TEMA 054: DISPOSITIVOS PERSONALES DE PC Y DISPOSITIVOS MÓVILES. LA CONECTIVIDAD DE LOS DISPOSITIVOS PERSONALES. MEDIDAS DE SEGURIDAD Y GESTIÓN PARA EQUIPOS PERSONALES Y DISPOSITIVOS MÓVILES.

Actualizado a 07/10/2020

1 DISPOSITIVOS PERSONALES: PC

Se trata de ordenadores de propósito general, orientados a su uso por usuarios finales, sin necesidad de conocimientos técnicos avanzados.

Pueden ser pc de sobremesa o portátiles. En el caso de los portátiles pueden ser de distintos tipos: tabletas, ultraligeros, workstation, etc.

1.1 COMPONENTES

1.1.1 PLACA BASE

Es una placa con circuitos impresos sobre la que se instalan el resto de componentes, sirviendo de vía de comunicación entre ellos.

Los principales elementos de la placa base son los siguientes:

- Zócalos (socket o slot) para procesador: son puertos con distintas características según el modelo de procesador.
- Zócalos (slot) para memoria: El formato más habitual es **DIMM** en equipos sobremesa y **SODIMM** en portátiles y otros equipos de reducido tamaño. Las memorias más comunes son DDR3, DDR4 y DDR5.
- El chipset son un conjunto de chips que hace de puente entre la cpu, la memoria principal y los buses del sistema. Los buses más habituales son PCI o PCI-Express.
- La **BIOS** (*Basic Input Output System*) es un chip EPROM que contiene un software mínimo, que permite el arranque del equipo y proporciona servicios básicos al sistema operativo.
- Slots de tarjetas de expansión: Constituyen el interfaz a los buses del sistema.
- Generador de señal de reloj, para sincronizar el resto de componentes. Este reloj marca la frecuencia de trabajo del **FSB** o *Front Side Bus*. Esta frecuencia será a la que funcionen todos los componentes de la placa para comunicarse. El procesador, internamente, puede funcionar a una frecuencia mayor mediante un multiplicador de esta frecuencia. Otros componentes pueden también utilizar multiplicadores y divisores para modificar su frecuencia interna de trabajo.
- Batería: Pequeña pila que mantiene la alimentación del reloj interno y de los valores de configuración utilizados por la BIOS.
- Puertos:
  - Serie (COM1, COM2): En desuso en la actualidad, Pueden ser de 9 o 25 patillas.
  - Paralelo (LPT): Habitualmente para conexión de impresoras, en desuso actualmente.
  - USB: Puertos serie de alta velocidad, según la versión del estándar. Permiten conectar múltiples tipos de dispositivo.
  - IEEE 1394 (Firewire): Se ha utilizado sobre todo para dispositivos que requierenen gran tasa de transferencia como videocámaras o discos duros. Está siendo reemplazado por USB3.
  - Audio

- Video: Puede ser VGA, HDMI, Display port o DVI
- RJ45 para conexión a red.

- Conectores internos:
  - Para discos: IDE, EIDE, SATA, SAS, NVMe
  - Alimentación de la placa

1.1.2 MICROPROCESADOR

Circuito integrado que realiza el procesamiento de datos. Sus características más importantes son su arquitectura (ej: x86, arm), proceso de fabricación y frecuencia de trabajo.

Componentes:

- **Registros**: Memoria de baja capacidad y alta velocidad integrada en el procesador.
- **Unidad Aritmético-Lógica**: ejecuta operaciones aritméticas básicas y operaciones lógicas entre valores de los registros.
- **Unidad de cálculo en coma flotante**: realiza operaciones en coma flotante (números reales extremadamente pequeños o grandes)
- **Unidad de control**: busca instrucciones en la memoria, las decodifica y las ejecuta
- **Caché**: Memoria de alta velocidad situada en el procesador, para la mejora del rendimiento mediante la lectura por predicción del código que se deberá ejecutar. Pueden existir varios niveles (generalmente 2 o 3).

Los procesadores actuales, pueden ser *multicore*, agrupando en un único chip varios cores, cada uno con gran parte de los componentes anteriores, si bien pueden compartir algunos de ellos (por ejemplo habitualmente la memoria caché).

La ejecución de las instrucciones se realiza en varias fases:

- **Prefetch**, prelectura de la instrucción desde la memoria principal.
- **Fetch**, envío de la instrucción al decodificador.
- **Decodificación** de la instrucción: determinar qué instrucción es y qué se debe hacer.
- **Lectura** de **operandos**.
- **Escritura** de los **resultados** en la memoria principal o en los registros.

De acuerdo con el juego de instrucciones que implementan los procesadores pueden ser:

- **RISC** (*Reduced Instruction Set Computer*): El procesador provee un juego de instrucciones pequeño y sencillo, de tamaño fijo y número reducido de formatos. Sólo las instrucciones de carga y almacenamiento acceden a la memoria de datos. Suelen tener un número alto de registros homogéneos de propósito general.

- **CICS** (*complex instruction set computer*): Las instrucciones del procesador pueden implicar la ejecución de varias operaciones de bajo nivel. Al contrario que RISC las instrucciones pueden tener longitud variable, y no tienen instrucciones de carga o almacenamiento diferenciadas. También en contraposición a RISC pueden tener registros específicos, con usos diferenciados.

1.1.3 Memoria RAM

Es un dispositivo de almacenamiento de acceso aleatorio basado en tecnología **MOS** (*Metal Oxyde* Semiconductor). Es volátil, requiere alimentación eléctrica para mantener la información.

Dos tipos:

- **SRAM** (RAM estática): Retiene la información mientras tenga corriente, sin necesidad de refresco. Requiere varios transistores por celda, haciendo que la densidad de memoria sea menor.
- **DRAM** (RAM dinámica): Requiere ciclos regulares de **refresco** para mantener la información. El interfaz de acceso es más complejo, pero requiere un único transistor por celda, consiguiendo mayor densidad y por tanto memorias de más capacidad. Es la utilizada habitualmente en pc.

1.1.4 Buses

Son los encargados de transferir los datos entre los componentes de un equipo. Pueden ser serie o paralelo. Algunos de los más comunes son los siguientes:

- **PCI** (*Peripheral Component Interconnect*)

  Utilizado para conectar dispositivos internos en un equipo. Es independiente del procesador, pudiendo funcionar con varias arquitecturas. Es un bus paralelo, síncrono mediante señal de reloj. Los dispositivos pueden ser chips sobre la placa base o tarjetas de expansión sobre slots PCI.

  PCI sustituyó al bus ISA, inicialmente era un bus de 32 bits a 33 MHz, pero evolucionó con estándares sucesivos a 64 bits (v 1.0). Posteriores versiones incrementaron frecuencia de trabajo. Se creó una versión específica para servidores **PCI-X** con mejores prestaciones. También se incluyó una sub-especificación para portátiles: **Mini Pci**. La especificación **AGP** es también una evolución de este bus para tarjetas gráficas.
- **PCI-e** (PCI Express)

  Se trata de un bus serie interno diseñado para reemplazar a los PCI/PCI-X/AGP anteriores. Ofrece más flexibilidad y rendimiento que los anteriores, utilizando un menor espacio. Frente al bus compartido de PCI, PCI-e establece un canal dedicado ***full duplex*** para cada dispositivo, cada uno de los cuales puede funcionar a frecuencia diferente. Permite diferentes rendimientos mediante la agrupación de líneas de comunicación (entre 1 y 32). Existe un formato "**PCI Express Mini Card**" de espacio reducido equivalente al anterior Mini PCI.
- **ExpressCard**: Interfaz para conectar periféricos a portátiles. Sustituye a **PCCard** (PCMCIA).
- Bus **USB**

  Se trata de un bus serie para la conexión de dispositivos externos, o equipos entre si. Permite la provisión de alimentación eléctrica por el mismo bus. Consigue rendimientos superiores según la versión (1.0 → 1,5 Mbits/seg, 2.0 → 480 Mbits/seg, 3.0 → 5 Gbits/seg, 4.0 → 40 Gbits/seg). La versión 4.0 es además compatible con thunderbolt 3.
- **SATA** (serial ATA): Bus serie de acceso a dispositivos internos de almacenamiento. Sustituyó a PATA (*Parallel ATA*). Permite la conexión o desconexión de dispositivos en caliente (*hot plug*). La adaptación **eSATA** permite la conexión de dispositivos externos. Versiones/rendimiento : 1.0 → 1,5 Gbits/s, 2.0 → 3 Gbits/s, 3.0 → 6 Gbits/s.

- **SAS** (*Serial Attached SCSI*): Bus serie interno para la conexión de dispositivos de almacenamiento. Sustituyó a SCSI, y utiliza el mismo conjunto de comandos. Ofrece compatibilidad con dispositivos SATA. Llega en la especificación SAS-5 a 45 Gbits/s.

1.1.5 Dispositivos de Almacenamiento

Proporcionan almacenamiento persistentes al equipo. Los más comunes son los discos duros (magnéticos o SSD), cintas, memorias flash o CD/DVD/BluRay.

- Discos duros magnéticos

  Son dispositivos que utilizan almacenamiento magnético para almacenar y recuperar datos digitales, utilizando uno o más platos que rotan a velocidad uniforme, con material magnético en su superficie. Una cabeza magnética, articulada en un brazo móvil permite leer o guardar los datos.

  Sus principales características son la capacidad del disco, la velocidad de rotación (rpm) y la memoria caché. Utiliza interfaces específicas de disco como SATA o SAS para su conexión.

- Discos duros **SSD** (*Solid State Drive*)

  Se trata de almacenamiento de estado sólido que utiliza circuitos integrados para el almacenamiento de la información. Son más eficientes energéticamente, silenciosos, rápidos y tienen menor latencia que los discos magnéticos; como desventajas los discos SSD tienen un número máximo de ciclos de escritura, tras lo cual pueden fallar; por este motivo tienen algoritmos para repartir las escrituras en distintas zonas del disco, que hacen que los *firmware* de estos discos sean menos fiables y más complejos. Además según la tecnología utilizada los datos pueden perderse si se deja mucho tiempo sin corriente, por lo que no son aptos para archivado.

  Al contrario que los discos magnéticos precisan un comando de borrado **TRIM** para la eliminación de bloques de datos, manteniendo el rendimiento del dispositivo. Puede utilizar los interfaces genéricos de disco descritos como SATA o SAS, pero dado que se trata de memoria y no un disco puede beneficiarse de la especificación **NVMe**, para acceder a los datos del dispositivo directamente mediante el bus PCIe.

2 Dispositivos Móviles

Se entiende incluido en este apartado principalmente los teléfonos inteligentes, si bien caben también aquellos dispositivos con enfoque similar como tablets, relojes inteligentes, dispositivos de realidad aumentada, etc.

2.1 COMPONENTES

Los principales componentes de los dispositivos móviles son esencialmente los mismos que en ordenadores de escritorio, si bien adaptados para un menor tamaño, consumo y disipación de calor. Se pueden destacar los siguientes componentes:

- El procesador suele estar integrado con otros componentes en un único chip, conocido como **SOC** (system on a chip). La arquitectura de procesadores más habitual en dispositivos móviles es **ARM**. Esta arquitectura RISC está licenciada por la compañía ARM Holdings, permitiendo que

distintas empresas fabriquen distintos procesadores siguiendo un estándar. Sus ventajas son un rendimiento suficiente con un bajo consumo energético y disipación de calor.

- La memoria es habitualmente **LPDDR** (Low-Power Double Data Rate), similar a la de equipos de sobremesa pero configurada para un bajo consumo de energía.
- Pantallas: Si bien las tecnologías de base y características son similares a las de equipos de sobremesa. Destacan las pantallas **LED**, más finas y con menos consumo que las TFT tradicionales, y las pantallas **OLED**, capaces de apagar completamente los pixeles no iluminados y que por lo tanto proporcionan un contraste excelente. Las pantallas **IPS** son una variación de las LED que permiten un mayor ángulo de visión.
- Otros dispositivos: cámaras, GPS (geolocalización), acelerómetro (inclinación, caída), giroscopio (detección de la rotación), brújula, sensor de proximidad, lector de huella dactilar, etc.

2.2 SISTEMAS OPERATIVOS

2.2.1 ANDROID

Sistema operativo *open source* de Google, basado en el núcleo linux. Se han desarrollado variantes para ejecutarse en otros dispositivos como coches, televisiones, etc.

Sus principales características son:

- Interfaz gráfico basado en pantallas táctiles y en "**gestos**" (pulsar, deslizar, etc.) similares a las acciones de usuario del mundo real. Utiliza los sensores y característica del dispositivo para conseguir un interfaz responsivo ante las acciones del usuario, por ejemplo la vibración, giroscopio, sensor de proximidad, etc. La interfaz es muy configurable, tanto por el usuario como por los distribuidores del sistema operativo.
- Habitualmente se incluyen junto con el sistema operativo varias aplicaciones del ecosistema de Google, si bien estas no son de código abierto. Es el caso de la misma tienda de aplicaciones de Google, Play Store.
- Se soporta el desarrollo en varios lenguajes de programación, habiendo pasado **kotlin** a sustituir a **java** como lenguaje recomendado. Se proporciona un entorno de desarrollo integrado (**Android Studio**) junto con un sdk con herramientas de depuración, librerías, documentación, etc. Las aplicaciones se empaquetan en ficheros **APK**, siendo el principal punto de distribución de las aplicaciones **Google Play Store**, aunque existen otras tiendas de aplicaciones de terceros. Las aplicaciones se ejecutan sobre una máquina virtual denominada **Dalvik** para versiones anteriores a la 5.0, o **ART** para versiones posteriores, con una función similar a la máquina virtual de java en otros entornos.
- Como sistema operativo móvil Android incluye distintas técnicas para optimizar al máximo el consumo de energía, como puede ser la suspensión de aplicaciones o tareas no activas.

2.2.2 IOS

Sistema operativo de Apple originalmente desarrollado para los teléfonos Iphone, y posteriormente utilizado para otros dispositivos (ipad, ipod touch). Dispone de una interfaz fluida y sencilla de usar, incluyendo como en el caso de Android gestos de usuario y sensores del dispositivo.

Dispone de un sdk para el desarrollo de aplicaciones con el entorno integrado **xCode**, que incluye un diseñador gráfico de interfaces de usuario, así como soporte de múltiples lenguajes de programación. Las aplicaciones se empaquetan en ficheros **IPA**.

2.3 CONECTIVIDAD DE LOS DISPOSITIVOS PERSONALES

2.3.1 BLUETOOTH

Es una tecnología de comunicación inalámbrica que opera en la banda de 2.402 - 2.480 GHz, estandarizada en la IEEE 802.15.

Permite definir redes de área personal (PAN – *Personal Área Networks*), agrupando un dispositivo "maestro" y 7 "esclavos" en una *piconet*. Un dispositivo puede formar parte de dos o más *piconet*, formando una *scatternet*, actuando de forma indistinta como maestro o esclavo en cada una de las *piconet*.

Las sucesivas versiones del estándar han ido mejorando tanto el rendimiento como la eficiencia energética, integrando BLE (Bluetooth Low Energy).

2.3.2 NFC (*NEAR-FIELD-COMMUNICATION*)

Es un protocolo de comunicación para dispositivos en un entorno de proximidad del rango de 4 cm. Ofrece una conexión de baja velocidad (424 Kbit/s), que puede utilizarse para establecer una comunicación con otros protocolos inalámbricos con mejor rendimiento. Puede actuar como proveedor de identidad, permitiendo el pago electrónico de forma inalámbrica.

Puede funcionar en tres modos:

- Emulación de tarjeta: Permite a un dispositivo como un smartphone actuar como una smartcard, permitiendo la identificación del usuario y transacciones como pagos.
- Lectura/escritura: Permite leer o escribir información almacenada sobre etiquetas NFC.
- Igual a igual: Permite a dos dispositivos NFC comunicarse para intercambiar información.

2.3.3 WIFI DIRECT

Si bien muchos dispositivos móviles soportan redes wifi, son habituales las situaciones en que se encuentran dos dispositivos que soportan el estándar pero no disponen de un punto de acceso al que conectarse.

En estos casos la norma ***wifi direct*** permite la conexión directa entre ambos sin precisar de un punto de acceso. Un ejemplo de aplicación sería la impresión directa por wifi desde un teléfono móvil a una impresora.

2.3.4 USB / MICROUSB

La mayoría de dispositivos permiten mediante un conector usb o microusb realizar la carga de la batería, así como la transferencia de datos con otros dispositivos.

En el caso de disponer de USB OTG (*On the go*) es posible que el dispositivo móvil actúe como un dispositivo genérico de almacenamiento.

En el caso de dispositivos Apple, el conector utilizado es el Lightning, de tecnología propietaria, que permite también la carga del dispositivo y la transferencia de información.

3 MEDIDAS DE SEGURIDAD Y GESTIÓN

El uso a nivel corporativo de dispositivos móviles presenta retos específicos, que es preciso abordar para que estos no se conviertan en una puerta de entrada para las amenazas, debido a un nivel insuficiente de seguridad.

Entre las amenazas dirigidas a usuarios o dispositivos móviles están las aplicaciones falsas y potencialmente maliciosas, el phising y robo de datos, los virus o malware en general, la pérdida o robo de dispositivos con información sensible, etc.

Las herramientas de seguridad y gestión de dispositivos se han convertido por tanto en un elemento esencial, que además ha evolucionado mucho los últimos años:

- MDM (Mobile Device Management): centrado en la gestión de los dispositivos.
- EMM (Enterprise Mobile Management): pone el foco en la seguridad de la información corporativa y las aplicaciones, en lugar de la protección del dispositivo en si mismo. Se reconoce el reto de las políticas *byod* y el uso de dispositivos con información personal junto con la laboral, protegiendo esta última y permitiendo dar soporte al usuario.
- UEM (*Unified Endpoint Management*): Incorpora todos los tipos de dispositivo final de usuario en una única herramienta, sean dispositivos móviles, portátiles, equipos de escritorio, etc. Permite para ello la gestión de dispositivos con múltiples sistemas operativos y aplicaciones, de una manera integrada.

Las funcionalidades que ofrecen este tipo de soluciones son entre otras:

- Registro e inventario de los dispositivos
- Monitorización de los dispositivos, envío de alertas ante incumplimientos de las políticas de seguridad.
- Cifrado de datos. En algunos casos es posible diferenciar la parte de dispositivo utilizada para uso personal de la de uso laboral, por ejemplo para el uso de dispositivos personales de los usuarios (byod).
- Restricciones de hardware y software: según las políticas de seguridad se puede evitar el acceso o uso de determinadas aplicaciones o características del dispositivo.
- Actualización de software y mantenimiento remoto de las aplicaciones
- Borrado de datos remoto, por ejemplo en el caso de robo del dispositivo.
- Localización del dispositivo.
- Mobile Threat Prevention (MTP) y Mobile Threat Defense (MTD): solución de seguridad para proteger tanto los dispositivos como el acceso a las redes corporativas.
- Realización de copias de seguridad.

Existen tres **estrategias** para abordar un modelo ***byod***:

- **Virtualización**: Se proporciona un acceso remoto virtualizado a los sistemas corporativos, no existen aplicaciones ni datos locales más allá del software de virtualización (ej: citrix XenApp).

- **Aislamiento** o uso de **contenedores**: Las aplicaciones y datos de uso corporativo se encuentran dentro de un contenedor seguro en el dispositivo, encriptado y aislado de los datos personales.
- **Coexistencia** controlada: se instala un agente que gestiona las políticas de seguridad del dispositivo, los datos y aplicaciones conviven con los personales.