiente de entre 17 y 19 ºC, generan mucho ruido, asique deben estar en un entorno de aislamiento acústico y térmico y especiales. Deben estar operativos las 24h todos los días del año y se controlas desde fuera de la sala desde dentro por la red local o remotamente mediante concentradores KVM.

***Concentradores KVM***: es un controlador de consolas que permite, mediante un teclado, pantalla y ratón, acceder de forma remota a las consolas de los servidores del CPD que están conectados a éstos.

* Racks de servidores
* Climatización
* Sistema de extinción de incendios
* SAI
* Generadores de copias de seguridad
* Sistemas de seguridad

**Sistemas de seguridad del CPD**

* ***Sistemas contra incendios***: utilizar ***agua nebulizada***
* Sistemas eléctricos: las instalaciones eléctricas tienen que ser adecuadas a la carga estimada que van a soportar. El diseño de las canalizaciones debe aislar adecuadamente los cables, de manera que se colocan en falsos techos y falsos suelos. Las canalizaciones deben asegurar el perfecto aislamiento de las líneas eléctricas frente a interferencias, humedades… debe de existir fuentes de alimentación redundantes

***Climatización***

*Pasillos fríos y pasillos calientes: el aire caliente emitido por los servidores en los pasillos calientes se canaliza hacia los pasillos fríos.*

**Datos**

Se necesitan equipos robustos para soportar sistemas de comunicación ***SAN*** (***Storage*** ***Area Networks***), ***NAS*** (***Network Attached Storage***), ***granjas de distintos tipos de servidores, servidores “blade” y otros dispositivos diversos***. ***Los cables*** adecuados ***son*** ***Ethernet y de fibra óptica*** y se mantienen ***separados de los cables eléctricos para evitar interferencias electromagnéticas***.

***Centros de respaldo***

Son ***réplicas*** más o menos ***exactas del CPD principal***, ***tomando el control*** ***en caso*** de que ***no esté funcional dicho CPD. Suelen estar entre 20 y 40km de distancia***.

Tipologías:

* ***Cold site o sala fría:*** es un *CPD externo a la organización* con toda la *infraestructura necesaria* en cuanto a *climatización*, *potencia eléctrica*… *en* caso de *contingencia*, se *trasladan los servidores y se reinstala todo el sistema a partir de copias de seguridad.*
* ***Hot site o sala caliente:*** es un ***CPD*** con ***comunicaciones***, ***sistema***s y ***software análogo al principal***. ***En*** caso de ***contingencia*** se ***restauran los datos con el último backup.***
* *Mutual backup: se acuerda con otra organización que ejerza de centro de backup mutuo entre sí*.
* Mirror site o centro espejo: es una versión de la sala caliente, pero los datos se replican en tiempo real de un CPD a otro.
* *Configuraciones activo-activo: los sistemas están configurados en clústeres geográficos repartidos en ambos CPD, de manera que, si uno deja de funcionar, el servicio no se ve afectado.*

# Tema 3

**Concepto de seguridad lógica**

Es el conjunto de medidas destinadas a la protección de datos y aplicaciones informáticas, garantizando el acceso a la información solo a personas autorizadas.

* Políticas de seguridad corporativa: establecer normas indicando lo que se puede hacer y lo que no en el sistema informático. Son el conjunto de normas que definen medidas de seguridad y los protocolos de actuación:
  + Instalación, mantenimiento y actualización de equipos
  + Control de acceso a áreas críticas de la empresa y a recursos críticos del sistema.
  + Utilización de recursos de las redes informáticas
  + Mantenimiento de las redes
  + Adquisición, instalación y actualización de software
  + Privacidad de la información
  + Autenticación de usuarios
  + Información de errores o accesos al sistema
  + Contraseñas

Algunas medidas son:

* Autenticación de usuarios
* Listas de control de accesos
* Criptografía
* Certificados digitales: documentos digitales con un número de serie único y un periodo de validez vinculados con una clave pública.
* Firmas digitales: conjunto de datos para identificar al firmante
* Cifrado de unidades de discos o sistemas de archivos

**Acceso a sistemas operativos y aplicaciones**

* Contraseñas: sistema de autenticación que permite el acceso a aplicaciones y sistemas operativos.

Amenazas:

* + Sniffers: registra la actividad de un equipo informático interceptando las comunicaciones “escuchando” para obtener datos y contraseñas.
  + Keyloggers: programas o dispositivos que capturan las pulsaciones de un teclado.
  + Fuerza bruta: probar todas las posibles combinaciones para acceder al sistema.
  + Por diccionario: genera diccionarios con términos relacionados con el usuario, probándolos como contraseñas para acceder al sistema.
  + Por ingeniería social: engañar a los usuarios para que proporcione sus contraseñas a los intrusos suplantando la identidad de amigos, familiares…

Políticas de seguridad en materia de contraseñas:

* + No deben contener palabras usuales ni relacionadas con el entorno de usuario
  + No deben ser palabras con significado
  + Como mínimo debe tener 8 caracteres
  + Evitar que el usuario utilice la misma contraseña en varios sitios
  + Cambiar las contraseñas proporcionadas por defecto

Comunicación de las contraseñas:

En caso de compartir la contraseña vía WiFi, cable, etc, se debe encriptar la información para dificultar su acceso en caso de ser interceptada.

Almacenamiento de las contraseñas:

En caso de almacenar las contraseñas en un equipo, se debe recurrir al uso de programas gestores de contraseñas.

Papel de administrador del sistema:

Hay que tomar medidas adicionales como:

* Establecer un número máximo de intentos para acceder al sistema
* Obligar al usuario a que establezca contraseñas con un mínimo de ocho caracteres alfanuméricos que combinen una mayúscula, una minúscula, un número y un signo de puntuación.
* Obligar al usuario a cambiar la contraseña cada cierto tiempo.
* Impedir al usuario repetir las últimas tres contraseñas utilizadas.

Las políticas relacionadas con las contraseñas se gestionan, en Windows, desde la consola de Directivas de seguridad local.

**Listas de control de acceso (ACL)**

Son una herramienta que permite controlar qué usuarios pueden acceder a distintas aplicaciones, sistemas, recursos, dispositivos…

Ventajas:

* Posibilidad de mejorar el rendimiento de la red limitando determinado tráfico.
* Posibilidad de permitir o denegar el acceso de equipos a ciertas zonas de la red.
* No permiten ejecutar determinados comandos por la red destinados a fines malintencionados.

Windows distingue dos tipos de privilegios:

* Permisos: establecen la forma de acceder a un objeto concreto, como escribir un archivo NTFS.
* Derechos: establecen qué acciones se pueden realizar en el sistema, como iniciar sesión.

El propietario de un recurso es quien asigna permisos sobre dicho recurso a través del cuadro de diálogo de propiedades del mismo.

ACL en Linux: permiso de lectura (r), escritura (w) y ejecución (x).

Las entradas de la ACL son:

* La categoría: usuario (u), grupos (g), otros (o) o máscara (m).
* UID (identificador de usuario) o GID (identificador de grupo).
* Cadena con los permisos asignados

**Acceso a aplicaciones por internet**

Normas generales aplicables a todas las aplicaciones web para los usuarios:

* Mantener actualizados tanto el sistema operativo como el navegador y, dependiendo de la situación, un antivirus actualizado.
* Tener una correcta administración de los nombres de usuario y las contraseña.
* Desconfiar de las webs en las que para regenerar una contraseña permiten introducir una cuenta de correo.
* Acceder a las distintas aplicaciones desde un ordenador seguro si los datos son muy sensibles.
* No facilitar por correo electrónico ni telefónicamente las contraseñas, ni modificarlas por estas vías.
* No acceder nunca a través de enlaces a la página web de una empresa u organismo público para realizar un trámite.
* Cerrar la sesión correctamente.

Plataformas de pago: es un servicio de comercio electrónico que autoriza pagos realizados a través de Internet.

**Autenticación de usuarios**

Security token: dispositivo hardware que autentica al usuario que lo lleva y permite su acceso a la red. Su autenticación es de dos factores:

* El usuario tiene un número de identificación personal (PIN), que le autentica como el propietario del dispositivo
* El dispositivo muestra un número que identifica al usuario y le permite el acceso a determinado servicio.

Identificación biométrica: sistemas que permiten la autenticación de usuarios mediante características personales inalterables, como las huellas digitales, rasgos faciales, el iris del ojo, etc.

**Autorización de usuarios**

Single Sign-On: se utiliza un proveedor de autenticación una única vez.

Web Single Sign-On:

Identidad federada: establece una relación de confianza entre los distintos sistemas de SSO de forma que los usuarios puedan acceder a las aplicaciones a las que estén autorizados con las mismas credenciales en todas las sedes.

OpenID: aplicación de identidad federada a Internet. Ofrece la posibilidad de crear una identidad federada entre todos los sitios web que decidan utilizar el sistema.

Tema 4

**Definiciones:**

* Criptología: krypto (oculto) y oculto (estudio), estudio de los criptosistemas, sus áreas principales son la criptografía y el criptoanálisis.
  + Criptografía: krypto (oculto) y graphos (escribir). Es el arte de escribir con clave secreta o de un modo enigmático ocultando únicamente el significado del mensaje.
  + Criptoanálisis: ciencia que se ocupa el descifrar criptogramas rompiendo la clave utilizada para descubrir el contenido del mensaje.
* Criptosistema: conjunto de claves y equipos de cifra que, utilizados coordinadamente, ofrecen un medio para cifrar y descifrar.

Cifrar: transcribir, utilizando una clave, un mensaje cuyo contenido se quiere ocultar.

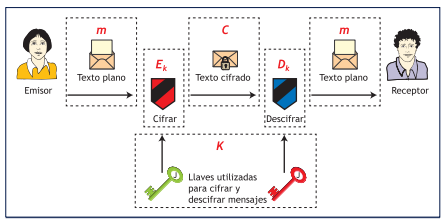
Clave: conjunto de signos utilizados para la transmisión de un mensaje privado cuyo contenido se quiere ocultar.

Los sistemas criptográficos se basan en dos técnicas:

* Transposición: los signos o símbolos se cambian de posición.
* Permutación o sustitución: los signos o símbolos del mensaje original son sustituidos por otros.

**Elementos de un criptosistema**

* Mensajes sin cifrar, texto plano o texto nativo (m): documentos originales sin cifrar.
* Mensajes cifrados (C) o criptogramas.
* Conjunto de claves (K): datos o llaves que permiten cifrar los mensajes.
* Transformaciones de cifrado (E): existe una transformación diferente para cada valor de la clave k.
* Transformaciones de descifrado (D).

****

**Cifrado de clave simétrica**

Hay dos grandes grupos de algoritmos de cifrado:

* Cifradores de flujo: cifran bit a bit.
* Cifradores de bloque: cifran un bloque de, generalmente, 64 bits como una unidad.

El emisor y el receptor conocen la clave y se utiliza tanto para cifrar como para descifrar.



* Criptoanálisis: aprovecha las características del algoritmo para intentar averiguar el texto originario o la clave secreta que se está utilizando.
* Método de fuerza bruta: probar todas las combinaciones de las posibles claves empleadas para cifrar el texto.

**Cifrado de clave asimétrica**

