# TEMA 18

***Informática básica:***

***Conceptos fundamentales sobre el hardware y el software.***

***Sistema de almacenamiento de datos.***

***Sistemas operativos.***

***Nociones básicas sobre seguridad informática.***

# INDICE

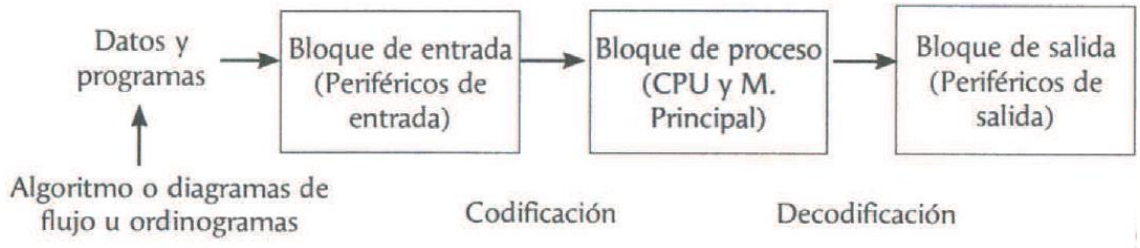
# 1. INTRODUCION. EL TRATAMIENTO DE LA INFORMACION

La palabra informática, término inventado por Phillippe Dreyfus en 1962, nace de la contracción de las palabras "información" y "automática" y se puede definir como el "tratamiento o procesamiento automático de la información mediante una máquina denominada computador".
La información es un término genérico. Representa ideas, hechos, relaciones y pro-piedades de los objetos, de las personas y del universo en general.
Por otra parte, un dato es un concepto mucho más preciso: podemos pensar en un dato como en una información concreta y no demasiado extensa. Por ejemplo, en la biografía de una persona leemos que nació en una determinada fecha, lo que se considera un dato.
El tratamiento de la información nos permite agrupar datos y obtener resultados.

El ordenador es el instrumento idóneo para el tratamiento de la información. Y precisamente, el esquema básico del ordenador responde a esta necesidad.

Se dice que un ordenador para su funcionamiento necesita de la siguiente información: datos y programas, entendiendo estos últimos como un conjunto de instrucciones que le dicen al ordenador qué tiene que hacer con los datos para obtener un resultado. Antes de realizar un programa se puede crear un algoritmo que se puede definir como el conjunto de pasos que hay que realizar para solucionar un problema (descripción en forma textual). O también se puede realizar un ordinograma que en principio es lo mismo que el algoritmo, pero representado gráficamente.

Un ordenador se estructura en tres bloques bien diferenciados:




El primer bloque es lo que se denomina bloque de entrada de información, está compuesto por los dispositivos de entrada (teclado, ratón,) del ordenador mediante los cuales podemos introducir la información que queremos tratar, en el caso de la informática esta información son los datos y los programas.
Una vez que introducimos la información que viene expresada en un lenguaje natural hay que traducirla a 0 y 1 (lenguaje binario), a este proceso se le denomina codificación. Una vez que la información está en binario se transfiere al segundo bloque conocido como bloque de proceso. En este bloque es donde los programas le dirán al computador qué tiene que hacer con los datos para obtener un resultado. Los componentes principales de este bloque son la CPU (Unidad Central de Proceso) y las memorias principales.
Para terminar, el ordenador tendrá que mostramos los resultados. Para tal fin utilizaremos el bloque de salida que constará de los periféricos de salida, que pueden ir desde una pantalla o una impresora (para mostrar los resultados por papel).

# 2. EL ORDENADOR

## 2.1. Equipo Físico y Equipo Lógico

En informática, hemos de distinguir varias partes fundamentales:

- **El HARDWARE,** equipo físico: se refiere a la máquina en sí, al conjunto de cables, circuitos, etc. El hardware representa la parte material o tangible del sistema informático, es decir, la parte que puede tocarse con las manos (teclado, pantalla, circuitos electrónicos, memorias, etc.).
- **El SOFTWARE**, equipo lógico o parte inmaterial: constituido por los programas del ordenador, que indican a la máquina los pasos que ha de ir realizando para obtener los resultados deseados. El software (también denominado "LOGICAL") dota al equipo físico de la capacidad para realizar cualquier tipo de tarea. Algunos tipos especiales de software son el freeware (programas gratuitos), shareware (programas de evaluación) o el groupware (programas para el trabajo en grupo).

**El FIRMWARE**: es el "software que viene grabado de fábrica". Se refiere a los programas grabados en memorias ROM. Dentro de esta categoría encontramos la BIOS (Basic Input Output System) Sistema básico de entrada y salida.

Las dos partes son imprescindibles, no siendo posible su funcionamiento de un ordenador si faltara una de ellas.

Otros elementos que no pertenecen propiamente al ordenador, pero que también son imprescindibles para su funcionamiento, son los llamados **periféricos**.

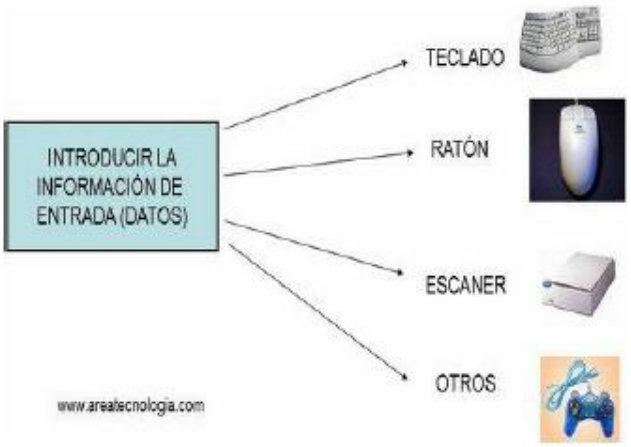
Los periféricos son elementos externos al propio ordenador, por eso se llaman periféricos (están en la periferia del ordenador). Algunos de los periféricos más conocidos son por ejemplo el teclado o el ratón para introducir información en el ordenador o la impresora para sacar la información del ordenado en papel.

Hay tres tipos de periféricos según su uso:

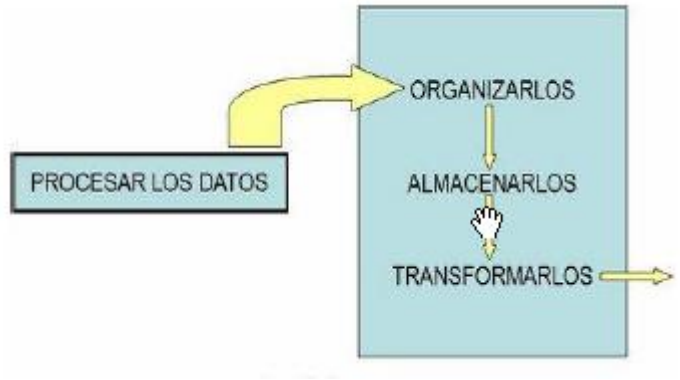
. Entrada
. Salida
. Entrada / Salida

**¿Cómo funciona reamente un sistema informático u ordenador?**

Para entender cómo funciona un sistema informático primero metemos los datos o información mediante los periféricos de entrada.

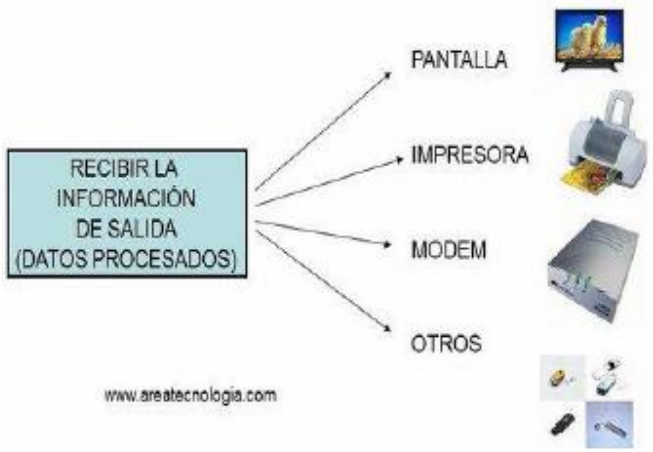


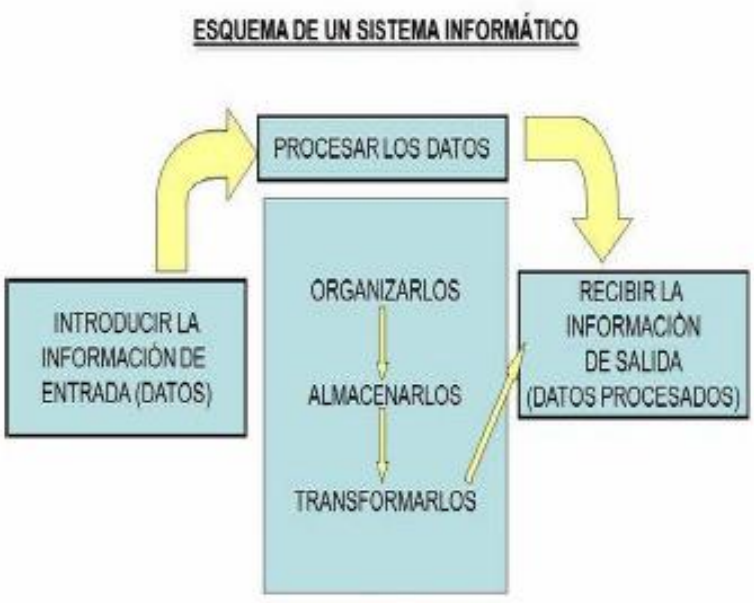
Una vez que se introducen los datos al sistema informático este debe procesarlos. Pero… ¿Qué es eso de procesar los datos? Pues es muy simple, organizarlos, almacenarlos y transfórmalos.




Según lo dicho una vez que introducimos los datos en el sistema informático este los organiza, los almacena temporalmente y cuando pueda los transforma según las instrucciones recibidas. Esto normalmente lo realiza el **microprocesador**.
Una vez transformados debemos recoger los datos transformados de alguna forma. Estos datos transformados es lo que llamamos información de salida.

La información de salida la recogemos mediante los periféricos de salida o de entrada/salida.



Dentro del software se distinguen:

. **DE SISTEMAS**: Sistemas Operativos: Es el conjunto de programas que gobiernan el funcionamiento del ordenador y un requisito para que los programas de aplicación funcionen.

. **DE DESARROLLO**: Lenguajes de programación. Permiten la escritura de programas de aplicación (C, Pascal, Cobol, Natural Adabes, Visual, LISP…)

. **DE APLICACIÓN**: Programas de aplicación: Permiten la automatización de algún proceso. Producen resultados para el usuario.

### 2.2. Representación de la información en el ordenador

Aunque los datos pueden introducirse en el ordenador a través de un teclado semejante al de una máquina de escribir, utilizando los símbolos alfabéticos y numéricos convencionales (denominado "Lenguaje natural"), sus circuitos internos son incapaces de trabajar con este tipo de representación.
El ordenador es una maquina o sistema digital compuesto por infinidad de circuitos electrónicos que permiten detectar fácilmente si existe paso o no de corriente por ellos mismos. Por este motivo, el sistema con el que se representa la información dentro del equipo informático es el sistema en **base dos** o **sistema binario.**

A cada carácter en lenguaje natural le corresponde una única combinación de impulsos eléctricos. Estos impulsos eléctricos son una combinación de tensiones altas (positivas) y bajas (negativas). Es por esto por lo que se dice que el lenguaje maquina es el código binario formado por únicamente dos dígitos (0 y 1).

- Estado lógico 1: interruptor cerrado, presencia de tensión.
- Estado lógico 0: interruptor abierto, ausencia de tensión


Cada uno de estos dígitos representa un **bit** (**b**inary dig**it**).

**Bit:** es la unidad más pequeña de representación de información en un ordenador, que se corresponde con un digito binario, 0 o 1.

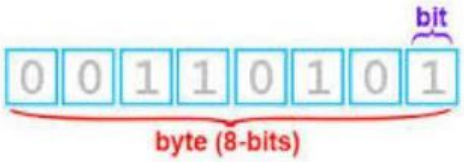
Para poder representar todos los caracteres existentes (alfabéticos, numéricos y especiales) en lenguaje maquina se necesitan 8 bits, estos bits forman 1 **byte** (u octeto).

**Un Byte** = conjunto de 8 bits, que es lo que ocupa un numero o un carácter (letra o símbolo) en el sistema de codificación usado en informática.

En informática podríamos asignar a cada letra o símbolo (caracteres) o número, un numero en binario de 8 cifras (8 ceros y unos) y así obtener un código mediante el cual podamos entendernos con el ordenador. Este código se llama código ASSCII. Este código utiliza los 8 bits (1 byte) para poder representar un total de 256 caracteres.

Por ejemplo, la letra A es el número 10100001. Cuando apretamos la tecla de la letra A, le mandamos la información al ordenador, su correspondiente código binario de 8 cifras, es decir el número (10100001) y el interpreta que le estamos diciendo que queremos que nos saque en la pantalla el símbolo de la letra A.

La letra A (y cualquier carácter) en este código se expresa con 8 bits.




¿Cuánto ocupara un documento formado por 1000 caracteres? Pues muy sencillo 1000 bytes.

**El byte es la unidad básica de almacenamiento en informática** (como metro es de la longitud). Nos sirve para saber lo que ocupa un documento o cualquier programa (instrucciones que tendrá el programa).

Como esta unidad es muy pequeña se suelen utilizar múltiplos de ellas:
1 Byte = 8 bits (una letra, un numero o un espacio en blanco en un documento)
1 Kilobyte = 1024 bytes
1 Megabyte = 1024 Kilobytes
1 Gigabyte = 1024 Megabytes.

Existe otra asociación de bits, que es la **palabra** o también conocida como **longitud de palabra o tamaño de palabra** y se puede definir como el número de bits que un ordenador puede procesar en una única operación. Las longitudes de palabra más habituales en los ordenadores actuales son de 32 y 64 bits dependiendo de la potencia de la máquina.

### 2.3. Clasificación de los ordenadores

Como ordenador, podríamos determinar cualquier dispositivo que tenga en su interior un microprocesador y disponga de memoria e interfaces de entrada/salida para interactuar con el usuario. Antes de ver los componentes que conforman un ordenador, vamos a ver qué tipos de ordenadores podemos encontrar en la actualidad.

1. Supercomputador
2. Computador (mainframe)
3. Miniordenadores
4. Microcomputador (PCs y estaciones de trabajo):
    - De sobremesa
    - Portátiles
    - Tablet, PDA, Palm Top o Pocket
5. Nanoordenadores (computadoras que son sumamente pequeñas, a escalas manométricas o microscópicas).

- **Supercomputadoras:** Es el más poderoso y más rápido, claro que también mucho más caro. Fue desarrollado en 1980. Se utiliza para procesar gran cantidad de datos y para resolver problemas científicos complejos. Es capaz de realizar más de un trillón de cálculos por segundo. En un solo supercomputador miles de usuarios pueden estar conectados al mismo tiempo y la supercomputadora maneja el trabajo de cada usuario por separado. Las supercomputadoras se utilizan en las grandes organizaciones, laboratorios de investigación, centros aeroespaciales, las grandes industrias, Pronóstico del tiempo, Investigación sobre la energía nuclear, Diseño de Aviones, Diseño de Automóviles etc. y normalmente se componen de varios procesadores trabajando en

paralelo. Son equipos con una gran capacidad de cálculo (+ de 1000 billones de operaciones x segundo).

- **Mainframes:** Un mainframe o computadora central es una computadora grande, potente y costosa. Es usada por compañías que procesan gran cantidad de información, como, por ejemplo, para el procesamiento de transacciones bancarias. Soporta la comunicación de miles de usuarios conectados de manera simultánea, que se conectan mediante terminales.
- **Miniordenadores:** similar a mainframes, pero a baja escala, suelen ser ordenadores centrales de pequeñas empresas
- **PC (Personal Computer/Ordenador Personal):** es el ordenador por excelencia. Una microcomputadora es un tipo de computadora que utiliza un microprocesador como unidad central de procesamiento (CPU). Generalmente son computadoras que ocupan espacios físicos pequeños
    - **Ordenador de sobremesa:** No está diseñado para moverse**.** Son grandes y disponen de dispositivos de entrada y salida difícilmente transportables (grandes monitores). Se usan para localizaciones permanentes. Cuentan con elementos adheridos como el ratón o el teclado y entre sus características destacan su gran capacidad de almacenamiento y una mayor potencia que la de los ordenadores portátiles.
    - **Portátiles:** están diseñados para ofrecer prestaciones interesantes facilitando la movilidad de los mismos, es por ello que, a igual de prestaciones que un Pc de sobremesa, suelen ser bastante más costosos. A diferencia de los de sobremesa, los portátiles tienen integradas piezas como el ratón y el teclado, además del disco duro o la memoria. Todo está compactado en un solo dispositivo. Estos equipos incluyen también una batería propia que los dota de autonomía para que se puedan utilizar durante varias horas sin necesidad de enchufarlos a la corriente eléctrica.
    - **PDA:** con la irrupción del iPad en el mercado, el formato PDA se ha extendido como la pólvora. Hace unos años la PDA era prácticamente una agenda con alguno que otro programa como el Office, que ayudaba a hacer las tareas más cotidianas de una oficina. Hoy en día los avances tecnológicos han incrementado el auge de las PDA. Se denominan comúnmente TABLETS, son finos, potentes, con pantallas táctiles y ofrecen gran autonomía.
- **Nanoordenadores:** La nanocomputadora es una computadora con una circuitería tan pequeña que sólo puede verse a través de un microscopio.

**DEFINICION DE TERMINOS:**

**Servidor:** Otro de los ordenadores que tenemos disponibles es el servidor, aunque sus funciones son totalmente distintas. En este caso, este dispositivo va a ofrecer servicios para que otros ordenadores funcionen correctamente, siempre basándose en una red local o en su defecto en Internet. Están diseñados específicamente para ello. Muchos tienen doble microprocesador, grandes cantidades de memoria y múltiples discos duros en

*array*[1]

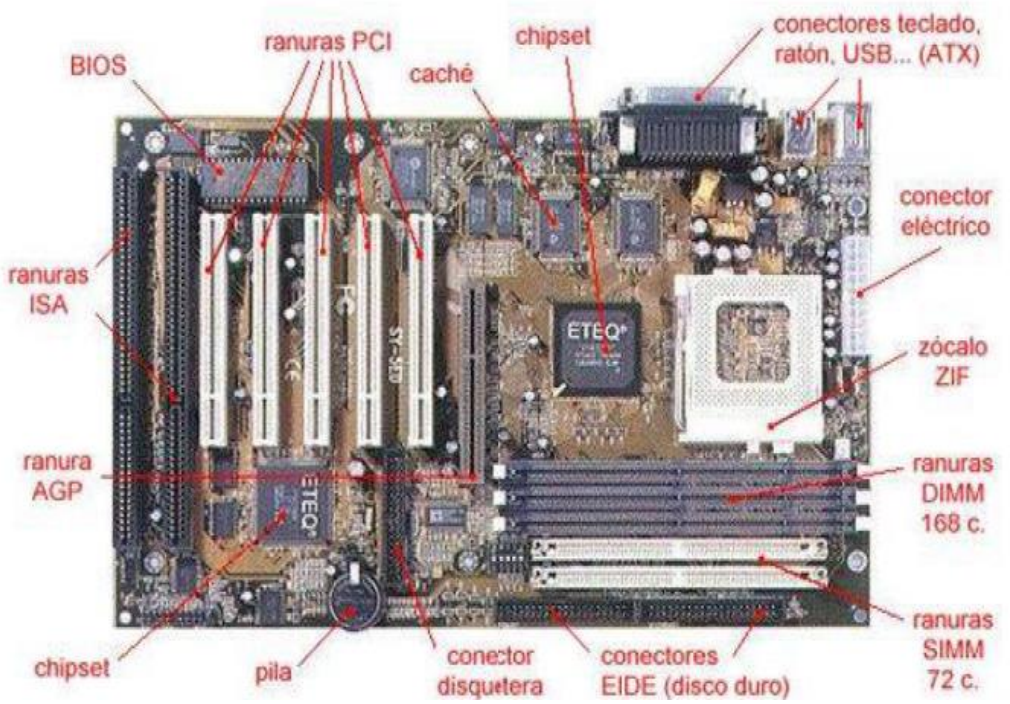
para garantizar que la información nunca se pierda. Su diseño les permite están funcionando las 24 horas del día los 7 días de la semana.

**Workstation:** es un ordenador de sobremesa más potente de lo habitual con microprocesador y componentes más fuertes y diseñados especialmente, que realizan tareas especiales o específicas y más complejas que un ordenador de sobremesa común, dentro de un campo de trabajo. Suelen ser de gran tamaño y peso.

# 3. COMPONENTES DEL ORDENADOR

Cuando hablamos del diseño de un ordenador tenemos que hablar necesariamente de tres bloques diferentes. El primer bloque y el ultimo, como puede verse en el esquema anterior es por donde se introduce o se muestra la información, es lo que vamos a conocer con el nombre de periféricos. El bloque central está formado generalmente por los elementos incluidos dentro de la caja del ordenador. Dos de las partes más importantes son la CPU (Central Pocesing Unit) o UCP (Unidad Central de Proceso) y la memoria principal.

## 3.1. Placa Base

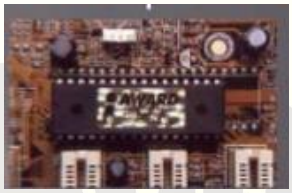



Cuando abrimos un ordenador todos los elementos que hay dentro están montados encima de la placa base con lo cual podemos decir que otro elemento fundamental dentro de los componentes de los ordenadores es la **placa base** o **mainboard**, también conocida con el nombre de **motherboard** o **placa madre.**

[1] Un grupo/matriz redundante de discos independientes (también, RAID, del inglés redundant array of independent disks) hace referencia a un sistema de almacenamiento de datos que utiliza múltiples unidades (discos duros o SSD), entre las cuales se distribuyen o replican los datos.

Los principales elementos situados en la placa base son los siguientes:

- **Buses:** conjunto de cables que nos permiten transferir información de un lugar a otro. Existen tres tipos diferentes: Datos, Dirección y Control
    - Datos: Permite el intercambio de datos entre la CPU y el resto de unidades. Por ejemplo, desde la memoria RAM a la unidad de control.
    - Dirección: Se encarga de llevar las direcciones del lugar de origen o destino de la información que circulan por el bus de datos.
    - Control: se encargan de llevar señales que sirven para controlar los componentes del ordenador.
- **Slots o ranuras de expansión:** es donde vamos a insertar las tarjetas que necesitemos en nuestro ordenador. Existen varios tipos dependiendo de la cantidad de información con la que pueden trabajar como PCI, AGP, PCI EXPRESS.
- **Chipset:** conjunto de chips que se encargan de controlar la información que fluyen a través de la placa del ordenador. Con lo cual es uno de los elementos más importantes dentro de la placa.
- **Memorias principales (RAM y ROM):** Se verán más en detalle.



- **Microprocesador:** elemento encargado de realizar todas las operaciones que se llevan a cabo en el ordenador. También conocido como CPU o UCP:
- **Disipador y ventilador**: Elementos que se colocan encima de algunos chips para enfriarlos. Normalmente siempre lo tendremos como mínimo en el microprocesador para refrigerar la CPU. Primero se coloca el disipador y a continuación el ventilador.

### 3.2. La Unidad central de Proceso (microprocesador)

Es el verdadero cerebro del ordenador ya que coordina y supervisa el funcionamiento de todo el sistema (controla todos los procesos que ocurren en el ordenador) y procesa las instrucciones que compone los programas.

Actualmente la CPU está formada por un conglomerado de circuitos electrónicos integrados en un chip denominado **microprocesador.**


Se estructura en varias unidades:

- Varios registros de acceso rapido donde se almacenan datos temporalmente.
- Memoria cache de primer nivel (L1) y de segundo nivel (L2)
- La Unidad de Control
- Las unidad aritmetico logica.

**Unidad de control (UC):** controlar todos los procesos que ocurren en el sistema. Este componente es responsable de dirigir el flujo (en que orden deben ir, y cuando) de las instrucciones y de los datos dentro de la CPU. Los elementos principales de la unidad de control son registro de instrucción, registgro contador del programa, decodificador, secuenciador y reloj.

**Unidad aritmetica logica(ALU):** esta unidad realiza todos los calculos matematicos de la CPU. La ALU puede sumar, restar, multiplicar, dividir y realizar otros calculos u operaciones con los numeros binarios (funcion logica SI por ejemplo).

### 3.2.1. Características principales de la CPU:

- **La velocidad:** indica el número de operaciones básicas que se realizan en el ordenador. La velocidad de un microprocesador se mide en **MEGAHERTZIOS** (un millón de ciclos por segundo) o **GIGAHERTZIOS.** Que no son más que múltiplos del Hertzio que es el que se puede tomar como unidad básica de medida.
  Ejemplo: suponiendo que tuviésemos un ordenador que fuese a 1 Hz dicho ordenador podría realizar una operación básica por segundo.
- **La longitud de palabra**: se mide en **bits** o valores binarios. La longitud de palabra indica que cantidad de información es capaz de manejar el microprocesador cada vez que realiza un ciclo.

## 3.3. Las memorias del ordenador.

Las memorias que existen en un ordenador se pueden clasificar de muchas maneras, pero la principal clasificación es atendiendo a la ubicación de las mismas. Teniendo en cuenta esto podemos decir que existen dos tipos de memorias, las que están dentro de la placa base del ordenador, denominadas **memorias principales** o centrales y las que están fuera de la plaza base del ordenador, denominadas **memorias secundarias** o memorias de almacenamiento masivo.

### 3.3.1. La memoria central o principal.

La función principal de la memoria principal es almacenar datos e instrucciones de programa de forma temporal. La memoria esta estructurad en forma de una colección de celdas, en cada una de las cuales cabe una unidad específica de información: octetos o palabras. El contenido de cada una de las posiciones de memoria podrá ser bien dato o instrucción. Cada celda tiene asignada una posición relativa con respecto a un origen, cuyo valor numérico constituye la dirección de la misma y que no se encuentra almacenado en ella.

La memoria se caracteriza por lo que llamamos CAPACIDAD o cantidad de máxima de información que puede almacenar. Utilizamos múltiplos de byte como unidades de medida de la capacidad de memoria:

1 kilobyte (1Kb) = 1024 bytes

1 Megabyte (1 MB = 1024 kilobytes

1 Gigabyte (1Gb) = 1024 Megabytes

1 Terabyte (1Tb) = 1024 gigabytes

1 Petabyte (1PB) = 1024 Terabytes

1 Exabyte (1 EB) = 1024 Petabytes

Zettabyte (1 ZB) = 1024 Exabyte

1 Yottabyte (1YB) = 1024 Zettabyte

1 Brontobyte (1BB) = 1024 Yottabyte

1 Geopbyte (1 GeB) = 1024 Brontobyte

1 Saganbyte (1 SB) = 1024 GeB

1 Jotabyte (1 JB) = 1024 SB

Para pasar de una unidad más grande a otra más pequeña, se multiplica por 1024.

TB -- GB --MB -- KB --B

Para pasar de una unidad más pequeña a otra más grande, se divide por 1024.

B -- KB -- MB -- GB – TB

Ejemplos:

¿Cuántos MB de memoria RAM tiene un ordenador que tiene 1GB?

GB--MB(multiplicar)
1GB x 1024MB = 1024MB

¿Cuántos GB de memoria RAM tiene un ordenador que tiene 2048MB?

MB -- GB (dividir)
2048MB / 1024MB = 2GB

La memoria principal de un ordenador se puede dividir principalmente en memorias ROM y RAM.

A) **Memoria RAM.** (Random Access Memory / Memoria de Acceso Aleatorio)

Sus características principales son:

- Su principal función es el almacenamiento intermedio de los datos, es temporal porque los datos y programas permanecen en ella mientras que el ordenador este encendido y el programa en ejecución.
- Es una memoria volátil, es decir en el momento de apagarse el ordenador los datos que hay en ellas se pierden.
- Memoria de acceso aleatorio: Se denominan «de acceso aleatorio» porque se puede leer o escribir en una posición de memoria con un tiempo de espera igual para cualquier posición, no siendo necesario seguir un orden para acceder (acceso secuencial) a la información de la manera más rápida posible.

Hay dos tipos básicos de memoria RAM:

- RAM estática (SRAM). Memoria estática de acceso aleatorio.
- RAM dinámica (DRAM). Memoria dinámica de acceso aleatorio.

También podemos encontrar la **memoria cache** de segundo nivel (L2) que es una memoria muy rápida llamada SRAM que se coloca entre la memoria principal y la CPU. Su función es conseguir que los datos usados estén lo más cerca del procesador para ser accedidos de la manera más rápida.

**B) Memoria ROM**

Sus características principales son:

- Es una **memoria permanente**, es decir, que no pierde los datos cuando se apaga el ordenador.
- Es una memoria de solo lectura
- Se utiliza principalmente para contener los programas de inicialización del ordenador y los programas de chequeo del ordenador (BIOS).

La **BIOS** es un elemento fundamental de cualquier PC. Inicializa y chequea durante el arranque todos los componentes de hardware. Como el disco duro, el teclado, la pantalla, el ratón, la memoria RAM. Luego prepara el equipo para que Windows se cargue y se ejecute.
Su nombre viene de las siglas de BASIC INPUT OUTPUT SYSTEM (Sistema Básico de Entrada/Salida).

Está instalado en la placa base, en ella se encuentran los chips de la ROM BIOS. En él está grabado el software (firmware) que regula lo que tiene que hacer y el modo de hacerlo. El trabajo de la BIOS empieza justo en el momento en que enciendes el PC. Hace de intermediaria entre el hardware (placa, procesador, RAM, discos, etc.) y Windows u otros sistemas operativos.

Al arrancar el equipo el hardware y el software están separados. Ninguno de los dos "sabe" que el otro existe. Tampoco Windows. La BIOS se encarga entre otras cosas de resolver ese problema. Primero comprueba que está todo bien. Luego le dice al hardware dónde buscar el sistema operativo y a Windows qué hardware hay y si está o no disponible.

Si la BIOS detecta un problema grave ni siquiera deja que Windows se cargue. Eso da una idea de lo esencial que es.

Tipos de memoria ROM:

- **PROM**: ROM programable de solo lectura. La característica de una PROM es que sólo se puede escribir una vez en ella, en el momento que escribimos en ella se convierte en una memoria de solo lectura igual que la ROM.
- **EPROM**: ROM programable borrable de sólo lectura. puede ser borrada usando luz ultravioleta y se reprograman electrónicamente.
- **EEPROM**: ROM programable y borrable eléctricamente. Similar en cuanto a comportamiento a la memoria EPROM, la única diferencia es que el borrado se hace mediante electricidad en vez de realizarse con rayos ultravioletas.

### 3.3.2. Jerarquía de Memoria y memoria cache

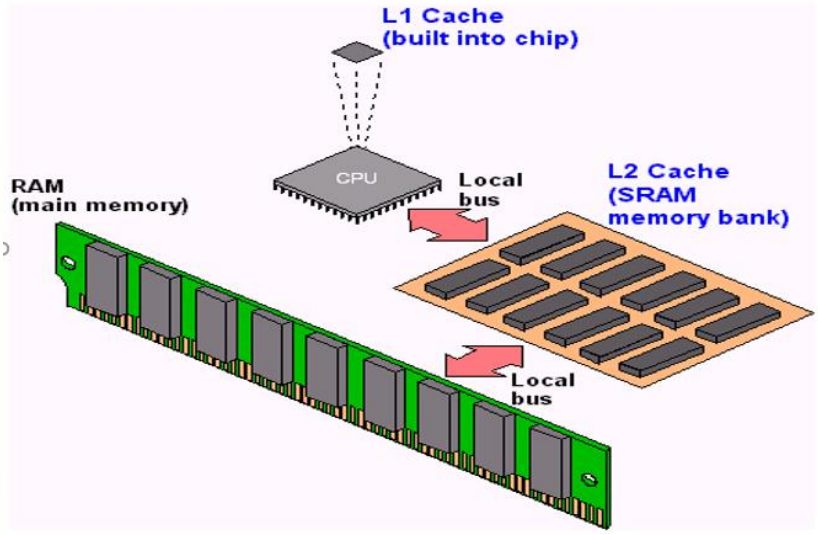
El problema fundamental de la memoria es la relación velocidad /precio. Para leer o escribir un dato en memoria se tarda un tiempo que generalmente es muy grande comparado con la velocidad a la que trabaja la UCP (para leer o escribir en la memoria RAM se necesitan muchos ciclos de reloj). De este modo la UCP debe estar mucho tiempo "esperando" a que lleguen los datos hasta sus registros desde la memoria principal o viceversa. Hacer que la memoria principal vaya a la misma velocidad que la UCP es extremadamente caro.

Hay dos principios en informática que se han demostrado muy eficaces que son:

- Principio de localidad temporal: cuando un dato se acaba de usar, es muy probable que se vuelva a usar próximamente.
- Principio de localidad espacial: cuando un dato se acaba de usar, es muy probable que se usen datos que se encuentran en direcciones de memoria próximas.

En estos principios se basa la utilización de memoria cache. La memoria cache es una memoria más rápida y más pequeña que la memoria principal, que se coloca entre los registros de la UCP y esta. Cuando se necesita el contenido de una dirección de memoria, primero se busca en la memoria cache y, si está allí se utiliza; si no está, se lee de la memoria principal, pero dejando el dato también en la memoria cache.

Los ordenadores actuales suelen trabajar con al menos dos niveles de memoria cache: cache de nivel 1 que se encuentra dentro de la propia UCP y, cache nivel 2 que se encuentra en la placa del ordenador.




Así podemos hablar de una jerarquía de memoria que comienza en los niveles más próximos a la UCP (en los que hay poca memoria, pero muy rápida). Es importante notar que la jerarquía es válida, por lo general, tanto para la velocidad de acceso a la memoria, como para el tamaño de la misma:

- Registro de la UCP
- Memoria Cache
- Memoria Principal
- Memoria secundaria o memoria externa (dispositivos externos, E/S).

### 3.4. Periféricos o unidades de entrada / salida

Podemos definir a los periféricos como elementos capaces de intercambiar información entre la CPU y un soporte. Para que un periférico pueda ser utilizado por el ordenador, necesita instalar sus drivers o controladores (software que permite al sistema operativo reconocer y utilizar los diferentes periféricos).

Se pueden clasificar siguiendo distintos criterios:

- Según el sentido en que se transmite la información:
    - **Unidades de entrada**: El usuario pregunta al ordenador, le dice que tiene que hacer (instrucciones) y con que hacerlo (datos). Mediante estas unidades se introduce en el ordenador información a procesar.
    - **Unidades de salida**: EL ordenador contesta al usuario, le muestra los resultados de las operaciones realizadas en base a lo requerido. Mediante estas unidades se muestran los resultados obtenidos de las operaciones realizadas.
    - **Unidades de E/S:** realizan los dos sentidos de la comunicación, introducen información al ordenador y muestran los resultados. Mención especial a los periféricos de E/S denominados unidades de almacenamiento o memorias secundarias, que se pueden considerar como periféricos de e/s por el sentido en que se realiza la comunicación.
- Según la distancia del ordenador:
    - **Periféricos locales**: se conectan directamente a la CPU.
    - **Periféricos remotos**: No conectado directamente al ordenador. Por ejemplo, impresora de red.

La comunicación de los periféricos con el ordenador se realiza mediante **CANALES DE E/S.** Pueden ser **unidireccionales** si la información fluye en único sentido o **bidireccionales** si fluye en ambas direcciones.

Estos canales se conectan en el ordenador en unos puntos denominados puertos de comunicaciones. Dichos puertos pueden ser de dos tipos: **Puertos serie** donde la transmisión de información se realiza bit a bit (COM1, COM2, PS/S, USB, FIREWIRE) y **puerto paralelo** donde la transmisión se realiza byte a byte (LPT1).

#### 3.4.1. Periféricos de entrada:

- Teclado
- Ratón o mouse
- TrackBall
- Touchpad
- Lápiz óptico
- Lector de bandas magnéticas
- Joystick
- Escáner
- Tableta digitalizadora
- Webcam
- Micrófono (necesita tarjeta de sonido)

### 3.4.2. Periféricos de salida

- **Pantalla:**

  Normalmente funciona por la interface VGA que es la interfaz analógica basada en la tecnología RGB (red blue Green) o HDMI interfaz digital que muestra la imagen y la codifica en formato digital obteniendo mucha mejor calidad.

  Actualmente la calidad de las pantallas ha evolucionado enormemente pasando del estándar VGA que era de 640x480 o 1024x768 a FullHD (1080) e incluso 4K. También han evolucionado desde los antiguos monitores de tubo CRT a las pantallas leds actuales.

  Para la comunicación con el ordenador y la pantalla se utiliza otro periférico denominado **tarjeta gráfica o adaptador gráfico**. Esta controla la resolución de la pantalla, la paleta de colores y la tasa de refresco.
  Ejemplos de tarjetas de video: MDA, CGA, EGA, VGA, SVGA O XGA.

  **Características:**

  - El tamaño del monitor se mide en pulgadas.
  - Resolución: se define como el número de puntos luminosos (pixel) de los que consta la pantalla.
  - Dot pitch: describe la distancia entre puntos del mismo color.
  - Tasa de refresco: Indica el número de veces por segundo que la imagen en pantalla se actualiza. Se mide en hercios (Hz), una unidad que indica la frecuencia con la que ocurre algo en un segundo. Ejemplo, si nuestro monitor es de 30 hercios, la imagen se actualizará 30 veces cada segundo.

- **Impresora.**

  Las impresoras se pueden dividir en categorías siguiendo diversos criterios.
  La distinción más común se hace entre:

  - **Impresoras de impacto**: golpean el papel con algún medio mecánico. Matriciales (la impresión se produce al golpear una aguja o una rueda de caracteres contra una cinta con tinta) de líneas o banda etc.

  - **Impresoras de no impacto**: Abarcan todos los demás tipos de mecanismos de impresión, incluyendo:

    - impresoras térmicas, la impresión se realiza mediante la aplicación de calor a los cabezales de la impresora (impresión de tickest, etiquetas, faxes).
    - impresoras de inyección o impresoras de chorro de tinta, utilizan cartuchos de tinta.
    - impresoras láser. Tecnología láser, utilizan Tóner.

Además, se pueden seguir otros criterios para clasificar las impresoras como son:

**1. Por el método de impresión (número de caracteres que pueden escribir simultáneamente)**

. **Impresoras de caracteres**. Impresión carácter a carácter de forma secuencial. (Matriciales, de inyección de tinta, térmicas, de margarita). La velocidad de impresión se mide en CPS (caracteres por segundo).

. **Impresoras de líneas.** Realizan la impresión línea a línea. Las impresoras de líneas se subdividen en impresoras: de cinta, de cadena y de tambor. La velocidad de impresión se mide en LPM (líneas por minuto).

. **Impresoras de páginas**. Imprimen una página de una vez. Entre las impresoras de páginas se encuentran las electrofotográficas, como las impresoras láser. La velocidad de impresión se mide en páginas por minuto (PPM).

**2. Por el Método de transmisión**

Esta clasificación se refiere al medio utilizado para enviar los datos a la impresora:

- **Paralelo**: transmisión byte a byte.
- **Serie:** transmisión bit a bit.

Actualmente, la tendencia es a favor de las impresoras en serie, a través del estándar USB o bien integrarlas en la red LAN mediante cable de red o inalámbrico por Wifi.
También podemos encontrar impresoras integradas en equipos multifunción que disponen de escáner o captura de imágenes y capacidades de fotocopiadoras.

- **Plotter.** También llamados trazadores. Trabajan con la tecnología de inyección de tinta. Permite realizar proyectos de impresión de grandes dimensiones. Se utiliza en el ámbito de la arquitectura para dibujo de planos, para proyectos publicitarios etc.
- **Altavoces.** Reproducción del sonido procedente de la tarjeta de sonido. El sistema de altavoces puede ir desde el sistema básico con dos altavoces estero hasta otros sistemas multicanal, como el Dolby Digital (6 canales de audio-6 altavoces); también existen diferentes modelos en función de su potencia. Un ejemplo de reproductor de sonido son los auriculares, que solo permiten la salida de audio a través de su canal.
- **Proyector**. Dispositivo que recibe la señal de viedo y la proecta sobre una superficie, mediante un sistema de lentes.

### 3.4.3. Periféricos de entrada y salida

Dichos periféricos cumplen las dos funciones introducir y sacar información del ordenador. Se dividen en dos categorías: aquellos que están destinados a introducir y sacar información del ordenador y las memorias secundarias que están destinadas al almacenamiento de la información dentro del ordenador.

- **Periféricos propiamente dichos:**
  - Lectoras perforadoras de tarjetas
  - Consola: formada por teclado y pantalla
  - Pantalla táctil
  - Modem
  - Tarjeta de red.

### 3.5. Memorias secundarias. Sistemas de almacenamiento de datos.

Destacan los discos duros como dispositivo de almacenamiento interno, los DVD con sus correspondientes grabadores en el equipo como dispositivos de almacenamiento externo y Pendrives o memorias USB que están ganando terreno por el aumento de la velocidad y capacidad de los mismos.

- **Dispositivos de almacenamiento por medio magnéticos**
    - **Disquetes** en desuso, han sido reemplazadas por las memorias USB.
    - **Cintas magnéticas o streamer**, se utilizan principalmente para realizar copias de seguridad o backups.
    - **Discos duros** llamados discos Winchester, Harddisk o DisKpack. Alta capacidad de almacenaje (ya hay discos duros de 8TB o más). Podemos conectar discos duros al ordenador de diferentes formas:
        - Discos duros externos: son discos duros portables.
        - Discos duros internos se instala en el PC o portátil. Hay de dos tamaños 2.5" y 3.5" y tienen distintas capacidades que alcanzan hoy en día los 19 Tb. Para conectarse con la placa base usa la interfaz SATA, aunque antiguamente se utilizaba otro interfaz denominado IDE.
    - **Disco duro de Estado sólido (SSD):** utiliza una tecnología diferente debido a que no dispone de cabezales como el anterior, Es más rápido, fiable y caro.
    - **Pendrive** (lápices de memoria, memoria externa, USB, llavero USB, memorias flash). Ttecnología flash, mediante impulsos eléctricos. Usado para llevar la información de un sitio a otro. Hay de muchas capacidades distintas (1GB, 2,4,8,16,32,64,128,256,512,1TB y 2TB) y según la velocidad de trasferencia (USB 1.0, 1.1,2.0,3.0, y ya se habla de USB 4.0) podrán ser más o menos caros.
- **Dispositivos de almacenamiento por medio óptico**
    - **CD** La información se registra en una superficie donde se generan minúsculas perforaciones denominadas PITS, capaces de ser leídas utilizado la reflexión de un haz laser.
    - **DVD** (Disco Versátil digital): Es el sucesor del CD y la diferencia entre ellos radica en que el DVD tiene una capacidad de almacenamiento y una velocidad de acceso y transferencia muy superiores al CD. (CD= 700 MB; DVD= 17GB).
    - **Blu-ray** es un formato de disco óptico de nueva generación para video de alta definición y almacenamiento de datos de alta densidad. Su capacidad de almacenamiento puede llegar a 50 GB.
    - **M-Disc** (DVD MDisc o Blu-ray MDisc) es el sistema óptico más avanzado hasta el momento, se le conoce como Milennial Disc. Son dispositivos muy resistentes que garantizan la durabilidad y conservación de los datos, incluso en ambientes poco favorables.

Para evitar pérdidas de información por daño en los discos duros, se utilizan los denominados **RAID**. Los RAID son formas de conectar los diferentes discos duros para llevar a cabo redundancia en la información. Para ello el dispositivo debe permitir usar esta característica y disponer de varios discos duros.

Los formatos RAID más extendidos son**:**

**Raid 0**: Reparte los datos entre todas las unidades del grupo RAID. No se almacena ninguna información de redundancia. Esto significa que si falla o hay avería en unos de los discos conlleva la pérdida total de los datos.
**Raid 1**: Duplica en espejo todos los datos de cada unidad de forma sincronizada a una unidad de duplicación exacta. Si se produce algún fallo o avería en alguna de las unidades nos ser pierde ningún dato.
**Raid 5**: Es de tres o más unidades de disco duro con los datos que se dividen en bloques administrables denominados divisiones La principal ventaja de RAID 5 son la capacidad de almacenamiento y de protección de datos.

En la actualidad existe otro medio de almacenamiento de datos que se está extendiendo mucho y es lo que conocemos como **NUBE**. Consta de varios servidores gestionados por terceras personas y que garantizan el almacenamiento de la información en Internet con suficiente seguridad y confidencialidad.

## 4. EL SOFTWARE O ELEMENTO LOGICO

El software es la parte lógica del ordenador, la parte intangible, incluye el Sistema Operativo, los programas, el Interface, es decir, lo que puede ser modificado con relativa facilidad en contraposición al hardware que requiere de elementos físicos.

Desde el punto de vista de su funcionalidad podemos clasificar al software en tres grandes grupos:

- **Software de sistema**: (Software básico o fundamental): Controla y optimiza la operación de la máquina. Actúa como intermediario (interfaz) entre el usuario y el hardware.
    - Sistema Operativo
    - Controladores de dispositivos
    - Software de diagnostico
- **Programas de aplicación**: Es un tipo de software que funciona como un conjunto de herramientas diseñado para realizar tareas y trabajos específicos en tu computador. Indican a la maquina como resolver problemas específicos del usuario.
    - Aplicaciones ofimáticas
    - Aplicaciones de calculo
    - Aplicaciones para diseño asistido por ordenador (CAD)
    - Aplicaciones empresariales

- **Lenguajes de programación**: lenguaje empleado para escribir un programa para un ordenador, formado por un conjunto de técnicas con una sintaxis y unas normas propias.
    - Entornos de desarrollo es una aplicación informática que proporciona servicios integrales para facilitarle al desarrollador o programador el desarrollo de software, es un editor de código fuente.
    - Compiladores un compilador es un programa informático que transforma código fuente escrito en un lenguaje de programación o lenguaje informático (el lenguaje fuente), en otro lenguaje informático (el lenguaje objetivo, estando a menudo en formato binario conocido como código objeto)
    - Depuradores es un programa usado para probar y depurar (eliminar) los errores de otros programas (el programa "objetivo").

### 4.1. Como funciona un Sistema Operativo

El sistema operativo actúa como una capa intermedia entre el hardware y los programas de aplicaciones. Se encarga de interpretar las órdenes y adecuarlas al hardware para que el usuario trabaje más fácilmente. Debe realizar diferentes funciones como son:

- Administrar el procesador
- Gestión de memoria del sistema
- Gestión de entradas y salidas
- Gestión de ejecución de aplicaciones
- Administración de autorizaciones
- Gestión de archivos.

Hay varios sistemas operativos para ordenadores en el mercado entre ellos podemos destacar los siguientes:

- **Windows** sistema operativo por excelencia para el usuario medio.
- **Unix** Sistema operativo multitarea, portable y multiusuario.
- **Linux** sistema operativo libre. Hay muchas variantes de LINUX (Ubuntu, Red Hat, etc.)
- **Mac OS** sistema operativo propio de los Mac

**¿Qué partes componen un Sistema Operativo?**

- **Núcleo o Kernel (**núcleo en alemán**)** es aquella parte de un sistema operativo que interactúa de forma directa con el hardware de una máquina. Entre las funciones principales del kernel se encuentran:
    - La gestión de memoria.
    - La administración del sistema de archivos.
    - La administración de servicios de entrada/salida.
    - La asignación de recursos entre los usuarios.
- **Interprete de comandos** posibilita la interacción con el sistema operativo a través de una serie de comandos que independiza al usuario de las características de los dispositivos.

# 5. Nociones básicas de Seguridad informática.

Veremos algunos aspectos en los que hay que incidir dentro de la política de seguridad de la organización, atendiendo a las diversas áreas de actuación de la misma y a las problemáticas que podemos encontramos. Atenderemos a los diversos activos que debemos proteger en función de la tipología de intrusión que pueda darse:

- **Interceptación de las comunicaciones**: las comunicaciones pueden ser interceptadas y modificar o capturar la información contenida en ellas. Esta interceptación puede ser de varias maneras y debemos tenerlas en cuenta para evitarla en la medida de lo posible.
- **Acceso no autorizado a ordenadores y redes**: aquí englobaremos los intentos de acceso a la información contenida en algún ordenador de la organización a los recursos de las redes (impresoras, discos duros etc.)
- **Virus y posibles modificaciones de datos**: habrá que protegerse sobre posibles virus que alteren los datos y la información almacenada en el sistema.
- **Accesos mediante suplantaciones de usuarios**: hay que asegurarse bien de tener medios de identificar adecuadamente a los usuarios para evitar accesos al sistema utilizando falsas identidades.
- **Accidentes:** no hay que olvidar posibles accidentes que puedan influir en la perdida de datos o en la eventual caída de sistemas (tormentas, incendios, inundaciones etc.). También habrá que contemplar estas posibles contingencias en el plan de seguridad.

Algunas de las medidas que podemos tomar para proteger el sistema de información de la organización son:

- **Firewall:** es un elemento hardware que impide la entrada de intrusos en la red interna de la organización.
- **Antivirus:** es un software que supervisa constantemente los flujos de información existentes en la organización y que detecta y elimina los posibles virus que puedan dañar la información.
- **Gestión de usuarios**: los softwares para gestión de redes, suelen presentar siempre gestión de usuarios para proteger el sistema de usos indebidos.
- **Actualización y parches**: Es muy importante tener actualizado nuestro sistema informático, con las últimas actualizaciones del sistema operativo. Windows en sus últimas versiones ya incorpora una aplicación destinada para dicho fin denominada Windows Update.
- **Copias de seguridad**
- **SAI:** Sistema de Alimentación Ininterrumpida. Es una batería que permite que el ordenador siga funcionando, aunque no haya corriente eléctrica.

**Recuerde que:**

- Nunca deshabilite el antivirus
- No confié en emails de remitentes desconocidos o con asuntos extraños o sin asunto
- Nunca entre en webs de bancos a través de enlaces directos que le envíen.
- Procure tener claves largas con mezcla de números, letras, mayúsculas y minúsculas.
- Modifique las claves periódicamente
- Siempre tenga su usuario de Windows protegido por contraseña.

## 5.1. Responsabilidad personal de los documentos manipulados

### 5.1.1. Confidencialidad de los datos tratados

Tras la entrada en vigor de la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD), se han protegido enormemente los datos de carácter personal y existen duras sanciones por su filtración o manipulación.

**Artículo 1**. **Objeto:** La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

Además de los medios indicados en el plan de seguridad de la organización, deberemos aplicar medidas extraordinarias para prevenir la filtración de datos. Una parte muy importante de estas medidas reside en el encriptado de la información cuando circule por nuestra organización. De este modo, ante una posible filtración de la información se hace más difícil la visión de los datos contenidos gracias al encriptado.

Lo que buscamos principalmente, es que los datos solo sean conocidos por el emisor y el receptor al que van dirigidos.

Existen técnicas criptográficas basadas en el cifrado de la información como es la Criptografía que es la parte de la criptología[2] que se ocupa del cifrado de mensajes. Se basa en que el emisor emite un mensaje en claro, que, mediante un cifrador con la ayuda de una clave, creara un texto cifrado. Este texto mediante un canal de comunicación, llega al descifrador que con la ayuda de otra clave convierte el texto cifrado en texto claro original. Las dos claves implicadas en el proceso de cifrado/descifrado pueden ser o no iguales dependiendo del sistema de cifrado utilizado.

Los tipos de cifrado pueden ser:

- **Simétrico**. Son aquellos que utilizan la misma clave para cifrar y descifrar un documento.
- **Asimétrico.** También llamado sistema de cifrado de clave pública, usa dos claves diferentes, una clave pública y otra clave privada.
- **Hibrido.** Usa tanto los sistemas de clave simétrica como el de clave asimétrica.

### 5.1.2. Utilización de datos de forma exclusiva

Para que se utilicen los datos de forma exclusiva, necesitamos un **sistema de gestión de usuarios**, ya que de otro modo no podemos identificar de ninguna forma a la persona que está accediendo a los mismos.

Estos sistemas de gestión de usuarios nos permitirán:

- Gestionar usuarios y sus datos de identificación
- Asignarles permisos en función de sus necesidades
- Controlar el acceso a los recursos.

[2] **Cristología**: estudio y practica de los sistemas de cifrado destinados a ocultar el contenido de mensajes enviados entre emisor y receptor

Estos sistemas de gestión de usuarios permitirán y facilitarán la gestión de estos permisos, accesos a recursos, etc. dentro de la red de nuestra organización.

Entre las diversas opciones que existen nos podemos encontrar las siguientes:

- **Control de acceso a la red corporativa**: estos sistemas evitaran el acceso indebido a los recursos de la red corporativa desde el exterior (o desde el interior por usuarios malintencionados). Controlan el acceso de usuarios, dispositivos y otras redes, a la red corporativa.
- **Gestión de identidad y autenticación y servidores de autenticación**: son sistemas centrados en gestionar la identidad y la correcta autenticación de los usuarios en la red y en la organización. Están centralizados y permiten otorgar de una forma rápida y segura los privilegios, roles, autenticaciones, etc. necesarios para el correcto funcionamiento de la organización. La autenticación es el proceso de verificación de la identidad del remitente de una información o de un intento de acceso al sistema.
- **Inicio de sesión único:** permiten el acceso a diversos recursos, programas o dispositivos de la red, mediante un identificador único.
- **Sistema de identidad**: permiten acceder a varias localizaciones, portales de redes mediante una única identificación de usuario.
- **Sistemas de control de presencia y acceso**: estos sistemas cuentan con técnicas biométricas (características propias de cada individuo, como voz, huella dactilar, rostro etc.) o bien tarjetas de acceso, para controlar quien y cuando está presente en alguno de los sistemas o dispositivos de la organización.

Para gestionar los usuarios se deberán llevar a cabo una serie de pasos básicos, que los llevara a cabo el **Administrador del sistema**, y son:

- **Evaluación de las necesidades**. Debemos ver que empleados necesitan acceder y que datos necesita para poder tener acceso a ellos.
- **Creación de usuarios**. Se crearán los usuarios necesarios para las personas que deban acceder a la red.
- **Creación y asignación de permisos**. Se crearán los diferentes niveles de accesos y se asignarán en función de su necesidad.
- **Asignación de códigos de usuario.** Por ultimo a cada usuario se le asignara un código de acceso único, para garantizar su privacidad y que sus permisos queden bajo su responsabilidad.

Tras llevar a cabo la gestión de usuarios en nuestro sistema, podremos garantizar que cada uno de ellos solo podrá ver la información que le sea necesaria y le quedará oculta aquella a la que no deba acceder.

### 5.1.3. Respuesta y responsabilidad ante errores o infracciones cometidas en la manipulación de datos.

Es el administrador del sistema quien debe dar respuesta a las incidencias que ocurren en la red y es su responsabilidad garantizar la integridad y el buen estado de la misma.

Generalmente los principales datos de una organización se encuentran en una base de datos, ya que es el método más eficaz de guardar la gran cantidad de información que se suele manejar. Sera responsabilidad del administrador del sistema realizar **copias de seguridad** periódicas de las bases de datos y de toda la información necesaria e indispensable para el correcto funcionamiento y restauración de la actividad de la empresa tras un posible fallo informático.

Las **copias de seguridad o backups** son copias periódicas de la base de datos y de los archivos con contenido importante de la empresa, que se hacen periódicamente, generalmente de manera automática, mediante algún software específico.

Las copias de seguridad solo serán accesibles para el administrador.

Si se dispone de los suficientes recursos, es conveniente establecer diversos sistemas redundantes, de manera que ante la caída de uno se pueda seguir funcionando con otro.

El administrador además de gestionar las copias de seguridad deberá velar por la fluidez y correcto funcionamiento de todo el flujo de datos y de información dentro de la organización.

Ante una infracción por parte del usuario, será el responsable, atendiendo al plan de seguridad establecido en la organización, quien determine las sanciones oportunas.

## 5.2. FIRMA DIGITAL

**Firma digital,** es el conjunto de caracteres que se añaden al final de un documento o cuerpo de un mensaje para informar, dar fe o mostrar validez y seguridad. Consiste en la utilización de un método de encriptación llamado asimétrico o de clave pública.

La firma digital sirve para identificar a la persona emisora de dicho mensaje y para certificar la veracidad de que el documento no se ha modificado con respeto al original.

No se puede negar haberlo firmado, puesto que esta firma implica la existencia de un certificado oficial emitido por un organismo o institución que valida la firma y la identidad de la persona que la realiza. La firma digital se basa en los sistemas de criptografía de clave pública (PKI – Public Key Infrastructure) que satisface los requerimientos de definición de firma electrónica avanzada.

De esta manera, la firma digital es la que tiene validez legal, evita la suplantación de identidad y permite la autenticación e identificación en toda clase de procesos administrativos, burocráticos o fiscales, entre otros.

### 2.1 Las Autoridades de Certificación

Una Autoridad de Certificación (AC, en inglés CA) es una entidad de confianza del emisor y del receptor del mensaje. Esta confianza de ambos en una 'tercera parte confiable' permite que cualquiera de los dos confíe a su vez en los documentos firmados por la Autoridad de Certificación, en particular, en los documentos que identifican cada clave pública con su propietario correspondiente y se denominan certificados.

Para obtener el certificado digital podemos optar por un tipo de certificado contenido en una tarjeta, DNIe o por un certificado que se guarda en un fichero informático.

En ambos casos es necesaria la identificación del usuario del certificado lo que conlleva que este se persone en una oficina de la Autoridad de Registro para que se compruebe su identidad.

- **Certificado en Tarjeta (DNIe).** Este tipo de certificado debe entregarse directamente al usuario en la oficina de la Autoridad Certificadora (Dirección General de Policía).
- **Certificado Software**. La solicitud y descarga de este tipo de certificados se realiza desde el navegador del usuario, que deberá asegurarse de realizar los dos tramites desde el mismo dispositivo.

El principal proveedor de certificados software es la Fábrica Nacional de Moneda y Timbre (FNMT) a través de su departamento CERES (Certificación Española).

Emite certificados electrónicos reconocidos por la mayoría de las Administraciones Publicas: FNMT Clase 2CA y AC FNMT Usuarios.

Otros proveedores de certificación son: Agencia Catalana de Certificació, Agencia Notarial de Certificación(ANCERT), Banco de España o Gerencia de Informática de la Seguridad Social (GISS), Autoridad de certificación de la abogacía (ACA) entre otros.

# ANEXO

## TERMINOLOGÍA BÁSICA DE SEGURIDAD INFORMÁTICA[3]

- **3DES** (Triple DES): algoritmo de cifrado
- **AES**: algoritmo de cifrado
- **Amenaza**: elemento potencial de causar daños en sistema.
- **Antivirus**: software para proteger el equipo de virus
- **BlackListing** (lista negra): Proceso de bloqueo de programas o equipos malicioso o desconocidos.
- **Ciberseguridad**: campo de estudio dedicado a la seguridad informática.
- **Cifrado**: procedimiento para proteger la información mediante algoritmos.
- **Encriptado**: procedimiento para ocultar la información mediante algoritmos.
- **Firewall**: elemento para evitar accesos no autorizados.
- **Gusanos**: programas que se copian a si mismo con el objetivo de colapsar los ordenadores para impedir el trabajo normal de los mismos.
- **Hacker**: persona experta en vulnerar sistemas informáticos.
- **Hacking**: acceso no autorizado a sistemas informáticos por parte de terceras personas (Hackers).
- **Malware**: programas diseñados para dañar un sistema informáticos
- **Negación de Servicio** (DoS): ataque masivo a sistemas para colapsar sus servicios y que no permitan su utilización a los usuarios legales de los mismos.
- **Pishing**: termino con el que se designa la suplantación de páginas web para obtener daos de los usuarios como cuentas bancarias, PIN de tarjetas, etc.
- **PKCS7**: conjunto de normas para cifrar y encriptar.
- **Spam**: correo no deseado.
- **SpyWare**: aplicación que realiza seguimiento no autorizado del uso del PC y lo envía a terceros.
- **TKIP**: algoritmo de cifrado.
- **Troyano**: software malicioso que bajo una apariencia engañosa permite obtener el control del equipo.
- **WEP**: algoritmo de cifrado.
- **WPA** o WPA2: algoritmos de cifrado
- **Zombi**: PC controlado remotamente por algún Hacker.

[3] En www.incibe.es (Instituto Nacional de ciberseguridad) podemos encontrar un completo glosario de términos. El enlace es el siguiente: **https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf**