TEMA 1: INFORMÁTICA BÁSICA: CONCEPTOS FUNDAMENTALES SOBRE EL HARDWARE Y EL SOFTWARE. SISTEMAS DE ALMACENAMIENTO DE DATOS. SISTEMAS OPERATIVOS. NOCIONES BÁSICAS DE SEGURIDAD INFORMÁTICA.

Cuerpo General Auxiliar de la Administración del Estado · Programa

1. Marco Normativo e Introducción

El uso de las tecnologías de la información en la Administración General del Estado se fundamenta en los principios de eficacia, celeridad y funcionamiento electrónico regulados en el artículo 103 de la Constitución Española, desarrollados orgánicamente por la Ley 39/2015 del Procedimiento Administrativo Común de las Administraciones Públicas, la Ley 40/2015 de Régimen Jurídico del Sector Público y el Real Decreto 203/2021 por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

2. Informática básica: conceptos fundamentales sobre el hardware y el software

Concepto de informática y arquitectura de ordenadores

La informática es el tratamiento automático y racional de la información mediante sistemas computarizados.

La arquitectura tradicional de Von Neumann define el esquema básico de funcionamiento de los ordenadores actuales mediante bloques funcionales interconectados.

- Unidad Central de Proceso (CPU): procesa las instrucciones y coordina los demás elementos.
- Memoria principal: almacena temporalmente los programas en ejecución y los datos a procesar.
- Buses de comunicación: líneas físicas que transmiten datos, direcciones y señales de control entre componentes.
- Unidad de Entrada y Salida (E/S): gestiona el intercambio de información con dispositivos periféricos.
- Ciclo de instrucción básico: búsqueda (fetch), descodificación (decode) y ejecución (execute).

> **Atención Opositor:** *Pregunta recurrente de examen C2: La arquitectura Von Neumann se caracteriza por almacenar conjuntamente en la misma memoria física tanto los datos como las instrucciones del programa.*

Componentes del Hardware: CPU, memorias y periféricos

El hardware constituye el soporte físico tangible del sistema informático.

Se estructura en torno al procesador, la placa base, las memorias internas y los periféricos de interconexión.

- Unidad de Control (UC): interpreta instrucciones, genera señales de sincronización y dirige el tráfico de datos.
- Unidad Aritmético-Lógica (ALU): realiza operaciones matemáticas (suma, resta) y lógicas (comparaciones booleanas AND, OR, NOT).
- Registros internos: memorias ultrarrápidas de capacidad mínima integradas en el procesador.
- Memoria RAM (Random Access Memory): volátil, de acceso aleatorio, lectura y escritura rápida.
- Memoria ROM (Read Only Memory): no volátil, contiene el firmware o BIOS/UEFI de arranque del equipo.
- Memoria Caché: niveles L1, L2 y L3, actúa como puente de alta velocidad entre la RAM y la CPU.
- Buses del sistema: Bus de Datos (bidireccional), Bus de Direcciones (unidireccional desde CPU) y Bus de Control (señales de estado).
- Periféricos de entrada: teclado, ratón, escáner, lector de código de barras.
- Periféricos de salida: monitor, impresora, altavoces.
- Periféricos mixtos (E/S): pantallas táctiles, discos duros externos, tarjetas de red, impresoras multifunción.

Tipo de Memoria	Volatilidad	Operación	Función Principal
RAM	Volátil (pierde datos sin corriente)	Lectura y Escritura	Ejecución de programas activos y datos en curso
ROM / UEFI	No volátil (permanente)	Solo Lectura (generalmente)	Arranque básico del sistema (POST) y carga del SO
Caché (L1/L2/L3)	Volátil (alta velocidad)	Lectura y Escritura	Reducir tiempos de espera entre CPU y RAM

> **Atención Opositor:** *Atención al bus de direcciones: es estrictamente unidireccional; la CPU indica la posición de memoria requerida y no recibe datos por esa vía.*

El Software: concepto, tipología y modelos de licencia

El software es el soporte lógico e intangible constituido por los programas, rutinas y datos que hacen operativo al hardware.

Se clasifica según su finalidad operativa y su régimen de distribución y propiedad jurídica.

- Software de sistema: programas que administran directamente los recursos físicos (sistemas operativos, controladores de dispositivos, utilidades de diagnóstico).

- Software de programación: entornos de desarrollo, compiladores, intérpretes y depuradores empleados para crear nuevos programas.
- Software de aplicación: programas orientados a tareas específicas del usuario final (ofimática, gestores de bases de datos, navegadores web).
- Software propietario o privativo: código fuente cerrado, distribución de licencias de uso restrictivas comerciales.
- Software libre (Free Software): respeta las cuatro libertades (usar, estudiar, distribuir y mejorar el código fuente).
- Código abierto (Open Source): foco práctico en la disponibilidad del código y desarrollo colaborativo.
- Freeware vs. Shareware: freeware es gratuito sin límite de tiempo (pero no siempre modificable); shareware es versión de evaluación con límite temporal o de funciones.

Categoría de Software	Disponibilidad Código Fuente	Coste de Adquisición	Ejemplos Relevantes
Propietario / Comercial	Cerrado	Pago por licencia (habitual)	Microsoft Windows, Adobe Photoshop
Software Libre / Open Source	Abierto y accesible	Habitualmente gratuito	GNU/Linux, LibreOffice, Apache
Shareware	Cerrado	Gratis temporalmente	Versiones demo de utilidades comerciales

> **Atención Opositor:** *En la Administración Pública rige el principio de neutralidad tecnológica (art. 156 Ley 40/2015), fomentando la reutilización de código mediante repositorios como el Centro de Transferencia de Tecnología (CTT).*

3. Sistemas de almacenamiento de datos

Unidades de medida de la información

La unidad mínima elemental de información en un sistema digital binario es el bit (0 o 1).

La agrupación estándar de 8 bits forma un Byte u octeto, base sobre la cual se calculan los múltiplos decimales y binarios.

- Bit (b): unidad mínima lógica binaria (dígito 0 o 1).
- Byte (B): octeto compuesto por 8 bits continuos.
- Kilobyte (KB): 1.024 Bytes (en base binaria 2^10) o 1.000 Bytes (base decimal).
- Megabyte (MB): 1.024 KB (2^20 Bytes).
- Gigabyte (GB): 1.024 MB (2^30 Bytes).
- Terabyte (TB): 1.024 GB (2^40 Bytes).
- Petabyte (PB): 1.024 TB (2^50 Bytes).
- Exabyte (EB), Zettabyte (ZB) y Yottabyte (YB): escalas superiores de procesamiento masivo (Big Data).

> **Atención Opositor:** *Cuidado en los enunciados tipo test: 'b' minúscula designa 'bit' (usado comúnmente en velocidades de red: Mbps), mientras que 'B' mayúscula representa 'Byte' (usado en capacidad de almacenamiento: MB).*

Tecnologías y soportes de almacenamiento físico y lógico

Las tecnologías de almacenamiento secundario conservan la información de manera permanente sin requerir suministro eléctrico constante.

Han evolucionado desde sistemas mecánicos magnéticos hacia memorias semiconductoras de estado sólido y almacenamiento virtualizado en red.

- Almacenamiento Magnético: HDD (Hard Disk Drive), platos giratorios con cabezales mecánicos de lectura/escritura; menor coste por GB, mayor fragilidad.
- Almacenamiento Óptico: lectura y escritura por haz láser (CD: ~700 MB; DVD: 4,7 GB en simple capa; Blu-ray: 25 GB en simple capa).
- Almacenamiento en Estado Sólido (SSD): memorias flash NAND, sin piezas móviles mecánicas, alta velocidad (SATA III, NVMe por interfaz PCIe).
- Dispositivos Flash extraíbles: memorias USB (pendrives) y tarjetas de memoria (SD, MicroSD) de interfaz serie de alta velocidad.
- Almacenamiento Conectado en Red (NAS): dispositivo de almacenamiento dedicado conectado directamente a una red local TCP/IP.
- Redes de Área de Almacenamiento (SAN): red de alta velocidad independiente concebida para conectar servidores con matrices de discos compartidos.
- Almacenamiento en la Nube (Cloud Storage): servicios virtuales (IaaS) escalables accesibles por Internet con copias geolocalizadas.

Parámetro	Disco Duro Mecánico (HDD)	Unidad de Estado Sólido (SSD)
Mecanismo interno	Platos magnéticos y cabezal mecánico	Circuitos integrados y memoria Flash NAND
Velocidad de transferencia	Moderada (100 - 200 MB/s aprox.)	Muy alta (500 MB/s SATA a más de 7.000 MB/s NVMe)
Resistencia a impactos	Baja (sensible a golpes y caídas)	Alta (carece de piezas mecánicas en movimiento)
Consumo y ruido	Mayor consumo eléctrico y emite ruido	Bajo consumo y completamente silencioso

> **Atención Opositor:** *El Real Decreto 311/2022 (Esquema Nacional de Seguridad) impone requisitos estrictos sobre copias de seguridad de los soportes de almacenamiento, distinguiendo medidas según la calificación de la información (Básica, Media o Alta).*

4. Sistemas operativos

Concepto, funciones y componentes

El sistema operativo es el software de base esencial que gestiona los recursos de hardware y proporciona servicios comunes a las aplicaciones de usuario.

Actúa como interfaz intermedia entre el usuario, las aplicaciones de software y el hardware físico del ordenador.

- Gestión del procesador: administración del tiempo de CPU mediante algoritmos de planificación.
- Gestión de la memoria principal (RAM): asignación, protección y liberación de espacio para procesos.
- Gestión de entrada/salida: control de periféricos mediante controladores específicos (drivers).
- Gestión del sistema de archivos: organización de directorios, permisos de acceso y almacenamiento secundario.
- Núcleo o Kernel: parte fundamental del SO que se carga al inicio y opera en modo privilegiado.
- Shell o interfaz: entorno de interacción con el usuario, ya sea gráfica (GUI) o de línea de comandos (CLI).

Criterio de clasificación	Tipo de Sistema Operativo	Características representativas
Por número de usuarios	Monousuario / Multiusuario	Monousuario gestiona una sesión única; Multiusuario administra múltiples perfiles simultáneos con aislamiento.
Por número de tareas	Monotarea / Multitarea	Monotarea ejecuta un único proceso a la vez; Multitarea alterna rápidamente entre varios procesos (tiempo compartido).
Por número de procesadores	Monoproceso / Multiproceso	Monoproceso opera con una sola CPU; Multiproceso distribuye cargas simétricas (SMP) o asimétricas entre varios núcleos.

> **Atención Opositor:** *En los exámenes de AGE suelen preguntar la diferencia entre multitarea apropiativa (el SO arrebata la CPU) y no apropiativa o cooperativa (el proceso cede voluntariamente la CPU).*

Sistemas de archivos y principales familias de sistemas operativos

El sistema de archivos estructura y nombra los datos almacenados en los soportes físicos de memoria secundaria.

Las familias predominantes en puestos de trabajo de la Administración son Microsoft Windows y distribuciones GNU/Linux.

- FAT32: compatibilidad universal, pero limita el tamaño máximo de archivo a 4 GB.

- NTFS: sistema nativo de Windows con permisos ACL, compresión nativa, cifrado EFS y registro de transacciones (journaling).
- ext4: estándar en distribuciones GNU/Linux con alta tolerancia a fallos y journaling eficiente.
- Windows 10/11: entornos propietarios dominantes en el puesto administrativo tipo de la AGE.
- GNU/Linux: software libre/código abierto con kernel modular, ampliamente usado en servidores estatales y puestos específicos.

5. Nociones básicas de seguridad informática

Dimensiones de la seguridad de la información

La seguridad de la información busca salvaguardar los activos digitales frente a incidentes fortuitos o ataques deliberados.

El marco de referencia en la Administración General del Estado viene fijado por el Esquema Nacional de Seguridad (ENS).

- Confidencialidad: acceso a la información restringido exclusivamente a personas o procesos autorizados.
- Integridad: garantía de exactitud y completitud de los datos, evitando modificaciones no autorizadas.
- Disponibilidad: acceso garantizado a los recursos y datos cuando los usuarios legitimados lo requieran.
- Autenticidad: constatación fehaciente de la identidad del emisor o del origen del dato.
- Trazabilidad: capacidad de rastrear e imputar cada acción en el sistema a un sujeto o proceso concreto.

> **Atención Opositor:** *El acrónimo mnemotécnico CIDAT (Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad) recoge las 5 dimensiones oficiales del artículo 5 del Real Decreto 311/2022 (ENS).*

Amenazas, malware y mecanismos de protección

El software malicioso (malware) representa el principal vector de vulneración de los sistemas informáticos.

La protección requiere una estrategia defensiva en profundidad que combine controles físicos, lógicos y organizativos.

- Virus: requiere un archivo anfitrión para propagarse e infectar el sistema.
- Gusano: se propaga de forma autónoma por la red sin necesitar modificar archivos anfitriones.
- Troyano: se camufla como software legítimo para abrir puertas traseras (backdoors) sin replicarse.
- Ransomware: secuestra y cifra los archivos del equipo exigiendo un rescate económico para su recuperación.

- Phishing: técnica de ingeniería social mediante correos o enlaces falsos para suplantar identidades y capturar credenciales.
- Cortafuegos (Firewall): barrera que filtra el tráfico entrante y saliente según reglas predefinidas.
- Copias de seguridad (Regla 3-2-1): tres copias de los datos, en dos soportes distintos, con al menos una fuera del recinto.

Tipo de Malware	Mecanismo de Propagación	Objetivo Principal / Daño Típico
Virus	Infección de ejecutables o ficheros anfitriones	Corrupción de datos, alteración del sistema o consumo de recursos.
Gusano (Worm)	Autorreplicación directa por redes de comunicaciones	Colapso de ancho de banda y sobrecarga de memoria de servidores.
Ransomware	Descarga de adjuntos, exploits o enlaces maliciosos	Cifrado de ficheros y extorsión económica mediante rescate.
Spyware	Instalación encubierta asociada a otros programas	Recopilación ilegítima de hábitos, pulsaciones de teclado y datos personales.

> **Atención Opositor:** *Diferencie siempre malware de ingeniería social: el ransomware o spyware son software, mientras que el phishing o el vishing son técnicas de manipulación humana.*

6. Claves para el Examen

Análisis sistemático de trampas semánticas, plazos críticos y distinciones determinantes para las pruebas de selección:

Trampas habituales de los tribunales

- Confundir 'Gusano' con 'Virus': el virus exige ejecutar un programa anfitrión infectado; el gusano se propaga por la red de forma autónoma sin dicho archivo portador.
- Intercambiar 'Confidencialidad' e 'Integridad': confidencialidad evita accesos no autorizados; integridad evita modificaciones o borrados indebidos.
- Asumir que el cortafuegos sustituye al antivirus: el cortafuegos bloquea puertos y tráfico de red no autorizado, pero no analiza virus en el interior de ficheros admitidos.
- Confundir software libre con software gratuito (freeware): el software libre confiere cuatro libertades de uso, estudio, modificación y distribución, pudiendo ser de pago comercial.

Plazos críticos de obligada memorización

- 72 horas: plazo máximo para notificar a la Agencia Española de Protección de Datos (AEPD) una brecha de seguridad que afecte a datos personales (Art. 33 RGPD).

- Inmediato / urgente: comunicación de incidentes de seguridad de impacto muy alto o alto al CCN-CERT conforme a la Guía CCN-STIC del ENS.
- 4 Gigabytes: límite de tamaño máximo para un archivo individual gestionado bajo sistema de ficheros FAT32.

Artículos clave y preguntas frecuentes

- Real Decreto 311/2022 (ENS), Art. 5: dimensiones de la seguridad (disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad).
- Real Decreto 311/2022 (ENS), Art. 13: principio de defensa en profundidad y líneas de defensa sucesivas.
- Reglamento (UE) 2016/679 (RGPD), Art. 32: medidas de seguridad técnicas y organizativas para garantizar la resiliencia y confidencialidad.
- Ley 40/2015, Art. 156: Esquema Nacional de Seguridad como base de la confianza digital en las Administraciones Públicas.

Distinciones conceptuales finas

- Cifrado simétrico vs Cifrado asimétrico: el simétrico utiliza una única clave compartida (rápido para grandes volúmenes); el asimétrico emplea un par público/privado (más seguro para autenticación y firma digital).
- Multitarea apropiativa vs cooperativa: en la apropiativa el SO gestiona las interrupciones y retira el control a los procesos; en la cooperativa los programas deciden cuándo ceder la CPU.
- Copia de seguridad incremental vs diferencial: la incremental guarda los cambios desde la última copia de cualquier tipo; la diferencial acumula todos los cambios desde la última copia completa.

7. Cuadro Resumen Esquemático

Concepto / Epígrafe	Fundamento Legal (Art. y Ley)	Elementos Clave / Plazos / Mayorías	Clave para Examen
Hardware y Procesador (CPU)	Concepto técnico fundamental	Unidad de Control (UC), Unidad Aritmético-Lógica (ALU) y Registros. Frecuencia en GHz.	La memoria caché (L1, L2, L3) es la más rápida pero volátil; los registros están integrados dentro de la CPU.
Sistemas de Almacenamiento	Concepto técnico fundamental	Primario (RAM, ROM) y Secundario (HDD, SSD, Ópticos). Límite FAT32 en 4 GB; NTFS con journaling y ACL.	La RAM es de lectura/escritura volátil; la ROM almacena firmware de arranque inalterable (BIOS/UEFI).
Sistemas Operativos	Concepto técnico fundamental	Kernel, gestión de procesos, memoria, E/S y ficheros. Multitarea,	El SO coordina el hardware y aísla las aplicaciones del usuario

		multiusuario, multiproceso.	del acceso directo y caótico a memoria.
Dimensiones de Seguridad	Art. 5 RD 311/2022 (ENS)	Cinco pilares: Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad (CIDAT).	Pregunta clásica de test: suelen omitir trazabilidad o sustituir autenticidad por anonimato para inducir a error.
Notificación de Brechas de Seguridad	Art. 33 Reglamento (UE) 2016/679	Plazo de 72 horas ante la AEPD desde que el responsable tenga constancia de la brecha con riesgo para derechos.	Cifra estrella de examen en la AGE: 72 horas para la AEPD (sin dilación indebida).