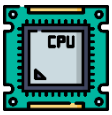
Tema 1 – Informática – opotify.com

Informática Básica



Conceptos Fundamentales de Hardware y Software

Estas dos palabras, a veces nos traen de cabeza para recordar que significan.

Pero no te preocupes, a partir de ahora no lo olvidarás, son palabras inglesas, y gracias a la traducción, verás qué fácil es:

- **Hardware:** Parte dura. Hard traducido al castellano, es duro. Las partes duras, ¿qué son? Las que puedes tocar. Es decir, los componentes físicos del ordenador.

- **Software:** Pues esta es fácil, Software son los programas. Con recordar Hardware, duro, el que puedes tocar, el software que es lo que te queda, son los programas.

Ahora que ya sabes esto tan sencillo, hay distintos tipos de hardware, y distintos tipos de software.

Para entender bien los distintos tipos, vamos a comenzar a comprender la estructura física del ordenador.

Tipos de Ordenadores

El hardware es la parte física de un PC. Esto incluye las placas, los cables, las memorias, los discos duros, los periféricos y cualquier otro material físico que ayuda a que el equipo funcione.

Hay distintos tipos de ordenadores (también llamados PC, computadoras, CPU – CPU se llama tanto a la torre del PC completa, como al microprocesador), vamos a ver los tipos de equipos informáticos:

PC, en formato Torre: Es la típica torre de ordenador que solía haber en las casas de las personas. Con el paso del tiempo, ya son más usadas por los gamers o en las oficinas. Estos tipos de ordenadores, son excelentes porque se pueden actualizar o ampliar, aumentar potencia, memoria, y añadir nuevas funciones. Los hay en formato ALL-IN-ONE, con pantalla integrada.

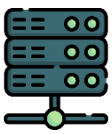
PC portátil: Son los clásicos portátiles – de toda la vida -, que con el paso de los años también han ido habiendo distintos tipos, los mini portátiles, los portátiles normales, o los súper portátiles. No son tan fáciles de ampliar, suelen estar más limitados y ser menos potentes. Llevan batería que permiten funcionar sin conectar a la red eléctrica.

Barebone: Son mini ordenadores, pequeños, del tamaño de un tupperware para comida de una sola persona.

Son muy útiles para poner en el salón, junto a la televisión, ocupan poco y dan 'internet' a la TV.

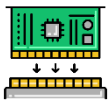
Mini Pc Stick: Son micro ordenadores del tamaño de un stick USB.

De potencia muy reducida y limitados, pero que algunos programadores con conocimientos avanzados saben usar de forma increíble.



Servidores: Son ordenadores especiales para usar a nivel de empresa. Pensados para distintos fines, almacenar datos, filtrar conexiones de internet, almacenar archivos en la nube, etc.

Los hay en formato torre, o en formato rack. Suelen tener para meter bastantes discos duros y nos ofrece soluciones avanzadas en tema de seguridad de datos.



El Hardware

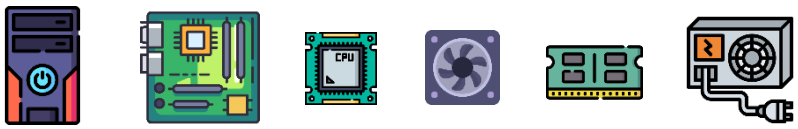
Ahora que ya sabemos que existen distintos tipos de ordenadores y los formatos que tienen, montaremos nuestro propio ordenador y hasta le instalaremos Windows, y todo ello en un abrir y cerrar de ojos (por encima, no te preocupes 😉).

Hardware Básico, o interno

Esta parte incluye la placa base (o placa madre), el procesador (microprocesador o CPU) y su correspondiente disipador con ventilador (para refrigerarlo), la memoria RAM, y la fuente de alimentación. Con estos componentes, un ordenador ya encendería. Podríamos hacer entre poco y nada, pero encendería.

Aunque asusta un poco imaginar como funciona un ordenador, su mecánica es muy sencilla, vamos a hacer la lista de la compra si quisiéramos montar nuestro propio ordenador, en formato torre:

- Una torre, o también caja. Es la 'carcasa' del ordenador. Las hay muy bonitas, de cristal, con leds, etc.
- Una placa base (o placa madre. Tiene un tipo de socket o zócalo, que es donde se instala el microprocesador o CPU.
- Un microprocesador o CPU, del mismo tipo de socket que el que tiene la placa base
- Un disipador con ventilador para refrigerar la temperatura del microprocesador o CPU
- Memoria RAM, compatible con el tipo de zócalo de memoria RAM de nuestra placa base
- Fuente de alimentación compatible con nuestra placa base



En estos dibujos, vemos la torre, después la placa base, el micro, el ventilador/disipador, la memoria ram, y la fuente de alimentación. No son más que piezas de un pequeño puzle, que encaja cada una en su sitio.

Para montarlo, sería fácil: en primer lugar se instala la placa base en la torre (caja). Luego, se instala la memoria RAM en la placa base, con dos clics, después, levantamos el zócalo o socket del microprocesador en la placa base, y lo instalamos, conectamos su disipador y ventilador.

Por último, conectamos la fuente de alimentación a la placa base, conectamos el ventilador del microprocesador a la placa base, y conectamos los botones de la torre o caja a la placa base.

Y tachán, con esto, dándole corriente al ordenador a través de la fuente de alimentación, ya arrancaría el ordenador.

Aunque eso sí, sin teclado, ratón, pantalla… ¡¡nos faltan los periféricos!!, que pueden ser de entrada, salida, o de entrada y salida simultáneamente (como una pantalla táctil).

Así que, para recordarlo, el hardware básico o interno, son todas las piezas que van dentro de la torre o PC, incluyendo la propia torre. Esto seguro que ya no se te olvida.

Periféricos de Entrada, Hardware externo

Permiten introducir datos al ordenador. El ratón, el teclado, un micrófono, una cámara web, un escáner, una unidad lectora de CD/DVD (ojo, unidad lectora, si fuera una grabadora, sería de entrada y salida).

En definitiva, cualquier dispositivo que nos permita introducir datos en un ordenador, es un periférico de entrada.

Periféricos de Salida, Hardware externo

Pues en este caso, son los dispositivos que sacan datos del ordenador. Un monitor, una impresora, unos altavoces, etc. Todo lo que nos valga para extraer datos de un ordenador, es un periférico de salida.

Por ejemplo un plotter, que es un trazador gráfico, para hacer grandes carteles publicitarios.

Periféricos de Entrada y Salida. También conocidos como mixtos E/S, Hardware externo

Pues ahora que ya conocemos los periféricos de entrada o de salida, vamos a ver los que nos permiten hacer las dos cosas.

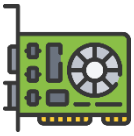
Son tanto de entrada como salida de datos. Y si no se te ocurre ninguno, vamos a ver algunos ejemplos, como son las pantallas táctiles que usan en los restaurantes mayoritariamente, puedes ver la información del ordenador y al mismo tiempo puedes hacer clics e introducir datos.

También tenemos las impresoras multifunción, que sirven para imprimir, escanear, leer tarjetas de memoria, etc.

También tenemos las unidades grabadoras de CD/DVD, unidades de almacenamiento, memorias USB…

Como ves, a nuestro ordenador que hemos montado, le conectamos el ratón, el teclado, la pantalla, incluso unos altavoces, y ya podríamos encenderlo y ver los datos en pantalla.

La Tarjeta Gráfica, Hardware interno (pero existen tarjetas gráficas externas)



Son las encargadas de enviar la información del ordenador al monito o pantalla.

Normalmente viene integrada en la propia placa base (o placa madre, motherboard), pero a su vez, es posible instalar una o varias tarjetas gráficas en slots PCI-E (o PCI, ISA, según la antigüedad).

Las tarjetas integradas siempre son de menor potencia y menor velocidad. Las que se instalan en slots PCI-E son más potentes, rápidas, y caras, o muy caras.

Las tarjetas gráficas, tienen distintos tipos de salida, digamos que cada tipo de salida tiene un conector diferente, y un monitor o pantalla debe ser compatible con la salida o salidas de nuestra tarjeta gráfica. Vamos a ver las salidas (o puertos de salida como se le llama), más comunes:

- **VGA:** Es antiguo, pero se usa aún en muchas oficinas y ordenadores.
- **DVI:** Solo para señal de vídeo, no incluye audio.
- **HDMI:** Señal de vídeo y audio.
- **DisplayPort:** Ideal para audio y vídeo, y puede transmitir datos desde desde 144Hz hasta 4K.
- **Thunderbolt USB C:** Incluye vídeo, audio, datos y alimentación.
- **MHL:** Típico en dispositivos móviles y compatible con USB C.

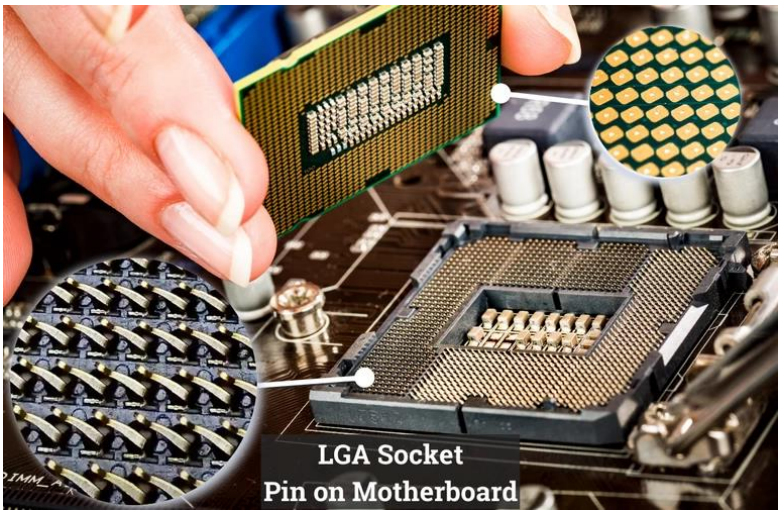
Tipos de Procesadores, Hardware básico e interno

Bueno, ahora que ya está nuestro ordenador montado y funcionado, y tenemos algo de idea, vamos a ver que hay distintos tipos de procesadores, que digamos que se agrupan entre marcas, y dentro de las marcas, distintos tipos de modelos o gama. Son como los coches, Ferrari y Lamborghini, y se 'pelean' por ser más rápidos y gastar menos (electricidad).

Los principales fabricantes son Intel y AMD. Intel nos los ofrece como por ejemplo Intel Core i9 13900K. Donde i9 es el modificador de la marca, el 13900 es el SKU, y la K es la línea del producto. Un i3 es más lento que un i9.

Los AMD, se organizan en series FX, Athlon, APU, o Ryzen. Las CPUs se agrupan por tipo de zócalo, y esto significa que un tipo de CPU puede no ser compatible con muchas placas base, ya que debe coincidir el zócalo de la placa base y el tipo de zócalo de la CPU. Si no coinciden, sería como intentar meter una pelota por un boquete más pequeño en forma de triángulo. Pues no, no se puede.

Aquí vemos como se introduce un microprocesador en un zócalo de la placa base:



Cortesía de https://greatpcreview.com/guides/cpu-socket

La BIOS, y el Firmware

Al encenderlo, sólo tendríamos acceso a la BIOS, que es el sistema básico de entrada y salida (basic input output system), que está ubicada en la placa base del ordenador, y no es más que un programa grabado en una memoria EEPROM (que viene a significar Memoria electrónicamente programable de sólo lectura).

En esta EEPROM, se almacena el sistema básico de la placa base, "el programa". Se le conoce como firmware (digamos que, cuando un programa está instalado en un chip o memoria EEPROM, o EPROM, se le llama firmware, para acordarte, piensa en un sargento, que siempre dice… ¡¡fiiiirmen!!, pues el firmware es un software muy rígido, como un sargento.

Nuestro ordenador, sólo nos permite acceder a la BIOS, y así no nos sirve para gran cosa. Si nos ponemos a tocar lo que no sabemos y queremos posteriormente hacer que olvide lo que hemos tocado, tenemos la opción de desconectar la pila o batería (mini pila de botón), que hay en la placa base, o usar el conector para puntear y hacer el reset. Aunque también lo podemos restaurar de fábrica desde dentro de la propia BIOS, con nuestro teclado buscamos la opción de restaurar de fábrica, lo hacemos, y se reinicia.

Bueno, poquito a poquito, vamos comprendiendo como funciona un ordenador. Ahora que ya sabemos lo de la BIOS, vamos a darle marcha a nuestro PC.

El Disco Duro

Vamos a instalar un disco duro, donde vamos a almacenar nuestro sistema operativo, y vamos a guardar datos.

El disco duro, es una memoria, es permanente, a diferencia de la memoria RAM que va colocada en la placa base y se borra cada vez que se apaga el ordenador.

Al instalar nuestro sistema operativo, como por ejemplo Windows 10, ya podremos comenzar a usar nuestro ordenador.

Existen distintos tipos de discos duros, tamaños, formatos, velocidad, etc. Más adelante los verás en este temario.

Software en Profundidad

El Software, son los programas tal y como ya hemos visto. Hay muchísimos programas, y existen distintas categorías fundamentales para organizar dicho software. Y son:

- Software de sistema
- Software de aplicación
- Software de gestión
- Software de programación

¡Uff! Esto ya suena a chino, pero no te preocupes. Ahora los vemos de uno en uno, y verás que sencillo 😉

El Software de Sistema

Es el más importante, ya que se encarga de que el hardware funcione, entrelaza el funcionamiento de todos los componentes, a través de unos drivers.

El software de sistema es por ejemplo el sistema operativo Microsoft Windows, aunque otros conocidos son el software de MacOS de Apple, o las distintas distribuciones de Linux, las cuales son normalmente gratis aunque existen algunas de pago.

El Software de Aplicación

Pues como dice su nombre, son los programas de aplicaciones, como el Photoshop para editar imágenes, los editores de audio como Goldwave, el Microsoft Paint para dibujar, y en definitiva, todo software con una utilidad en concreto.

También son los programas de empresa, diseño gráfico, diseño en 3D, en definitiva, casi cualquier programa que uses a diario en la empresa.

El Software de Gestión

Aunque están incluidos realmente dentro del Software de Aplicación, el Software de Gestión está vinculado con los programas que se usan en las empresas, incluyendo contabilidad, facturación, gestión de impuestos, nóminas, organización laboral, etc.

Aunque las empresas pueden tener software de diferentes proveedores para la gestión de empresas, hoy día existen paquetes ERP que incluyen “todo en uno”, de forma que simplifica mucho el trabajo ya que las interfaces de programas son muy similares al ser del mismo fabricante.

El Software de Programación

Este es el más aburrido, es el que usan los programadores. Pero este es muy importante porque es con el que se hace el resto de software.

Son por ejemplo los compiladores, que convierten un texto o código fuente en un programa usable de verdad.

Al existir distintos tipos de lenguajes de programación, nos quedamos con los más famosos, que son:

- Python
- C
- Java
- C++
- C#


Sistemas de Almacenamiento

Son los encargados de recopilar datos y conservar la información en formato digital, bits, bytes… para entender un poco lo que es un sistema de almacenamiento digital, hay que comprender que un ordenador es como un cerebro.

Existen dos tipos de memoria, a corto plazo y a largo plazo. En el ordenador, la memoria a corto plazo es la memoria RAM, que se borra cada vez que se apaga el ordenador. Y luego tenemos la memoria a largo plazo, que es la que se almacena en un soporte, disco duro, memoria flash, etc.

La ventaja de la memoria RAM, es que es una memoria muy rápida, lo típico que acaba de pasar en la calle y has visto con tus propios ojos, y tu amigo o amiga que va contigo, no lo ha visto. Pues corriendo se lo puedes explicar tal y como ha sucedido, acaba de pasar, está 'fresco', y lo puedes narrar a la perfección. Es como si estuviera en tu propia RAM dentro de tu cerebro, acceso instantáneo al recuerdo, muy rápido y fácil.

Sin embargo, al despertarte al día después, o una semana, o mes tras ocurrir, si alguien te pregunta… ¡uf! ¿de qué color era el coche que se pegó el tortazo contra aquella farola? Pues tu cerebro ya tiene que buscar en el 'archivo' de los recuerdos. Es como buscar en el disco duro la información. Se tarda mucho más en buscar dicha información, y ya tardas algo más de tiempo en recordar los detalles.

Explicado esto, así por encima, vamos a ver que tipos de memorias hay, así como los discos duros.

Memorias ROM. Read Only Memory, es decir, memorias de sólo lectura

Estas memorias son las que están almacenadas en los chips físicos. Por ejemplo, el firmware de la BIOS (el programa de la BIOS), está guardado en un chip. Interesante, ¿verdad?

- **PROM:** Este chip es una memoria de sólo lectura, programable una única vez.

- **EPROM:** Es una memoria de sólo lectura borrable y programable. Antes de reprogramar, hay que borrarla, y se borra con luz ultravioleta o altos niveles de voltaje.

- **EEPROM:** Es la más avanzada de las tres, ya que es una memoria de sólo lectura borrable y programable electrónicamente, sin requerir rayos ultravioleta, y se puede reprogramar de forma individual sin eliminar el conjunto completo.

Si alguna vez en tu juventud, viste un chip con una pegatina y se la quitaste, verías un cristal. Pues por ahí se le aplica la luz ultravioleta a esa EPROM para borrarla 😉

Memorias RAM, Random Access Memory, memorias de acceso aleatorio

Aunque hemos hablado algo de ellas antes, ya sabemos que son memorias que se borran al quedarse sin electricidad, y es muchísimo más veloz que la memoria ROM anterior. Los tipos de memoria RAM son:

- **SRAM:** Es la RAM estática (static ram), no requiere refresco. Las subfamilias son NVRAM y MRAM.
- **DRAM:** Es la RAM dinámica (Dynamic ram), y ésta, sí requiere refresco. Dentro de la DRAM, encontramos la DRAM asíncrona y la SDRAM, que es la síncrona.

Si te fijas, los nombres coinciden con la primera letra de su nombre. S de static, y D de Dynamic. Y dentro de la DRAM, la SDRAM es la DRAM con una S de síncrona delante. Por si se te olvida, piensa en las iniciales 😊.

Cuanta mayor sea la capacidad de la memoria RAM, más datos caben en el cerebro 'a corto plazo' del ordenador, y más rápido será el acceso a los datos.

Imagina que tienes un disco duro de 10 Gigabytes de tamaño, algo pequeño hoy día pero muy grande hace años. Si a un ordenador que maneja bases de datos actualmente del tamaño de 5 gigabytes, le instalas una memoria RAM de 16 gigabytes, significa que si configuras adecuadamente el software de base de datos, puedes cargar en la memoria RAM del ordenador los 5 gigabytes de la base de datos, y esto implica que el ordenador accedería a los datos de una forma muy rápida, y sería mucho más veloz que si tuviera que buscar los datos en un disco duro lento.

Memorias CACHÉ

Esta memoria es específica, sirve de apoyo al microprocesador, y puede trabajar a velocidad realmente elevadas.

Se divide en distintos niveles para poder actuar como almacenamiento de datos y de instrucciones, con el fin de ahorrar ciclos de trabajo al microprocesador, y de evitar accesos a la memoria RAM. Digamos que la memoria caché es el lugar donde se almacenan los trabajos que van a ser realizados de forma inminente y se puede ahorrar tiempo. Para no profundizar en exceso, vamos a ver los tipos de niveles que hay, ya que es por lo que suelen preguntar en exámenes de oposiciones.

- **Caché L1:** La básica, y más próxima al procesador, y la más rápida, por el contrario, la de menor capacidad.
- **Caché L2:** Mantiene el equilibrio entre capacidad, velocidad y cercanía al procesador.
- **Caché L3:** Más alejada del procesador, menos rápida, y de mayor capacidad. Cuanto más se aleja, más lenta.
- **Caché L4:** Este tipo de caché no es habitual, usada sobre todo como buffer de tarjetas gráficas integradas.

Discos Duros

Ahora que ya hemos visto los distintos tipos de memoria, vamos a entrar a ver los diferentes tipos de discos duros que existen, para almacenar la información 'a largo plazo'. Donde se guardará el sistema operativo instalado, los programas y nuestros datos.

A día de hoy, los discos duros más usados son los SSD, que ya no tienen discos giratorios magnéticos en su interior, seguidos de los discos duros giratorios y magnéticos, que suelen ofrecer mayor capacidad a menor precio, y por último, nos queda las memorias SSD que trabajan sobre placas PCI-Express, de grandísima velocidad.

Bits, Bytes, y ceros y unos

Ahora que ya tienes una idea sobre como se guardan los datos, vamos a ver primero que son exactamente los datos.

- **Bit:** es la unidad mínima de información, puede ser o bien un 0 ó 1.
- **Byte:** es el conjunto fijo de 8 bits de información. Es decir, un Byte puede ser 00000001, por ejemplo. Por eso se le conoce como octeto.
- **Nibble:** este es la mitad de un byte, medio octeto, un cuarteto 😉

Por ejemplo, ¿te gustaría saber como se representa la letra A mayúscula en un byte? Pues sería: 01000001.

Ahora que ya sabemos esto, imagina la cantidad de bytes que contiene el Quijote, o la Biblia, o la Trilogía de Harry Potter. Pues si la letra A se representa como 01000001, ¡imagina!.

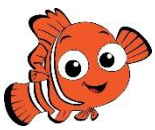
Así que para referirnos a las distintos tamaños de información, porque no vamos a ir por la vida diciendo que el Quijote ocupa 2.411.724 de bytes. Al igual que con los kilos y los litros, los documentos se 'miden' por tamaños y se usan multiplicando por 1.024 el anterior.

Nombre	Siglas	Tamaño
Kilobyte	(KB)	1024 Bytes
Megabyte	(MB)	1024 KB
Gigabyte	(GB)	1024 MB
Terabyte	(TB)	1024 GB
Petabyte	(PB)	1024 TB
Exabyte	(EB)	1024 PB
Zettabyte	(ZB)	1024 EB
Yottabyte	(YB)	1024 ZB
Brontobyte	(BB)	1024 YB
Geopbyte	(GeB)	1024 BB
Saganbyte	(SB)	1024 GeB
Jotabyte	(JB)	1024 SB

El truco para aprenderte cual es mayor que otra, o menor, consiste en:

Ke MaGeTe es el PEZ, Yo, Bronto Ge SaJo

Fíjate bien en las iniciales de esta frase "chorri". Magete está mal escrito. Se hace alternando mayúsculas y minúsculas. Y recuerda estos dibujos:



Ke **M**a**G**e**T**e es el **P.E.Z**

Yo

Bronto

Ge

SaJo

Si nos fijamos bien, ponemos en vertical las iniciales, usando las mayúsculas (el resto no es necesario aprenderlo, ya que no suelen preguntar metiendo una entremedias falsa, pero no está de más que te suenen).

K - ilo
M - ega
G - iga
T - era
P - etta
E - exa
Z – etta

Yo - tta
Bronto
Ge - op
Sa - gan
Jo - ta

Si se te olvidan los dibujos, piensa en NEMO, el pobre pescaíto "magete" que lo olvidaba todo… "**K**e **M**a**G**e**T**e es el **PEZ**"… y luego, la segunda parte, eres tu mism@, **YO**, el dinosaurio **Bronto**, la risita **GE** (recuerda, la risa está también mal escrita, como MaGeTe), y luego la chuleta de **SaJo**nia…

Con esto, te hables la tabla en VERTICAL, y recordando que KILO es la más pequeña, el resto ya es historia.

Sistemas Operativos

El primer Sistema Operativo fue creado en 1956, para ser usado en un ordenador IBM 704, y lo único que hacía era comenzar la ejecución de un programa cuando el anterior finalizaba.

A partir de 1960, aparecen conceptos como sistemas operativos multitarea, los multiusuario, los multiprocesadores y sistema de trabajo en tiempo real. Una verdadera revolución informática y mundial.

Es también en los '60s, cuando aparece el monstruo llamado UNIX, la base de la gran mayoría de sistemas operativos actuales y existentes hasta la fecha. UNIX fue creado por IBM, basado en lenguaje C.
Fue en 1980 cuando nació MS-Dos, Windows, y MacOS. Aunque los de Microsoft MS-Dos y Windows fueron los más usados, no fue hasta la llegada de la década de los 90 hasta que apareció una alternativa real, y de uso totalmente gratuito: Linux, que se convirtió en un sistema libre, similar a UNIX.

A pesar de lo explicado, el primer ordenador electrónico, fue el ENIAC de 1945, presentado en 1946. Pesaba 27 toneladas, ocupaba 167m2 y tenía 17.500 válvulas de vacío.

Un sistema operativo, básicamente tiene 3 partes esenciales, y son:

- Sistema de archivos
- Núcleo
- Comandos

Un sistema operativo, se encarga de administrar el microprocesador, direcciona entradas y salidas de los datos, administrar el sistema de archivos, gestionar el acceso a la memoria y el uso de la memoria de almacenamiento, entre oras cosas.

El sistema operativo, al fin y al cabo se encarga de hacer de intermediario entre el hardware y el usuario. Y como sabemos, los hay gratuitos, o de pago.

No obstante, muchos ordenadores cuando son adquiridos, vienen con licencias del sistema operativo incluidas en el precio.

Windows, de Microsoft

Se publicó por primera vez en 1985. Ha tenido numerosas versionas, las más conocidas han sido Windows 3.1, 98, XP, 7, y Windows 10. Aunque el histórico de versiones Windows es:

- Windows 1.0
- Windows 2.0
- Windows 3.0
- Windows NT
- Windows 95
- Windows 98
- Windows 2000
- Windows Me
- Windows XP
- Windows Vista
- Windows 7
- Windows 8
- Windows 8.1
- Windows 10
- Windows 11

También existen las versiones de sistemas operativos *Windows Server*, ideales para servidores, usadas en ámbito laboral.

Linux

Es el sistema favorito de los programadores informáticos de alto nivel. Por su facilidad para modificar su propio código y adaptar el sistema a las necesidades de cada uno. Es por norma el más fiable de todos, ya que la propia comunidad de usuarios de Linux se encarga de ir solventando los fallos de seguridad.

MacOS

Es el software de la manzana, el que llevan tanto los portátiles como ordenadores de Apple. Es exclusivamente de uso para los ordenadores de Apple, lo que permite optimizar al máximo el sistema ya que no debe ser compatible con tantos drivers y dispositivos.

Android, de Google

Es el que llevan los teléfonos móviles mayormente, a excepción de los que usan iOS de Apple, o los de Huawei que ahora cuentan con su propio sistema operativo mobile.

iOS, de iPhone/Ipad

Muy conocido en el mundo ya que cualquier iPhone o Ipad lo llevan instalado. Existen bastantes versiones.

Nociones básicas de seguridad Informática

La seguridad de los datos es algo de lo más importante en el mundo de la seguridad, ya que cualquier brecha de seguridad, puede conllevar a la pérdida total de los datos, tanto a nivel personal como nivel profesional en las empresas.

La búsqueda de agujeros de seguridad se lleva a cabo 24 horas, todos los días del año. Tanto a nivel humano como a nivel informático, se trabaja a destajo intentando localizar cualquier fallo de seguridad que permita a los hackers robar información para solicitar rescates económicos, o simplemente vender dicha información a terceros, como pueden ser países, empresas o individuos.

Por ello, los sistemas operativos incluyen las famosas 'actualizaciones automáticas', y éstas mayormente se hacen para tapar agujeros de seguridad, descubiertos por empresas o hackers – que a su vez llegan a acuerdos económicos con dichas empresas de software para evitar males mayores -.

En el caso de Windows, por ejemplo, tenemos un servicio interno llamado Windows Update, que se encarga de ayudarnos a proteger nuestro equipo de forma automática sin tener que complicarnos 'la cabeza'.

Vamos a ver en primer lugar, las principales amenazas a las que se enfrentan los equipos que se encargan de proteger la seguridad de los datos:

Virus Informáticos

Un virus informático no es más que un software que pretende alterar el funcionamiento normal de un equipo informático, sin autorización del usuario.

Siempre tiene un fin malicioso, reemplazar archivos ejecutables por otros con el mismo código del virus implantado para que se propague cuando se copien ficheros a otros ordenadores, trasladando así el código malicioso del virus de un ordenador a otro.

Hay que tener en cuenta que los virus pueden destruir información de forma intencionada o no, aunque bien es cierto que hay virus menos dañinos.

El virus, comienza con una pequeña carga dañina, llamada payload, que puede ser desde una simple broma, hasta tener el objetivo de dañar el sistema operativo o los datos, o incluso saturar el tráfico de una red.

Cuando un virus infecta un ordenador, éste, se instala en la memoria RAM del ordenador, de modo que todo lo que se toca, se infecta, y el virus se propaga así por todo el sistema operativo.

Como curiosidad, el primer virus, fue Creeper, creado en 1972. Esto dio comienzo a la creación del primer antivirus, que fue denominado Reaper.

Los virus se pueden colar en el sistema de dos formas generalmente, una con la propia colaboración del usuario de manera no intencionada, navegando o descargando software de dudosa procedencia, mediante la instalación de dispositivos USB o CD previamente infectados, o a través de vulnerabilidades del propio sistema operativo.

Hay distintas formas de protegerse ante los virus a nivel doméstico, manteniendo el sistema operativo actualizado, así como los programas que se usen, instalando un antivirus, e instalando filtros en el correo anti ficheros ejecutables.

A nivel profesional, hay soluciones más avanzadas, como la instalación de sistemas profesionales a nivel Enterprise, que nos permite por ejemplo bloquear cualquier tipo de ejecución de un programa, script o código de procesamiento no incluido en una lista de ficheros.

Esto se hace con las funciones de Active Directory de Windows Server, y versiones Enterprise de Windows. Cada fichero, tiene un hash único, que es un algoritmo matemático.

Si tenemos por ejemplo el fichero calc.exe, que es la calculadora oficial de Microsoft Windows, y añadimos este fichero a la lista de hashes permitidos, siendo su hash:

DA39A3EE5E6B4B0D3255BFEF95601890AFD80709

Si luego un troyano infecta calc.exe en otro ordenador sin este tipo de protección, el hash de este fichero cambiará, y si lo copiamos a ese ordenador que sí goza de esta protección, al intentar abrirlo no se ejecutará, ya que el nuevo hash, no está en la lista de los permitidos.

Un sistema fantástico, que no requiere de protección antivirus 😊 😊 😊

Para evitar infectarse por los virus, debemos abrir evitar archivos desconocidos, no deseados, instalar software antivirus, no descargar programas piratas, ni abrir correos electrónicos de desconocidos o conocidos con ficheros ejecutables.

Gusanos

Son código malicioso, puro y duro, cuyo objetivo es principalmente replicarse a sí mismo, y no requiere infectar otros archivos diferentes para multiplicarse. Busca infectar el mayor número de dispositivos posible.

No se dedica a infectar esos otros archivos ni a destruir o dañar equipos, pero es capaz de saturar redes informáticas ya que buscan vulnerabilidades en red para seguir copiándose de un sitio a otro.

Son capaces de abrir la libreta de contactos de nuestro programa de mensajería de correo electrónico, y enviarse de forma automática a todos esos contactos.

También suelen replicarse a través de redes de intercambio de ficheros como los Torrent, y demás redes P2P.

Esta práctica es muy usada por las propias empresas de películas, series, software informático, etc, ya que se aprovechan de este tipo de gusanos para hacer de ese tipo de redes un lugar menos seguro para los usuarios, haciendo que éstos dejen de usarlas en gran parte.

Suelen usar ingeniería social para conseguir más efectividad, con un tema o nombre atractivo para camuflar el código malicioso.

El primer gusano informático de la historia data de 1988, cuando el gusano Morris infectó una gran parte de los servidores existentes hasta esa fecha. Su creador, Robert Tappan Morris, fue condenado a tres años de prisión.

La forma de protegerse ante los gusanos, es mantener el sistema actualizado y con cortafuegos activo (más adelante vemos los que es un corta fuegos). También hay que evitar abrir correos no reconocidos o inesperados, y tener un antivirus actualizado.

Troyanos

¿Recuerdas la historia del caballo de Troya? Pues exactamente eso es un troyano. Te mandan una foto llamada “Tom Welling Desnudo.jpg”, y lo vas a abrir con toda la ilusión y ¡zas! Ni Tom Welling desnudo ni nada, te abre una ventana negra de MS-Dos, empieza a hacer cosas, y ¡boom! Abre una puerta trasera (backdoor) de tu ordenador, y te quedas sin ver al Tom Welling ☹

Has sido víctima de un troyano. Aunque los troyanos también pueden ser destructivos o menos destructivos, abriendo puertas traseras permitiendo accesos externos, instalar keyloggers para robar información y cuentas de usuario, etc.

La diferencia del troyano con respecto al virus y al gusano, es que el troyano suele abrir un agujero de seguridad, de ahí lo de caballo de troya.

AdWare (información directa de MalwareBytes, la mejor empresa antimalware 😊)

El adware es un software no deseado diseñado para mostrar anuncios en su pantalla, normalmente en un explorador de internet.

Algunos profesionales de la seguridad lo ven como un precursor de los PUP (programas potencialmente no deseados) de hoy en día.

Normalmente, recurre a un método subrepticio: bien se hace pasar por legítimo, o bien mediante piggyback en otro programa para engañarlo e instalarse en su PC, tableta o dispositivo móvil.

El adware genera beneficios a su programador desplegando automáticamente anuncios en la interfaz de usuario del software o en la pantalla emergente que salta durante el proceso de instalación.

Una vez que el adware secuestra su dispositivo, puede hacer que efectúe todo tipo de tareas no deseadas.

Las funciones del software pueden haberse diseñado para analizar la ubicación y los sitios web que visita, y mostrar anuncios acordes a los bienes y servicios que se muestran en ellos.

Pese a que el adware es molesto, pero no constituye una amenaza de malware peligrosa para su seguridad informática, si los creadores del adware venden la información sobre sus hábitos de navegación a terceros, estos pueden usarlo para bombardearle con anuncios personalizados.

Estos son algunos signos reveladores de que tiene adware en su sistema:

- Aparecen anuncios en lugares en los que no deberían.
- La página de inicio de su navegador ha cambiado misteriosamente sin su permiso.
- Algunos de los sitios web que visita con frecuencia no se muestran correctamente.
- Los enlaces le redirigen a sitios web diferentes de los que deberían.
- Su explorador web va muy lento.
- Han aparecido en su explorador, de repente, nuevas barras de herramientas, extensiones o plugins.
- Su Mac instala de forma automática aplicaciones de software no deseadas.
- Su explorador se bloquea.

Hay dos formas principales por las que el adware se cuela en su sistema. En la primera, usted descarga un programa (normalmente freeware o shareware) que instala el adware sin que se dé cuenta y sin su permiso.

La segunda forma es igual de traicionera: usted está navegando por un sitio web. Puede ser de confianza, o tal vez lo ha abierto de pasada.

Rootkits

Es un programa que permite acceso de administrador o acceso privilegiado a una persona ajena al ordenador. Lo hace de forma oculta, al control de los administradores.

Viene a significar “root” -> raíz , y “kit” -> herramientas.

Se esconde tanto a él mismo como al resto de “herramientas” que incluye, se oculta a la perfección para evitar ser detectado, pero sin perder el derecho de acceso al intruso, para extraer de forma remota información sensible, mediante acciones o comandos.

Una vez que el rootkit ha sido instalado, permite que el atacante disfrace la siguiente intrusión y mantenga el acceso privilegiado a la computadora por medio de rodeos a los mecanismos normales de autenticación y autorización.

La detección del rootkit es complicada pues es capaz de corromper al programa que debería detectarlo.

Los métodos de detección incluyen utilizar un sistema operativo alternativo confiable; métodos de base conductual; controles de firma, controles de diferencias y análisis de volcado de memoria.

La eliminación del rootkit puede ser muy difícil o prácticamente imposible, especialmente en los casos en que el rootkit reside en el núcleo; siendo a veces la reinstalación del sistema operativo el único método posible que hay para solucionar el problema.

Keyloggers

Los keyloggers realizan un seguimiento y registran cada tecla que se pulsa en una computadora, a menudo sin el permiso ni el conocimiento del usuario.

Un keylogger puede estar basado en hardware o software, y se puede usar como herramienta lícita de control de TI, tanto profesional como personal.

Sin embargo, los keyloggers también se pueden utilizar con fines delictivos.

Por regla general, los keyloggers son un spyware malicioso que se usa para capturar información confidencial, como contraseñas o información financiera que posteriormente se envía a terceros para su explotación con fines delictivos.

Cuando no sabes que todo lo que escribes en el teclado de la computadora se está registrando, es posible que sin quererlo reveles contraseñas, números de tarjeta de crédito, comunicaciones, números de cuentas corrientes y otra información confidencial a terceros.

Para proteger tu equipo de los keyloggers. Mantener actualizados tu sistema operativo, productos de software y navegadores con los últimos parches de seguridad debe ser siempre una parte de tu solución de seguridad, pero la mejor defensa es instalar un buen producto antispyware.

Man in the Middle

Un ataque de intermediario (man-in-the-middle attack, MitM o Janus) es un ataque en el que se adquiere la capacidad de leer, insertar y modificar a voluntad información.

El atacante debe ser capaz de observar e interceptar mensajes entre las dos víctimas y procurar que ninguna de las víctimas conozca que el enlace entre ellos ha sido violado.

El ataque MitM es particularmente significativo en el protocolo original de intercambio de claves de Diffie-Hellman, cuando este se emplea sin autenticación. Hay ciertas situaciones donde es bastante simple, por ejemplo, un atacante dentro del alcance de un punto de acceso wifi sin cifrar, donde este se puede insertar como intermediario.

Para comprender mejor esta técnica, del hombre en el medio, vamos a ver el ejemplo siguiente:

En primer lugar, Patricia le pregunta a Robert por su clave pública. Si Robert envía su clave pública a Patricia, pero Tom es capaz de interceptarla, un ataque de intermediario puede comenzar. Tom envía un mensaje falsificado a Patricia que dice ser de Robert, pero en cambio incluye la clave pública de Tom. Patricia, creyendo que esta clave pública sea de Robert, cifra su mensaje con la clave de Tom y envía el mensaje cifrado de nuevo a Robert. Tom intercepta otra vez, descifra el mensaje utilizando su clave privada, posiblemente altera si ella quiere, y vuelve a cifrar con la clave pública de Robert que fue enviada originalmente a Patricia. Cuando Robert recibe el nuevo mensaje cifrado, él cree que vino de Patricia.

1. Patricia envía un mensaje a Robert, que es interceptado por Tom:

   Patricia "Hola Robert, soy Patricia. Dame tu clave." → Tom Robert

2. Tom reenvía este mensaje a Robert; Robert no puede decir que no es realmente de Patricia:

   Patricia Tom "Hola Robert, soy Patricia. Dame tu clave." → Robert

3. Robert responde con su clave de cifrado:

   Patricia Tom ← [clave de Robert] Robert

4. Tom reemplaza la clave de Robert con la suya, y transmite esto a Patricia, afirmando que es la clave de Robert:

   Patricia ← [clave de Tom] Tom Robert

5. Alicia encripta un mensaje con lo que ella cree que es la clave de Robert, pensando que sólo Robert puede leer:

   Patricia "¡Nos vemos en la parada de autobús!" [Cifrada con la clave de Tom] → Tom Robert

6. Sin embargo, debido a que en realidad estaba cifrada con la clave de Tom, Tom puede descifrarlo, leerlo, modificarlo (si se desea), volver a cifrar con la clave de Robert, y lo remitirá a Robert:

   Patricia Tom "¡Nos vemos en la furgoneta de al lado del río!" [Cifrada con la clave de Robert] → Robert

   Robert cree que este mensaje es una comunicación segura de Patricia.
   Robert va a la furgoneta sin ventanas y Tom le atraca.

Denial Of Service (DoS) – Ataque de denegación de servicio

Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

Normalmente provoca la pérdida de la conectividad con la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema atacado.

Los ataques DoS se generan mediante la saturación de los puertos con múltiples flujos de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando su servicio.

Por eso se le denomina denegación, pues hace que el servidor no pueda atender la cantidad enorme de solicitudes. Esta técnica es usada por los crackers o piratas informáticos para dejar fuera de servicio servidores objetivo.

A nivel global, este problema ha ido creciendo, en parte por la mayor facilidad para crear ataques y también por la mayor cantidad de equipos disponibles mal configurados o con fallos de seguridad que son explotados para generar estos ataques.

Se ve un aumento en los ataques por reflexión y de amplificación por sobre el uso de botnets.

Distributed Denia lof Service (DDoS) – Ataque distribuido de denegación de servicio

El cual se lleva a cabo generando un gran flujo de información desde varios puntos de conexión hacia un mismo punto de destino.

La forma más común de realizar un DDoS es a través de una red de bots, siendo esta técnica el ciberataque más usual y eficaz por su sencillez tecnológica.

En ocasiones, esta herramienta ha sido utilizada como un buen método para comprobar la capacidad de tráfico que un ordenador puede soportar sin volverse inestable y afectar los servicios que presta. Un administrador de redes puede así conocer la capacidad real de cada máquina.

Firewall o Cortafuegos

Un firewall es un dispositivo de seguridad de la red que monitoriza el tráfico entrante y saliente y decide si debe permitir o bloquear un tráfico específico en función de un conjunto de restricciones de seguridad ya definidas.

Los firewalls han sido la primera línea de defensa en seguridad de la red durante más de 25 años.

Establecen una barrera entre las redes internas seguras, controladas y fiables y las redes externas poco fiables como Internet.

Un firewall puede ser hardware, software o ambos.

Firewall proxy

Se trata de un tipo de dispositivo de firewall que funciona en fases iniciales y hace la función de gateway entre una red y otra para una aplicación determinada.

Los servidores proxy pueden aportar otras funciones como contenido de caché y seguridad, ya que evitan conexiones directas desde fuera de la red. Sin embargo, esto puede afectar a otras funciones y a las aplicaciones que respaldan.

Stateful inspection firewall

Ahora considerado un firewall "tradicional", un stateful inspection firewall (firewall de inspección de estados) permite bloquear el tráfico según criterios basados en el estado, el puerto y el protocolo. Monitoriza toda la actividad desde la apertura de una conexión hasta que se cierra.

Las decisiones con respecto al filtrado se toman en función tanto de las restricciones definidas por el administrador como del contexto.

Para esto, ambos elementos utilizan información de conexiones anteriores y paquetes que pertenecen a la misma conexión.

Firewall para gestión unificada de amenazas (UTM)

Un dispositivo UTM normalmente combina de forma independiente las funciones de un stateful inspection firewall, con prevención de intrusiones y antivirus. También puede incluir otros servicios como la gestión en la nube. Este firewall se centra en la sencillez y en la facilidad de uso.

Firewall de última generación (NGFW)

Los firewalls han evolucionado y ahora son mucho más que un simple paquete de filtrado y una inspección de estados. Muchas compañías están implementando firewalls de última generación para detener amenazas modernas como malware avanzado y ataques en la capa de aplicación.

Según la definición de Gartner, Inc. estas son las ventajas que debe incluir un firewall de última generación:

- Funciones estándar de firewall como la inspección de estados
- Prevención de intrusiones integrada
- Detección de aplicaciones y control para visualizar y bloquear aplicaciones que puedan generar riesgos
- Actualizar rutas para añadir futuras fuentes de información
- Técnicas que permitan hacer frente a los cambios en las amenazas para la seguridad

Estas funciones están cada vez más presentes en muchas empresas, pero un firewall de última generación puede aportar mucho más.

NGFW centrado en las amenazas

Este tipo de firewall cuenta con las funciones de un firewall de última generación tradicional y también ofrece detección y remediación de amenazas avanzadas.

Esto es lo que podrá hacer con un NGFW centrado en las amenazas:

- Conocer qué sectores corren más riesgo, gracias a su completa visibilidad del contexto
- Reaccionar rápidamente a los ataques a través de la automatización de una seguridad inteligente que establece políticas y refuerza sus defensas de manera dinámica
- Detectar de manera más efectiva las actividades evasivas o sospechosas gracias a la vinculación de la red y el evento del terminal
- Reducir de manera significativa el tiempo entre la detección y la limpieza a través de una seguridad retrospectiva que monitoriza de manera continua para buscar actividades y comportamientos sospechosos incluso después de una inspección inicial
- Simplifica la gestión y reduce la complejidad gracias a políticas unificadas que aportan protección durante todo el ciclo del ataque

En términos de seguridad, el fabricante Cisco, ofrece las más avanzadas soluciones de seguridad informática a través de sus distintos tipos de Cortafuegos.

Si quieres descubrir más sobre los Firewalls, consulta esta página web:

https://www.cisco.com/c/es_es/products/security/firewalls/what-is-a-firewall.html

Antivirus

Prevenir, identificar o eliminar son las tres posibilidades que se presentan para acabar con un virus y, de acuerdo con ellas, existen tres modelos de antivirus:

- **Antivirus preventores:** se caracterizan por anticiparse a la infección para evitar la entrada de un programa malicioso en el ordenador. Por tanto, su nombre hace referencia a su capacidad de prevenir el ataque de los virus a los sistemas informáticos. No obstante, al almacenarse en la memoria de la computadora, no son los más utilizados, ya que pueden ralentizar el funcionamiento del equipo.

- **Antivirus identificadores:** su función es, como indica su nombre, identificar amenazas que pueden afectar al rendimiento del sistema operativo. Para ello, exploran el sistema y examinan las secuencias de bytes de los códigos que están relacionados con los programas peligrosos.

- **Antivirus descontaminadores:** su objetivo se centra en acabar con la infección que ha dañado el ordenador, eliminación para ello los virus. Asimismo, también trata de devolver al sistema el estado en el que se hallaba antes de ser atacado por el programa malicioso.

Por otro lado, los Antivirus, pueden ejecutarse de diferentes formas, de forma pasiva, que sólo se ejecuta cuando el usuario lo solicita, de forma activa, que está continuamente analizando y buscando bichitos para liquidarlos, incluso al abrir una aplicación, antes de que se abra, lo analiza y si detecta algo impide que se ejecute.

También existen los antivirus online, que son realmente pasivos, pero comienzan a funcionar cuando lo abres, a petición, y requiere internet obviamente.

La ventana de los online es que están totalmente actualizados, aunque los antivirus activos suelen estar también actualizados de forma periódica, salvo el usuario le indique lo contrario al programa.