TEMA 19 OFIMATICA: Informática básica:

ÍNDICE:

1. Conceptos Fundamentales sobre el Hardware y el Software.

El trabajo en un PC viene determinado por dos elementos, que son el Hardware y el Software. La combinación de ambos hará que pueda realizar tareas en el equipo y obtener resultados óptimos de las mismas. Veremos en qué consiste cada uno.

1.1. Hardware

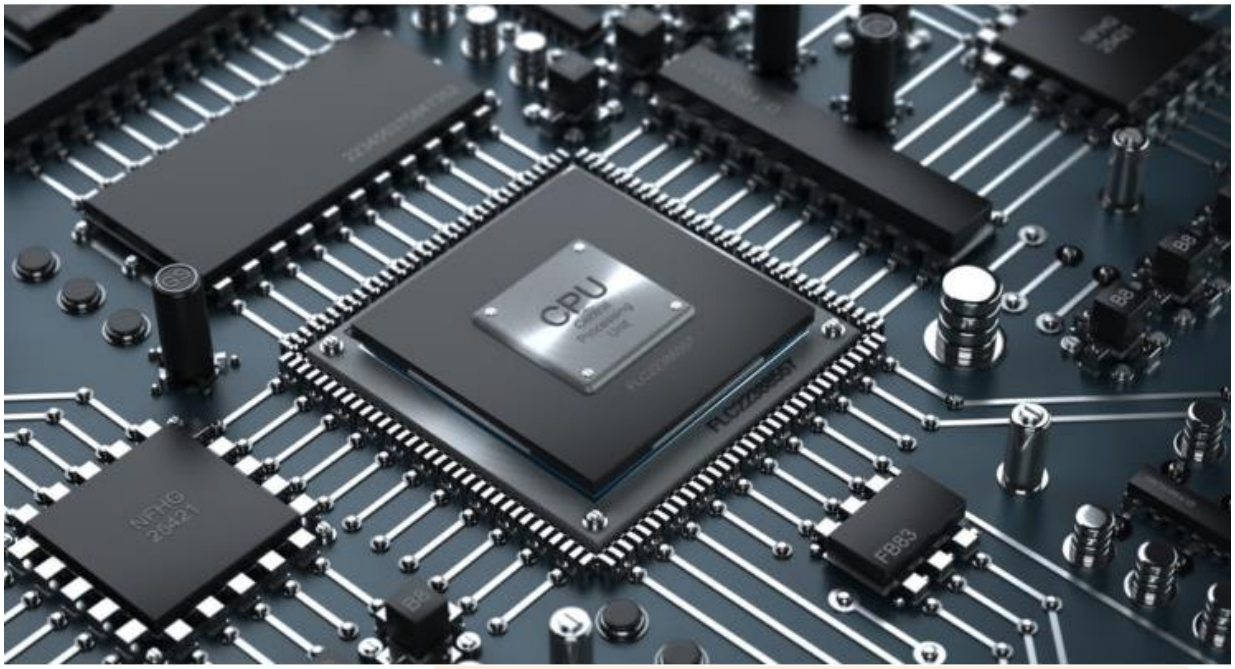
El Hardware es la parte física del ordenador, la parte tangible. Son los elementos que se pueden tocar, coger, etc. Se pueden clasificar de diversas formas, tal y como veremos **a continuación.**

1.1.1. Tipología y clasificaciones

Hay distintas formas de clasificar los elementos físicos de un equipo. La más utilizada es distinguir entre **Hardware Básico,** que sería indispensable para el funcionamiento de un equipo y **Hardware Complementario,** que supondría mejoras en el rendimiento de este.

¿Qué necesita un PC como mínimo para funcionar? **El Hardware Básico** incluiría al menos los siguientes elementos:

- **CPU Unidad Central de Proceso:** para poder procesar la información y llevar a cabo acciones.
- **Memoria:** para poder almacenar las acciones a realizar.
- **Dispositivo entrada/salida:** para poder recibir los datos y enviar las acciones a realizar en función de ellos.



CPU

Memoria

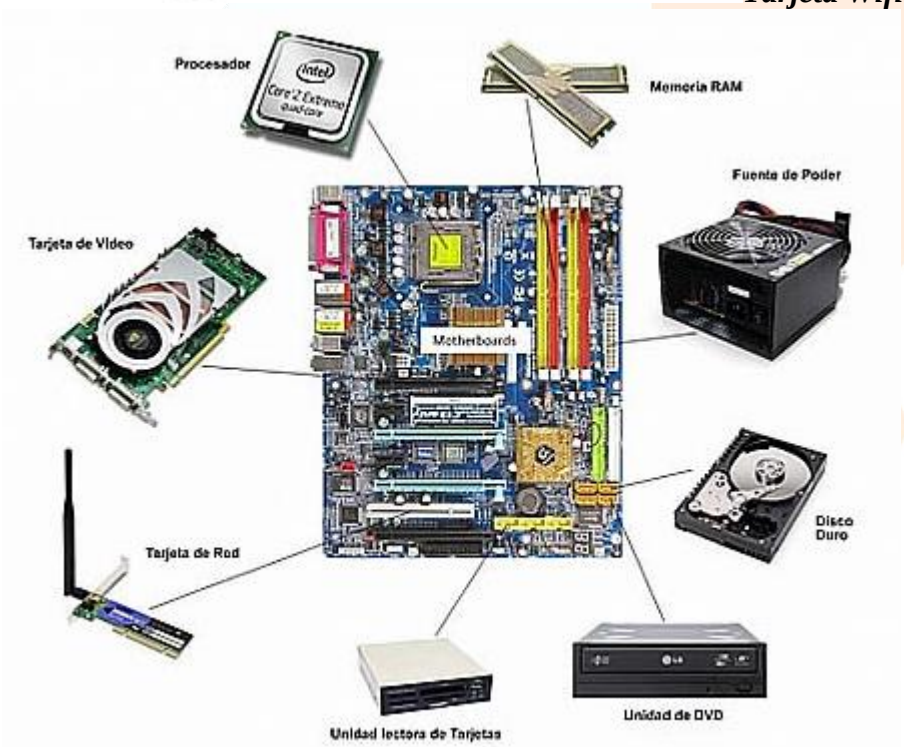
Dispositivos E/S

El **Hardware Complementario** mejoraría las prestaciones del Hardware básico dotándolo de diversos elementos adicionales, como pueden ser tarjetas gráficas 3D, graba dores de DVD, lectores de tarjetas, tarjetas de red o Wifi, etc.

Tarjeta gráfica

Lector DVD

Tarjeta Wifi



Conjunto de elementos de un PC

Una vez que se han podido ver los dos tipos de Hardware que hay, ¿cómo se clasifican los distintos elementos Hardware? Lo más habitual es atender a una clasificación relacionada con la funcionalidad de los elementos. Así tendríamos los siguientes grupos:

- **Almacenamiento:** este hardware permite almacenar información, bien para breves espacios de tiempo, como es el caso de la memoria RAM, o de manera más prolongada, como ocurre con los discos duros, memorias USB, DVD, etc.

- **Proceso:** es el hardware encargado de llevar a cabo las operaciones, procesos, etc. Pueden ser el Microprocesador, la ALU (Unidad Aritmético Lógica, que realiza operaciones matemáticas) o los Chipset presentes en las placas Base para agilizar las **comunicaciones.**

- **Entrada:** sirven para recibir los datos desde el exterior; pueden englobarse en este apartado los teclados, ratones, puertos de entrada de datos, etc.

- **Salida:** se usan para sacar la información al exterior; he aquí los monitores, impresoras, puertos de datos de salida, etc.
- **Bidireccional:** funcionan tanto de entrada como de salida, por ejemplo, la tarjeta de red.

Sabías que...

El **bit** es la unidad mínima de información empleada en informática. Con él, podemos representar todos los valores, basta con asignar uno de ellos al estado de "apagado" (O), y el otro al estado de "encendido".

El **byte** es la unidad de capacidad de almacenamiento estándar. Con esta unidad de medida se mide desde el almacenamiento de datos has ta la capacidad de memoria de un ordenador. Representa un carácter (un número, una letra, un espacio, o cualquier otro signo) y está consti tuido por 8 bits consecutivos, de forma que un byte equivaldría a 8 bits. Hay 256 combinaciones de 8 bits posibles, por lo que hay 256 caracteres.

Existen otras magnitudes que se utilizan para capacidades superiores y que son múltiplos del byte (Múltiplos de 8).

1 **KiloByte (KB)** = 1024 Bytes	1 **MegaByte (MB)** = 1024 KB
1 **GigaByte (GB)** = 1024 MB	1 **TeraByte (TB)** = 1024 GB
1 **Peta Byte (PT)** = 1024 TB	1 **ExaByte (EB)** = 1024 PT
1 **ZetaByte (ZB)** = 1024 EB	1 **YottaByte (YB)** = 1024 ZB
1 **BrontoByte (BB)** = 1024 YB	1 **GeopByte (GpB)** = 1024 BB

En algunos estamentos (no es la norma) se toman las unidades antes mencionadas como múltiplos de 10 (es decir, se multiplican por 1000 en lugar de por 1024) y se reservan los múltiplos relacionados con 1024 ... Kibibyte... MebiByte.

Antes de ver los componentes que conforman un ordenador, veremos **qué es un ordenador** y qué tipos nos podemos encontrar en la actualidad. Hoy en día, el ordenador forma parte de nuestra vida cotidiana, aunque esto no siempre fue así. No concebimos el día a día actual sin nuestro móvil, PC, portátil, etc.

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. Dentro de esa definición de ordenador caben muchas posibilidades, algunas de las cuales enumeraremos a continuación para conocer las diversas opciones existentes hoy en día en lo referente a tipos de ordenador:

PC *(Personal Competer):* es el ordenador por excelencia. Está diseñado para un uso general y puede ser utilizado por varias personas. Como veremos en los siguientes tipos, algunos de ellos se refieren a los PC (portátiles o de sobremesa). Entre los diversos PC se pueden distinguir dos grandes ramificaciones que enumeraremos **a continuación:**

* **MAC:** son ordenadores personales Apple, basados en sus procesadores RISC y su sistema operativo Macintosh. Son usados principalmente para tratamiento de imágenes y vídeos, aunque en los últimos tiempos se está extendiendo su utilización gracias a la aparición del iPhone.

*** No MAC:** ¿cómo englobar al resto de ordenadores personales? Si bien los MAC se pueden denominar así por ser específicos y concretos, el resto de ordenadores personales tienen una diversidad tal que no se podrían enumerar. Fuera de los MAC tenemos ordenadores personales con micro INTEL o AMD y estos pueden funcionar a su vez bajo sistemas operativos diversos como Windows o Linux. La gran mayoría de los PC utilizados comúnmente se basan en el sistema operativo Windows.

- **PC de sobremesa:** no están diseñados para moverse. Son grandes y disponen de dispositivos de entrada y salida difícilmente transportables (grandes monitores). Se usan para localizaciones permanentes. Generalmente ofrecen más versatilidad, potencia y facilidad de expansión con menos coste que los dispositivos portátiles.

- **Portátil:** están diseñados para ofrecer prestaciones interesantes facilitando la movilidad de los mismos, es por ello que, a igualdad de prestaciones que un PC de sobremesa, suelen ser bastante más costosos. Todo está integrado para poder usarse de forma autónoma y disponen de una batería para utilizarlo en lugares sin acceso a la corriente eléctrica.

- **PDA y Tableta:** los PDA o asistentes personales digitales son dispositivos portátiles con calendario, lista de contactos, calculadora y bloc de notas. En 201O, los PDA dieron paso a los teléfonos inteligentes, los cuáles, además de las funciones anteriores permiten hacer llamadas y acceder a Internet. La tableta o table es un dispositivo que tiene todos sus componentes de hardware alojados en una pantalla táctil plana; permiten la introducción de datos de forma táctil, con lápiz o mediante teclado. Son muy populares por su tamaño portátil y funcionalidad. Las tabletas también están diseñadas para manejar diferentes tipos de medios, tales como fotos, música, vídeos y libros.

- **Workstation:** es un ordenador de sobremesa más potente de lo habitual con microprocesador y componentes más fuertes y diseñados especialmente, que realizan tareas más intensas y complejas que un ordenador de sobremesa común.

- **Servidor:** son ordenadores que dan servicio a una red local o de Internet. Están di señados específicamente para ello. Muchos tienen doble microprocesador, gran des cantidades de memoria *y* múltiples discos duros en *array* para garantizar que la información nunca se pierda. Su diseño les permite estar funcionando las 24 horas del día los 7 días de la semana.

PC Workstation

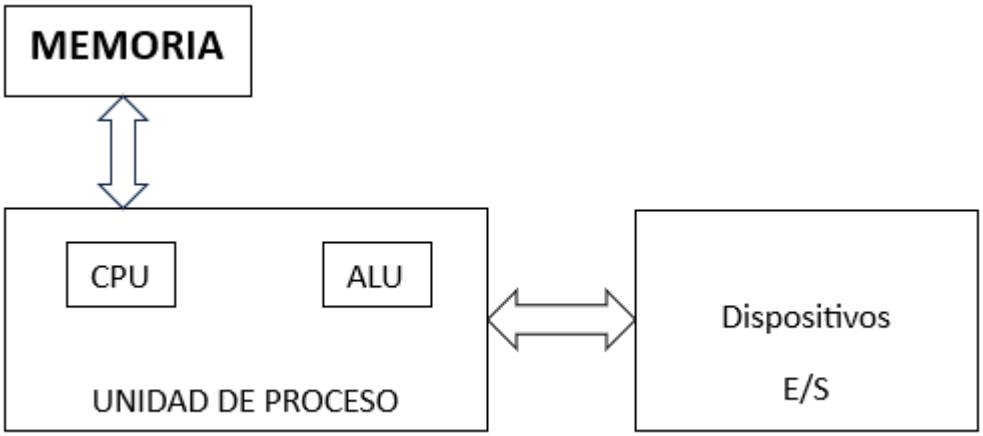
Portátil

Tablet y smartphones

Servidor

También sería bueno conocer cómo funciona un PC. La arquitectura de **un** equipo informático básico no ha sufrido excesivas variaciones desde su concepción original hasta nuestros tiempos. La base de todo sigue siendo la **arquitectura *Van Neumann.***

Tal *y como* vemos en la figura, en esta arquitectura los elementos básicos del Ordenador, CPU, MEMORIA *y* DISPOSITIVOS DE ENTRADA/SALIDA están interconectados por Buses de datos.



Arquitectura Van Neumann

En este tipo de arquitectura, los dispositivos de entrada entregan la información a la Unidad de proceso, que hará uso de la memoria para llevar a cabo las distintas operaciones que necesite *y* posteriormente usará los dispositivos de salida para actuar en función de las operaciones realizadas.

Toda la comunicación entre los elementos se llevará a cabo por los llamados **buses de datos,** que no son sino autopistas por las que la información viaja de un lugar a otro del sistema.

Estos **buses** estarán implementados en la **placa base** o *motherboard*, que es donde se insertan los demás elementos para que estén comunicados entre sí.

1.1.2.1. Componentes: Unidad Central de Proceso (CPU), memoria central y tipos de memoria

Comenzaremos a ver un poco más en profundidad algunos elementos importantes del sistema de un PC:

- **CPU (Unidad Central de Proceso):** es el núcleo del sistema, ya que llevará a cabo todas las operaciones necesarias en él. Hoy en día, gracias a los avances tecnológicos, prácticamente todas llevan la ALU (Unidad Aritmético Lógica) integrada. Tenemos dos tipos principales de tecnologías en la creación de las CPU: CISC y RISC.

* **CISC:** contienen un conjunto de instrucciones complejo para realizar las operaciones. Usado por la mayoría de los procesadores lntel, AMD, etc.

* **RISC:** contienen un conjunto de microinstrucciones simples que deberán ir combinándose para llevar a cabo las operaciones. Usado por el PowerPC presente en los Macintosh y consolas de juego actuales.

- **Memoria central:** es la memoria que usa la CPU para llevar a cabo sus operaciones.

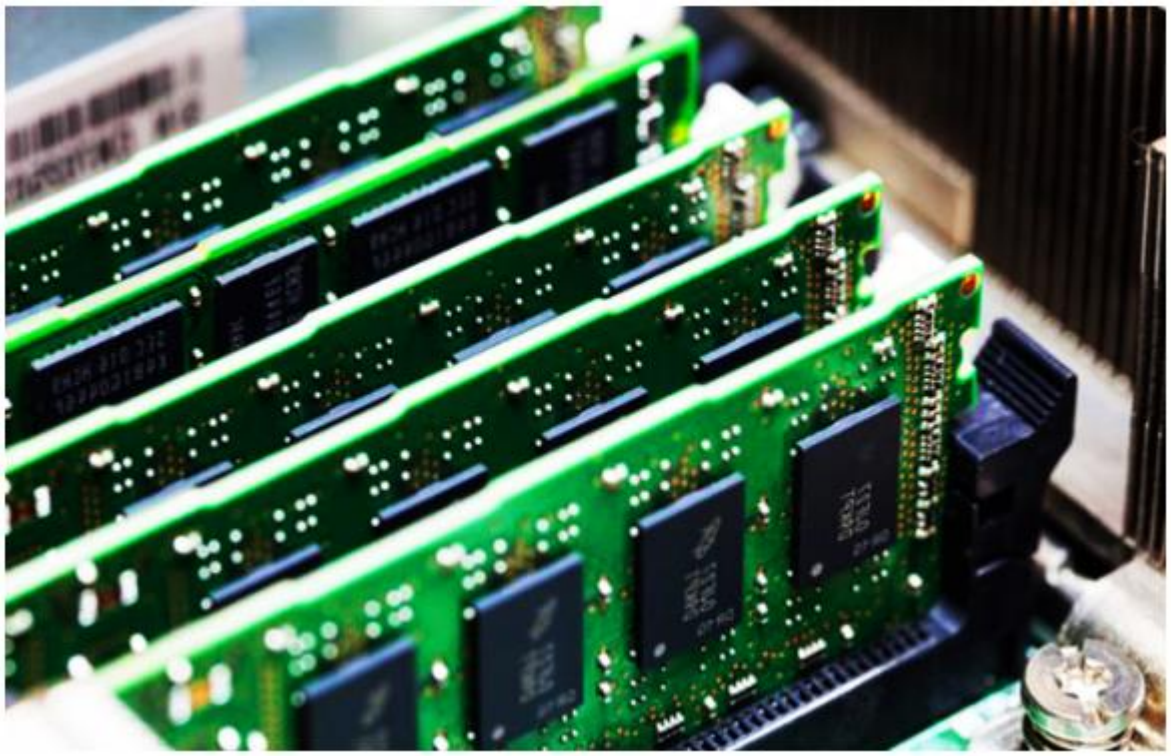
Suele ser muy escasa y está integrada en los microprocesadores actuales. Se apoya en la memoria externa a ellos para llevar a cabo operaciones de tipo más complejo.

- **Tipos de memoria:** hay varios tipos de memoria a tener en cuenta:

* **Memoria volátil:**

RAM (Lectura/Escritura): se usa mientras el sistema está encendido para llevar a cabo tareas del Sistema Operativo. Cuando se apaga el PC se borra.

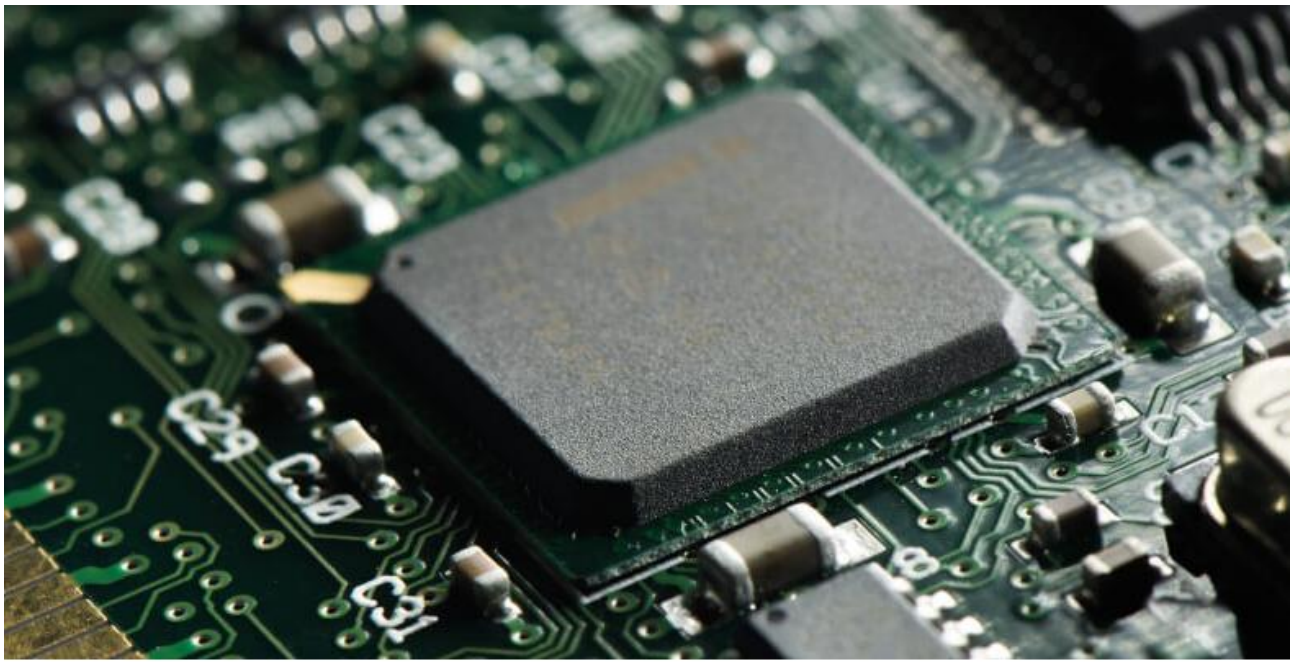
Hay de diversos niveles en función de su rapidez, uso y capacidad (Caché, RAM DDR, DDR2, DIMM, etc.).



RAM

* **Memoria no volátil:**

ROM (Solo Lectura): es la memoria que mantiene vivo el PC. No se puede borrar y es donde está grabada la llamada BIOS, que es el sistema que hace que se realicen las operaciones pertinentes para arrancar el PC y poder comenzar a trabajar con él.



ROM

Dispositivos de almacenamiento: aunque los datos en estos dispositivos pueden ser borrados, se mantienen, aunque se apague el equipo, por lo que este tipo de memorias las clasificaremos aquí, en una· posición intermedia, aunque lo estudiaremos en el siguiente punto.

Dispositivos de almacenamiento

1.1.2.2. Periféricos: dispositivos de entrada y salida, dispositivos de almacenamiento y dispositivos multimedia

Casi tan importantes como el propio núcleo de trabajo, que lo constituyen la CPU y las memorias, están los periféricos, ya que son los elementos utilizados para dar entrada y salida a la información gestionada, así como para guardar los datos que necesitemos:

- **Dispositivos de entrada y salida:** constituyen los elementos que nos permitirán recibir y mostrar la información. Destacan el teclado y el ratón como dispositivos de entrada y la tarjeta gráfica, el monitor, la impresora y los puertos de datos como dispositivos de salida.

- **Dispositivos de almacenamiento:** se utilizarán para guardar archivos durante un tiempo que el usuario estime. Destacan los discos duros como dispositivos de almacenamiento interno y los DVD, con sus correspondientes grabadores en el equipo, como dispositivos de almacenamiento externo. Gracias al avance de la tecnología, los pendrives o memorias USB están ganando terreno por el aumento de la velocidad y capacidad de los mismos, llegando en la actualidad a manejar unos 32, 64 o 128 GB de datos o más.

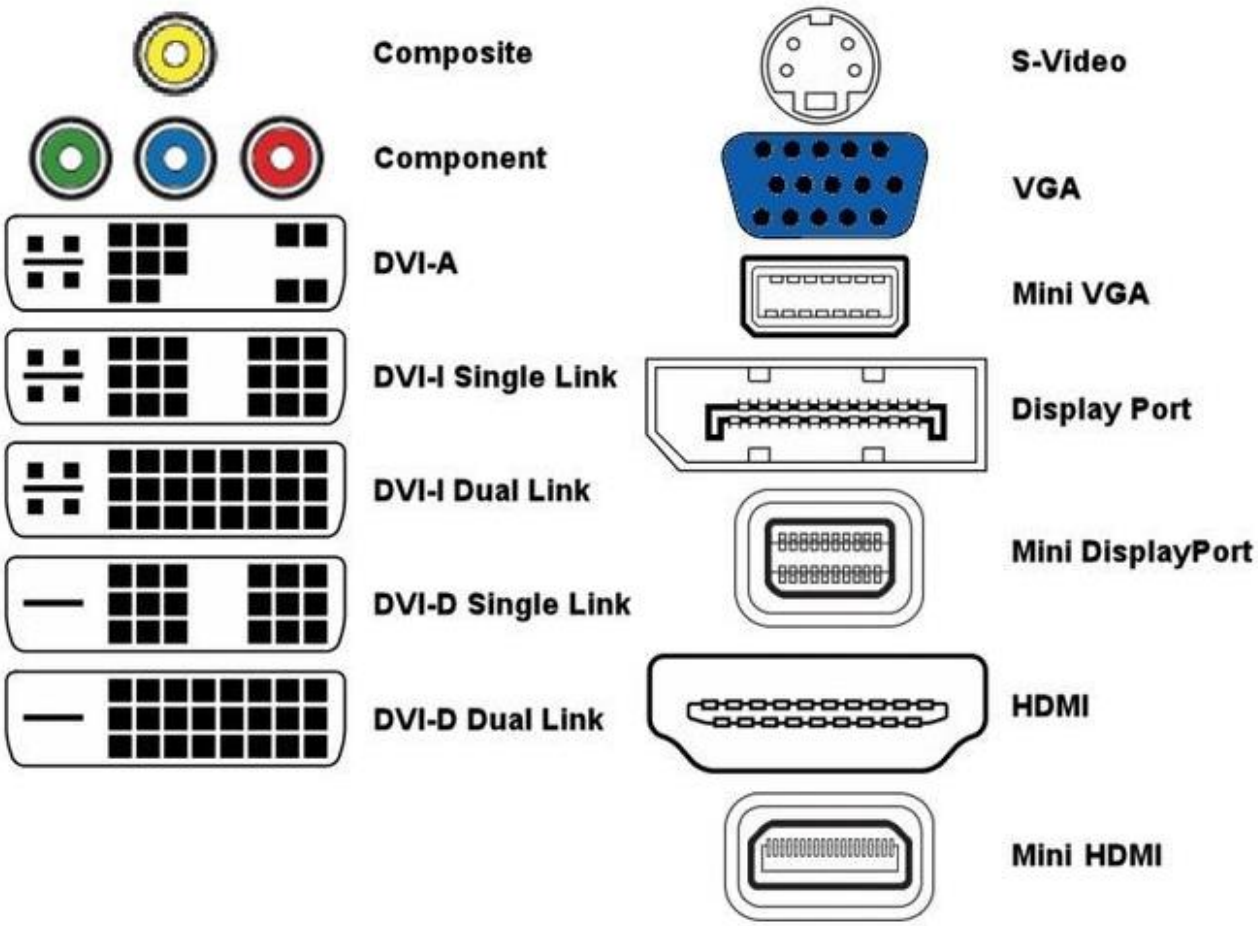
- **Dispositivos Multimedia:** en este apartado tendremos los periféricos que nos proporcionan elementos multimedia, es decir, de imagen y sonido. Podemos tener aquí los altavoces 5.1 o las Webcam como ejemplo.

1.1.2.2.1. Monitor

Se puede considerar al monitor como el periférico de salida más importante, ya que es el sistema para que el usuario compruebe la información que puede proporcionar el ordenador.

Al igual que el resto de periféricos ha sufrido grandes avances en su tecnología, pasando de monitores monocromo y de tubo de 1O u 11" hasta los actuales monitores led de grandes dimensiones y resoluciones 4 K.

Primero hablaremos de los **diferentes tipos de interface del monitor con el PC.** Aunque hay algunos más como, por ejemplo, el S-VIDEO; prácticamente se estandarizaron 3 clases que son VGA, DVI y HDMI, que son las que trataremos a continuación:



- **VGA *(Video Trapicas Array):*** es la salida de vídeo por antonomasia, aunque data de 1988 sigue hoy en día en vigencia. La salida proporciona una señal analógica, aunque los procesos para conseguirla sean digitales. Evolucionó hasta el SVGA que da más calidad de vídeo y que ha sido el que se ha mantenido y mantiene hoy en día en muchos equipos como salida base de monitor. El conector lo conforman 15 pines divididos en tres filas y como norma suele ser de color azul.

-**DVI (Digital Visual Interface):** vino para sustituir al VGA y otorgaba salida digital, por lo que los procesamientos realizados por las tarjetas gráficas, cada vez más potentes, no tenían que ser convertidos a señal analógica. Existen varios tipos de conector según las funcionalidades de la tarjeta y prácticamente todas las tarjetas de hace unos años de gamas media-alta lo traían incorporado, al igual que los **monitores más modernos.**

-**HDMI *(High Definición Multimedia Interface):*** es el último estándar y ha llegado para quedarse. Ofrece una muy alta calidad a través de señal digital y es capaz de transmitir elementos multimedia como imágenes y sonido (no solo imágenes, como ocurría en los casos anteriores). Las grandes posibilidades que otorga en cuanto a transmisión hacen de él, de momento, el interfaz por excelencia para elementos de gran potencia gráfica.

Una vez hemos visto los conectores más habituales, hemos de decir que la mayoría de las tarjetas gráficas hasta hace poco seguían el estándar SVGA que proporcionaba 16 millones de colores (denominado true color 24 bits por pixel) con unas resoluciones desde 640 x 480 hasta 1600 x 1280 pixeles o puntos, aunque estas resoluciones y colores cada vez van aumentando más, ya que la tecnología en las tarjetas gráficas está aumentando vertiginosamente por diversos motivos, como las exigencias de los juegos y sobre todo últimamente por su uso para conseguir criptomonedas.

En cuanto a los **monitores,** se ha pasado, como indicamos, de monitores de tubo monocromos basados en la fluorescencia del fósforo, hasta modernos monitores extra planos con tecnología led, de grandes dimensiones y de resoluciones 4K.

Ejemplo de monitor antiguo

Ejemplo de monitores sincronizados

Como vemos, las exigencias de los usuarios con juegos y programas de diseño cada vez más potentes han hecho mejorar de una forma descomunal el apartado gráfico de los PC.

Aunque ha habido diferentes tipos de monitores con sus correspondientes tecnologías a lo largo de la historia, hoy en día prácticamente todos los monitores de ordenador son de tecnología LED, ya que la tecnología OLED es aún muy costosa, aunque ofrece mejores prestaciones.

Las diferentes tecnologías con las que se han fabricado son: CRT, TFT-LCD, Plasma, LED, OLED.

Las características principales a tener en cuenta en un monitor son las siguientes:

- **Tamaño:** se mide habitualmente en pulgadas. Lo normal hace unos años eran 15 o 17"; ahora cada vez se utilizan más grandes e incluso los llamados "panorámicos'; que son rectangulares en lugar de cuadrados, pudiendo encontrar normalmente monitores de hasta 29". Ese tamaño lo da la medida de la diagonal del monitor.

- **Resolución:** indica los pixeles que tendremos en la pantalla. A más resolución más definición y mejor imagen. Se debe elegir en función de la tarjeta gráfica para adaptarse a ella de la mejor forma posible. Lo normal hoy en día es encontrar resoluciones FullHD e Incluso 4K. Las resoluciones más estándares son:

* **VGA:** 640 x 480 pixeles.

* **HD:** 1280 x 720 pixeles.

* **full HD:** 1920 x 1080 pixeles.

* **4K:** 3840 x 2160 pixeles.

Aunque estas resoluciones se pueden llamar "estándares" o "base'; en función de los monitores podemos encontrar otros formatos de resolución como 1024 x 768, entre otros. La resolución de un monitor es fundamental, ya que este no podrá mostrar imágenes no permitidas por sus formatos de resolución.

- **Relación de aspecto:** hemos hablado antes de los monitores en formato panorámico. Esto tiene que ver con la relación de aspecto, que es la relación entre el ancho y el alto del monitor. Los monitores cuadrados tienen una relación de aspecto (4:3) y ya están prácticamente en desuso, mientras que los panorámicos tienen una relación de aspecto (16:9) y suelen ser los más habituales hoy en día.

- **Tiempo de respuesta:** se mide en milisegundos y se refiere al tiempo que tarda un pixel en cambiar de color. Mientras más rápido sea, mejor se verán las transiciones de imágenes cuando sometamos al monitor a altas exigencias, como por ejemplo en los videojuegos. Un tiempo bastante bueno es de unos 5 mseg.

- **Tasa de refresco o frecuencia de actualización:** representa el número de veces que el monitor actualiza la imagen. Se mide en Hertzios (Hz). Esto quiere decir que, por ejemplo, si un monitor tiene una tasa de refresco de 60 Hz actualizará la imagen de la pantalla 60 veces en un segundo. Mientras mayor sea esta tasa mejor responderá el monitor, siendo fácil encontrar hoy en día monitores con tasas de refresco de 144 o más Hz.

-**Brillo, contraste, color, ángulo de visión:** son características propias de cualquier pantalla que no debemos pasar por alto a la hora de valorar un monitor.

1.1.2.2.2. Elementos de impresión

Veremos primeramente de qué forma podemos y podemos conectar un elemento de impresión con nuestro PC (para simplificar hablaremos de impresoras), para ver luego cómo lo podemos gestionar y terminaremos indicando los fallos que más comúnmente nos podemos encontrar.

La impresora es el dispositivo a través del cual transferimos a papel u otros soportes físicos nuestros documentos.

Además de la tecnología propia de impresión, existen diferentes formas de conectar la impresora con el PC. Los medios más habituales son: puerto paralelo, puerto USB, Wifi, red y algunas Bluetooth que no tendremos en cuenta por ser minoría.

Como tecnologías de impresión disponemos de impresoras de las siguientes características:

- **Matriciales:** también denominadas por impacto. El mecanismo es similar al de las máquinas de escribir. El cabezal genera una serie de impactos sobre la cinta de tinta, de forma que queda impreso en el papel. Prácticamente están en desuso y se utilizan sobre todo para imprimir papeles con calco y que salgan varias copias (pagarés, facturas, etc.).

- **Inyección:** son las más extendidas en la actualidad por su relación coste-rendimiento.

La impresión se realiza gracias a la proyección de tinta sobre el papel por el cabezal.

- **Térmicas (sublimación):** necesitan un papel especial sensible al calor y la impresión se genera por aplicación de calor. Se suelen usar en máquinas para pegatinas y pequeñas Impresiones.

- **Láser:** muy buena calidad y bajo coste para pequeñas oficinas o grandes empresas.

El funcionamiento es similar al de las fotocopiadoras y hacen uso del tóner (polvo de tinta) para generar las imágenes pasando por los diversos elementos de la misma. Son muy rápidas y económicas para muchas copias.

También podemos considerar dispositivos de impresión a las impresoras 3D, que cada vez se están haciendo más accesibles a los consumidores. Estas impresoras permiten generar objetos de tipo plástico partiendo de esquemas.

Los plóteres son impresoras especiales para proyectos, ya que se suelen usar para imprimir planos en grandes formatos. Originalmente en lugar de tinta al uso utilizaban unas plumas de un color o varios con los que iban generando las imágenes a imprimir mediante motores que las gobernaban. Actualmente se ha impuesto la tecnología de inyección de tinta.

1.1.2.2.3. Escáner

El dispositivo por excelencia para la digitalización de documentos es el escáner. El escáner permite, mediante su tecnología, representar un documento u otro elemento en una serie de señales eléctricas o de información capaces de ser interpretadas como información por un sistema.

Existen varios tipos de escáneres, algunos vinculados de pleno al tema informático y otros no. Por ejemplo, estarían los escáneres ópticos, los escáneres de huellas, de retina, los escáneres médicos para realizar diagnósticos y los de los aeropuertos para visualizar elementos sospechosos, pero todos tienen en común que traducen, según la tecnología empleada, los elementos a información visible para el usuario.

La mayoría de los escáneres hoy en día utilizan el puerto USB para comunicarse con el ordenador que los gobierna. También hay escáneres que son capaces de crear archivos directamente en pendrives o en algún disco duro de la red. Las conexiones con el resto de elementos se mantienen igual que ocurrió con las impresoras.

Uno de los elementos a tener en cuenta en un escáner es su resolución, que viene determinada por el CCD del mismo, ya que es el elemento encargado de captar la imagen reflejada por los espejos que lo conforman. Otra capacidad interesante sería la posibilidad de llevar a cabo OCR (Reconocimiento óptico de caracteres), que no es más que transcribir los caracteres impresos en una hoja a un fichero de texto. Generalmente el OCR se lleva a cabo mediante paquetes SW adicionales.

Como ocurre con el resto de elementos, las tecnologías avanzan a pasos agigantados y ya se cuenta hasta con escáneres 3D capaces de hacer una fiel reproducción de un entorno tridimensional u objeto.

Dentro de los **tipos de escáner** podemos diferenciar de forma clara los siguientes:

-Escáner plano o de mesa: es el escáner más comúnmente conocido por todos los usuarios. También se conocen como de "cama plana". Es un dispositivo habitualmente del tamaño de un folio, que descansa sobre una base y sobre el que se depositan los documentos a escanear. Se utilizan para escanear hojas sueltas, documentos, etc. Actualmente dan una resolución muy buena en un tiempo de escaneado bastante optimizado.

-Escáner de mano: en este tipo de escáneres, es el usuario el que va realizando el recorrido que tiene que capturar el escáner y pasarlo a información. Este hecho provoca que dependa su fiabilidad en gran medida de la pericia del usuario en su uso, ya que, si no se hace la pasada con mano firme o velocidad homogénea, los resultados se verán afectados.

-Escáner rotativo o de tambor: son utilizados por los diseñadores gráficos debido a su alta resolución. Permiten obtener imágenes con gran resolución gracias a sus modelos de color CYMK o RGB.

-Escáner cenital: es un tipo de escáner que se utiliza para hacer copias de libros o documentos muy valiosos o antiguos, y que evita que se deteriore durante el proceso.

1.1.2.2.4. Fallos frecuentes

También veremos los fallos más comunes que pueden presentar sus dispositivos periféricos y cómo intentar solventar dichos fallos, ya que puede resultar muy útil en el día a día.

Como es de esperar nos centraremos en problemas y resoluciones básicas, ya que, en caso de presentar un problema de una índole más técnica, deberemos recurrir al responsable de los sistemas informáticos.

Podremos detectar problemas fácilmente en los periféricos de E/S y en los de almacenamiento. Veremos primero los de E/S y luego los de almacenamiento.

A) Monitor

Entre los distintos problemas que nos podemos encontrar, destacan los siguientes:

- No da imagen: comprobar que está alimentado correctamente. Comprobar el cable de VGA. Comprobar los niveles de brillo y contraste. Comprobar que el PC está encendido.

- La imagen se ve con los colores muy difusos: puede que el monitor esté imantado. Se puede llegar a esta conclusión cuando los colores se ven agrupados (todos los azules en un lado y los

verdes a otro, por ejemplo). Esto sucede si hay cerca dispositivos que puedan generar campos electromagnéticos (altavoces). La mayoría de los monitores, dentro de su menú, disponen de una opción para desimantar la pantalla y regularizar los colores.

- La imagen no está centrada: ir al menú del monitor y centrarla por medio de los ajustes tanto horizontal como vertical.

- La imagen parpadea: puede que el monitor esté físicamente estropeado o bien que la frecuencia de refresco emitida por la tarjeta de vídeo insertada en el PC no sea la más adecuada. Para comprobar esto último hay que ir a las propiedades de la imagen del escritorio y bajar la frecuencia de refresco.

- **No se aprecia una definición correcta:** observar en las propiedades del entorno gráfico la profundidad de color (8, 16, 32 bits habitualmente) y la resolución. Mientras más altas, más definición mostrará nuestra pantalla.

B) Teclado

El teclado nos servirá para introducir caracteres en los diversos programas del dispositivo. Entre los posibles fallos que podemos detectar, destacan:

- Las teclas no responden:

*En teclados inalámbricos, probablemente se hayan agotado las baterías. Sustituir y sincronizar de nuevo.

*En teclados cableados posiblemente se haya movido el conector. En este punto, si no es el puerto USB deberá desconectar el PC y colocar correctamente el conector.

- Las teclas presionadas no coinciden con las mostradas en pantalla: compruebe que como idioma en el entorno Windows tiene seleccionado el castellano. En caso de tener seleccionado teclado inglés, algunos símbolos no se corresponden con los mostrados en las teclas.

C) Ratón

Con el ratón podemos desplazar el cursor por toda la pantalla del ordenador, y gracias a sus botones podremos operar distintos comandos de una forma simple y rápida, evitando utilizar el teclado. Podemos encontrarnos varios fallos como pueden ser:

- **El cursor no responde a los movimientos del ratón:**

***Ratones ópticos:** estos ratones se distinguen por emitir una luz roja por su parte inferior. Generalmente, cuando no responden correctamente, la superficie sobre la que se está manejando no es la más adecuada. Probar sobre una superficie negra o uniforme.

***Ratones de bola:** no tienen luz en su parte inferior, sino una bola que va desplazando unos rodillos. Cuando estos se ensucian generalmente no se mueve correctamente el cursor. Deben ser limpiados con alcohol y probar de nuevo.

- **No funcionan los clics:** comprobar que no hay nada impidiendo el correcto desplazamiento del botón. Lo normal en estos casos es que el ratón esté averiado.

D) Impresora

La impresora es el dispositivo a través del cual transferimos a papel nuestros documentos. El fallo más generalizado es la falta de respuesta de la misma, que puede deberse a diversas causas, aunque aquí solo veremos la más básica:

- **La impresora no responde:** comprobar alimentación. Comprobar cable USB que la une al ordenador. Comprobar que dispone de papel para imprimir. Comprobar que la impresora seleccionada es aquella que estamos intentando hacer que imprima el documento. Comprobar que dispone de tinta o tóner. En otro caso contactar con el responsable informático, ya que puede ser un problema de Drivers o de un mal funcionamiento del dispositivo.

Según la tecnología que usen para realizar las impresiones se pueden distinguir varios tipos de impresoras: las impresoras matriciales, por inyección de tinta o láser. Podemos incluir también las nuevas impresoras 3D, que usan inyectores de elementos plásticos, pero aún no están muy estandarizadas. También hay varios tamaños de impresoras; una diferenciada por tamaño y tecnología es el plóter**,** que permite imprimir proyectos de grandes dimensiones con facilidad.

E) Unidades de almacenamiento

Las unidades de almacenamiento nos ayudarán a salvaguardar la información, por lo que debemos ser cuidadosos con ellas.

- **La lectora de CD/DVD no lee el disco:** comprobar que el disco se corresponde con el tipo de lectora utilizado (no se puede leer un DVD en una lectora de CD, aunque sí, al contrario). Comprobar que el disco esté limpio en su parte inferior y no presenta arañazos. En otro caso puede ser un problema de la lectora.

- Fallo del disco duro: es el fallo más temido. En cuanto se presente el más mínimo indicio de fallo en el disco duro contactar con el responsable informático. Aunque se arregle momentáneamente, podría reproducirse y provocar la pérdida de todos los datos almacenados.

- No funciona el Pendrive USB: cambiarlo de entrada USB y comprobar que el Windows reconoce adecuadamente el dispositivo.

Recuerda que...

Debes realizar periódicamente copias de seguridad de tus archivos más importantes y necesarios.

F) Dispositivos de sonido

Nos ayudarán a escuchar los sonidos emitidos por nuestro equipo, por ejemplo, referido a los altavoces ...

- **No escucho los sonidos producidos por mi PC:** comprobar que el cable está correctamente introducido en el conector adecuado. Comprobar la alimentación del altavoz, en caso de ser necesaria. Comprobar que el volumen está activado.

Una vez hemos tratado el hardware nos queda por ver la otra parte básica del funcionamiento de un ordenador, que es el software.

1.1.3. Modos generales de conexión

1.1.3.1. Firewire

Es un puerto de alta velocidad diseñado por Apple. Su denominación concretamente es IEEl 394, haciendo honor a la normativa que cumple.

Sus características principales son las siguientes:

- Alta velocidad, ya que puede alcanzar hasta 400 MBps.

- Flexibilidad, ya que permite conectar hasta 63 dispositivos.

- Longitud de cable de hasta 4.25 m.

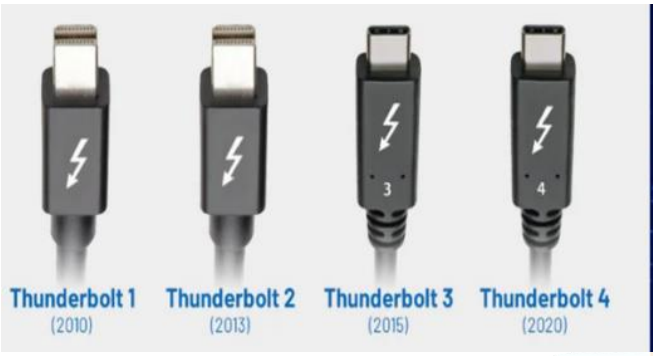
- Conexión en caliente (con PC encendido).

- Plug and Play.

Alimentación desde el propio bus de hasta 25 V, aunque hay un puerto con 4 conectores en lugar de 6 que no suministra alimentación.

1.1.3.2. Thunderbolt

Es la evolución del Firewire en los MAC. Utiliza la tecnología PCI Express para dotar al puerto de unas características de velocidad y flexibilidad espectaculares. Hay varias revisiones que mejoran en cada una de ellas sus prestaciones.



Hay cada vez más periféricos compatibles (sobre todo pantallas) y en sus diferentes revisiones, alcanza una tasa de transferencia de datos difícil de superar, así tendríamos las siguientes:

- **Thunderbolt:** 1O GB/s de entrada y de salida simultáneos a través de un solo conector.

- **Thunderbolt 2:** hasta 20 GB/s.

- **Thunderbolt 3:** hasta 40 GB/s.

- **Thunderbolt** 4: aunque el ancho de banda máximo se mantiene en 40 GB/s ofrece otro tipo de mejoras. Sus controladores Pacle, por ejemplo, pasan de los 16 Gbps mínimos a 32 Gbps mínimos. Además, incorporan una protección de seguridad DMA basada en VT-d mediante rem apeos para prevenir amenazas de seguridad y permiten también reiniciar desde el modo Hibernar.

- **Thunderbolt 5:** aún no se conoce la fecha de lanzamiento, pero se espera que alcance velocidades de 80 GB/s con picos de 120 GB/s y esté basado en USB-C.

1.1.3.3. Bluetooth

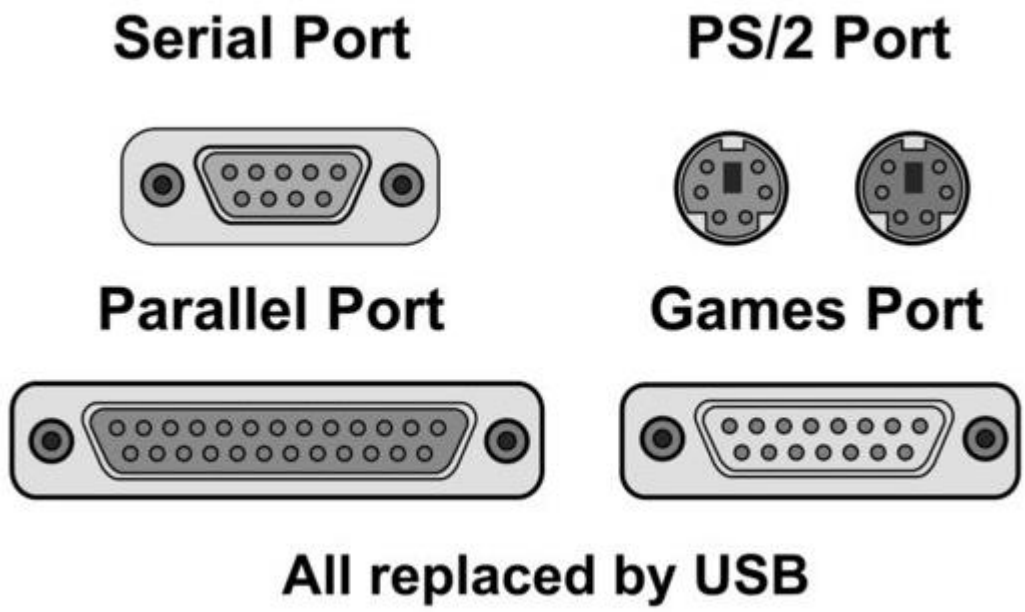
La tecnología Bluetooth nació con la finalidad de permitir una fácil interconexión entre dispositivos sin necesidad de cables y hoy en día está bastante extendida. La norma base establece una distancia efectiva de unos 1O m y la frecuencia de uso es unos 2.4 GHz.

Actualmente se usa en multitud de dispositivos para transmitir información como ficheros, voz, audio, etc., en plataformas de lo más vario pintas que van desde manos libres para móviles, **televisores, ordenadores, etc.**

1.1.3.4. USB

El puerto USB es el que más se ha extendido en los últimos años. A pesar de ser un puerto serie *(Universal Serial Bus),* se le ha dotado de una velocidad y una facilidad de conexión que ha hecho

que muchos periféricos lo adopten como sistema base de conexión. A lo largo del tiempo han ido mejorando sus prestaciones, pasando del USB al USB 2.0 y al USB 3.0, que le proporciona una velocidad bastante capaz de competir con los buses más rápidos. Actualmente se intenta trabajar en un estándar que evite que solo haya una forma de conectar el dispositivo, que es el mayor inconveniente con el que se encuentran los usuarios en la actualidad (siempre se intenta conectar como no es y hay que girar el dispositivo para hacerlo correctamente). El USB se ha adaptado a los dispositivos, incluyendo varios tipos de conector basados en el mismo estándar como micro USB, mini-USB y USB, por ejemplo.



Ha sido tal su éxito que ha reemplazado a los conectores más habituales en PCS antiguos.

El USB surgió en 1996 y a día de hoy se ha convertido en el sistema de conexión por excelencia.

Las velocidades van desde 1.6 Mbps del USB 1.0 hasta los 1O Gbps del último están dar, USB 3.1, lo que puede dar una idea de la evolución y aceptación de este sistema de conexión de periféricos externos. Hay que tener en cuenta que para obtener la máxima velocidad de transmisión el cable debe ser trenzado y apantallado. Si a eso le añadimos la facilidad de uso y la masiva implementación, podemos valorar su éxito.

- **USB 1.0:** 1.6 Mbps. 2 líneas para datos y 2 para alimentación.

- **USB 1.1:** 12Mbps. 2 líneas para datos y 2 para alimentación.

- **USB 2.0:** 480 Mbps. 2 líneas para datos y 2 para alimentación.

- **USB 3.0:** 4.8 Gbps (dispone de 5 contactos adicionales al 2.0).

- **USB 3.1:** 1O Gbps es el más usado por los nuevos conectores tipo C.

1.2. Definición y tipos de software

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.

Hay tres grandes tipos de software que serán divididos en más categorías.

- Software de Sistema: desvincula al usuario de las particularidades de su ordenador ofreciendo un Interfaz de alto nivel con el que poder trabajar.

- Software de Programación: es el conjunto de herramientas ofrecidas a los desarrolladores para llevar a cabo programas de aplicaciones.

- Software de Aplicación: es aquel que permite al usuario realizar tareas específicas en el ordenador, es decir, los programas para realizar distintos trabajos en el PC.

Como habrá visto, esta clasificación es a grandes rasgos y muy amplia; haremos una breve composición de distintas posibilidades dentro de cada uno de los grandes aparta dos del software para que su idea del mismo sea más concisa.

- **Software de Sistema:**

***** Sistema Operativo.

***** Controladores de Dispositivos.

***** Software de Diagnóstico.

- **Software de Programación:**

***** Entornos de Desarrollo.

***** Compiladores.

***** Depuradores.

- **Software de Aplicación:**

***** Aplicaciones Ofimáticas.

***** Aplicaciones para cálculo.

***** Aplicaciones para Diseño Asistido por ordenador (CAD).

***** Aplicaciones empresariales.

Veremos ahora con algo más de profundidad los fundamentos del Sistema Operativo, ya que es el cerebro lógico del ordenador y el encargado de ir gestionando todo lo que se lleva a cabo en el mismo.

2. Sistemas de almacenamiento de datos

2.1. Concepto de datos e información:

Para poder ir aportando lo necesario para comprender la Importancia y relevancia de la aparición de la informática en nuestra sociedad, nos centraremos en este apartado en los conceptos de datos e información:

- Datos: un dato es una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa; describen hechos empíricos, sucesos y entidades, pero de forma aislada pueden no contener información relevante.

- Información: tras procesar los datos bajo ciertas hipótesis, algoritmos o algún tipo de razonamiento, se puede obtener información que aporta hechos o elementos relevantes para el usuario.

Por lo tanto, ya podemos establecer una diferencia y un elemento común entre datos e Información. **Los datos individualmente no tienen por qué aportar ninguna información, pero se hacen necesarios para mediante el procesado de un conjunto de ellos obtener algún tipo de información.**

Los ordenadores, son máquinas ideadas para procesar información haciendo uso de reglas y algoritmos para poder tratar convenientemente los datos que reciben.

Una vez vistas las definiciones más importantes, entremos algo más en profundidad en cada uno de los elementos.

2.1.1. Datos

Aunque existen muchos tipos de datos, veremos en este caso tres de las posibles clasificaciones, para que se pueda ver cómo tratarlos. Tendremos, por lo tanto, una clasificación según el sistema de información utilizado, según la variación y según la información que almacenan.

Hemos elegido estas tres clasificaciones de datos para generar una idea y una comprensión más alta de lo que realmente significan:

Según el sistema de información: dependerá del medio de transmisión de los datos. Así podremos distinguir entre:

*** Datos de entrada:** son los datos necesarios para el procesamiento y consecución de la información. Se suministran al ordenador mediante periféricos de entrada.

*** Datos intermedios:** se obtienen tras el procesamiento de los datos de entrada.

*** Datos de salida:** son los datos que se muestran al usuario, normalmente ya agrupa dos y convertidos en información, disponibles a través de los periféricos de salida.

- Según la variación: como veremos posteriormente, la mayoría de los elementos/ programas de tratamiento de información disponen de datos que pueden sufrir alteraciones o no:

*** Datos fijos:** se mantienen constantes durante el procesamiento y tratamiento de los mismos. El nombre común en los lenguajes de programación es **constante.**

*** Datos variables:** permiten que se cambie el valor de los mismos a lo largo del procesamiento de la información.

- Según la información que almacenan: en este caso queremos hacer notar la diversidad de posibilidades que se ofrecen y solo pondremos algunos ejemplos de posibilidades, ya que en los diversos lenguajes de programación podremos encontrar alguna tipología más:

*** Datos numéricos:** números, por ejemplo, enteros, números en coma flotante, naturales, etc.

*** Datos alfabéticos:** letras, caracteres, etc.

*** Datos alfanuméricos:** letras y números, campos memos, etc.

*** Datos lógicos:** Booleano (verdadero o falso).

2.1.2. Información.

Como vimos, la información se obtiene tras el procesado según algún algoritmo de un conjunto ordenado de datos.

La clave en este caso es el concepto de **datos significativos,** ya que estos serán el objetivo de los sistemas de información. Los datos significativos son aquellos que contienen símbolos reconocibles, están completos y expresan una idea sin ambigüedad.

Se deben cumplir tanto la **integridad,** es decir, que todos los datos necesarios para generar la información estén disponibles, como el que sean **inequívocos,** es decir, que no se genere ninguna duda acerca de su significado, para considerar que el conjunto de datos aportados genera posibilidades de información. Esta información será **relevante** cuando responda a alguna petición formulada.

Haremos especial mención en este apartado a la llamada "minería de datos", que no es más que descubrir patrones dentro de grandes volúmenes de conjuntos de datos. Debido a la gran cantidad de datos que se recopilan diariamente por nuestra interconexión constante con Internet a través de Smart TV, móviles, navegación, dispositivos como Alexa de Amazon, formularios, etc. el trabajo con grandes volúmenes de datos se hace algo indispensable para las grandes empresas hoy en día. Conocido como *Bussiness Intelligence, Data Science,* o diferentes nomenclaturas, el trabajo con grandes cantidades de datos aplicando medios estadísticos, de inteligencia artificial, de bases de datos, etc. es un campo con muchas expectativas dada la importancia que está teniendo en la actualidad por sus aplicaciones: ofertas personalizadas para consumidores, estudio de clientes, estudio de acciones para mejorar productividad, prevención de acciones terroristas, etc.

2.2. Clasificación de los sistemas de almacenamiento de datos.

Los sistemas de almacenamiento de datos podemos clasificarlos de varias formas. En este apartado veremos una clasificación básica, en función del medio que utilicen para almacenar dichos datos. Existen diversos sistemas de almacenamiento de datos como pueden ser los siguientes:

- **Soporte óptico:** caídos ya un poco en desuso debido a las rápidas mejoras en las tecnologías de los discos duros, su funcionamiento se basa en la lectura/escritura de las pistas de datos por medio de un láser. Podemos observar los siguientes elementos:

* **CD:** su capacidad es de aproximadamente 700 MB. Con la aparición del DVD, el CD hoy en día prácticamente no se usa para almacenar datos, aunque para abaratar costes se sigue utilizando en los drivers que adjuntan algunos elementos. Dadas sus velocidades de lectura/escritura no es muy útil en los almacenamientos de datos del día a día.

*** DVD:** su capacidad se encuentra entre 4.7 GB *y* 8 GB aproximadamente. Su alta capacidad ha desplazado a los CD de la mayoría de sistemas de almacenamiento de datos.

*** Blu-Ray:** está llamado a ser el sustituto del DVD por su mayor capacidad de almacenaje (25 GB por capa) *y* su mayor velocidad de transferencia de información.

- **Soporte magnético:** aquí se encuentran la mayoría de los dispositivos utilizados en la actualidad para almacenar datos:

*** Disco Duro:** el dispositivo de almacenamiento de datos por excelencia. Tiene una alta capacidad de almacenaje (ya hay discos duros de más de 14TB). Son rápidos, fiables *y* hay una gran variedad de tipos para elegir, según las necesidades.

*** Disco Duro de Estado Sólido (SSD):** hacemos mención aparte a este tipo de disco, ya que utiliza una tecnología diferente, ya que no dispone de cabezales como el anterior. Es mucho más rápido, fiable y lógicamente, caro.

*** Pen drive:** dispositivo de almacenamiento externo, usado para llevar la información de un sitio a otro. Hay de muchas capacidades distintas *y* según la velocidad de transferencia podrán ser más o menos caros.

- **Nube:** hacer mención especial a esta nueva forma de almacenamiento que se está extendiendo últimamente. Consta de varios servidores gestionados por terceras personas *y* que garantizan el almacenamiento de la información en Internet con suficiente seguridad *y confidencialidad*. Permite descargar los discos duros de los equipos personales *y* evitar pérdidas accidentales de información.

3. Sistemas operativos.

Un Sistema Operativo es un programa o conjunto de programas que gestiona todas las tareas realizadas en un sistema informático.

Los objetivos básicos que debe cumplir un buen Sistema Operativo son los dos siguientes:

- Facilidad de manejo para los usuarios: debido a que el Sistema Operativo es el enlace entre la máquina *y* el usuario, se necesita que el manejo de este sea lo más intuitivo *y* fácil posible para que el usuario no se pierda en cuestiones innecesarias para él.

- Eficiencia: la otra gran cualidad que debe cumplir el SO es la eficiencia. De nada nos sirve un SO muy fácil de manejar si no es capaz de gestionar adecuadamente los recursos del sistema *y entorpece* en exceso el trabajo del usuario. Por eso es otra cualidad importante a cumplir.

¿Qué partes componen un Sistema Operativo?

- **Núcleo o Kern él:** realiza las funciones básicas del sistema, gestión de memoria procesos, entradas y salidas, etc.

- Intérprete 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.

- **Sistema de Archivos:** permite que los archivos se guarden de manera ordenada en el sistema.

3.1. ¿Cómo funciona un Sistema Operativo?

El Sistema Operativo actúa como una capa intermedia entre el hardware y los programas de apl1cac1ones. 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: distribuye el uso del Micro entre los distintos programas que quieren acceder a él.

- Gestión de memoria del sistema: distribuye el uso de la memoria del sistema entre los distintos programas que se están ejecutando de manera que el funcionamiento sea el más óptimo.

- Gestión de Entradas y Salidas: he aquí los famosos drivers de los elementos hardware, que hacen más fácil el acceso a los dispositivos por parte del resto de programas que integran el sistema.

- Gestión de Ejecución de aplicaciones: se encarga de asignar recursos a las aplicaciones que pretenden ejecutarse para que el Sistema no se sature.

- Administración de Autorizaciones: hace que todos los programas o usuarios no puedan acceder a todo el sistema. El acceso estará restringido por niveles para dar cierto grado de seguridad.

- Gestión de archivos: *se* gestiona la escritura, borrado y lectura de archivos asignando autorizaciones si así se cree conveniente.

Hay varios Sistemas Operativos para ordenadores en el mercado, entre todos ellos podemos destacar los siguientes:

-**Windows:** Sistema Operativo de Microsoft, implantado masivamente para el usuario medio.

-**UNIX:** Sistema Operativo multitarea y multiusuario.

-**Linux:** Sistema Operativo Ubre usado por usuarios algo más avanzados que dispone de diferentes distribuciones como Ubuntu, Debian, Mint, Fedora, etc.

-**Mac OS:** Sistema Operativo propio de los Mac de Apple.

-**Android:** también es un Sistema Operativo, aunque no es para PC sino para dispositivos móviles como teléfonos y tabletas, pero dado el auge de estos para el trabajo en el d1a a día también hay que mencionarlo.

- **iOS:** al igual que Android es un Sistema Operativo diseñado exclusivamente para dispositivos móviles, en este caso de Apple, como el iPhone.

Podemos, por tanto, definir un **Sistema Operativo como un conjunto de funciones y servicios que se encarga de gestionar y coordinar el funcionamiento del hardware y el software del equipo.** Es decir, se encarga de identificar el hardware, adecuarlo a los programas que se estén utilizando (software) y dotar al equipo de medios para que el usuario pueda realizar entradas de información, y obtener los resultados en forma de salidas de información adecuadas para su análisis.

Los diferentes sistemas operativos se pueden clasificar en función de varios parámetros.

a) Según el número de usuarios:

- **Monousuario:** el Sistema Operativo solo es utilizado por un usuario. Ejemplos de estos SO podría ser el MS-DOS y los antiguos sistemas Windows 3.1, etc.

- **Multiusuario:** en este caso varios usuarios pueden compartir el ordenador de trabajo, por lo que los recursos del sistema se deben repartir en función de la carga de trabajo que se demande en cada momento. Ejemplos: Unix, Windows Server, etc.

b) Según el número de procesos:

- **Monotarea:** el Sistema Operativo solo puede gestionar un programa.

- **Multitarea:** en este caso se pueden ejecutar varios programas simultáneamente. Esto no quiere decir que se ejecuten al 100% en paralelo, puesto que para ello se necesitarían tantos procesadores como programas se ejecuten. Lo que se hace es que el Sistema Operativo intercala los procesos de los programas que se están ejecutando haciendo que parezca que se ejecutan simultáneamente.

3.2. Sistema de archivos

Los sistemas operativos deben ser capaces de gestionar la gran cantidad de información generada por los diferentes programas.

Cada sistema operativo tramita los archivos de forma distinta, gestionando estos de forma particular y necesitando tener ciertas especificaciones, según el uso que se les dé.

Una de las características más diferenciadoras entre los distintos Sistemas Operativos se da en los nombres de los archivos, ya que cada uno aporta unos nombres y extensión acorde con la función que lleva a cabo el fichero.

La mayoría de los sistemas operativos gestionan los nombres de hasta 8 caracteres, aunque los más modernos pueden aceptar bastantes más. También algunos como por ejemplo Unix, son capaces de

distinguir mayúsculas de minúsculas y otros aceptan las denominadas extensiones, mencionadas antes para diferenciar más fácilmente las diferentes funcionalidades de los archivos.

Los archivos en la gran mayoría de los Sistemas Operativos se pueden diferenciar en:

-**Archivos estándar:** son los archivos de usuario.

-**Directorios:** se usan para gestionar mejor el almacenamiento de los archivos y contienen índices que apuntan a los archivos que les corresponden.

Archivos de sistema: los usa el Sistema Operativo para realizar gestiones y configuraciones de los diferentes elementos que lo componen.

Como la mayoría de los usuarios saben, a los archivos se les puede dotar de ciertos atributos para modificar su comportamiento habitual, por ejemplo, se puede decir que un **archivo es de solo lectura** si no se permite su modificación. Además, contienen datos acerca de él como la fecha de creación, modificación, etc., al ser dependientes del sistema operativo utilizado; no daremos más detalles sobre estos elementos.

Por último, veremos que cada Sistema Operativo de archivos dispone de un sistema de archivos propio. Así, por ejemplo, los primeros Windows usaban el FAT o FAT32 mientras que los últimos como Windows 7 o 1O utilizan el denominado NTFS. Por otro lado, el resto de Sistemas Operativos utilizan también sistemas de archivos propios, lo que hace que sean normalmente incompatibles los discos de almacenamiento entre unos y otros.

Mediante el sistema de archivos, se formatea o se le da un formato predefinido al elemento de almacenamiento principal, acorde con el sistema de trabajo del Sistema Operativo, para que almacene en él los distintos ficheros necesarios.

En la tabla adjunta se incluyen los más significativos:

Sistema Operativo	Sistema de archivos
MS-DOS	FAT16
Windows	FAT, FAT16, FAT32, NTFS (los últimos a partir de Windows XP)
Linux	Ext2, Ext3, ReiserFS, Linux Swap
MAcOS	HFS, MFS
OS/2	HPFS

4. 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 encontrarnos. Veremos 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 intercepción 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 o 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 pérdida de datos o en la eventual caída del sistema (tormentas, incendios, inundaciones, etc.). También habrá que contemplar estas posibles contingencias en el plan de seguridad.

Veremos algunas de las medidas que podemos tomar para proteger el sistema de información de la organización, a modo de ejemplos:

- 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 una gestión de usuarios para proteger el sistema de usos indebidos.

IMPORTANTE:

- Nunca deshabilites el antivirus.

- No confíes en emails de remitentes desconocidos o con asuntos extraños o sin asunto.

- Nunca entres en webs de bancos a través de enlaces directos que te envíen.

- Procura tener claves largas con mezcla de números, letras, mayúsculas y minúsculas.

- Modifica las claves periódicamente.

- Ten siempre tu usuario Windows protegido por contraseña.

4.1. Responsabilidad personal de los documentos manipulados.

Veremos dentro de este apartado las distintas responsabilidades derivadas del tratamiento de datos dentro de una organización. La información es un elemento vital hoy en día en cualquier organización y, por lo tanto, el trasiego de documentos debe hacerse de forma segura para que no haya problemas. La política de la empresa al respecto de las responsabilidades en el tratamiento de documentos debe quedar claramente definida y debe ser conocida por todos los trabajadores de dicha empresa.

Así, una manipulación indebida o malintencionada de los documentos o la información de la empresa, puede causar graves perjuicios y lógicamente el causante de estos debe ser debidamente sancionado.

Cuando manipulamos documentación de la empresa, debemos siempre hacerlo bajo las directrices de la misma. Hay que evitar que se vulnere la confidencialidad, el contenido y que no sea expuesto a personas ajenas a la empresa (siempre que sea un documento interno).

Es responsabilidad del trabajador el llevar a cabo con diligencia todas las operaciones sobre documentación e información en la empresa.

Confidencialidad de los datos tratados

En España, 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.

Articulo: *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.

Debemos, por lo tanto, mostrar especial cuidado cuando tratamos datos de carácter personal en la organización o empresa, para que estos no puedan ser vistos por ninguna persona ajena a nuestra organización ni por nadie que no esté autorizado para ello (aunque pertenezca a nuestra empresa).

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, y de hecho coincide con la definición más generalizada de la confidencialidad, es que los datos solo sean conocidos por el emisor y el receptor al que van dirigidos.

Por lo tanto, al margen de lo que se indique en el plan de seguridad de la organización, deberemos atenernos a la LOPD para garantizar la confidencialidad y protección de los datos personales, pudiéndose exigir tanto las medidas de seguridad indicadas en la ley, como las responsabilidades y sanciones expuestas en la misma, en cualquier situación.

4.2. Rigurosidad de los datos tratados.

Puesto que constantemente estamos manejando información, no es de recibo que esta no sea correcta. Es responsabilidad del usuario que está tratando la información hacer todo lo que esté en su mano para verificar que esta es correcta.

La rigurosidad de los datos tratados es un bien muy valioso para la organización, ya que unos datos falseados prácticamente no tienen utilidad alguna.

En el plan de seguridad se establecerán las correspondientes medidas de verificación de datos, así como las sanciones oportunas para aquellos que no cumplan con las indicaciones dadas.

Se deberá confirmar que los datos se transmiten adecuadamente por el sistema. Como hablamos hoy en día de datos de carácter informático, principalmente, deberemos asegurarnos de que los datos se tratan por los programas adecuados para su correcta visualización y transmisión.

Es decir, no podemos intentar ver unos datos transmitidos en un fichero Excel, abriendo los con el PowerPoint. Aunque se pudiera hacer, no se transmitiría adecuadamente toda la información contenida en los mismos. Es por ello que debemos velar por la adecuada gestión de la información y de los datos en nuestra organización.

4.3. Utilización de datos de forma exclusiva.

¿Qué veremos aquí?... Bien, 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.

¿Qué permitirán estos sistemas de gestión de usuarios?

- Gestionar usuarios y sus datos de identificación.

- Asignarles permisos, en función de sus necesidades.

- Controlar el acceso a los recursos.

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 podernos encontrar las siguientes:

- Control de acceso a la red corporativa: estos sistemas evitarán 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., necesarias para el correcto funcionamiento de la organización.

- Inicio de sesión único: permiten el acceso a diversos recursos, programas o dispositivos de la red, mediante un identificador común.

- Sistemas de identidad 2.0: permiten acceder a varias localizaciones, portales o redes mediante una única identificación de usuario.

- Sistemas de control de presencia y acceso: estos sistemas cuentan con técnicas biométricas (lectura de huellas, por ejemplo) o bien tarjetas de acceso, para controlar quién y cuándo está presente en alguno de los sistemas o dispositivos de la organización.

Ya hemos podido ver someramente que necesitaremos una buena gestión de usuarios para garantizar que los datos son tratados única y exclusivamente por las personas adecuadas para ello. Pero, ¿cómo se deben asignar estos usuarios?

Como en cualquier otro proceso que se precie, para gestionar los usuarios dentro de una organización, debemos llevar a cabo una serie de pasos básicos, que los llevará a cabo el **Administrador del sistema,** que son:

- Evaluación de las necesidades: inicialmente debemos evaluar las necesidades de la organización. Debemos ver qué empleados necesitan acceder al sistema y qué datos les hace faltan poder tener accesibles cada uno de ellos.

- Creación de usuarios: una vez se han determinado las personas que pueden acceder a la red, se crean los usuarios necesarios para ello. En los siguientes pasos les asignaremos los permisos adecuados.

- Creación de permisos: en este paso crearemos los diferentes niveles de acceso que hemos considerado necesarios tras la evaluación inicial.

- Asignación de permisos a los usuarios: tras haber creado los usuarios y los diferentes niveles de acceso que pueden darse en nuestro sistema, cada usuario o grupo de usuarios será asignado al nivel que le corresponda según la evaluación de las necesidades hecha anteriormente.

- Asignación de códigos de acceso: por último, a cada usuario se le asignará un código de acceso único, para garantizar su privacidad y que sus permisos queden bajo su responsabilidad.

Tras llevar a cabo la gestión de 1os 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. .

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

Lógicamente es el administrador del sistema quien debe dar respuesta a las incidencias que ocurran en la red y es su responsabilidad garantizar la integridad y el buen esta do de la misma.

Llegamos en este punto a ver qué debe hacer el administrador del sistema para dar respuesta ante los errores o infracciones cometidas en la manipulación de los datos.

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, para poder presentarla de una manera ágil y ordenada.

Será responsabilidad del Administrador del sistema realizar copias de seguridad periódicas de dicha base 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.

Estas copias de seguridad se deben hacer en un sistema inaccesible para todos los usuarios, exceptuando claro está al Administrador, de manera que no puedan verse comprometidas por accesos inoportunos a la red corporativa o por fallos del sistema.

En organizaciones con datos vitales para su funcionamiento, se llevan a cabo incluso *backups* de los *backups*, para así conseguir salvaguardar la mayor cantidad de información posible ante una eventual caída de los sistemas.

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. Es como los motores en un avión, que deben estar pensados para seguir en vuelo ante un fallo en uno de ellos.

Además de gestionar las copias de seguridad, de las cuales el administrador será el único responsable, 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 de un usuario, será el responsable, atendiendo al plan de seguridad establecido por la organización, quien determine las sanciones oportunas al respecto. El administrador en estos casos se encargará de solventar el problema ocasionado, advertir al usuario infractor e informar a quien corresponda por que establezca la sanción más adecuada a las circunstancias.

4.5. Amenazas, vulnerabilidades y principales delitos.

En primer lugar, distinguiremos entre qué es una amenaza y qué es una vulnerabilidad. Estos conceptos están ligados más a la seguridad informática, que, a la seguridad de la información, pero tal y como vimos al principio ambas están estrechamente ligadas:

- **Amenaza:** se considera amenaza a una acción o suceso que compromete la seguridad del sistema. Este hecho puede ser deliberado o no y si aprovecha una vulnerabilidad de nuestro sistema, puede ser realmente preocupante.

- **Vulnerabilidad:** una vulnerabilidad es cualquier debilidad o brecha que exponga al sistema a una amenaza comprometiendo la integridad del mismo.

Para resumir ambos conceptos, podemos decir que las amenazas podrían ser acciones que se aprovechan de una vulnerabilidad del sistema para comprometer la integridad del mismo.

Las vulnerabilidades las podremos clasificar según a qué etapa o funcionalidad del sistema afecte. Así, podemos encontrar:

- **Vulnerabilidades de Diseño:** debido a un mal diseño del sistema con malas políticas de seguridad o a lo que se denominan *puertas traseras* no convenientemente protegidas.

Vulnerabilidades de Implementación: a pesar de que el sistema tenga un diseño correcto, puede haber errores de programación en el mismo que hagan que sea vulnerable a ciertos ataques.

- **Vulnerabilidades de Usuario:** finalmente son los usuarios los que utilizan el sistema, y una mala actuación por parte de los mismos puede hacer que el sistema sea vulnerable en ciertos momentos.

En lo referente a las amenazas, podemos optar por varios criterios de clasificación de las mismas, teniendo en cuenta que normalmente aprovechan alguna de las debilidades del sistema. Así, hay dos grandes grupos de amenazas, las físicas y las lógicas, que ya hemos tratado de alguna forma en el apartado anterior. También se pueden clasificar *según qué o quién* las provoca, atendiendo a la naturaleza de las mismas, los tipos de daños que pueden provocar, etc.

Por ejemplo, dentro de los diferentes tipos de amenazas indicadas podremos encontrar:

- Qué o quién las provoca:

*** Personas:**

Personal de la compañía: en este caso suelen ser accidentes por descuidar el correcto seguimiento de los protocolos de seguridad instaurados.

Exempleados: puede ser más peligroso, ya que pueden intentar provocar daños graves en los datos de la compañía.

Curiosos: son hackers que solo miran y no hacen nada.

Hackers: pretenden romper los sistemas, y si se da el caso sacar algún provecho de ello.

Intrusos remunerados: buscan datos relevantes que puedan servir a otras compañías que les pagan para ello.

*** Desastres:**

Incendios. Inundaciones. Ter

remotos.

Algunas amenazas de tipo lógico pueden ser:

***** Virus.

***** Puertas traseras.

***** Bombas lógicas.

Terminología básica de seguridad informática:

Dentro de la terminología básica de seguridad Informática, nos encontramos los ***principales delitos*** a los que nos podemos enfrentar:

-**3DES (Triple DES):** algoritmo de cifrado.

-**AES:** algoritmo de cifrado.

-**Amenaza:** elemento con potencial de causar daños en sistema.

-**Antivirus:** software para proteger el equipo de virus.

-**Blacklisting** (Lista negra): proceso de bloqueo de programas o equipos maliciosos 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 sí mismos con el objetivo de colapsar los ordenadores para impedir el trabajo normal de los mismos.

-**Hacker:** persona experta en vulnerar sistemas informáticos ("pirata informático").

-**Hacking:** acceso no autorizado a sistemas informáticos por parte de terceras personas (Hackers).

-**Malware:** programas diseñados para dañar un sistema informático.

-**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.

-**Phishing:** término con el que se designa la suplantación de páginas web para obtener datos 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.

Aunque esta es la terminología más destacada, le animamos a ojear el glosario de términos que puede encontrar en www.incibe.es (Instituto nacional de ciberseguridad) en el siguiente enlace.

https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

Como se podrá deducir, es conveniente tener siempre correctamente configurado y actualizado el Firewall que se esté utilizando para prevenir en la medida de lo posible accesos no deseados. Los elementos más peligrosos que podemos encontrarnos son los **virus.** De sobra conocidos por todos los usuarios informáticos, los virus no son más que programas que se ejecutan sin permiso del usuario en el PC, llevando a cabo instrucciones y operaciones no autorizadas por el usuario y que pueden ser más o menos dañinas, según la maliciosidad del creador del mismo. Hay muchos tipos de virus y aunque estos aumentan con el paso del tiempo, indicaremos los tres o cuatro tipos más conocidos y usuales:

Gusanos *(Worms):* estos virus, una vez instalados en el sistema, se dedican a duplicarse y consumir recursos, haciendo que este se vuelva cada vez más lento e inoperativo.

-**Troyanos:** son virus que dan acceso al creador a parte de nuestro sistema, vulnerando así nuestra confidencialidad.

-**Bombas de tiempo:** se ejecutan ante un hecho o acción determinados (por ejemplo viernes 13) y pueden causar más o menos daño.

-**Zombi e:** dejan el PC inutilizado y lo utilizan como trampolín para generar nuevos **virus e infecciones.**

Con unas cuantas **normas de conducta o buenas prácticas** podemos hacer que el peligro ante los virus disminuya notablemente. Estas pueden ser:

-Tener el Firewall correctamente configurado y actualizado.

-Tener el antivirus del sistema correctamente configurado y actualizado.

-No abrir emails sospechosos.

-No abrir documentos sospechosos.

-No utilizar memorias USB y otros dispositivos de memoria de terceros sin escanearlos previamente.

-No aceptar contactos sospechosos.

Como se puede ver, son medidas bastante lógicas, pero al final muchas personas dejan de tenerlas en cuenta y favorecen la propagación de estos programas llamados Malware.

Los **antivirus** son programas (Software) creados para intentar luchar contra los virus. Los hay gratuitos y de pago, según las necesidades, y pueden ofrecer más o menos herramientas opcionales, aunque todos en su mayoría ofrecen buena protección. Es conveniente que estén siempre operativos funcionando en lo que se llama *segundo plano*, para favorecer la interceptación de posibles ataques y siempre deben estar correctamente actualizados para que puedan detectar nuevas creaciones de virus antes de que puedan llegar a infectar nuestros sistemas.

En el mundo digital actual, es crucial adoptar medidas de seguridad robustas para nuestras **contraseñas**. Para garantizar que no sean vulnerables a la decodificación, es esencial crear contraseñas largas, de al menos 8 caracteres, que combinen letras, números, mayúsculas, minúsculas y caracteres especiales, como @, #, o !. Esta combinación hace que las contraseñas sean considerablemente más difíciles de descifrar para cualquier persona que intente acceder de manera no autorizada.

Además, es prudente cambiar periódicamente nuestras contraseñas para evitar posibles intentos de hackeo a lo largo del tiempo. Este hábito reduce la posibilidad de que alguien pueda acceder a nuestras cuentas mediante métodos de prueba y error.

Es importante también recordar que las contraseñas son personales y confidenciales, y nunca debemos compartirlas con nadie, ya que esto podría comprometer la seguridad de nuestras cuentas.

Mantener un nivel adecuado de precaución y vigilancia en relación con nuestras contraseñas es fundamental para proteger nuestra información en línea.

Guardar las contraseñas en archivos en nuestros dispositivos electrónicos puede ser riesgoso, ya que si el dispositivo es comprometido o perdido, las contraseñas podrían caer en manos equivocadas. Es mejor utilizar gestores de contraseñas seguros que encripten y protejan nuestras credenciales de forma más efectiva.

Respecto a los correos electrónicos, es fundamental tomar precauciones para proteger nuestra privacidad y seguridad en línea. Algunas medidas típicas incluyen:

No abrir correos electrónicos sospechosos: Si recibimos correos de remitentes desconocidos o que parecen ser spam, es mejor no abrirlos y eliminarlos de inmediato para evitar posibles ataques de phishing o malware.

Verificar la autenticidad de los remitentes: Antes de hacer clic en enlaces o descargar archivos adjuntos en correos electrónicos, siempre es prudente verificar la autenticidad del remitente. Los correos electrónicos falsos pueden parecer legítimos, pero su contenido puede contener enlaces maliciosos o archivos infectados.

No compartir información sensible por correo electrónico: Evitar enviar información personal o confidencial, como números de tarjeta de crédito o contraseñas, a través del correo electrónico, ya que este método de comunicación no siempre es seguro y podría ser interceptado por terceros no autorizados.

Utilizar autenticación de dos factores (2FA): Cuando sea posible, activar la autenticación de dos factores en nuestras cuentas de correo electrónico para agregar una capa adicional de seguridad. Esto requiere no solo la contraseña correcta, sino también un segundo factor de autenticación, como un código enviado a nuestro teléfono móvil.

Mantener el software actualizado: Asegurarse de que tanto el cliente de correo electrónico como el sistema operativo estén actualizados con los últimos parches de seguridad para protegerse contra vulnerabilidades conocidas.

Adoptar estas precauciones puede ayudar a reducir el riesgo de comprometer nuestra seguridad y privacidad al utilizar el correo electrónico.

Estas mismas precauciones que aplicamos al correo electrónico también deben extenderse a los sistemas de Office y otros programas que utilizamos en nuestros dispositivos. Aquí hay algunas medidas adicionales que podemos tomar para proteger nuestros datos en estos sistemas:

Verificar la procedencia de los archivos adjuntos: Antes de abrir cualquier archivo adjunto en programas como Word, Excel, PowerPoint o PDF, es importante verificar la autenticidad del remitente y asegurarse de que el archivo sea legítimo. Si recibimos archivos de remitentes desconocidos o inesperados, es mejor no abrirlos y eliminarlos de inmediato.

Utilizar software de seguridad: Mantener instalado y actualizado un software antivirus y antimalware puede ayudar a detectar y eliminar archivos maliciosos antes de que puedan causar daño a nuestro sistema.

Configurar la seguridad de los programas Office: Muchos programas de Office, como Microsoft Office, ofrecen opciones de seguridad avanzadas que pueden ayudar a proteger nuestros archivos

contra amenazas. Configurar estas opciones según nuestras necesidades y mantenerlas actualizadas puede proporcionar una capa adicional de protección.

No habilitar macros automáticamente: Las macros en documentos de Word, Excel u otros programas de Office pueden ser utilizadas por los atacantes para ejecutar código malicioso en nuestro sistema. Por lo tanto, es importante configurar nuestros programas para que no se ejecuten las macros automáticamente y solo permitir su ejecución si confiamos en la fuente del documento.

Estar atento a las señales de phishing: Los archivos adjuntos maliciosos en documentos de Office pueden ser utilizados en ataques de phishing para engañarnos y hacernos descargar malware en nuestros sistemas. Por lo tanto, es importante estar atentos a las señales de phishing, como correos electrónicos inesperados o solicitudes de información sensible, y evitar abrir archivos adjuntos de remitentes no confiables.

Al seguir estas precauciones y mantenernos alerta, podemos reducir el riesgo de comprometer nuestros datos y sistemas al abrir archivos en programas de Office u otros formatos.