Persevera

AL ALCANCE DE QUIEN ESTUDIA

BLOQUE VI · INFORMÁTICA BÁSICA Y OFIMÁTICA

Tema 1

Informática básica

Cuerpo General Administrativo de la Administración del Estado

INGRESO LIBRE · EDICIÓN 2026

perseveraoposiciones.com

AL ALCANCE DE QUIEN ESTUDIA

Estudiar una oposición ya cuesta bastante. Dinero, tiempo, esfuerzo. Lo que se ofrece habitualmente añade fricción: temarios caros y no redistribuibles, academias con horarios fijos y mensualidades que no todos pueden pagar.

Persevera publica los temarios enteros, en abierto. Lees, copias, imprimes y compartes con quien quieras.

Esta es la primera entrega. Los siguientes cuerpos los decidiremos contigo: nos cuentas qué oposición te interesa.

El temario es un producto vivo: hay erratas, hay matices que pueden afinarse, hay decisiones de redacción que pueden discutirse. Si encuentras algo que pueda mejorar, escríbenos. Lo leemos todo y publicamos las correcciones.

ÍNDICE

TEMA 1

Epígrafe 1 — Informática básica: conceptos fundamentales sobre el hardware y el software

1. Concepto de informática y de ordenador

El término **informática** procede del francés *informatique*, acuñado por el ingeniero francés **Philippe Dreyfus** en **1962** como contracción de las palabras *information* y *automatique*. Designa la disciplina que estudia el tratamiento automático de la información mediante máquinas.

La **Real Academia Española** define la informática como el conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de computadoras. La fórmula condensa los tres elementos nucleares de la disciplina: una **base teórica** (conocimientos científicos y técnicas), un **objeto** (la información) y un **medio** (la computadora u ordenador).

Un **ordenador** es cualquier dispositivo electrónico que integre un **microprocesador**, **memoria** e **interfaces de entrada/salida**. Su función esencial es procesar información en cuatro fases sucesivas: **admitir datos**, **procesarlos**, **almacenarlos** y **mostrar resultados**. La definición abarca desde el PC de sobremesa doméstico hasta el servidor del centro de datos corporativo.

> **RECUERDA**
>
> El término *informatique* fue acuñado por Philippe Dreyfus en 1962 en Francia; el español lo adoptó por traducción. La regla de estudio para reconocer un ordenador es **microprocesador + memoria + interfaces de E/S**: si falta cualquiera de los tres, el dispositivo no encaja en la definición habitual de ordenador del temario.

2. Generaciones del ordenador

La historia del ordenador se organiza en **cinco generaciones** según la tecnología empleada para fabricar sus componentes lógicos. Las fechas son **orientativas** y varían según la fuente; el dato consolidado es la **tecnología** asociada a cada generación.

Generación	Período aproximado	Tecnología clave
1.ª	1938 – 1952	Válvulas de vacío
2.ª	1953 – 1962	Transistores
3.ª	1963 – 1971	Circuitos integrados
4.ª	1972 – 1987	Microprocesadores
5.ª	1988 – actualidad	Inteligencia artificial

MATIZ

Las fechas de las generaciones varían entre fuentes y manuales; el dato estable es la **tecnología asociada**, no el año concreto. 3.ª generación = circuitos integrados, no «década de los sesenta». 4.ª generación = microprocesadores, no «década de los setenta». La pareja generación–tecnología es la que se fija.

3. Tipos de ordenador

Tipo	Características principales
PC *(Personal Computer)*	Ordenador de uso general. Categoría paraguas que incluye sobremesa y portátil.
Mac	PC fabricado por Apple con procesadores propios (chips M-series desde 2020). Sistema operativo macOS. Históricamente orientado a edición de imagen y vídeo; hoy de uso generalizado.
PC de sobremesa	No diseñado para moverse. Mayor versatilidad, potencia y facilidad de expansión a menor coste que el portátil.
Portátil	Componentes integrados y batería para uso autónomo. A igualdad de prestaciones, más caro que el sobremesa equivalente.

Tableta	Pantalla táctil con todo integrado en un único cuerpo, sin teclado físico fijo. Categoría moderna popularizada por el iPad (2010); evolución de la PDA.
PDA *(Personal Digital Assistant)*	Asistente personal digital de los años 90 y primeros 2000. **Sustituido por los smartphones a partir de 2010** figura en los temarios por su valor histórico, no por su uso actual.
Workstation	Sobremesa de alto rendimiento con componentes especializados (CPU multinúcleo, GPU profesional, RAM ECC) para tareas intensivas: diseño asistido por ordenador, ingeniería, simulación científica, edición de vídeo 4K/8K.
Servidor	Diseñado para dar servicio simultáneo a múltiples usuarios o equipos de una red local o de Internet. Doble procesador, gran memoria, discos en array para redundancia, alimentación redundante. Funcionamiento 24/7.

RECUERDA

La diferencia nuclear entre **workstation** y **servidor** está en el destinatario del servicio: la *workstation* atiende a **un usuario individual** con tareas intensivas; el servidor da servicio a **múltiples usuarios o equipos** simultáneos a través de la red.

4. El hardware: clasificación y función

El **hardware** es el conjunto de componentes físicos del ordenador. El **software** es la parte lógica e intangible: los programas que dirigen el funcionamiento del hardware. Las dos categorías son indisociables: un ordenador sin software no opera, y un software sin hardware no se ejecuta.

4.1. Hardware básico vs hardware complementario

El **hardware básico** es el mínimo imprescindible para que el equipo arranque y funcione: **CPU**, **memoria** y **dispositivos de entrada/salida**. La ausencia de cualquiera de los tres impide el arranque del ordenador.

El **hardware complementario** amplía o mejora las prestaciones del básico sin ser imprescindible: tarjetas gráficas dedicadas, grabadoras de DVD, lectores de tarjetas, tarjetas de red Wi-Fi adicionales, capturadoras de vídeo, etc.

MATIZ

La calificación como básico o complementario depende del caso concreto. La **gráfica integrada** en la CPU o en la placa base es hardware **básico** (sin ella no habría salida de imagen). Una **tarjeta gráfica dedicada** de alto rendimiento (Nvidia RTX, AMD Radeon) es hardware **complementario** que añade capacidades sobre el básico.

4.2. Clasificación del hardware por función

Categoría	Función	Ejemplos representativos
Almacenamiento	Conserva información a corto o largo plazo.	RAM, disco duro (HDD), unidad de estado sólido (SSD), memoria USB, DVD.
Proceso	Ejecuta operaciones aritméticas, lógicas y de control.	Microprocesador (CPU), unidad aritmético-lógica (ALU), chipset.
Entrada	Recibe datos del exterior y los introduce en el equipo.	Teclado, ratón, webcam, escáner, micrófono, sensor de huella.
Salida	Materializa la información procesada al exterior.	Monitor, impresora, altavoces, proyector.
Bidireccional	Actúa simultáneamente como entrada y como salida.	Tarjeta de red, pantalla táctil, impresora multifunción, módem.

RECUERDA

La **tarjeta de red** es el ejemplo canónico de dispositivo **bidireccional**: recibe datos de la red (entrada) y los envía hacia la red (salida). Clasificarla solo como entrada o solo como salida es un error frecuente.

5. La arquitectura Von Neumann

Casi un siglo después de su formulación, la **arquitectura Von Neumann** sigue siendo la base de prácticamente todos los ordenadores modernos. Su principio es elegante: tres bloques funcionales (**CPU**, **memoria** y **dispositivos de E/S**) interconectados por **buses de datos** —las autopistas por las que viaja la información—, todo ello implementado sobre la **placa base** (*motherboard*).

FIGURA

Diagrama de la arquitectura Von Neumann: tres bloques (CPU / Memoria principal / Dispositivos de E/S) interconectados por buses de datos, dirección y control.

El **flujo de trabajo** sigue siempre la misma secuencia: los dispositivos de entrada entregan información a la CPU, que utiliza la memoria principal para llevar a cabo las operaciones necesarias y después actúa sobre los dispositivos de salida con los resultados.

RECUERDA

Junto a Von Neumann existe la **arquitectura Harvard**, que separa la memoria en dos partes independientes: una para **instrucciones** y otra para **datos**. Es la base de muchos microcontroladores actuales y de la **caché L1** de los procesadores modernos, que se divide en L1 de instrucciones (L1I) y L1 de datos (L1D). Los procesadores comerciales combinan ambas arquitecturas: Harvard a nivel de caché L1 y Von Neumann en el resto.

6. La CPU: motor del sistema

La **CPU** (*Central Processing Unit*, Unidad Central de Proceso) es el núcleo del sistema: ejecuta todas las operaciones del ordenador. Internamente se compone de cuatro elementos:

- **ALU** *(Arithmetic Logic Unit, Unidad Aritmético-Lógica)*: realiza las operaciones aritméticas (suma, resta, multiplicación, división) y lógicas (AND, OR, NOT, comparaciones).

- **Unidad de Control (UC)**: dirige y coordina al resto de componentes; interpreta cada instrucción y ordena su ejecución.
- **Registros**: memorias ultrarrápidas internas que almacenan los datos con los que la CPU está operando en cada instante.
- **Reloj del procesador**: oscilador que marca los ciclos de trabajo en gigahercios (GHz). A más GHz, mayor número de ciclos por segundo y mayor velocidad teórica.

Un microprocesador puede ser **multinúcleo**: combina dos o más núcleos independientes dentro de un único circuito integrado, lo que permite **procesamiento paralelo** real (varios programas o varios hilos ejecutándose simultáneamente).

6.1. CISC vs RISC: dos filosofías de diseño

Arquitectura	Descripción	Uso habitual
CISC *(Complex Instruction Set Computer)*	Juego de instrucciones amplio y complejo. Cada instrucción puede realizar operaciones complejas en un solo paso.	Procesadores Intel y AMD (PC y portátiles con Windows o Linux).
RISC *(Reduced Instruction Set Computer)*	Microinstrucciones simples que se combinan para formar operaciones complejas. Mayor eficiencia energética por ciclo.	Apple (chips M-series), procesadores ARM, consolas de videojuegos modernas.

MATIZ

En la clasificación clásica del temario, los **Mac** actuales (M1, M2, M3, M4, lanzados desde 2020) usan chips con arquitectura **RISC** (Apple Silicon, base ARM), mientras que la mayoría de PC con Windows o Linux usa procesadores **CISC** de Intel o AMD (familia x86). La asociación memorable es **Mac = RISC** vs **PC = CISC**, aunque conviene saber que existen PC modernos con procesadores ARM (RISC) y que los x86 actuales traducen internamente instrucciones complejas a microoperaciones más simples.

7. El firmware: BIOS y UEFI

Dentro del software existe una categoría especial: el **firmware**. Es un programa que establece la lógica de más bajo nivel para controlar los elementos físicos del equipo. Viene **grabado de fábrica** en un chip de memoria no volátil (tradicionalmente ROM; hoy típicamente flash SPI).

7.1. La BIOS

El firmware fundamental del equipo se denomina **BIOS** (*Basic Input Output System*, sistema básico de entrada y salida). Cumple dos funciones nucleares al encender el equipo:

- **POST** *(Power-On Self-Test, autocomprobación de encendido)*: verifica que todos los componentes —memoria, CPU, gráfica, almacenamiento— estén presentes y funcionen correctamente.
- **Arranque del sistema operativo**: una vez superado el POST, la BIOS localiza el dispositivo de arranque (disco duro o SSD) y entrega el control al cargador del sistema operativo.

> **FIGURA**
>
> Captura de la interfaz de la BIOS en modo texto: pantalla con fondo oscuro, menú navegable solo con teclado y opciones de configuración (fecha y hora del sistema, secuencia de arranque, parámetros de memoria, opciones de la CPU).

7.2. La UEFI

Con el avance tecnológico, la BIOS ha sido sustituida en los sistemas modernos por la **UEFI** (*Unified Extensible Firmware Interface*, interfaz de firmware extensible unificada). Sus funciones conceptuales son las mismas que las de la BIOS, pero la implementación aporta mejoras significativas:

Característica	BIOS	UEFI
Interfaz de usuario	Solo teclado, modo texto	Ratón y teclado, modo gráfico
Velocidad de arranque	Más lenta	Más rápida (arranque optimizado)
Conectividad de red	Sin acceso a red	Puede conectarse a Internet (actualizaciones, diagnóstico)

Seguridad en el arranque	Básica	**Secure Boot**: verifica la firma digital del cargador del SO antes de ejecutarlo
Capacidad de almacenamiento gestionado	Hasta 2,2 TB (tabla MBR)	Sin ese límite (tabla GPT)

FIGURA

Interfaz de la UEFI de un equipo moderno: pantalla gráfica con información en tiempo real de CPU, temperaturas, velocidad de la memoria RAM y prioridad de arranque, navegable con ratón.

RECUERDA

La **UEFI** sustituye a la BIOS en los sistemas modernos. La novedad más característica es **Secure Boot**: verifica que el cargador del sistema operativo esté firmado digitalmente antes de ejecutarlo, lo que dificulta la ejecución de software malicioso durante el arranque. La función del firmware (POST + arranque del SO) es la misma en BIOS y en UEFI.

8. Tipos de memoria: volatilidad y jerarquía

La memoria no es un componente único: es una **familia** de componentes con características muy distintas. La clasificación más útil distingue por **volatilidad** —si los datos sobreviven o no al apagado del equipo—.

8.1. Clasificación por volatilidad

Tipo	Volatilidad	Descripción y uso
Registros CPU	Volátil	Los más rápidos y los de menor capacidad. Almacenan los datos que la CPU necesita de inmediato para la instrucción en curso.

Caché (L1, L2, L3)	Volátil	Copia de los datos accedidos con más frecuencia. Integrada en la CPU. L1 es la más pequeña y rápida, L3 la mayor y más lejana. Usa tecnología SRAM.
RAM *(Random Access Memory)*	Volátil	Memoria principal del equipo. Se borra al apagar. Almacena los programas en ejecución y los datos en uso. Usa tecnología DRAM.
ROM *(Read-Only Memory)*	No volátil	Memoria de solo lectura. Contiene el firmware del equipo (BIOS/UEFI). No se borra al apagar.
CMOS	Volátil	Pequeño chip que almacena la configuración del firmware y el reloj de tiempo real. Alimentado por la **pila CMOS** (pila botón CR2032 en la placa base) que mantiene la información cuando el equipo está desconectado.
Búfer	Volátil	Memoria intermedia que almacena datos temporalmente durante una transferencia entre dos componentes a distinta velocidad. Se usa una sola vez (a diferencia de la caché, que reutiliza los datos).

MATIZ

RAM = volátil (se borra al apagar), lectura **y** escritura, usada para ejecutar programas. **ROM** = no volátil (no se borra), tradicionalmente solo lectura, contiene el firmware. Intercambiar las dos definiciones es uno de los errores más frecuentes. La regla mnemotécnica es: **R**andom y **R**ead-Only — la primera R es la única letra común; el resto las distingue.

8.2. SRAM vs DRAM: dos tecnologías de RAM

Tipo	Tecnología interna	Velocidad	Uso
SRAM *(Static RAM)*	Transistores. Retiene la carga sin necesidad de refresco.	Muy rápida	Memoria caché de la CPU (L1, L2, L3)
DRAM *(Dynamic RAM)*	Condensadores. Necesita circuito de refresco periódico que reescribe la carga miles de veces por segundo.	Más lenta que SRAM	Módulos de RAM principal del equipo (DDR4, DDR5)

8.3. Tipos de ROM: PROM, EPROM, EEPROM

Tipo	Característica diferenciadora
PROM *(Programmable ROM)*	Programable una sola vez después de su fabricación. Tras la primera grabación ya no puede modificarse.
EPROM *(Erasable Programmable ROM)*	Programable y borrable mediante exposición a **luz ultravioleta**. Permite reprogramación bajo condiciones específicas.
EEPROM *(Electrically Erasable Programmable ROM)*	Borrable y reprogramable **eléctricamente**, sin necesidad de extraer el chip. Soporta mayor número de ciclos de borrado y es la base tecnológica de las **memorias flash** actuales (USB, SSD, tarjetas SD).

8.4. Jerarquía de memorias y unidades de medida

FIGURA

Pirámide de jerarquía de memorias. De arriba (vértice) a abajo (base): registros · caché L1 / L2 / L3 · RAM · almacenamiento masivo (SSD, HDD). Hacia el vértice: velocidad mayor, capacidad menor. Hacia la base: velocidad menor, capacidad mayor.

Los ordenadores trabajan en **binario** (0 y 1). La unidad mínima es el **bit** ocho bits forman un **byte**. En codificaciones clásicas (ASCII, ISO-8859) un byte representa un carácter; en codificaciones modernas como **Unicode (UTF-8)**, un carácter puede ocupar **uno o varios**

bytes (entre uno y cuatro). A partir del byte, las unidades crecen en potencias de **1.024** (2^{10}):

Unidad	Símbolo	Equivalencia
Bit	b	1 ó 0
Nibble	–	4 bits
Byte	B	8 bits
Kilobyte	KB	1.024 bytes
Megabyte	MB	1.024 KB
Gigabyte	GB	1.024 MB
Terabyte	TB	1.024 GB
Petabyte	PB	1.024 TB
Exabyte	EB	1.024 PB
Zettabyte	ZB	1.024 EB
Yottabyte	YB	1.024 ZB

RECUERDA

La progresión nemotécnica es **K-M-G-T-P-E-Z-Y** (KiloMega-Giga-Tera-Peta-Exa-Zetta-Yotta). Cada salto multiplica por **1.024** (no por 1.000). El bit es la unidad de información; el byte agrupa ocho bits y, en codificaciones clásicas, representa un carácter (en Unicode/UTF-8 un carácter puede ocupar más de un byte).

9. La placa base: componentes internos y conectores externos

La **placa base** o *motherboard* es la placa de circuito impreso donde se interconectan el resto de componentes del equipo. Tiene tres funciones nucleares: **conectar físicamente** los componentes principales (CPU, RAM, almacenamiento), **distribuir la energía eléctrica** entre ellos y **soportar** los puertos de conexión de dispositivos periféricos.

9.1. Componentes internos de la placa base

Componente	Función clave
Zócalo de CPU *(Socket)*	Lugar donde se aloja el microprocesador. Suele ocupar la zona central de la placa base.
Ranuras de RAM *(Slots)*	Alojan los módulos de memoria RAM en formato **DIMM** *(Dual In-line Memory Module)*. Suelen disponerse en pares para funcionamiento en doble canal.
BUS	Canales formados por «hilos» por los que circulan señales eléctricas. Tipos funcionales: **bus de datos** (transporta la información), **bus de dirección** (origen y destino) y **bus de control** (sincronización). La transmisión puede ser en serie o en paralelo.
Chipset	Conjunto de chips que coordinan la transferencia de datos entre los componentes del equipo.
Ranuras PCI-Express *(PCIe)*	Conectores de expansión para tarjetas dedicadas: gráficas, de red, de sonido o SSD adicionales.
SATA *(Serial ATA)*	Interfaz para la transferencia de datos entre la placa base y los dispositivos de almacenamiento (HDD, SSD, lectores DVD).
Pila CMOS	Pila tipo botón (formato CR2032) que mantiene la configuración del firmware y el reloj de tiempo real cuando el equipo está desconectado de la corriente.
Disipadores	Reducen la temperatura del procesador y otros chips. Pueden ser ventiladores, sistemas de refrigeración líquida o disipadores pasivos (placas metálicas).
Fuente de alimentación	Transforma la corriente alterna de la red eléctrica en corriente continua a las tensiones que necesita cada componente. Protege frente a sobretensiones.

FIGURA

Fotografía de una placa base ATX con etiquetas: zócalo de CPU, ranuras DIMM de RAM, ranuras PCI-Express, conectores SATA, pila CMOS, chipset, chip de firmware (BIOS/UEFI), conectores de la fuente de alimentación y backplate de conectores externos.

9.2. Conectores externos de la placa base

Conector	Función y características clave
USB *(Universal Serial Bus)*	Bus universal en serie. Tecnología plug and play (conectar y usar). Distintas versiones con velocidades crecientes (ver tabla 9.3).
Thunderbolt	Conexión de alta velocidad desarrollada por Intel. Desde su versión 3 utiliza conector USB-C y se identifica con el icono de un rayo.
VGA *(Video Graphics Array)*	Conexión analógica entre el equipo y la pantalla. Transmite solo imagen. En desuso.
DVI *(Digital Visual Interface)*	Sucesor del VGA. Señal digital. Transmite solo imagen. En desuso progresivo.
HDMI *(High-Definition Multimedia Interface)*	Transmite imagen de alta definición y audio digital en un único cable. **HDMI 2.1** (2017) ofrece hasta 48 Gbps; **HDMI 2.2** (2025) eleva el ancho de banda hasta 96 Gbps.
DisplayPort	Estándar similar a HDMI con prestaciones ligeramente superiores. Transmite imagen y audio digital. Habitual en monitores profesionales.
RJ45	Puerto Ethernet para cable de red de pares trenzados.
Jack de audio	Conector de audio analógico de 3,5 mm. Entrada (micrófono) o salida (auriculares, altavoces).

MATIZ

VGA y **DVI** transmiten **solo imagen**. **HDMI** y **DisplayPort** transmiten **imagen y sonido** en un único cable. Es una de las distinciones más frecuentes.

RECUERDA

Resoluciones estándar: VGA 640 × 480 · HD 1.280 × 720 · Full HD 1.920 × 1.080 · 4K 3.840 × 2.160. La denominación «4K» se refiere a los ≈ 4.000 píxeles del eje horizontal.

9.3. Velocidades USB y Thunderbolt

Versión USB	Año	Velocidad máxima	Notas
USB 1.0	1996	1,5 Mbps (Low-Speed) / 12 Mbps (Full-Speed)	Dos modos de funcionamiento.
USB 1.1	1998	1,5 / 12 Mbps	Misma velocidad que 1.0; revisión técnica.
USB 2.0	2000	480 Mbps (High-Speed)	Multiplica por 40 la velocidad del Full-Speed.
USB 3.0	2008	5 Gbps (SuperSpeed)	Estándar oficial USB-IF.
USB 3.1 Gen 1	2013	5 Gbps	Renombrado del USB 3.0.
USB 3.1 Gen 2	2013	10 Gbps (SuperSpeed+)	Duplica el ancho de banda.
USB 3.2 Gen 1×1	2017	5 Gbps	Equivalente al USB 3.0 / 3.1 Gen 1.
USB 3.2 Gen 1×2 / Gen 2×1	2017	10 Gbps	Equivalente al USB 3.1 Gen 2.
USB 3.2 Gen 2×2	2017	20 Gbps	Dos canales de 10 Gbps.
USB4	2019	20 / 40 Gbps	Basado en Thunderbolt 3. Conector USB-C obligatorio.
USB4 v2.0	2022	Hasta 80 Gbps (bidireccional)	Ancho de banda doblado respecto a USB4.

MATIZ

El **conector USB-C** no es exclusivo de una versión concreta del estándar USB: se introdujo con USB 3.1 pero también puede llevar señal USB 2.0 (cables simples) o USB4 (cables certificados). El conector y la velocidad son dos cosas distintas: un puerto USB-C **no garantiza** la velocidad máxima del estándar más reciente.

Versión Thunderbolt	Año	Velocidad máxima	Conector	Novedades principales
Thunderbolt 1	2011	10 Gbps	Mini DisplayPort	Primera versión, desarrollada por Intel y Apple.
Thunderbolt 2	2013	20 Gbps	Mini DisplayPort	Agrupación de los dos canales de 10 Gbps de TB1.
Thunderbolt 3	2015	40 Gbps	**USB-C**	Adopción del conector USB-C; integra USB 3.1 Gen 2.
Thunderbolt 4	2020	40 Gbps	USB-C	Soporte de hub obligatorio; protección DMA mediante Intel VT-d.
Thunderbolt 5	2023 (anuncio) / 2024 (primeros equipos)	**80 Gbps simétrico** · hasta **120 Gbps asimétrico** unidireccional para pantallas	USB-C	Carga hasta **240 W** PCIe Gen 4 × 4 (64 Gbps). Primeros Apple con TB5: **Mac mini M4 Pro** y **MacBook Pro M4 Pro/Max** (octubre 2024).

MATIZ

Thunderbolt 5 no es «120 Gbps» a secas: la cifra de 120 Gbps es **asimétrica** y se reserva al envío unidireccional hacia pantallas (por ejemplo, dos monitores 8K a 60 Hz). El **modo bidireccional simétrico** —el habitual para transferencia de datos— es de **80 Gbps**. La asociación memorable es: TB5 = 80 Gbps simétrico / 120 Gbps asimétrico para pantallas.

FIGURA

Tipos de conector USB: Type-A (USB 2.0 en negro, USB 3.0/3.1 en azul), Type-B, Mini-USB, Micro-USB y Type-C reversible. Sobre USB-C se añade el icono del rayo cuando admite Thunderbolt.

10. Periféricos

Los **periféricos** son los dispositivos hardware externos que permiten la comunicación entre el ordenador y el mundo exterior. Se clasifican en **entrada** (reciben datos), **salida** (los materializan al usuario) y **bidireccionales** (cumplen ambas funciones).

10.1. Periféricos representativos

Tipo	Periféricos
Entrada	Teclado (distribuciones QWERTY, QWERTZ, AZERTY), ratón, escáner (CCD; OCR para texto editable), cámara, micrófono, sensor de huella, lector de códigos de barras.
Salida	Monitor, impresora, altavoces, proyector.
Bidireccional	Tarjeta de red, pantalla táctil, impresora multifunción (escanea e imprime), módem, auriculares con micrófono.

10.2. Tipos de impresora

Las impresoras trasladan información digital a soportes físicos. La clasificación por **tecnología** es la consolidada:

Tipo	Mecanismo	Uso habitual
Matricial (impacto)	Cabezal con agujas que golpea una cinta entintada contra el papel.	En desuso; sobrevive para multicopia (pagarés, facturas con varias hojas autocopiativas).
Inyección de tinta	Microgotas de tinta proyectadas sobre el papel desde inyectores.	Habitual en uso doméstico por su coste inicial bajo y buena calidad de impresión en color.
Térmica (sublimación)	Papel especial sensible al calor que se oscurece o recibe tinte por sublimación.	Máquinas de fotos pequeñas, etiquetas, recibos, pegatinas.
Láser	Tóner (polvo de tinta) fijado al papel mediante un proceso similar al de la fotocopiadora.	Muy rápida y económica para grandes volúmenes; estándar en oficina.
Impresora 3D	Inyectores que depositan material plástico o resina por capas sucesivas.	Genera objetos tridimensionales a partir de modelos digitales.
Plóter	Inyección de tinta sobre soportes de gran formato.	Impresión de planos arquitectónicos, mapas, carteles de gran dimensión.

11. El software: categorías y formas de comercialización

Si el hardware es el cuerpo del ordenador, el **software** es su mente: la parte lógica e intangible que le dice qué hacer.

11.1. Clasificación por función

Categoría	Función	Ejemplos
Software de sistema	Gestiona el hardware del equipo y ofrece una interfaz de alto nivel al resto del software.	Sistema operativo (Windows, macOS, Linux), controladores (*drivers*), software de diagnóstico.
Software de programación	Proporciona herramientas a los desarrolladores para crear nuevos programas.	Entornos de desarrollo integrados (IDE), compiladores, intérpretes, depuradores (Visual Studio, Eclipse, Lazarus).
Software de aplicación	Permite al usuario realizar tareas específicas concretas.	Suite ofimática (Word, Excel), CAD, navegadores web, apli-

		caciones empresariales (ERP, CRM), videojuegos.

Dos definiciones complementarias dentro del software de sistema:

- **Driver o controlador**: software que gestiona la comunicación entre el sistema operativo y un dispositivo hardware concreto (impresora, tarjeta gráfica, teclado, escáner). Sin el driver adecuado, el sistema operativo no puede utilizar el dispositivo.
- **Plug and play**: tecnología que permite al sistema detectar y configurar automáticamente un nuevo dispositivo hardware sin intervención manual del usuario. El usuario «conecta y usa»: el SO localiza el driver, lo instala y deja el dispositivo operativo.

11.2. Clasificación por forma de comercialización

Tipo	Características
Software libre	Ofrece al usuario la posibilidad de **analizar, modificar, ampliar y redistribuir** el código fuente. Puede ser gratuito o de pago.
Software privativo	Restringe el acceso al código fuente: el usuario no puede estudiarlo, modificarlo ni redistribuirlo. Puede ser gratuito o de pago.
Freeware	Software **gratuito**, sin coste para el usuario. Puede ser libre o privativo.
Shareware	Se distribuye como **versión de demostración o evaluación**, con características o tiempo de uso limitados, hasta que el usuario adquiera la versión completa.

MATIZ

Software libre ≠ software gratuito. El software libre es aquel cuyo **código fuente** es accesible y modificable; puede ser de pago. El **freeware** es gratuito pero puede ser de código cerrado (privativo). Un programa de pago puede ser libre (LibreOffice Enterprise) y un programa gratuito puede ser privativo (versiones gratuitas de Adobe Reader).

RECUERDA

Asignación canónica de programas a categorías: un **compilador** es software de programación, no de sistema; el **sistema operativo** es software de sistema, no de aplicación; **Word, Excel y Outlook** son software de aplicación, no de sistema. Los **drivers** son software de sistema porque median entre el SO y el hardware.

Términos complementarios de hardware que conviene fijar:

- **AMD** *(Advanced Micro Devices)*: empresa estadounidense fabricante de microprocesadores y procesadores gráficos, competidora directa de Intel. Sus series actuales son **Ryzen** (consumo y profesional), **Athlon** (gama de entrada) y **EPYC** (servidores).
- **DIMM** *(Dual In-line Memory Module)*: formato físico estándar de los módulos de memoria RAM que se insertan en las ranuras (*slots*) de la placa base.
- **VRAM** *(Video Random Access Memory)*: memoria RAM dedicada integrada en la tarjeta gráfica. Almacena los datos de imagen y vídeo que la GPU necesita procesar. A mayor VRAM, mayor resolución y nivel de detalle gráfico posibles.

TEMA 1

Epígrafe 2 — Sistemas de almacenamiento de datos

1. Sistemas de numeración: la base del almacenamiento

El ordenador es un dispositivo electrónico binario: en su nivel físico sólo distingue dos estados, **encendido (1)** y **apagado (0)**. Toda la información que almacena —texto, imágenes, sonido, vídeo, instrucciones de programa— acaba representada como una secuencia de ceros y unos. Por eso, antes de estudiar los soportes físicos donde se guardan los datos, conviene fijar los **sistemas de numeración** que el ordenador y los técnicos emplean para representarlos.

El sistema de numeración cotidiano humano es **decimal** (base 10). Los ordenadores usan internamente **binario** (base 2), y para representar cantidades binarias de forma más compacta los profesionales recurren al **octal** (base 8) y al **hexadecimal** (base 16).

Sistema	Base	Dígitos válidos	Uso principal
Decimal	10	0 – 9	Uso cotidiano humano.
Binario	2	0, 1	Lenguaje máquina; representación de datos en hardware.
Octal	8	0 – 7	Representación compacta de binario (un dígito octal = 3 bits).
Hexadecimal	16	0 – 9 y A (10), B (11), C (12), D (13), E (14), F (15)	Direcciones de memoria, códigos de colores RGB, depuración.

1.1. Conversión entre sistemas

De cualquier base a decimal: sumar cada dígito multiplicado por la base elevada a su posición, contando desde 0 por la derecha.

- Binario: $101_2 = 1 \times 2^0 + 0 \times 2^1 + 1 \times 2^2 = \mathbf{5}$ en decimal.

- Hexadecimal: $A6_{16} = 6 \times 16^0 + 10 \times 16^1 = 6 + 160 = \mathbf{166}$ en decimal.

De decimal a otra base: división sucesiva entre la base objetivo; se anotan los restos y se leen **en orden inverso** (de abajo a arriba).

- Ejemplo: convertir 590 a hexadecimal.
  - 590 ÷ 16 = 36, resto **14 (E)**
  - 36 ÷ 16 = 2, resto **4**
  - Cociente final = **2**
  - Lectura inversa → $\mathbf{24E_{16}}$.

MATIZ

Al leer el resultado de la división sucesiva, los restos se leen **en orden inverso** al que se han obtenido: el último cociente va en la posición más significativa (a la izquierda) y el primer resto va en la posición menos significativa (a la derecha). Invertir el orden de lectura es el error más frecuente en las conversiones de base.

RECUERDA

En hexadecimal: **A = 10, B = 11, C = 12, D = 13, E = 14, F = 15**. Un dígito hexadecimal equivale a **4 bits** (un *nibble*); un byte (8 bits) se expresa, por tanto, en **exactamente 2 dígitos hexadecimales**. De ahí que los colores RGB se representen como `#RRGGBB`: dos hex por canal, valor 00-FF (0-255).

2. Datos e información: una distinción fundamental

En informática, **dato** e **información** no son sinónimos. La distinción es nuclear porque condiciona el modelo de procesamiento y el diseño de los sistemas de almacenamiento.

- **Dato**: representación simbólica de un atributo o variable que, de forma aislada, puede carecer de significado relevante. Ejemplo: el número «37» o la letra «M».

- **Información**: resultado de **procesar y contextualizar** un conjunto de datos bajo algún algoritmo o razonamiento; aporta valor al usuario. Ejemplo: «La temperatura del paciente es de 37 °C y su sexo es masculino».

> **MATIZ**
>
> Los datos individualmente **no** aportan información: sólo cuando se procesan y contextualizan se convierten en información. La afirmación «datos e información son sinónimos» es falsa.

2.1. Clasificación de los datos

Criterio	Tipos
Por flujo (posición en el proceso)	Datos de **entrada** · Datos **intermedios** (resultados parciales) · Datos de **salida**.
Por variabilidad	**Fijos** o constantes (no cambian durante el procesamiento, p. ej. el valor de π) · **Variables** (pueden modificarse, p. ej. el saldo bancario).
Por tipo de contenido	**Numérico** · **Alfabético** · **Alfanumérico** · **Lógico** o booleano (sólo dos valores: Verdadero / Falso).

> **MATIZ**
>
> El **dato lógico** o booleano sólo admite dos valores: **Verdadero (True)** o **Falso (False)**. Aunque en hardware se represente como 1 y 0, no es un dato numérico: no admite operaciones aritméticas, sino lógicas (AND, OR, NOT).

3. Soportes de almacenamiento

Los soportes físicos de almacenamiento se clasifican en tres familias por su tecnología: **ópticos** (lectura láser), **magnéticos** (platos giratorios) y **de estado sólido** (memoria flash).

3.1. Soportes ópticos: CD, DVD y Blu-Ray

El almacenamiento óptico graba y lee pistas de datos mediante un **láser**. Dentro de cada familia hay subtipos según la capacidad de escritura:

Soporte	Subtipos	Capacidad
CD *(Compact Disc)*	**CD-ROM** (solo lectura) · **CD-R** (grabable una sola vez) · **CD-RW** (regrabable)	≈ 700 MB. Prácticamente en desuso.
DVD *(Digital Versatile Disc)*	DVD-ROM, DVD-R, DVD-RW, DVD+R, DVD+RW	**4,7 GB** (simple capa) · **8,5 GB** (doble capa).
Blu-Ray *(BD)*	**BD-R** (grabable una vez) · **BD-RE** (regrabable) · **BDXL** (alta capacidad)	**BD-25**: 25 GB · **BD-50**: 50 GB (doble capa) · **BDXL**: 100 GB (triple capa) / 128 GB (cuádruple capa). Usa láser azul de **405 nm**.

RECUERDA

Progresión de capacidad óptica: **CD (≈ 700 MB) → DVD (4,7–8,5 GB) → Blu-Ray (25–128 GB)**. La clave técnica del Blu-Ray es la **longitud de onda más corta** del láser azul (405 nm) frente al rojo del DVD (650 nm): la onda más corta enfoca en pits más pequeños y, por tanto, permite mayor densidad de datos en la misma superficie. Subtipos genéricos: **ROM** (solo lectura), **R** (grabable una sola vez), **RW/RE** (regrabable).

3.2. Soportes magnéticos y de estado sólido

Dispositivo	Tecnología	Características
Disco duro (HDD) *(Hard Disk Drive)*	Magnética: varios platos giratorios con cabezas lectoras/escritoras móviles.	Alta capacidad (más de 14 TB en formato 3,5"). Económico por GB. **Sensible a golpes** por sus partes mecánicas móviles. Velocidad limitada por la rotación del eje (7.200 / 10.000 / 15.000 rpm).
Unidad de estado sólido (SSD) *(Solid State Drive)*	**Flash NAND**: chips de memoria sin partes móviles, con un con-	Mucho más **rápido**, **silencioso** y **resistente** que el HDD. Más caro por GB. Vida útil acotada en

	trolador que gestiona la lectura y escritura.	número de ciclos de escritura (el controlador la gestiona con técnicas de *wear leveling*).
Pen drive / memoria USB	Flash.	Dispositivo externo portátil con conector USB integrado. Capacidades comerciales actuales desde varios GB hasta 1-2 TB.
Tarjeta SD *(Secure Digital)*	Flash.	Formato compacto para cámaras, móviles, drones y dispositivos integrados. Misma tecnología base que el pen drive. Variantes por capacidad: SD (≤ 2 GB), SDHC (≤ 32 GB), SDXC (≤ 2 TB), SDUC (≤ 128 TB).

FIGURA

Diagrama comparativo SSD vs HDD. SSD: placa con chips NAND flash y controlador etiquetados, sin elementos móviles. HDD: vista lateral con platos apilados en un eje central y brazos de las cabezas lectoras. Pie: «mecánico vs electrónico».

MATIZ

HDD = tecnología **magnética**, partes mecánicas móviles, más barato por GB, mayor capacidad disponible y sensibilidad a golpes. **SSD** = tecnología **flash NAND**, sin partes móviles, más rápido, más resistente y más caro por GB. La pareja **HDD = magnético / SSD = flash** y la relación inversa precio-rendimiento son los datos consolidados.

NVMe: el protocolo de los SSD modernos

Los SSD pueden conectarse al equipo por dos vías. La tradicional usa la interfaz **SATA** (la misma de los HDD), heredada del mundo mecánico y limitada a unos 600 MB/s. La moderna emplea **NVMe** *(Non-Volatile Memory Express)*, protocolo diseñado desde cero para memoria no volátil que viaja directamente por el bus **PCI Express**. La especificación NVMe 1.0 se publicó en 2011 y aprovecha el ancho de banda completo del PCIe (varios GB/

s), reduce la latencia y soporta miles de colas paralelas, lo que multiplica el rendimiento frente a un SSD SATA.

> **RECUERDA**
>
> Un **SSD SATA** comparte interfaz con los HDD y queda limitado por el ancho de banda SATA. Un **SSD NVMe** se conecta directamente al bus **PCIe** y multiplica varias veces el rendimiento del SATA. Cuando un examen pregunta por «SSD más rápido», la respuesta es **NVMe**.

4. Estructura interna del disco duro (HDD)

El HDD se compone de varios **platos** unidos por un eje central que gira a alta velocidad. En la superficie de cada plato se graban los datos magnéticamente mediante **cabezas lectoras/escritoras**. La superficie de cada plato se organiza jerárquicamente:

Elemento	Descripción
Pista	Anillos concéntricos en los que se divide la superficie del plato.
Sector geométrico	Porción del plato definida por dos radios (forma de «porción de tarta»).
Sector de pista	Intersección entre una pista y un sector geométrico. Es la **unidad mínima física** de lectura/escritura (clásicamente 512 bytes; en discos modernos, 4 KB – *Advanced Format*).
Clúster	Agrupación de varios sectores de pista. Es la **unidad mínima lógica** que el sistema de archivos asigna a un archivo.

FIGURA

Diagrama HDD: platos apilados en eje central con cabezas lectoras a uno y otro lado de cada plato. Detalle ampliado de la superficie del plato mostrando pistas concéntricas, sectores geométricos radiales y la intersección que define el sector de pista. Resaltar la agrupación en clúster.

La **desfragmentación** es la operación que reorganiza las porciones de archivos dispersas por el disco (fragmentadas, almacenadas en clústeres no contiguos) y las agrupa en ubicaciones contiguas. El resultado: el cabezal recorre menos distancia y el acceso al archivo es más rápido. La desfragmentación **no es necesaria ni recomendable en SSD**, porque éstos carecen de partes móviles y la lectura es uniforme en toda la memoria flash; además, las escrituras innecesarias acortan la vida útil del SSD.

MATIZ

La **desfragmentación** sólo aporta valor en HDD (con partes mecánicas móviles). En SSD es **contraproducente**: no mejora la velocidad y consume ciclos de escritura que reducen la vida útil del dispositivo. Los sistemas operativos modernos detectan automáticamente el tipo de disco y desactivan la desfragmentación en SSD.

5. Particiones, formato, RAID y almacenamiento en red

5.1. Particiones y formateo

Una **partición** es una división lógica dentro de un mismo dispositivo físico de almacenamiento. Cada partición se comporta como si fuera una unidad independiente, con su propio sistema de archivos. Un único disco puede contener varias particiones (por ejemplo, un SSD con Windows en una partición y Linux en otra, lo que se conoce como *dual boot*).

Formatear una unidad realiza dos acciones simultáneas: elimina todos los datos que contiene y le asigna un **sistema de archivos** (FAT32, exFAT, NTFS, ext4, APFS, HFS+…). Tras el formateo, la unidad queda lista para ser usada por un sistema operativo.

5.2. RAID: varios discos actuando como uno

RAID *(Redundant Array of Independent Disks, matriz redundante de discos independientes)* es una tecnología que combina varios discos físicos para que el sistema los reconozca como una única unidad lógica. Los niveles RAID persiguen tres objetivos en distinta proporción: **rendimiento**, **redundancia** y **capacidad utilizable**.

Nivel RAID	Mínimo discos	Objetivo principal	Tolerancia a fallos
RAID 0 *(Striping)*	2	**Rendimiento máximo**: los datos se distribuyen entre todos los discos en bloques alternados.	**Ninguna**: si falla un disco, se pierden todos los datos del conjunto.
RAID 1 *(Mirroring)*	2 (puede ser más)	**Seguridad máxima**: los datos se copian de forma idéntica en dos o más discos espejo.	Tolera la pérdida de hasta n−1 discos en un conjunto de n.
RAID 5	3	**Equilibrio** entre rendimiento y redundancia mediante paridad distribuida.	Tolera la pérdida de **un** disco; los datos se reconstruyen a partir de la paridad.

MATIZ

RAID 0 no aporta redundancia pese a contener la «R» de *Redundant*: distribuye los datos para acelerar la lectura/escritura, pero si falla un solo disco se pierde la información de todos. La asociación memorable es **0 = velocidad sin red de seguridad / 1 = espejo / 5 = paridad con mínimo 3 discos**.

5.3. Almacenamiento en red: NAS y SAN

Sistema	Descripción	Caso de uso típico
NAS *(Network Attached Storage)*	**Dispositivo único** de almacenamiento conectado a la red local. Tiene su propio sistema opera-	Pymes, usuarios domésticos avanzados, entornos corporativos medianos.

	tivo embebido, funciona 24/7 y los clientes acceden a sus carpetas a través de protocolos de red (SMB, NFS).	
SAN *(Storage Area Network)*	**Red dedicada** exclusivamente al almacenamiento, formada por múltiples dispositivos a los que acceden varios servidores con tecnologías de alta velocidad (Fibre Channel, iSCSI).	Grandes empresas, centros de datos, entornos que requieren rendimiento y escalabilidad máximos.

MATIZ

NAS es **un dispositivo** conectado a la red local —el «servidor de archivos» doméstico o de pyme—. **SAN** es **una red completa** de dispositivos de almacenamiento de alta velocidad, propia de centros de datos. La diferencia esencial: NAS = dispositivo único accesible por la LAN existente; SAN = infraestructura de red dedicada al almacenamiento.

6. La nube: almacenamiento y computación como servicio

La **nube** *(cloud)* es un modelo de almacenamiento y computación basado en servidores gestionados por terceros, accesibles a través de Internet. Más allá del almacenamiento puro, la nube ofrece distintos niveles de servicio según qué parte de la pila gestiona el proveedor y qué parte gestiona el cliente.

El **NIST** (en su Special Publication 800-145, referencia consolidada en la materia) define **tres modelos canónicos** de servicio: IaaS, PaaS y SaaS. La práctica comercial añade un cuarto, **CaaS**, como categoría intermedia entre IaaS y PaaS.

Modelo	Nombre completo	Gestiona el proveedor	Gestiona el cliente
IaaS	Infraestructura como Servicio	Hardware, red, virtualización.	Sistema operativo, *middleware*, aplicaciones y datos.
CaaS	Contenedores como Servicio	Hardware, red y entorno de contenedo-	Código de aplicación y datos.

		res (Docker, Kubernetes).	
PaaS	Plataforma como Servicio	Hardware, sistema operativo, *middleware* y entorno de desarrollo.	Código de aplicación y datos.
SaaS	Software como Servicio	Todo: infraestructura + plataforma + aplicación.	Sólo el uso de la aplicación, normalmente vía navegador.

RECUERDA

Mnemónico «**I-C-P-S**»: IaaS → CaaS → PaaS → SaaS. Cuanto más a la derecha del eje, **más** gestiona el proveedor y **menos** gestiona el cliente. **SaaS** es el servicio más completo para el usuario final: sólo necesita un navegador (Gmail, Microsoft 365, Salesforce). **IaaS** es el más flexible: el cliente gestiona desde el sistema operativo hacia arriba (AWS EC2, Azure VM).

MATIZ

El **NIST SP 800-145** reconoce **únicamente** IaaS, PaaS y SaaS como modelos canónicos. **CaaS** no es un modelo NIST: surgió como categoría comercial intermedia entre IaaS y PaaS al popularizarse Docker y Kubernetes. Identificar el modelo correcto por la descripción del reparto de responsabilidades: «sólo navegador» → SaaS · «código sin gestionar infraestructura» → PaaS · «contenedores gestionados por el proveedor» → CaaS · «SO y apps sobre infraestructura del proveedor» → IaaS.

7. Conceptos complementarios de almacenamiento y archivos

- **Extensión de archivo**: sufijo de tres o cuatro caracteres situado al final del nombre del archivo, separado por un punto (`.docx`, `.jpg`, `.pdf`, `.exe`, `.iso`). Identifica el tipo de archivo y permite al sistema operativo abrirlo con la aplicación adecuada.

- **Compresión**: reducción del tamaño de uno o varios archivos para ahorrar espacio o facilitar su transmisión. Los formatos más extendidos son **ZIP** (formato abierto, manejado por programas como WinZip, 7-Zip o el compresor integrado del sistema operativo) y **RAR** (formato propietario, asociado al programa WinRAR). Un archivo comprimido puede agrupar varios ficheros en uno solo, manteniendo la estructura de carpetas original.
- **Archivo autoextraíble**: archivo comprimido que contiene en su interior los archivos originales **y** el programa descompresor necesario para liberarlos. Se ejecuta como si fuera un programa (extensión `.exe` en Windows) y libera su contenido sin requerir software adicional instalado en el equipo.
- **Disco de arranque** (*boot disk*): unidad de almacenamiento que contiene los archivos necesarios para iniciar el sistema operativo. Normalmente es el disco interno principal del equipo, aunque también puede ser una unidad externa (USB, DVD) usada como medio de instalación o de recuperación cuando el SO interno falla.
- **ISO** *(International Organization for Standardization)*: organización internacional cuyo objetivo es desarrollar normas y estándares técnicos para asegurar calidad, seguridad e interoperabilidad de productos, servicios y tecnologías a escala mundial. El término **ISO** tiene un segundo uso técnico: una **imagen ISO** (extensión `.iso`) es un archivo único que contiene la copia exacta de un sistema de archivos completo, típicamente el contenido de un CD/DVD. Las distribuciones de sistemas operativos se descargan habitualmente como imagen ISO.
- **DirectX**: conjunto de interfaces de programación de aplicaciones (API) desarrollado por Microsoft para mejorar el rendimiento multimedia en equipos Windows: gráficos 2D y 3D, sonido, vídeo y videojuegos. La versión vigente es **DirectX 12 Ultimate** (2020), requerida por las tarjetas gráficas modernas y por las consolas Xbox Series X|S.
- **Copia de seguridad** (*backup*): copia de los datos de un sistema realizada para prevenir pérdidas de información ante fallos de hardware, errores de software, ataques de seguridad o errores humanos. La operación complementaria, **restauración** (*restore*), recupera los datos desde el *backup* cuando el original se ha perdido o corrompido.

TEMA 1

Epígrafe 3 — Sistemas operativos

1. El sistema operativo: capa intermedia entre hardware y aplicaciones

Un **sistema operativo (SO)** es un programa —o, más exactamente, un conjunto coordinado de programas— que gestiona todos los recursos de un sistema informático y actúa como **capa intermedia** entre el hardware y los programas de aplicación. Sin sistema operativo, el usuario no podría interactuar con la máquina: las aplicaciones se comunican con el hardware **a través del SO**, no directamente.

Un sistema operativo cumple dos objetivos esenciales:

- **Facilitar el uso del equipo al usuario**, ocultando la complejidad del hardware tras una interfaz coherente y abstrayendo las diferencias entre dispositivos (procesador, memoria, almacenamiento, periféricos).
- **Gestionar los recursos de forma eficiente** para maximizar el rendimiento del sistema: reparto del tiempo de CPU, asignación de memoria, planificación de las operaciones de entrada/salida.

2. Anatomía del sistema operativo: kernel, shell y sistema de archivos

Todo sistema operativo se descompone en tres partes diferenciadas, cada una con una función específica:

Componente	Función clave
Kernel *(núcleo)*	Gestión básica del hardware: memoria, procesos, operaciones de entrada/salida. Contacto **directo** con el hardware. Opera en el nivel más bajo del sistema y es **invisible para el usuario**.
Shell *(intérprete de comandos)*	Capa de interacción con el usuario, que puede ser **CLI** *(Command-Line Interface,* línea de

	comandos: terminal, *bash*, PowerShell) o **GUI** *(Graphical User Interface,* interfaz gráfica: escritorio, ventanas, menús). Independiza al usuario del hardware.
Sistema de archivos	Organiza y gestiona el almacenamiento de datos en el disco: nombres de archivos, ubicaciones, atributos, permisos y acceso a los datos. Determina la estructura interna del soporte cuando se formatea.

MATIZ

El **kernel** opera en el nivel más bajo y es **invisible para el usuario**: gestiona memoria, procesos y E/S sin interfaz directa. La **shell** es la cara visible del SO, ya sea como línea de comandos (CLI) o como escritorio gráfico (GUI). Confundir las funciones de cada parte es uno de los errores más frecuentes.

3. Las seis funciones del sistema operativo

El sistema operativo ejecuta seis funciones de gestión nucleares:

Función	Qué gestiona
Administrar el procesador	Distribuye el tiempo de CPU entre los programas en ejecución mediante algoritmos de planificación *(scheduling)*.
Gestionar la memoria	Asigna y libera RAM entre los procesos. Cuando la RAM física es insuficiente, gestiona la **memoria virtual** apoyándose en el disco *(swap, paging)*.
Gestionar la entrada/salida	Controla el acceso a los dispositivos hardware mediante **controladores (*drivers*)** específicos para cada periférico.
Gestionar la ejecución de aplicaciones	Asigna recursos a cada aplicación en marcha, evita la saturación del sistema y permite la **multitarea**.
Administrar autorizaciones	Controla qué usuarios y qué programas pueden acceder a qué recursos (memoria, ficheros, dispositivos).

Gestionar archivos	Lee, escribe y elimina archivos; asigna permisos de acceso por usuario y por grupo.

RECUERDA

Son **seis** funciones del SO. Mnemónico «**Pro-Me-EE-Eje-Au-Ar**»: **Pro**cesador · **Me**moria · **E/S** (drivers) · **Eje**cución de aplicaciones · **Au**torizaciones · **Ar**chivos.

4. Clasificación de los sistemas operativos

Los sistemas operativos se clasifican según dos criterios fundamentales:

Criterio	Tipo	Ejemplo
Por número de usuarios simultáneos	**Monousuario**	MS-DOS, Windows 3.1 (en desuso).
	Multiusuario	UNIX, Linux, Windows Server.
Por número de procesos simultáneos	**Monotarea**	MS-DOS en modo básico (en desuso).
	Multitarea	Todos los sistemas operativos modernos: Windows, macOS, Linux, Android, iOS.

MATIZ

Multitarea no equivale a multinúcleo. La multitarea **no exige** varios procesadores: un único núcleo puede gestionar varios programas intercalando su ejecución a tal velocidad que el usuario percibe simultaneidad (multitarea por reparto de tiempo). El **paralelismo real** —ejecución física simultánea de varias instrucciones— sí requiere múltiples núcleos.

MATIZ

macOS Server fue discontinuado por Apple el 21 de abril de 2022. Si en una tabla o pregunta aparece como ejemplo «vivo» de sistema multiusuario, está desfasado: en la actualidad los ejemplos vigentes son **UNIX**, **Linux** y **Windows Server**.

5. Los grandes sistemas operativos del mercado

SO	Fabricante	Tipo de dispositivo	Versión vigente (mayo 2026)	Dato clave
Windows	Microsoft	PC, portátil, servidor	**Windows 11** es la versión vigente; Windows 10 conserva soporte solo mediante **ESU** (*Extended Security Updates*, de pago) hasta el **13/10/2026**.	El SO de escritorio más extendido. Sistema de archivos: **NTFS**.
UNIX	Múltiples (base abierta)	Servidor, estaciones de trabajo	Múltiples variantes (AIX, Solaris, HP-UX, BSD)	Base histórica del mundo Unix-like. Referencia de estabilidad para entornos críticos.
Linux	Comunidad (software libre)	PC, servidor, embebido, supercomputación	Distribuciones: Ubuntu, Debian, Fedora, Mint, Red Hat…	**Unix-like** (compatible con POSIX, no derivado directo del código UNIX original). Código abierto. Sistema de archivos: **ext4** (por defecto).
macOS	Apple	Mac (sobremesa y portátil)	**macOS 26 Tahoe** (15/09/2025)	Deriva de **Darwin** (núcleo Unix-like de Apple); macOS obtuvo certificación UNIX 03

				a partir de OS X 10.5 Leopard. Exclusivo de hardware Apple. Sistema de archivos: **APFS**.
Android	Google	Móvil, tableta, *wearable*	**Android 16** (10/06/2025)	Basado en el **kernel Linux**. Distribución abierta sobre la que los fabricantes superponen sus propias capas.
iOS	Apple	iPhone	**iOS 26** (15/09/2025)	Cerrado. Comparte base **Darwin** con macOS pero es un sistema distinto. Exclusivo del iPhone.
iPadOS	Apple	iPad	**iPadOS 26** (15/09/2025)	Variante de iOS desde su separación formal en **2019 (iOS 13 / iPadOS 13)** con funciones específicas de tableta (multitarea con ventanas, *Apple Pencil*, *Stage Manager*).

MATIZ

iOS no es macOS. Aunque ambos son de Apple y comparten la base **Darwin**, son sistemas distintos: **macOS** gobierna los Mac (sobremesa y portátil); **iOS** es exclusivo del iPhone; **iPadOS** es la variante de iOS para iPad desde 2019. La pregunta «¿Qué SO usa el iPhone?» se responde **iOS**, nunca macOS.

RECUERDA

Desde 2025 Apple **renumeró todos sus sistemas operativos** al año del modelo siguiente: macOS pasó de 15 Sequoia a **macOS 26 Tahoe** iOS de 18 a **iOS 26** iPadOS, watchOS, tvOS y visionOS siguen el mismo esquema. No existió macOS 16, 17… ni iOS 19, 20… — Apple saltó directamente al «26» (correspondiente al año modelo 2026).

5.1. Capas de personalización de Android

Sobre el Android base de Google (AOSP, *Android Open Source Project*) los fabricantes superponen su propia capa de personalización. Las capas vigentes a mayo 2026:

Fabricante	Capa actual	Predecesor histórico
Samsung	**One UI**	TouchWiz (hasta 2017)
OPPO	**ColorOS**	–
Huawei	**HarmonyOS**	EMUI (sustituido a partir de 2021; HarmonyOS 5 «NEXT» eliminó el código Android en oct. 2024)
Xiaomi	**HyperOS**	MIUI (sustituido a partir del 17/10/2023)
Motorola	**My UX**	–
Sony	**Xperia UI**	–
Google Pixel	**Pixel Launcher** *(Android puro, sin capa adicional)*	–
Realme	**Realme UI**	–

RECUERDA

Asociaciones fabricante → capa actual: **Samsung = One UI · OPPO = ColorOS · Huawei = HarmonyOS · Xiaomi = HyperOS**. Las denominaciones históricas EMUI (Huawei) y MIUI (Xiaomi) siguen apareciendo en manuales antiguos pero han sido formalmente reemplazadas por sus sucesores; HarmonyOS 5 ha eliminado además todo código Android, lo que lo convierte de hecho en un SO distinto en los dispositivos Huawei más recientes.

6. El sistema de archivos: cómo el SO ordena los datos

Cada sistema operativo gestiona los archivos en el disco mediante su propio **sistema de archivos** *(file system)*: el esquema que define cómo se nombran, organizan y acceden los datos. El sistema de archivos determina la estructura interna del soporte de almacenamiento cuando éste se formatea.

Plataforma	Sistema de archivos
Windows antiguo (hasta XP)	**FAT** / **FAT32**
Windows moderno (Vista, 7, 8, 10, 11)	**NTFS** *(New Technology File System)*
Linux	**ext2** / **ext3** / **ext4** (por defecto en la mayoría de distribuciones)
macOS antiguo (hasta Sierra)	**HFS** / **HFS+**
macOS moderno (desde High Sierra, 2017)	**APFS** *(Apple File System)*
Dispositivos extraíbles (USB, SD)	**FAT32** / **exFAT** (compatibilidad multiplataforma)

MATIZ

Caracterización de los tres sistemas de archivos más preguntados:

- **FAT32**: Windows antiguo y unidades extraíbles. **Límite de 4 GB por archivo**. Sin permisos ni cifrado. Máxima compatibilidad con otros SO.
- **NTFS**: Windows moderno (desde NT/Vista). Sin límite práctico de tamaño de archivo. Soporta **permisos por usuario**, **cifrado** (EFS) y ***journaling*** (registro de transacciones para recuperación tras fallo).
- **exFAT**: diseñado para unidades extraíbles. **Compatibilidad universal** entre Windows, macOS y Linux. Sin el límite de 4 GB del FAT32.

7. Virtualización

La **virtualización** es la tecnología que permite instalar y ejecutar **varios sistemas operativos de forma simultánea** sobre un único hardware físico. Cada sistema operativo virtualizado funciona como si residiera en una máquina propia, con sus recursos asignados (CPU, memoria, almacenamiento, red), sin interferir con los demás sistemas que se ejecutan en paralelo.

La virtualización se implementa mediante un software especializado denominado **hipervisor** *(hypervisor)* o **virtualizador**, encargado de asignar, distribuir y gestionar los recursos de la máquina física entre los distintos sistemas operativos virtuales. Los hipervisores se clasifican en dos tipos:

- **Hipervisor tipo 1** ***(bare-metal)***: se ejecuta directamente sobre el hardware, sin sistema operativo anfitrión. Ejemplos: VMware ESXi, Microsoft Hyper-V Server, Xen. Habitual en centros de datos.
- **Hipervisor tipo 2** ***(hosted)***: se ejecuta como una aplicación sobre un sistema operativo anfitrión. Ejemplos: VMware Workstation, Oracle VirtualBox, Parallels Desktop. Habitual en equipos de escritorio para uso individual.

Los usos más habituales de la virtualización son tres:

- **Ejecutar aplicaciones compatibles sólo con otro sistema operativo** (por ejemplo, ejecutar Windows dentro de un Mac).

- **Crear entornos de prueba aislados** (*sandbox*) sin riesgo para el sistema anfitrión.
- **Optimizar el aprovechamiento del hardware** en centros de datos consolidando varios servidores virtuales en una sola máquina física.

RECUERDA

El **hipervisor** o virtualizador es el software que reparte los recursos de la máquina física entre los sistemas operativos virtualizados. Tipo 1 = *bare-metal*, directamente sobre el hardware (entornos profesionales); tipo 2 = sobre un SO anfitrión (uso personal).

TEMA 1

Epígrafe 4 — Nociones básicas de seguridad informática

1. La información como activo: confidencialidad y normativa de protección de datos

En cualquier organización, la información es un **activo crítico**. Su tratamiento indebido puede causar daños graves —patrimoniales y reputacionales— y acarrear responsabilidades legales. Por eso la seguridad informática no es solo una cuestión técnica: empieza por las **personas** y por la cultura de responsabilidad que la organización exige a sus empleados.

La **confidencialidad** es uno de los tres pilares clásicos de la seguridad (junto con la **integridad** y la **disponibilidad**, la tríada CIA). Su objetivo es que los datos solo sean conocidos por el emisor y por el receptor al que se dirigen. La medida técnica más extendida para garantizarla es el **cifrado** (o **encriptado**): aunque la información se intercepte durante la comunicación, su contenido queda ilegible sin la clave de descifrado correspondiente.

En España, la protección de los datos personales se rige por dos normas que operan en cascada:

- **Reglamento (UE) 2016/679, de 27 de abril, General de Protección de Datos** *(RGPD)*: norma europea de aplicación directa desde el 25/05/2018.
- **Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales** *(LOPDGDD)*: ley española que adapta el RGPD al ordenamiento interno y añade el catálogo de derechos digitales del Título X.

RECUERDA

La tríada clásica de la seguridad informática es **CIA**: **C**onfidencialidad (solo accede quien debe), **I**ntegridad (los datos no se alteran sin autorización), **D**isponibilidad (los recursos están operativos cuando se necesitan). El marco normativo de protección de datos es el binomio **RGPD (UE) 2016/679 + LOPDGDD (LO 3/2018)**.

2. Gestión de usuarios: los cinco pasos

Para garantizar que los datos son tratados exclusivamente por las personas autorizadas, toda organización necesita un sistema de **gestión de usuarios**. El administrador del sistema sigue una secuencia ordenada de cinco pasos:

Paso	Acción
1.º	**Evaluar necesidades**: identificar quién necesita acceso y a qué recursos.
2.º	**Crear usuarios**: dar de alta a cada persona en el sistema.
3.º	**Crear permisos**: definir los niveles de acceso disponibles.
4.º	**Asignar permisos a usuarios**: vincular cada usuario con su nivel correspondiente.
5.º	**Asignar códigos de acceso**: entregar credenciales únicas (usuario + contraseña, certificado, token…) a cada persona.

MATIZ

Son **cinco pasos**, no cuatro. La secuencia es lógica e inalterable: no se pueden **asignar** permisos (paso 4.º) antes de **crearlos** (paso 3.º); y no se pueden **crear usuarios** (paso 2.º) sin haber **evaluado necesidades** previas (paso 1.º).

El **administrador del sistema** es la figura técnica responsable de la operación segura de la red y de los sistemas de información del organismo. Sus tareas habituales incluyen: realizar **copias de seguridad** *(backups)* periódicas, velar por el flujo correcto de información y, ante un incidente, solventarlo y elevarlo al responsable del tratamiento o al órgano competente conforme al protocolo interno y al **Esquema Nacional de Seguridad** (Real Decreto 311/2022). La responsabilidad jurídica formal sobre el tratamiento de datos personales recae sobre el **responsable del tratamiento** —no sobre el administrador técnico— de acuerdo con el RGPD y la LOPDGDD.

3. Amenazas y vulnerabilidades

Concepto	Definición	Clave
Amenaza	Acción o suceso con potencial de comprometer el sistema.	Puede ser deliberada (ataque) o accidental (fallo, error humano). Las amenazas **aprovechan** vulnerabilidades.
Vulnerabilidad	Debilidad o brecha que expone el sistema a una amenaza.	Sin vulnerabilidad, la amenaza no puede materializarse en daño real.

3.1. Tipos de vulnerabilidad

Tipo	Origen
De diseño	Malas políticas de seguridad o **puertas traseras** *(backdoors)* introducidas en la arquitectura del sistema.
De implementación	Errores de programación en el código fuente *(bugs)* que un atacante puede explotar.
De usuario	Actuaciones incorrectas: contraseñas débiles, reutilización de credenciales, descarga de archivos sospechosos, clic en enlaces de phishing.

4. Tipos de malware

El **malware** *(malicious software,* software malicioso) engloba todos los programas diseñados para dañar un sistema o extraer información sin autorización. Las categorías principales:

Malware	Característica diferenciadora
Virus	Necesita un archivo **huésped** para propagarse. Al ejecutarse el archivo huésped, el virus ejecuta instrucciones no autorizadas.
Gusano *(worm)*	Se replica **por sí solo**, sin necesidad de un archivo huésped. Viaja por la red consumiendo recursos hasta saturar o colapsar el sistema.
Troyano *(trojan)*	Se disfraza de software legítimo. **No se replica**: su función es abrir una **puerta trasera** *(backdoor)* que permite al atacante el control remoto del equipo.
Bomba lógica	Programa que permanece inactivo hasta que se cumple una condición específica (fecha, acción del usuario, evento del sistema) y entonces ejecuta su carga maliciosa.
Zombie	Equipo controlado remotamente por un atacante. Se usa como trampolín en ataques coordinados a gran escala (**botnets**, redes de zombies).
Spyware	Espía la actividad del usuario y envía información a terceros sin permiso (hábitos de navegación, credenciales, datos personales).
Ransomware	**Cifra los archivos del sistema** y exige un **rescate económico** –típicamente en criptomonedas– a cambio de la clave de descifrado.
Phishing	Suplantación de webs o identidades para que el usuario revele credenciales o datos confidenciales. Es **ingeniería social**, no software malicioso instalado en el equipo.

MATIZ

Tres distinciones nucleares que se confunden con frecuencia:

- **Virus ≠ Gusano**: el virus **necesita** un archivo huésped; el gusano **viaja solo** por la red.
- **Troyano ≠ Virus**: el troyano **no se replica** su función es abrir acceso remoto encubierto.
- **Phishing ≠ Malware**: el phishing es **ingeniería social** (engaño al usuario), no un programa instalado en el equipo. El ataque ocurre fuera del sistema, en la mente del usuario.

5. Medidas de protección

Herramienta	Qué hace	Tipo
Firewall *(cortafuegos)*	Filtra el tráfico de red entrante y saliente; impide accesos no autorizados según reglas configuradas.	Hardware o software
Antivirus	Detecta y elimina malware mediante bases de firmas y análisis de comportamiento. Debe permanecer **siempre activo y actualizado**.	Software
Cifrado *(encriptado)*	Vuelve ilegible la información sin la clave correcta. Aplicable a datos en reposo (disco cifrado) y datos en tránsito (HTTPS, VPN).	Técnica criptográfica
Gestión de usuarios y permisos	Restringe el acceso a recursos según el rol de cada usuario *(principio de mínimo privilegio)*.	Organizativa + técnica
Copias de seguridad *(backups)*	Permiten restaurar los datos tras una pérdida o un ataque (especialmente útil frente a ransomware).	Organizativa

MATIZ

El **firewall** puede ser **hardware** (dispositivo físico instalado en la red, típicamente entre el router y la LAN) o **software** (aplicación instalada en el equipo, como el Firewall de Windows Defender). Ambas formas son igualmente válidas: cuando una pregunta defina el firewall solo como hardware o solo como software, ambas respuestas son técnicamente correctas.

6. Identificación y firma en el procedimiento administrativo

La regulación de la identidad y la firma electrónicas en las relaciones del ciudadano con las Administraciones Públicas combina el plano jurídico —**Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas** (en adelante, **LPACAP**)— y el plano técnico —**Reglamento (UE) 910/2014 (eIDAS)**, actualizado por el Reglamento (UE) 2024/1183 (eIDAS 2.0)—.

6.1. La distinción nuclear: identificación vs firma

Concepto	Para qué	Cuándo se exige
Identificación	Acreditar **quién** es el interesado.	Con carácter **general**, para cualquier actuación en el procedimiento.
Firma electrónica	Acreditar la **voluntad y consentimiento** del interesado.	Solo en los **cinco supuestos tasados** del art. 11.2 LPACAP.

MATIZ

Para realizar **cualquier actuación** en el procedimiento administrativo basta con **identificarse**. La **firma** solo se exige en cinco supuestos concretos del art. 11.2 LPACAP. Confundir ambos conceptos y exigir firma generalizada es uno de los errores más extendidos.

6.2. Artículo 9 LPACAP · Sistemas de identificación de los interesados en el procedimiento

1. Las Administraciones Públicas están obligadas a verificar la identidad de los interesados en el procedimiento administrativo, mediante la comprobación de su nombre y apellidos o denominación o razón social, según corresponda, que consten en el Documento Nacional de Identidad o documento identificativo equivalente.
2. Los interesados podrán identificarse electrónicamente ante las Administraciones Públicas a través de los sistemas siguientes:

a) Sistemas basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la «Lista de confianza de prestadores de servicios de certificación».

b) Sistemas basados en certificados electrónicos cualificados de sello electrónico expedidos por prestadores incluidos en la «Lista de confianza de prestadores de servicios de certificación».

c) Cualquier otro sistema que las Administraciones públicas consideren válido en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad y previa comunicación a la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital. Esta comunicación vendrá acompañada de una declaración responsable de que se cumple con todos los requisitos establecidos en la normativa vigente. De forma previa a la eficacia jurídica del sistema, habrán de transcurrir dos meses desde dicha comunicación, durante los cuales el órgano estatal competente por motivos de seguridad pública podrá acudir a la vía jurisdiccional, previo informe vinculante de la Secretaría de Estado de Seguridad, que deberá emitir en el plazo de diez días desde su solicitud.

> Las Administraciones Públicas deberán garantizar que la utilización de uno de los sistemas previstos en las letras a) y b) sea posible para todo procedimiento, aun cuando se admita para ese mismo procedimiento alguno de los previstos en la letra c).
>
> 3. En relación con los sistemas de identificación previstos en la letra c) del apartado anterior, se establece la obligatoriedad de que los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de dichos sistemas se encuentren situados en territorio de la Unión Europea, y en caso de tratarse de categorías especiales de datos a los que se refiere el artículo 9 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en territorio español. En cualquier caso, los datos se encontrarán disponibles para su acceso por parte de las autoridades judiciales y administrativas competentes.
>
> Los datos a que se refiere el párrafo anterior no podrán ser objeto de transferencia a un tercer país u organización internacional, con excepción de los que hayan sido objeto de una decisión de adecuación de la Comisión Europea o cuando así lo exija el cumplimiento de las obligaciones internacionales asumidas por el Reino de España.
>
> 4. En todo caso, la aceptación de alguno de estos sistemas por la Administración General del Estado servirá para acreditar frente a todas las Administraciones Públicas, salvo prueba en contrario, la identificación electrónica de los interesados en el procedimiento administrativo.

El art. 9 LPACAP fija **tres** sistemas de identificación electrónica: **a) certificado cualificado de firma**, **b) certificado cualificado de sello** y **c) otros sistemas** que la Administración considere válidos. Los sistemas a) y b) deben **garantizarse siempre** para todo procedimiento (aun cuando para ese mismo procedimiento se admita también un sistema de la

letra c). El sistema c) es **opcional** y se sujeta a un régimen reforzado tras la reforma operada por la **Ley 11/2022, de 28 de junio** (vigente desde 30/06/2022): exige **comunicación previa** a la Secretaría General de Administración Digital, acompañada de **declaración responsable** sobre el cumplimiento de la normativa. Antes de su eficacia jurídica deben transcurrir **dos meses** desde la comunicación; en ese plazo, el órgano estatal competente por motivos de seguridad pública puede **acudir a la vía jurisdiccional**, previo informe vinculante de la Secretaría de Estado de Seguridad (a emitir en **diez días**).

MATIZ

Tras la reforma de la **Ley 11/2022** ya **no se exige autorización previa** de la Secretaría General de Administración Digital para los sistemas de la letra c): basta con **comunicación previa + declaración responsable**. El plazo de espera antes de la eficacia jurídica es de **dos meses** (no tres), y el control no se articula mediante silencio positivo, sino dejando abierta la **vía jurisdiccional** al órgano estatal competente por seguridad pública. Los sistemas a) y b) **siempre** deben estar disponibles para todo procedimiento; el c) es **adicional y opcional**. Confundir comunicación con autorización, dos meses con tres, o aplicar silencio positivo, son errores frecuentes en preguntas sobre el art. 9 LPACAP.

6.3. Artículo 10 LPACAP · Sistemas de firma admitidos por las Administraciones Públicas

1. Los interesados podrán firmar a través de cualquier medio que permita acreditar la autenticidad de la expresión de su voluntad y consentimiento, así como la integridad e inalterabilidad del documento.
2. En el caso de que los interesados optaran por relacionarse con las Administraciones Públicas a través de medios electrónicos, se considerarán válidos a efectos de firma:

a) Sistemas de firma electrónica cualificada y avanzada basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores

incluidos en la «Lista de confianza de prestadores de servicios de certificación».

b) Sistemas de sello electrónico cualificado y de sello electrónico avanzado basados en certificados electrónicos cualificados de sello electrónico expedidos por prestador incluido en la «Lista de confianza de prestadores de servicios de certificación».

c) Cualquier otro sistema que las Administraciones públicas consideren válido en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad y previa comunicación a la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital. Esta comunicación vendrá acompañada de una declaración responsable de que se cumple con todos los requisitos establecidos en la normativa vigente. De forma previa a la eficacia jurídica del sistema, habrán de transcurrir dos meses desde dicha comunicación, durante los cuales el órgano estatal competente por motivos de seguridad pública podrá acudir a la vía jurisdiccional, previo informe vinculante de la Secretaría de Estado de Seguridad, que deberá emitir en el plazo de diez días desde su solicitud.

Las Administraciones Públicas deberán garantizar que la utilización de uno de los sistemas previstos en las letras a) y b) sea posible para todos los procedimientos en todos sus trámites, aun cuando adicionalmente se permita alguno de los previstos al amparo de lo dispuesto en la letra c).

3. En relación con los sistemas de firma previstos en la letra c) del apartado anterior, se establece la obligatoriedad de que los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de dichos sistemas se encuentren situados en territorio de la Unión Europea, y en caso de tratarse de categorías especiales de datos a los que se refiere

> el artículo 9 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en territorio español. En cualquier caso, los datos se encontrarán disponibles para su acceso por parte de las autoridades judiciales y administrativas competentes.
>
> Los datos a que se refiere el párrafo anterior no podrán ser objeto de transferencia a un tercer país u organización internacional, con excepción de los que hayan sido objeto de una decisión de adecuación de la Comisión Europea o cuando así lo exija el cumplimiento de las obligaciones internacionales asumidas por el Reino de España.
>
> 4. Cuando así lo disponga expresamente la normativa reguladora aplicable, las Administraciones Públicas podrán admitir los sistemas de identificación contemplados en esta Ley como sistema de firma cuando permitan acreditar la autenticidad de la expresión de la voluntad y consentimiento de los interesados.
> 5. Cuando los interesados utilicen un sistema de firma de los previstos en este artículo, su identidad se entenderá ya acreditada mediante el propio acto de la firma.

El art. 10 LPACAP replica el esquema tripartito a) / b) / c) del art. 9, pero referido ahora a la **firma** —no a la identificación— y con dos matices importantes. Primero, la **garantía** del párrafo final del apartado 2 es más exigente que en el art. 9: los sistemas a) y b) deben estar disponibles **«para todos los procedimientos en todos sus trámites»** (no solo «para todo procedimiento»). Segundo, el régimen de la letra c) es **idéntico** al del art. 9 tras la reforma de la **Ley 11/2022**: comunicación previa, declaración responsable, dos meses antes de la eficacia jurídica y posible vía jurisdiccional. Dos reglas complementarias cierran el artículo: el **apartado 4** permite admitir como firma los sistemas de identificación cuando acrediten voluntad y consentimiento; el **apartado 5** declara que **el acto de firma ya implica acreditación de la identidad**.

6.4. Artículo 11 LPACAP · Uso de medios de identificación y firma en el procedimiento administrativo

1. Con carácter general, para realizar cualquier actuación prevista en el procedimiento administrativo, será suficiente con que los interesados acrediten previamente su identidad a través de cualquiera de los medios de identificación previstos en esta Ley.
2. Las Administraciones Públicas sólo requerirán a los interesados el uso obligatorio de firma para:

a) Formular solicitudes.

b) Presentar declaraciones responsables o comunicaciones.

c) Interponer recursos.

d) Desistir de acciones.

e) Renunciar a derechos.

El art. 11 LPACAP es la pieza nuclear de toda la regulación: la **regla general** del 11.1 (identificación suficiente para cualquier actuación) y la **lista cerrada** del 11.2 con los **cinco** supuestos en que la firma es obligatoria.

RECUERDA

Cinco supuestos del art. 11.2 LPACAP que exigen firma electrónica obligatoria: a) **S**olicitudes · b) **D**eclaraciones responsables o comunicaciones · c) **R**ecursos · d) **D**esistir de acciones · e) **R**enunciar a derechos. Mnemónico «**SDRDR**» o, más memorable: **el ciudadano firma cuando pide, declara, recurre, desiste o renuncia**.

7. Firma electrónica y certificado digital

7.1. Marco normativo

El marco legal de la firma electrónica se asienta en dos normas europeas y una española:

- **Reglamento (UE) 910/2014, de 23 de julio, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior** *(eIDAS)*: en vigor desde el **17/09/2014**, aplicación efectiva desde el **01/07/2016**. Deroga la Directiva 1999/93/CE.
- **Reglamento (UE) 2024/1183, de 11 de abril de 2024 (eIDAS 2.0)**: modifica el 910/2014 e introduce la **Cartera Europea de Identidad Digital** *(European Digital Identity Wallet, EUDI Wallet)*. **Cada Estado miembro está obligado a proporcionar** al menos una cartera europea de identidad digital en el plazo previsto en el Reglamento; el **uso por los ciudadanos es voluntario**.
- **Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza**: norma española que adapta el ordenamiento interno al eIDAS y deroga la Ley 59/2003 de firma electrónica.

7.2. Niveles de firma electrónica

El eIDAS distingue tres niveles de firma electrónica con efectos jurídicos crecientes:

Nivel	Clave diferenciadora	Efectos legales
Firma electrónica simple	Datos en forma electrónica asociados al firmante. Identificación básica.	Tiene valor probatorio; **no equivale** a la firma manuscrita.
Firma electrónica avanzada	Identifica al firmante de forma única + permite **detectar cambios** posteriores en el documento + está bajo control exclusivo del firmante.	Valor probatorio reforzado; **no equivale** a la firma manuscrita por sí sola.
Firma electrónica cualificada *(o reconocida)*	Firma avanzada 1. **certificado cualificado + dispositivo cualificado de creación de firma** .	**Equivale legalmente a la firma manuscrita** en toda la UE (art. 25.2 eIDAS).

MATIZ

Solo la **firma electrónica cualificada** (también llamada «reconocida» en la doctrina española) tiene el **mismo valor jurídico que la firma manuscrita**. La firma simple y la firma avanzada tienen valor probatorio pero **no alcanzan** esa equivalencia plena. La asociación memorable es: **cualificada = manuscrita**.

7.3. Requisitos técnicos de la firma electrónica

Para que una firma electrónica cumpla su función jurídica debe satisfacer **tres requisitos técnicos**:

- **Identificación**: garantiza la identidad del firmante de forma única.
- **Integridad**: garantiza que el contenido del documento no ha sido alterado desde su firma.
- **No repudio**: garantiza que el firmante no puede negar haber firmado el documento.

RECUERDA

Los tres requisitos técnicos de la firma electrónica son **identificación**, **integridad** y **no repudio**. Mnemónico **«I-I-NR»**: el firmante es quien dice ser, el documento es el que se firmó y nadie puede luego negar la firma.

7.4. Certificado digital y DNI electrónico

	Certificado digital (FNMT)	DNI electrónico (DNIe)
¿Qué es?	Fichero informático criptográfico.	Documento físico oficial con chip integrado.
Emitido por	FNMT-RCM y otras entidades autorizadas incluidas en la Lista de confianza.	Dirección General de la Policía.
Cómo se usa	Instalado en el navegador o en un almacén de certificados del sistema operativo.	Mediante lector de tarjetas físico (DNIe 2.0) o vía **NFC** con un teléfono móvil compatible (a partir de DNI 3.0, 2015; consolidado en DNI 4.0, 2021).

Función	Identificación y firma electrónica ante las AAPP y otras entidades.	Identificación física **y** electrónica + firma electrónica.

MATIZ

El **DNIe** ya **no exige obligatoriamente lector de tarjetas físico**. Desde el **DNI 3.0 (2015)** incorpora **NFC** (*Near Field Communication*) y puede usarse con un teléfono móvil compatible para identificación y firma electrónicas. La versión vigente es el **DNI 4.0 (2021)**, con todas las capacidades NFC consolidadas.

RECUERDA

Marco normativo de la firma e identidad electrónicas: **Reglamento (UE) 910/2014 (eIDAS) + Reglamento (UE) 2024/1183 (eIDAS 2.0, EUDI Wallet) + Ley 39/2015 LPACAP arts. 9, 10 y 11 + Ley 6/2020 (adaptación española)**. El DNIe acredita identidad física **y** electrónica y constituye el documento oficial de identificación de las personas físicas españolas a todos los efectos previstos en la normativa que lo regula (LO 4/2015 y normativa de desarrollo).

8. Conceptos complementarios de ciberseguridad

- **Huella digital** (o **huella electrónica**): rastro de datos que un usuario deja al navegar e interactuar en Internet (sitios visitados, búsquedas, correos enviados, publicaciones en redes sociales, geolocalización). Se clasifica en **huella activa** (información que el usuario comparte deliberadamente, p. ej. una publicación) y **huella pasiva** (datos recopilados sin que el usuario sea consciente, p. ej. cookies y *fingerprints* de navegador).
- **Segmentación de red** *(network segmentation)*: técnica de seguridad que divide una red en **subredes** más pequeñas e independientes (mediante VLAN, *subnetting*, firewalls internos). Cada subred tiene sus propios controles de acceso, de modo que un incidente en una subred **no se propaga automáticamente** al resto de la red.

- **Ingeniería inversa** *(reverse engineering)*: proceso de análisis de un producto o programa para obtener información sobre su diseño, funcionamiento o código fuente sin disponer de la documentación original. En ciberseguridad se emplea principalmente para **analizar malware** y entender su comportamiento. También se usa para auditar la seguridad del software propio.
- **Bot**: programa que realiza funciones de forma automatizada, sin intervención humana, imitando el comportamiento de un usuario. En ciberseguridad, los **bots maliciosos** pueden formar **botnets** —redes de equipos *zombie* coordinados por un atacante— para lanzar ataques distribuidos de denegación de servicio (**DDoS**), enviar spam masivo o realizar fraude publicitario a gran escala.

TRES FORMAS DE EMPEZAR

La app Persevera complementa este temario con las herramientas para estudiarlo:

tests · flashcards con repaso espaciado · supuestos

simulacros · mindmaps · tutor IA · planificador

Suscripción mensual sin permanencia. Cancelas cuando quieras desde la app.

WEB

perseveraoposiciones.com

IOS

iPhone / iPad

ANDROID

Google Play