# Unidad 4 – Clase 1:
# Seguridad Informática

# Seguridad informática

Se enfoca en **proteger objetos** de valor de los sistemas de computación:

- Hardware: computadora, dispositivos, red
- Software: sistema operativo y aplicaciones
- Datos: documentos, fotos, videos, emails, etc. (almacenados y en tránsito).

Se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a lograr un sistema de información seguro y confiable.

# Objetivos de la Seguridad Informática

**Confidencialidad**

**Integridad (y autenticidad)**

**Disponibilidad**

**No repudio**

Objetos = hardware/software/datos

La enumeración no presupone un orden de importancia.

Cada organización deberá priorizar esos aspectos de acuerdo a sus propias características de negocio.

# Confidencialidad

Se refiere a que los recursos sean accedidos solo por las personas que tienen autorización para hacerlo.

Ejemplo: Un informe de la situación salarial del personal debe ser leído solamente por el Gerente General y por el Gerente de RRHH.

# Integridad

Se refiere a que los recursos pueden ser creados, cambiados o eliminados solo por aquellos sujetos que tienen autorización para hacerlo. Es decir, se busca mantener los datos exactamente tal cual fueron generados, sin manipulaciones ni alteraciones por parte de terceros.

> Ejemplo: El cambio de domicilio de una persona solo puede ser solicitado por la misma persona. Habría un problema de integridad si se hace un cambio de domicilio sin el consentimiento de la persona afectada.

## Autenticidad

Este aspecto a veces se lo considera como parte de la integridad o puede considerarse de forma separada.

La autenticidad es una cualidad que permite identificar al creador de una información (ej. ¿un mensaje realmente me lo envía quien dice ser?). La autentificación se encarga de determinar con quién se está hablando antes de revelar información delicada o hacer un trato de negocios.

# Disponibilidad

Se refiere a que los recursos estén disponibles para ser accedidos por las personas cuando los requieran.

Ejemplo: Un corte en las líneas de comunicación impide el envío y recepción de correo electrónico.

# No repudio

Permite probar la participación de las diferentes partes intervinientes en una comunicación.

No repudio de origen: el emisor no puede negar que realizó el envío de un mensaje porque el destinatario tiene pruebas de la emisión.

No repudio de destino: el receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción.

# ¿Contra qué protegerse?

**Vulnerabilidades**

**Amenazas**

**Ataques**

# Vulnerabilidades

Son los **puntos débiles** de los sistemas.

Todos los componentes del sistema tienen vulnerabilidades.

En otras palabras: Ningún sistema está libre de problemas.

# Vulnerabilidades

Una clasificación:

En el hardware: vida útil de los discos, golpes de energía, calidad de los materiales, etc.

En el software: bugs, puertas traseras, etc.

En los datos: contraseñas débiles, falta de cifrado en los datos, legibilidad, etc.

# Vulnerabilidades

Otra clasificación:

Físicas: lugar donde están los equipos.

Naturales: inundaciones, terremotos.

Emanaciones: ondas electromagnéticas.

Comunicaciones: cableadas, inalámbrica.

Humanas: errores, mala intención, falta de capacitación.

# Vulnerabilidades

Publicación de vulnerabilidades:

https://www.incibe.es/protege-tu-empresa/avisos-seguridad

# Vulnerabilidades

¿Hacking ético?

# Vulnerabilidades

¿Hacking ético? Personas que ayudan a identificar vulnerabilidades.

# Amenazas

Son los peligros potenciales a los que se expone un sistema a partir de la existencia de las vulnerabilidades.

Afectan a la totalidad de los componentes: hardware, software y datos.

Cuanto más vulnerabilidades tiene un sistema, más amenazas existen sobre él.

# Amenazas clásicas

**Interrupción**: un objeto del sistema desaparece, no esta disponible, o es inutilizable. Ejemplo: archivos borrados, sitio web caído, disco rígido dañado, etc.

**Interceptación**: significa que una parte (persona/programa) no autorizada ha obtenido acceso a un objeto. Ejemplo: copia ilícita de un archivo o programas, escuchar conversaciones privadas, etc.

**Modificación**: significa que alguien o algo (programas) realizan alteraciones no autorizadas sobre un objeto. Ejemplo: alterar los contenidos de una base de datos, de una página web, cambio del funcionamiento de un programa, etc.

**Fabricación**: algo o alguien puede fabricar objetos falsos dentro de un sistema. Ejemplo: registros adicionales en una base de datos, mails, etc.

# Ataques

Los ataques son la concreción de las amenazas mediante la explotación de las vulnerabilidades de los sistemas.

# Ataques

Una clasificación según el origen:

- Externos: ejecutados por personas ajenas a la organización atacada.
- Internos: realizados por personas que pertenecen a la organización atacada.

La práctica demuestra que los ataques más efectivos utilizan una combinación de atacantes internos y externos.

# Ataques

Clasificación según como se producen:

- Intencionales: son los realizados a propósito.

  El atacante sabe conscientemente lo que está haciendo.

- Accidentales/negligencia: cuando se producen sin que exista la intención de atacar.

  Se deben casi siempre a la capacitación insuficiente del personal.

# ¿Un sistema seguro?

- Ningún sistema es completamente **seguro**.
- En otras palabras, TODOS los sistemas son vulnerables.

Entonces, hay que protegerlos (aún una PC en un hogar).

# Implementación

- Seguridad Física y Ambiental: destinada a proteger los componentes físicos del sistema. Ej.: sala de servidores adecuada, cerraduras, instalación eléctrica según normas, etc.
- Seguridad Lógica: Destinada a proteger datos y programas. Ej.: passwords, auditorías, backups, control de acceso a datos, etc.
- Seguridad de Comunicaciones: Destinada a proteger los medios de comunicación y los datos que se transmiten por ellos. Combina seguridad física y seguridad lógica. Ej.: cableado según normas, firma digital, criptografía, etc.

# Criptografía

- Criptografía viene del griego:
  - kripto: ocultar
  - graphos: escritura.
- Según la Real Academia Española, la Criptografía es:

  "el arte de escribir con clave secreta o de un modo enigmático".

# Criptografía

- Una definición más técnica:

  “Rama de la Matemática -y en la actualidad de la Informática- que hace uso de métodos y técnicas con el objeto principal de cifrar un mensaje o archivo por medio de un algoritmo, usando una o más claves”

- Y por último, una definición más práctica:

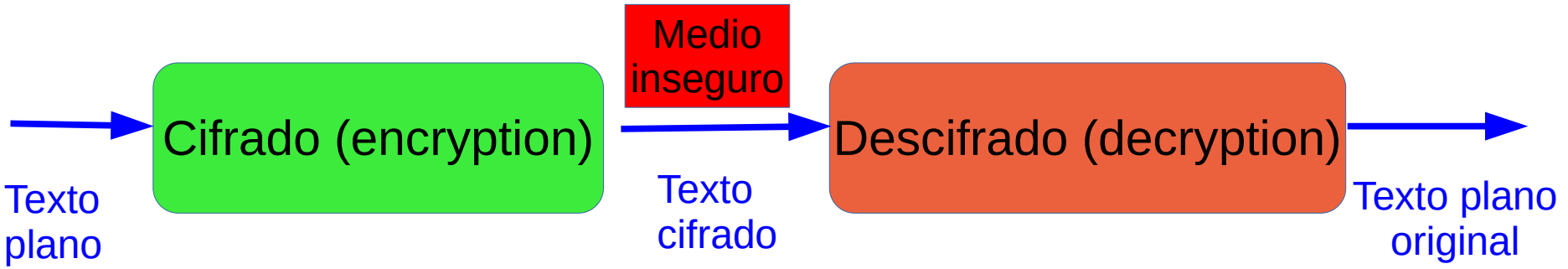
  “Herramienta que sirve para ocultar información con el objeto de protegerla”.

# Criptografía

La motivación principal para el uso de la criptografía es mantener la confidencialidad de los datos. En la actualidad se busca además:

- Autenticidad: que el creador/emisor de un mensaje sea quien dice ser, y no otro.
- Integridad: que el mensaje recibido sea igual al que fue enviado.
- No repudio: que el emisor no pueda negar el haber enviado el mensaje o que el receptor no pueda negar haberlo recibido.

# Criptografía




Un **algoritmo criptográfico** define reglas de cifrado y descifrado.

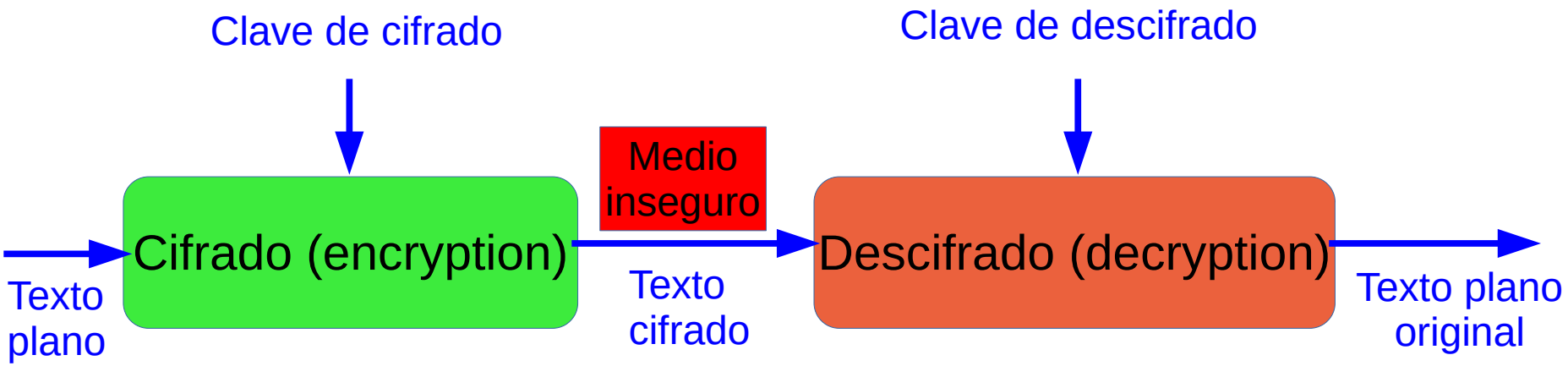
**Cifrado (encryption)** es el proceso de codificar un mensaje de modo que su contenido no sea obvio a los ojos de cualquier observador. **Descifrado (decryption)** es el proceso inverso por el que se transforma un mensaje previamente cifrado a su forma original.

# Criptografía

Algunos algoritmos criptográficos utilizan una clave. Normalmente basan su fortaleza en la **clave** mientras que el propio algoritmo es revelado. En estos casos, el texto cifrado (C) depende tanto del texto plano (P) de entrada como de la clave (K). Matemáticamente:

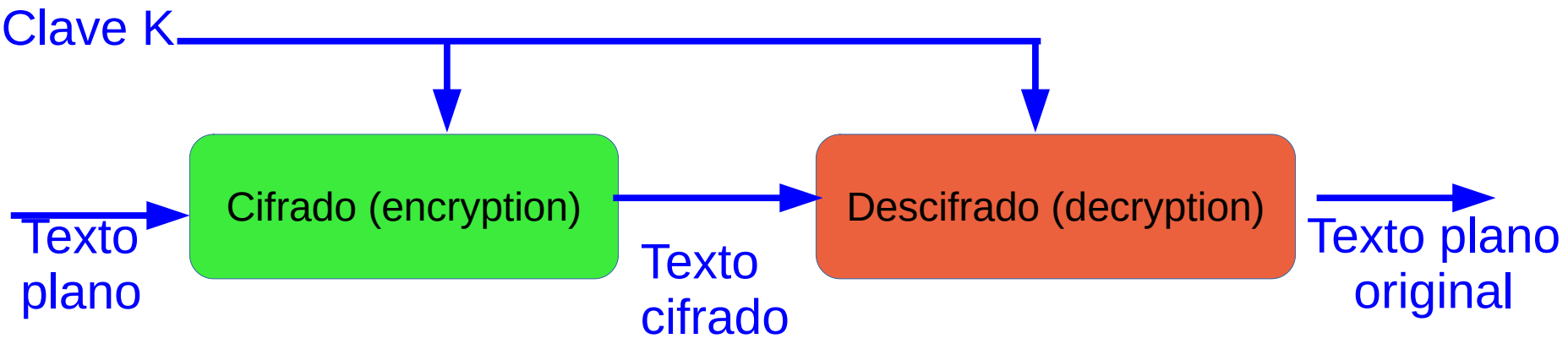
$$\mathbf{C=E(K_E,P)\ \ y\ P=D(K_D,E(K_E,P))}$$

El mismo texto plano resulta en distintos textos cifrados con solo cambiar la clave.



# Criptografía simétrica

Cuando la clave de cifrado y descifrado son idénticas hablamos de **cifrado simétrico (o de clave privada)**.




Ejemplos: DES, TDES (triple DES), IDEA, AES.

Para cada par de usuarios que intercambian mensajes existe una clave única, que debe ser conocida y mantenida en secreto por ambos.

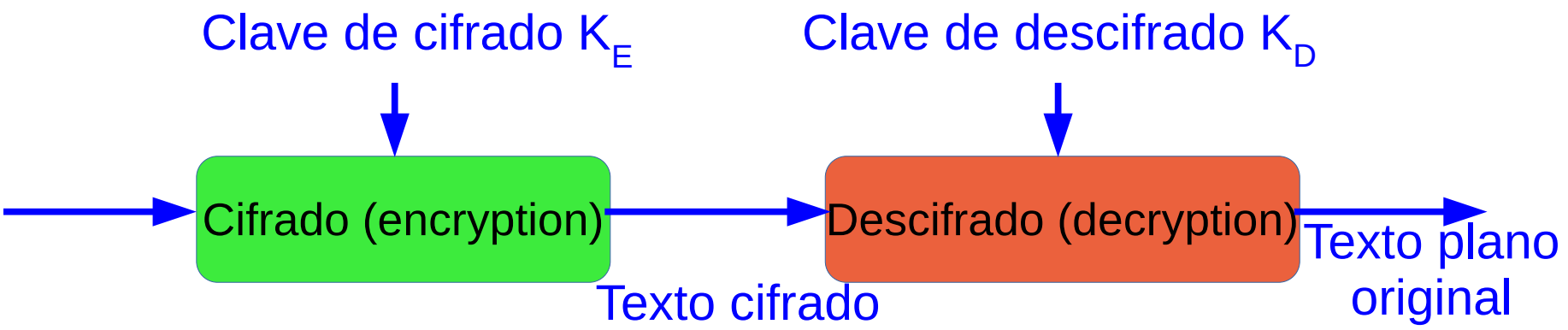
**Desventaja**: la clave debe ser secreta y por lo tanto debe protegerse, sin embargo es un problema asegurar esto ya que la clave requiere distribuirse.

**Ventaja**: poco cómputo

# Criptografía asimétrica

En los sistemas criptográficos **asimétricos (o de clave pública)** los algoritmos utilizan **pares de claves** $K_E$ y $K_D$ de modo que una de ellas se utiliza para cifrar ($K_E$) y la otra para descifrar ($K_D$). Matemáticamente**:**

**$C=E(K_E,P)$ y $P=D(K_D,E(K_E,P))$** donde **$K_E \neq K_D$**



# Criptografía asimétrica

Cada par de claves está asociado a un único usuario, quien difunde su clave pública y debe mantener en secreto su clave privada.

**Ventajas**:

- No requiere distribuir una clave secreta.
- Se requiere menor número de claves a administrar, ya que bastará con un par de claves por parte. Mientras que en el esquema de cifrado simétrico es necesario establecer una clave secreta $K_{AB}$ por cada par A-B que deseen comunicarse.

**Desventaja**: requieren mucho cómputo

# Criptografía asimétrica

## Aplicación: Cifrado con clave pública

- El emisor cifra el mensaje con la clave pública del receptor y lo transmite.
- El receptor recibe el mensaje y lo descifra con su clave privada. Como solo él conoce la clave, nadie más puede descifrar el mensaje.
- ¿Qué objetivo de la seguridad informática se asegura?

# Criptografía asimétrica

**Aplicación: cifrado con clave privada**

- Si el emisor cifra un mensaje con su clave privada y envía el texto cifrado, *cualquier usuario* que conozca la clave pública del emisor podrá descifrar y leer el mensaje.

- Quien reciba el mensaje podrá certificar la identidad del emisor, pues si el mensaje fue descifrado con la clave pública del emisor, significa que fue cifrado con la clave privada de este, que solamente él conoce.

# Bibliografía

**Computer Networking. A Top-Down Approach. Kurose, Ross.**

**Security in computing. Charles P. Pfleeger.**

**Redes de computadoras. Tanenbaum, 5ta edición**