Hardware y software de base en sistemas digitales aplicados al entorno productivo

https://cienciamorada.es

Sumario

Dispositivos digitales. Clasificaciones: Sobremesa, servidor, tableta, 'smartphone', 'smartwatch', 'smart tv' u otros.

Ordenador de sobremesa

Un **ordenador de sobremesa** es un ordenador diseñado y construido para ser utilizado en una oficina o similar, sin que esté previsto que se mueva habitualmente. Su forma más habitual es la de una "torre" conectada a una serie de periféricos (monitor, teclado, impresora, escáner, etc), pero puede tener distintos tamaños e incluso estár integrado en un monitor, por ejemplo.

Portátil

Un **portátil** es un ordenador diseñado para ser fácilmente transportado de un lugar a otro y ser utilizado en cualquier lugar. Lo habitual es que incluya, en un mismo dispositivo, pantalla, teclado, unidad central de proceso y todo lo necesario para conectarse a otros dispositivos.

Tablet

Una **tableta o tablet** es un dispositivo táctil aún más ligero que un portátil. No suele tener teclado integrado, aunque algunos modelos se venden con un teclado que puede separarse y la mayoría admiten conexiones a un teclado por Bluetooth o USB.

Smartphone

Un **smartphone** es un dispositivo de tamaño de bolsillo, con una tecnología similar a la de una tablet, que permite ser utilizado como teléfono.

Smartwatch

Un **smartwatch** es un dispositivo de pulsera con conectividad a las redes (habitualmente a través de una conexión a un smartphone). Además de los usos tradicionales de un reloj puede conectarse a redes sociales, responder a llamadas telefónicas, monitorizar la actividad física de su usuario, etc.

Smart TV

Una **smart TV** es una televisión diseñada para conectarse a Internet. Suele utilizarse para conectarse a servicios de streaming, pero también pueden utilizarse para navegar por la WWW. Un televisor convencional puede utilizarse como una Smart TV conectándolo, a través de un puerto HDMI, a un dispositivo externo.

Servidor

Un **servidor** es un ordenador que es utilizado como emisor de información dentro de una red.

Esquema funcional de un dispositivo. Unidad central de proceso, memoria interna y externa, tipos y características.

Un ordenador ha sido diseñado y construido con el fin de recibir, almacenar, procesar y emitir información. Cada uno de sus componentes ha sido diseñado y construido para realizar alguna de esas funciones:

- **Entrada y salida de información:** se realiza a través de puertos de distinto tipo (USB, HDMI, VGA, etc).
- **Procesamiento:** se realiza en la CPU (Unidad Central de Procesamiento), construida con uno o varios microprocesadores.
- **Almacenamiento:** tradicionalmente se han venido utilizando discos duros, pero actualmente se utiliza todo tipo de dispositivos de almacenamiento, incluyendo pendrives USB, tarjetas de memoria o, incluso, almacenamiento en nube[1]. Es importante saber que hay varias formas de almacenamiento de la información en función de su temporalidad:
  - **La memoria RAM (Random Access Memory, o Memoria de Acceso Aleatorio)** es la que se utiliza durante el proceso de datos. Se está reescribiendo constantemente y puede

1 Es decir, en un dispositivo externo que puede ser incluso otro ordenador situado a kilómetros del usuario.

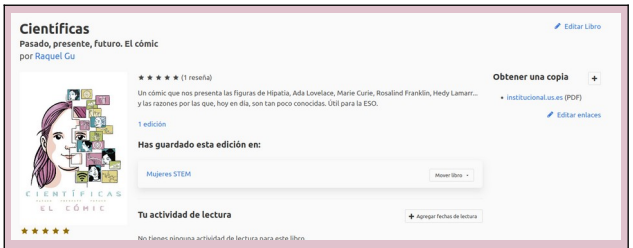
considerarse borrada cuando el dispositivo se apaga. La capacidad de procesamiento de un ordenadora puede aumentarse añadiendo módulos de memoria RAM al dispositivo. Algunos sistemas permiten, además, reforzar la capacidad de procesamiento mediante el uso de una partición del disco duro (**memoria SWAP o memoria de intercambio**) para esas funciones (aunque la velocidad de lectura y escritura en la memoria SWAP es mucho más baja que en la memoria RAM, por lo que la contribución a la velocidad de procesamiento es menor).

- **Dispositivos de almacenamiento regrabables:** discos duros, pendrives, tarjetas de memoria, almacenamiento en nube, etc.
- **Dispositivos no regrabables:** CD, DVD, BluRay.

Ada Lovelace (Imagen: Dominio público CC0 10 Universal)

Ada Lovelace pensó que era posible dar una serie de instrucciones a la máquina de calcular de Babbage (una calculadora mecánica que nunca llegó a construirse) para que funcionase de forma automática. Sería un ordenador con una unidad central de procesamiento totalmente mecánica y un sistema de almacenamiento basado en papel perforado.

En 1843 Ada publicó lo que se considera el primer programa informático de la historia. Pero enseguida se hizo pública su condición femenina y, en consecuencia, su idea fue olvidada.



Sobre Ada Lovelace y otras científicas e ingenieras podéis encontrar información en el cómic Científicas, de Raquel Gu.

Tipos de periféricos, dispositivos conectables y complementos. Teclados, ratones, pantallas, pantallas táctiles, impresoras. Procedimientos de configuración y conexión. Tipos de cable y conexión inalámbrica.

Un complemento necesario de cualquier ordenador son los periféricos, generalmente diseñados de forma que se permita el intercambio de información entre humanos y máquinas: teclados, ratones, monitores, cámaras, etc. Las conexiones entre la CPU y los periféricos pueden realizarse a través de cables o de forma inalámbrica:

- **Conexiones por cable:**
  - **USB**: para la mayor parte de los periféricos, tales como teclados, ratones, cámaras, smartphones, auriculares, etc.
  - **HDMI**: para conexiones multimedia (audio y vídeo) que requieran una alta calidad.
  - **Cable RJ45 (Ethernet)**: los cables RJ45 o Ethernet se utilizan para conectarse a Internet o a una Intranet (una red local) a la que pueden conectarse periféricos como, por ejemplo, las impresoras de un centro de trabajo. Esto facilita que cualquier ordenador conectado a dicha red tenga acceso a la impresora incluso aunque esté en otro lugar.
- **Conexiones inalámbricas:**
  - **Bluetooth**: suele utilizarse para conexiones a corta distancia, y directamente entre dos dispositivos sin necesidad de que las comunicaciones se transmitan a través de una red.
  - **WiFi**: la conexión de un ordenador a una red puede realizarse, además de mediante un cable RJ45, a tavés de WiFi, accediendo así a periféricos conectados a la misma red.

Finalmente debe tenerse en cuenta que todos estos dispositivos necesitan algún sistema de alimentación de energía. Algunos se alimentan directamente de la red eléctrica, mientras otros se alimentan del propio ordenador a través de alguno de sus puertos (un puerto USB proporciona alimentación eléctrica que, para algunos dispositivos de bajo consumo, puede ser suficiente).

Hedy Lamarr, estrella de Hollywood e inventora de un sistema utilizado actualmente en comunicaciones inalámbricas como Wifi y otras (Imagen: dominio público).

Hedy Lamarr y el compositor George Antheil patentaron un sistema de comunicaciones por radio en el que emisor y receptor iban cambiando de frecuencias constantemente pero de forma sincronizada, haciendo imposible la intercepción de comunicaciones.
El objetivo era equipar a los torpedos con un sistema de guía que no pudiese ser inutilizado por las fuerzas alemanas. El invento fue rechazado por la marina y olvidado en el fondo de un cajón durante años.
Actualmente la idea de Hedy Lamarr es la base de desarrollos tecnológicos como el Bluetooth o el WiFi.

La vida de Hedy Lamarr estuvo marcada por su pasión por la ciencia y la ingeniería, por su huída del régimen nazi y por su trabajo como actriz de Hollywood. El cómic Objetivo Hedy Lamarr es una ficción con algunas partes de realidad, pero sí os interesa otro cómic más fiel a la historia real podéis buscar en Científicas.

Actualización de sistemas operativos y software. Software privativo y software libre.

Tipos de software

Software[2] propietario

Software propietario es aquel cuyos derechos de copia, modificación y difusión están restringidos por derechos de propiedad intelectual. A veces está permitida su libre descarga y utilización, en cuyo caso estaremos hablando de **shareware**.

Software de código abierto (Open source software)

El software de código abierto es aquel del que se ha publicado su código fuente[3], facilitando así la comprensión de su funcionamiento[4].

Logo de la iniciativa Open Source

Software libre (Free software)

Logo de la Free Software Foundation

Software libre es aquel que cumple las cuatro libertades siguientes:

- **Libertad 0**: la libertad de usar el programa, con cualquier propósito (uso)[5].
- **Libertad 1**: la libertad de **estudiar** cómo funciona el programa y modificarlo, adaptándolo a las propias necesidades (estudio)[6].

2 El software es el conjunto de programas informáticos de un ordenador. Los componentes físicos constituyen el hardware.

3 Instrucciones que sigue el ordenador al ejecutar el programa, escritas en un lenguaje inteligible para humanos (en el ordenador cualquier software es una sucesión ininteligible de unos y ceros, ilegible para seres humanos).

4 La mayor parte del software propietario no ha hecho público su código fuente, siendo este accesible solamente a los empleados de la empresa desarrolladora y a los de otras que trabajan bajo licencia.

5 El software propietario, salvo que sea shareware o alguna versión de prueba, no suele otorgar esta libertad si no se paga previamente.

6 Para esto es necesario que el código fuente haya sido publicado, lo que implica que el software libre debe ser de código abierto (aunque el software de código abierto podría no ser libre si no cumple alguna de las cuatro libertades).

- **Libertad 2**: la libertad de **distribuir** copias del programa, con lo cual se puede ayudar a otros usuarios (distribución)[7].
- **Libertad 3**: la libertad de **mejorar** el programa y hacer públicas esas mejoras a los demás, de modo que toda la comunidad se beneficie (mejora)[8].

Existen distintas licencias bajo las que se publica el software libre. La más extendida es la GPL (GNU Public License).

Elementos básicos del sistema operativo. Instalación y desinstalación de aplicaciones.

Todos los sistemas operativos tienen un núcleo con las instrucciones principales del sistema. Sobre este núcleo corren las aplicaciones que normalmente utilizamos.

Antiguamente era habitual la comunicación entre humanos y máquinas en modo texto, pero eso requería un proceso de aprendizaje lento y poco accesible para la mayor parte de la población.

En aquella época no se podía utilizar un ordenador si no se tenían unos conocimientos básicos de MS-DOS[9], Linux[10] o similares.

La situación cambió con la aparición de entornos gráficos como Windows[11], Gnome[12] y otros, que volvieron sencillo e intuitivo el uso de sistemas operativos. El uso del modo texto se ha quedado reducido a tareas de nivel medio o avanzado.

La instalación y desinstalación de aplicaciones también es ahora mucho más sencilla gracias a los entornos gráficos, aunque hay diferencias notables entre sistemas operativos. En Windows, por ejemplo, es habitual el uso de archivos autoejecutables que se ocupan de la instalación de aplicaciones, mientras que en GNU/Linux lo habitual es el uso de sistemas de gestión de software que acceden a repositorios *on line* e instalan los paquetes de archivos necesarios para el funcionamiento de un determinado software.

7 Es decir: que cualquiera que disponga de una copia del software lo puede distribuir libremente, cosa ilegal con la mayor parte del software propietario.

8 Es decir: no solo es posible estudiar su funcionamiento y modificarlo, sino que además es posible la difusión de la versión modificada. Todo esto sin necesidad de pedir ningún permiso, aunque cumpliendo con los requisitos de la licencia libre bajo la que el software haya sido publicado.

9 Microsoft Disk Operative System, utilizado por Microsoft antes de la existencia de Windows.

10 Aunque popularmente se llama "Linux" a todo el conjunto GNU/Linux lo cierto es que Linux es solamente el núcleo del sistema.

11 En sus primeras versiones Windows no era un sistema operativo sino un entorno gráfico que corría sobre MS-DOS.

12 Uno de los entornos gráficos más populares en sistemas GNU/Linux.

Configuración del entorno de trabajo. Administración y gestión de los sistemas de archivos. Gestión y edición de archivos.

Todos los sistemas operativos almacenan la información en forma de paquetes llamados **archivos**. Estos archivos se ordenan en conjuntos lógicos llamados **directorios o carpetas**. Una carpeta o directorio puede incluir otras subcarpetas o subdirectorios.

Todos estos archivos y carpetas o directorios se almacenan en partes de dispositivos de almacenamiento llamadas **particiones**. Un dispositivo de almacenamiento puede tener una o varias particiones.

En cada partición se gestionan los archivos y las carpetas o directorios conforme a unas normas que dependen del sistema de archivos utilizado. Es posible formatear un dispositivo de almacenamiento y cambiar su sistema de archivos[13].

¡CUIDADO! El formateo de una partición o de un dispositivo suele provocar la pérdida de la información que contiene.

A veces es posible recuperar parte de la información si se dispone de los medios y conocimientos adecuados, pero no siempre.

De hecho se recomienda el formateado de dispositivos de almacenamiento con la mejor forma de borrado de la información.

Los archivos pueden ser creados, copiados, transferidos de una carpeta o directorio a otra, modificados o borrados.

¡CUIDADO! Enviar un archivo a la papelera no es lo mismo que borrarlo. De la papelera se puede recuperar facilmente, mientras que si ha sido borrado, en teoría, no se puede recuperar.

En la práctica es posible recuperar un archivo que el usuario considera borrado. En realidad el ordenador no lo ha borrado realmente, sino que ha etiquetado la zona del dispositivo de memoria ocupada por el archivo como reescribible, pero sin que necesariamente la información haya desaparecido.

Algunos usuarios, además, desconocen la existencia de carpetas y archivos ocultos, incluyendo algunas papeleras de reciclaje.

Es por todo esto que se considera que la forma más segura de borrado es el formateo.

13 Los pendrives y tarjetas de memoria, por ejemplo, suelen venir formateados de fábrica con el sistema FAT 32, típico de antiguas versiones de Windows, pero es posible formatearlos para cambiar su sistema de archivos a EXT3, típico de sistemas GNU/Linux, por ejemplo.

Ciberseguridad del sistema: usuarios, roles, cortafuegos, antivirus.

Actualización del software[14]

Constantemente se están descubriendo vulnerabilidades tanto en los sistemas operativos[15] (GNU/Linux, Windows, MacOS, iOS, Android, etc) como en los programas que corren sobre ellos. Estas vulnerabilidades pueden ocasionar problemas que van desde la pérdida de archivos hasta el secuestro de sistemas informáticos por terceras personas, pasando por el robo de información confidencial y la suplantación de identidades.

Conscientes de estos riesgos los desarrolladores de software suelen publicar actualizaciones para evitar este tipo de problemas. Es conveniente mantener actualizado el software en la medida que sea posible.
Los sistemas operativos actuales tienen sistemas que revisan y actualizan el software, siempre y cuando las licencias estén actualizadas y el usuario dé su autorización.

Antivirus y firewalls

El término *malware* se refiere a cualquier tipo de software creado para acceder a sistemas informáticos ajenos y realizar acciones no deseadas por el usuario del sistema afectado. El *malware* puede propagarse de dos formas:

- Oculto en un archivo informático. Se instala cuando el usuario abre el archivo infectado. A este tipo de *malware* se le conoce como **virus**.
- Replicándose a sí mismo y difundiéndose a través de redes informáticas. En ocasiones pueden llegar a consumir tal ancho de banda que ralentizan el funcionamiento de las redes. A este tipo de software se le conoce como **gusano**.

Las acciones que puede realizar el malware son muy diversas. Algunas no pasan de ser una simple broma, pero otras constituyen graves delitos:

- Sustituir o modificar del navegador para introducir publicidad no deseada.
- Provocar el mal funcionamiento o el bloqueo de parte del software.
- Apertura de puertas traseras que permitan el control remoto del sistema informático por terceras personas. Al software que realiza esta acción se le conoce popularmente como **troyano**[16].
- Buscar información en el disco duro y enviarla a terceras personas.
- Secuestrar el sistema informático mediante el encriptado[17] de los discos duros.

14 Software: programas informáticos.
15 Software sobre el que funcionan las distintas aplicaciones que utilizamos en un ordenador.
16 En referencia a la leyenda del caballo de Troya, un caballo gigante de madera que los habitantes de la ciudad de Troya creyeron un regalo e introdujeron dentro de su ciudad sin saber que dentro llevaba un grupo de soldados griegos que, de noche, abrieron las puertas de la ciudad para iniciar su invasión.
17 Modificación de la información que la hace ilegible excepto para quien tiene las claves necesarias para desencriptarla. Se han dado casos de ataques en los que se encriptaba el sistema informático de la víctima y se pedía un rescate.

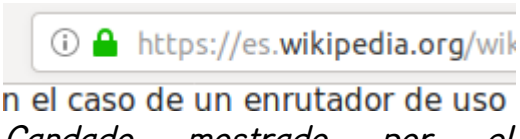
No existe sistema informático que sea totalmente inmune a este tipo de ataques, si bien algunos sistemas (por su diversidad, sistemas de permisos[18] y otros detalles) son más difíciles de atacar que otros. Se han desarrollado defensas para proteger a los sistemas informáticos:

- **Cortafuegos (firewall):** sistemas de software, hardware[19] o una combinación de ambos que filtran las comunicaciones de un sistema informático con el exterior bloqueando aquellas que no cumplan unas especificaciones de seguridad. En algunas redes se instalan varios firewalls entre distintos sectores según su uso, creando lo que se llama **zonas desmilitarizadas**, separadas por un firewall de la intranet[20] y por otro de una red externa, generalmente Internet.
- **Antivirus:** software que revisa el sistema informático buscando malware.

Hábitos de protección

Es conveniente seguir algunos hábitos de protección informática:

- Mantener actualizado el software, especialmente el antivirus.
- No abrir correos de procedencia dudosa[21], especialmente si llevan un adjunto[22].
- No rellenar formularios con nuestros datos personales en páginas web que no sean seguras. Las páginas seguras tienen una URL que comienza como **https://**, mientras que las páginas web normales comienzan por **http://** Algunos navegadores indican si la página es segura mostrando la imagen de un candado.



n el caso de un enrutador de uso

Candado mostrado por el navegador Firefox en la Wikipedia.

- Desconfíe de los correos electrónicos en los que se le envíe un enlace a un formulario donde se le pidan sus datos bancarios. Asegúrese, en todo caso, de que la página a la que se le ha dirigido es segura y que es realmente de la entidad bancaria en cuestión. En la mayoría de los casos no se trata de un mensaje de una entidad bancaria real, sino de una práctica

18 Es recomendable, en un ordenador, tener perfiles de administrador y perfiles de usuarios por separado. El perfil de administrador es el que tiene plenos poderes para la administración del sistema, mientras que los perfiles de usuarios normales solo pueden hacer uso de las herramientas que ha instalado el administrador. De esa forma es difícil que desde un perfil de usuario normal pueda afectarse a los demás perfiles de usuario y, en general, al resto del sistema informático.

19 Hardware: componentes físicos de un ordenador, tales como la unidad central del proceso, el teclado, el monitor, etc.

20 Una intranet es un grupo de ordenadores conectados entre sí, generalmente dentro de un mismo edificio o de un mismo organismo o empresa. A menudo se instalan firewalls que protegen la intranet de ataques externos.

21 Por ejemplo: un premio en un concurso en el que no hemos solicitado participar, imágenes o vídeos pornográficos, ofertas de empleo de origen desconocido, o cualquier otro contenido que pueda ser un cebo.

22 A menudo el adjunto (un archivo de texto, un vídeo, una fotografía, etc) está infectado con malware. Algunos tipos de malware tienen la capacidad de buscar los contactos de correo electrónico y enviar correos infectados a todas las direcciones que encuentre.

de búsqueda de datos personales conocida como **phishing**[23].

- Destruya la información en papel que contenga datos personales antes de tirarla a la basura. Esta información podría ser utilizada por terceras personas para introducirse en un sistema informático ajeno mediante **trashing**[24] e **ingeniería social**[25].
- No use claves fáciles de averiguar como su número de teléfono o fecha de cumpleaños. No las escriba en papel ni las comparta con otras personas.
- No se deshaga de soportes de memoria (discos duros, pendrives, etc) sin asegurarse de haberlos borrado primero, ya que podrían contener información personal. Lo más seguro es su formateo, ya que el simple borrado no elimina realmente la información, sino [26]el registro de donde se halla la información.
- Desconfíe de soportes de memoria (pendrives, CD, DVD) de procedencia desconocida. Podrían estar infectados[27].
- Guarde sus tarjetas en carteras con protección contra RFID, o estará expuesto a que le roben dinero simplemente acercando un dispositivo de lectura a su bolsillo.

Las tarjetas con tecnología RFID permiten realizar pequeños pagos simplemente con acercarlas a un lector, pero esto constituye un riesgo ya que un lector (oculto en un bolso, por ejemplo) podría realizar un cobro sin que el titular de la tarjeta fuese consciente de ello. Existen carteras que protegen a las tarjetas.

23 En inglés algo así como "ir de pesca". Los sistemas de webmail suelen incorporar filtros que desvían estos mensajes a la bandeja de spam (correo no deseado) pero no siempre funcionan: a veces permiten el paso de estos correos infectados hasta las bandejas de recepción de correos y otras envían a la bandeja de spam mensajes importantes (por eso conviene revisar la bandeja de spam de vez en cuando).

24 "Buscar en la basura": albaranes, facturas, expedientes y otros documentos aparentemente sin importancia pueden contener información personal utilizable por terceras personas.

25 A partir de unos pocos datos personales (obtenidos, por ejemplo, de documentos abandonados en la basura) es posible convencer a una persona de que está recibiendo una llamada telefónica de una empresa, institución o similar y utilizar su confianza para obtener así más información. El objetivo final suele ser el acceso remoto a un sistema informático o una suplantación de identidad.

26 Cuando "borramos" un archivo informático de un disco duro la información de dicho archivo, en realidad, no es borrada. Lo que hace el ordenador es eliminar las señales que localizan el archivo y dejar esa zona del disco duro como disponible para ser reescrita. Una búsqueda detallada de la información almacenada en el disco duro podría, en teoría, recuperar ese archivo que el sistema considera borrado. El formateo, sin embargo, elimina totalmente la información (recientemente fue objeto de juicio en los tribunales el caso de unos discos duros que fueron formateados 35 veces para eliminar la información que contenían).

27 Un viejo truco consiste en abandonar un pendrive infectado en una mesa de una cafetería frecuentada por los empleados de alguna gran empresa u organismo administrativo. Si uno de los empleados encuentrta el pendrive y, movido por la curiosidad, lo intenta abrir desde su puesto de trabajo podría dar acceso remoto a la persona que abandonó el pendrive en la cafetería.

Realización de copias de seguridad

Todos los ordenadores necesitan algún dispositivo para almacenar la información. Inicialmente se utilizaron tarjetas de papel perforadas, luego se crearon sistemas magnéticos y, finalmente, ópticos. En los últimos años se ha hecho popular el almacenamiento en la nube. Actualmente los sistemas de almacenamiento más habituales son:

- **Disco duro (HDD[28]):** basados en sistemas magnéticos, de gran capacidad pero pesados y frágiles debido a su mecanismo. Suelen ser internos, formando parte de muchos ordenadores, pero también los hay externos.
- **Unidad de estado sólido (SSD[29]):** basadas en memorias *flash*. No tienen partes móviles (lo que es una ventaja respecto a los HDD) y son muy rápidas. Sin embargo el riesgo de que dejen de funcionar inesperadamente y se pierda toda la información es mucho más alto que en los HDD.
- **Pendrives:** basados en memoria *flash*, como las SSD. Ligeros, con cierta resistencia a golpes y al polvo, baratos y sencillos de utilizar, pero con el riego de perder la información almacenada ante una variación del voltaje suministrado por un puerto USB.
- **Tarjetas de memoria:** basadas en memoria *flash*, rápidas, baratas, ligeras y de pequeño tamaño. Muy usadas en dispositivos pequeños como smartphones, tablets, cámaras digitales y ordenadores de placa única. Similares a los pendrives en cuanto a prestaciones, rapidez y fiabilidad.
- **Discos ópticos:** CD, DVD y BluRay principalmente, cada día menos utilizados. Su principal riesgo es que una rozadura los vuelva ilegibles.
- **Nube:** almacenamiento en red. Tiene la ventaja de estar accesible allí donde haya acceso a la red, sin necesidad de transportar ningún dispositivo. Esta práctica, además, permite compartir archivos de forma pública o con determinados usuarios.

Dado que no existe ningún dispositivo de almacenamiento totalmente seguro y que, además, siempre existe el riesgo de que se produzca un accidente o un robo, se recomienda almacenar los archivos importantes en distintos dispositivos o sistemas al mismo tiempo, y no guardarlos ni transportarlos físicamente en el mismo lugar.

---

28 **H**ard **D**isk **D**rive.
29 **S**olid **S**tate **D**rive.