

MODULO 1: INMERSION

CLASE 1 – BIENVENIDA:

¿QUÉ ES UNA COMPUTADORA?

La **computadora** es un dispositivo electrónico capaz de recibir instrucciones y ejecutarlas.

Las **instrucciones** son dadas por un usuario, por medio de una interfaz que presenta el sistema operativo.

El **sistema operativo** interpreta y ejecuta las instrucciones con los recursos que dispone, que son el hardware y el software.

INTRODUCCIÓN A LA HISTORIA DE LA INFORMÁTICA:

La computadora puede hacer cálculos complejos, procesar datos, interpretar datos, comunicarse con otros dispositivos, y comunicarse con seres humanos.

Programar es ordenarle a la computadora qué, cómo y cuándo hacer algo.



La arquitectura de Von Neumann dio lugar a distintas generaciones de computadoras que nos llevaron hasta el día de hoy:

- 40's: primera generación.
- 60's: transistor-chip.
- 70's: micro-chip.
- 80's: Windows, Apple, Linux.

IBM considera que, en vez de saltar a otra generación de computadoras, desde el 2011 entramos en la **era cognitiva**, donde existen tecnologías como las computadoras cuánticas que pueden ejecutar en 200 segundos cálculos que a una computadora convencional le llevaría 10000 años. Esto demuestra que continuamente se perfeccionan los recursos, acercándonos a la idea de *computadoras capaces de aprender a tomar decisiones por sí solas*.

Esto es conocido como **inteligencia artificial**. Un sistema flexible que percibe el entorno y lleva a cabo acciones que maximicen sus posibilidades de éxito en objetivos o tareas.

GLOSARIO TECNICO:

GLOSARIO TECNICO	
Hardware	<p>Entrada: Son aquellos componentes que permiten el ingreso de información, en general desde alguna fuente externa o por parte del usuario. Proveen el medio fundamental para transferir hacia la computadora (al procesador) información desde alguna fuente, sea local o remota. También permiten cumplir la tarea esencial de leer y cargar en memoria el sistema operativo y los programas informáticos, los que a su vez ponen operativa la computadora y hacen posible realizar las más diversas tareas.</p> <p>Entre los periféricos de entrada se puede mencionar: teclado, mouse, escáner, micrófono, cámara web, joystick, lectoras de CD, DVD o BluRay, entre otros.</p>
	<p>Salida: Son aquellos que permiten dar salida a la información resultante de las operaciones realizadas por la CPU. Los más comunes de este grupo son los monitores, las impresoras, las consolas, y los altavoces.</p> <p>Internos: El hardware interno es el conjunto de componentes físicos que forman parte del dispositivo principal, siendo inseparable de este.</p> <p>En otras palabras, cada parte del hardware interno es una pieza fundamental de cara al funcionamiento correcto del dispositivo. Ya que, si faltara alguna de las partes de este, podría bien no ejecutar alguna tarea e incluso directamente no funcionar.</p> <p>Ejemplos de hardware interno: Placa base, CPU, RAM, GPU, HDD, SSD.</p>
Software	<p>Software de sistema: Desvincula al usuario y al programador de los detalles del sistema informático en particular que se use, transparentando el procesamiento referido a las características internas de: memoria, discos, puertos y dispositivos de comunicaciones, impresoras, pantallas, teclados, etc. El software de sistema le procura al usuario y programador adecuadas interfaces de alto nivel, controladores, herramientas y utilidades de apoyo que permiten el mantenimiento del sistema global. Incluye entre otros:</p> <ul style="list-style-type: none">• Sistemas operativos.• Controladores de dispositivos.• Herramientas de diagnóstico.• Herramientas de corrección y optimización.• Servidores.• Utilidades. <p>Software de programación: Es el conjunto de herramientas que permite al programador desarrollar programas de informática, usando diferentes alternativas y lenguajes de programación, de una manera práctica. Incluyen en forma básica:</p> <ul style="list-style-type: none">• Editores de texto.

	<ul style="list-style-type: none"> • Compiladores. • Intérpretes. • Enlazadores. • Depuradores. • Entornos de desarrollo integrados (IDE). <p>Software de aplicación: Es aquel que permite a los usuarios llevar a cabo una o varias tareas específicas, en cualquier campo de actividad susceptible de ser automatizado o asistido, con especial énfasis en los negocios. Incluye entre muchos otros:</p> <ul style="list-style-type: none"> • Aplicaciones para Control de sistemas y automatización industrial. • Aplicaciones ofimáticas. • Software educativo. • Software empresarial. • Bases de datos. • Telecomunicaciones (por ejemplo, Internet y toda su estructura lógica). • Videojuegos. • Software de diseño asistido (CAD).
Servidores	<p>Servidor web: Almacena documentos HTML, imágenes, archivos de texto, escrituras, y demás material web compuesto por datos (conocidos colectivamente como contenido) y distribuye este contenido a clientes que lo piden en la red.</p> <p>Servidor de base de datos: Provee servicios de base de datos a otros programas u otras computadoras, como es definido por el modelo cliente-servidor. También puede hacer referencia a aquellas computadoras (servidores) dedicadas a ejecutar esos programas, prestando el servicio.</p> <p>Servidor de archivos: Es el que almacena varios tipos de archivos y los distribuye a otros clientes en la red.</p>
Interfaces de Usuarios (UI)	<p>Interfaz de línea de comandos (CLI): Interfaces alfanuméricas (intérpretes de comandos) que solo presentan texto.</p> <p>Interfaz gráfica de usuario (GUI): Permiten comunicarse con la computadora de forma rápida e intuitiva representando gráficamente los elementos de control y medida.</p> <p>Interfaz nativa de usuario (NUI): Pueden ser táctiles, representando gráficamente un "panel de control" en una pantalla sensible al tacto que permite interactuar con el dedo de forma similar a si se accionara un control físico; pueden funcionar mediante reconocimiento del habla, como, por ejemplo, Siri; o mediante movimientos corporales, como es el caso de Kinect.</p>

CLASE 2 – INTERFAZ DE USUARIO (CLI):

VISUAL STUDIO CODE:

Es un **entorno de desarrollo integrado (IDE)** desarrollado por Microsoft.

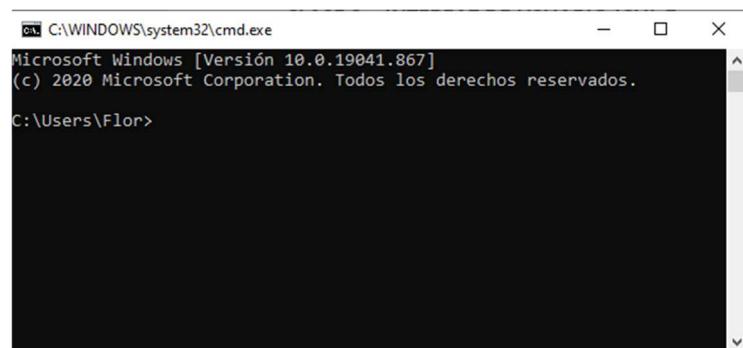
Un IDE es un conjunto de herramientas diseñadas para facilitar la creación y el desarrollo de los programas y aplicaciones.

¿QUÉ ES LA TERMINAL Y PORQUE ES IMPORTANTE?

La **terminal o interfaz de línea de comandos (CLI)** es un programa presente en todos los sistemas operativos, que nos permite darle ordenes a la computadora a través de la ejecución de comandos.

Los comandos son mas rápidos de ejecutar que una interfaz gráfica. Además, suelen ser muy flexibles, permitiendo lograr algo muy complejo de forma sencilla. Otra ventaja que tienen es que siempre funcionan de la misma manera.

En Windows, para abrir la terminal presionamos las teclas Win + R, y en la ventana emergente escribimos el comando “cmd.exe”. La misma se ve de esta manera:



¿QUÉ SON LOS COMANDOS Y CUALES EXISTEN?

Los comandos son instrucciones codificadas para ser interpretadas por un sistema operativo.

Todo comando tiene su propia sintaxis, es decir su manera de ser escrita para que la computadora pueda entender y ejecutar lo que el usuario le especifica por medio del comando.

Debemos tener en claro 2 cosas para ejecutar comandos:

- 1) ¿Cómo se escribe un comando?
- 2) ¿Cómo indicar una ruta?

COMANDOS BASICOS	
ls	[LiSt] En Mac y Linux, muestra los archivos de la carpeta en la que estamos ubicados. En Windows, también, si usamos el PowerShell.
dir	[DIRectories] En Windows, muestra los archivos de la carpeta en la que estamos ubicados.
cd ..	[Change Directory] Nos permite retroceder una carpeta.
rm nombreDeArchivo.extension	[ReMove] Elimina el archivo que le indiquemos (no debemos olvidarnos de escribir la extensión).
mv nombreAnterior nombreNuevo	[MoVe] Cambia el nombre de un archivo por el nombre nuevo que le indiquemos.
clear	Limpia todo lo que hayamos escrito en el terminal.
cd nombreDeCarpeta	[Change Directory] Nos permite acceder a la carpeta que le indiquemos.
mkdir nombreDeCarpeta	[Make Directory] Crea una carpeta con el nombre que le indiquemos.
touch nombreDeArchivo.extension	Crea un archivo de texto con el nombre que le indiquemos (debemos aclarar la extensión). Para PowerShell, usar el comando de abajo.
echo \$null > nombreArchivo.extension	

CLASE 3 – GIT / CLASE 4 - GITHUB:

INTRODUCCION A GIT:

GIT es una tecnología que permite hacer backup de los archivos y compartirlos con equipos de colaboradores. En sí, es un software de control de versiones que mantiene eficientemente las actualizaciones sobre el código fuente.

También lleva un registro de los cambios de los archivos, lo que permite tener un historial completo de versiones de un mismo archivo sin la necesidad de hacer varias copias del mismo.

CONCEPTOS DE GIT	
Repositorio	El repositorio es un almacén de archivos. Si el repositorio es local, se almacena en la computadora, en cambio si es remoto se almacena en GitHub. Para git, el repositorio remoto se llama “ origin ”. Debemos crear un repositorio por cada proyecto que estemos realizando. Cuando creamos repositorios en GitHub, la página nos da una URL única, que nos sirve para conectar el repositorio local con el remoto.
Commits	Son pequeños paquetes donde se almacenan los archivos. Permiten hacer un seguimiento de los cambios que se van realizando porque tienen una fecha de creación y un autor. Es decir, son el historial de cambios de los proyectos.
GitHub	Es el lugar en la nube donde podemos guardar los proyectos.
Ramas	Las ramas dentro del repositorio son copias alternativas dentro del mismo. Funciona como una línea de tiempo paralela a la rama original, a la cual le podemos agregar nuevas funcionalidades sin tener que modificar la línea original. La rama o línea original se llama “ master ”. Es decir, es una rama 2 del proyecto, que luego se puede fusionar o no con la rama original. Son muy utilizadas cuando trabajan muchas personas sobre el mismo proyecto.
COMANDOS DE GIT	
git init	Crea un repositorio local en la computadora. Para eso, nos ubicamos en la carpeta sobre la cual queremos crear el repositorio y ejecutamos el comando git init , el cual crea un repositorio vacío.
git config user.name "xxxxx"	Permite identificarnos en el repositorio. Parados en el repositorio correcto ejecutamos el comando. No nos mostrará texto de respuesta. Si existiera algún error, lo mostrará en la terminal. Luego debemos identificarnos con el correo que utilizamos para registrarnos en GitHub.
git config user.email "xxxxx"	Para verificar ambos pasos accionamos los comandos sin la parte entre comillas. Si es nuestra computadora y no queremos identificarnos siempre, utilizamos git config --global user.name xxxx y git config --global user.email xxxx . Con esto, cualquier repositorio de la computadora tendrá el nombre y e-mail seleccionado.
git add	Se utiliza para indicar que archivos queremos guardar en el repositorio. Si ejecutamos el comando git add . (con un punto), se agregan al repositorio todos los archivos que se encuentran en la ubicación en la que estamos. Cada vez que un archivo se modifica pasa a ser “nuevo”, por lo tanto no tiene seguimiento y hay que agregarlo nuevamente al repositorio.
git status	Nos dice el estado de los archivos, y el estado del mismo respecto al repositorio.
git commit -m "mensaje"	Los commits crean puntos cronológicos que permiten identificar el estado del proyecto hasta ese momento específico, y a su vez, volver sobre el mismo si llegara a ser necesario. El commit es la confirmación a través de la cual decimos al repositorio que los archivos que fuimos agregando los deseamos como un paquete. Este paquete tendrá una marca de tiempo y un autor. En cada estado importante debemos realizar un commit. Para crear un commit primero debemos tener agregados los archivos modificados al repositorio (lo que hacemos con git add), luego ejecutamos el comando git commit -m seguido de un mensaje entre comillas. La idea del mensaje es describir de manera resumida el trabajo hecho hasta el momento.
git log	Nos permite ver un historial de los cambios que hicimos en el proyecto (los commits).
git remote add origin URL	Nos permite conectar el repositorio remoto con el repositorio local. Es decir, le indica al repositorio local con qué repositorio remoto se deberá sincronizar.

git remote -v	Nos permite comprobar si una carpeta esta sincronizada con el repositorio remoto. Nos debería tirar esta respuesta: \$ git remote -v origin - https://github.com/mi-usuario/mi-repositorio.git (fetch) origin - https://github.com/mi-usuario/mi-repositorio.git (push)
git push origin master (puede ser main en vez de master)	Envía los archivos del repositorio local (aquellos que están commiteados) al repositorio remoto. Nos puede pedir el usuario y contraseña. Puede pasar que al momento de querer ejecutar el comando nos veamos restringidos. Esto puede pasar porque otro usuario puede haber realizado cambios. Entonces, lo que debemos hacer es descargar el archivo que contiene los cambios previos desde el repositorio remoto.
git clone URL	Permite crear una copia exacta en la computadora de todos los archivos existentes en un repositorio remoto. Este comando se ejecuta solo la primera vez que se van a descargar los archivos de ese repositorio (cuando los archivos no están en la computadora).
git pull origin master (puede ser main en vez de master)	Permite descargar las actualizaciones y archivos nuevos que haya en el repositorio remoto. No vuelve a descargar todos los archivos del repositorio, sino que lo actualiza. Puede suceder que dos personas hayan estado trabajando al mismo tiempo sobre un mismo archivo. Muchas veces Git resuelve solo ese conflicto haciendo una mezcla (merge) entre los cambios hechos entre todos. Pero si los cambios fueron en el mismo lugar, git no sabe cómo solucionarlo y nos avisa que debemos hacerlo nosotros manualmente. Una vez solucionado el conflicto, volvemos a hacer git add, git commit, y git push.

MODULO 2: HARDWARE Y SOFTWARE

CLASE 5 – ESTRUCTURA Y TECNOLOGIA DE COMPUTADORAS:

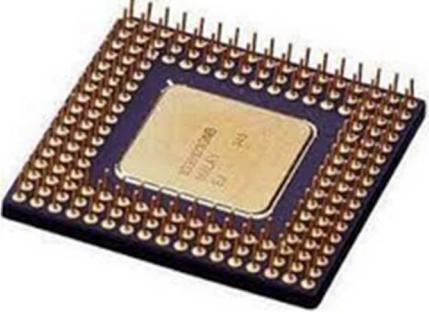
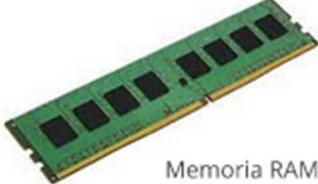
THE BIG PICTURE:

¿Qué características debe tener un dispositivo para ser considerado una computadora?

Una **computadora** es una máquina que recibe datos, los procesa y muestra los resultados, los cuales pueden ser almacenados, transmitidos o impresos.

Por ejemplo: cuando hacemos un clic, la información viaja a través de pulsos eléctricos hacia la computadora a través de medios llamados buses de datos. Los pulsos eléctricos son interpretados como ceros y unos, conocidos como bits. La información que enviamos, es recibida por el cerebro de la computadora, llamada Unidad Central de Proceso (CPU), la cual realiza millones de operaciones por segundos, pero para realizar cualquiera tarea necesita instrucciones. Cuando una petición llega a la CPU, esta debe buscar en la memoria principal las instrucciones necesarias para saber qué debe realizar a continuación. Una vez que tiene las instrucciones, envía la información al dispositivo de salida para que podamos ver reflejado lo que hemos solicitado.

COMPONENTES DE UNA COMPUTADORA	
COMPONENTES INTERNOS	
Son todos los elementos físicos inseparables de la computadora. Si faltara alguno de ellos puede no funcionar o hacerlo de manera incorrecta.	
<h3>Esquema general</h3> <p>Placa madre</p> <p>Procesador o CPU</p> <p>Disco rígido</p> <p>Memoria RAM</p> <p>Memoria ROM</p> <p>Tarjeta de video</p> <p>Tarjeta de sonido</p>	
	<p>Placa madre o motherboard: Es la placa principal de cualquier computadora, al que todos los demás dispositivos se conectan, tanto de manera directa (como circuitos eléctricos interconectados), como indirecta (a través de puertos USB u otro tipo de conectores).</p>

	<p>Procesador: También llamado unidad central de procesamiento (CPU), es el “cerebro” de la computadora. Su función es interpretar y ejecutar las instrucciones a través de operaciones básicas (aritméticas y lógicas). Se encarga de dirigir las operaciones que realiza la computadora.</p>
 Memoria RAM  Memoria ROM	<p>Memoria RAM y ROM: La memoria RAM es el componente que almacena la información de manera temporal. Tiene la particularidad de que el contenido de la misma se elimina cada vez que se apaga la computadora. La memoria ROM almacena información de manera permanente. Guarda todo lo relacionado a la configuración inicial para el arranque de la maquina y el funcionamiento básico.</p>
 Placa de video  Placa de sonido	<p>Placa de sonido y video: Son componentes internos que se conectan a la placa madre. La placa de video es la encargada de mostrar imágenes en el monitor. La placa de sonido permite a la computadora reproducir sonidos a través de auriculares o parlantes. También permite recibir sonidos a través de micrófonos.</p>
	<p>Dispositivo de almacenamiento secundario: Almacena los datos de manera permanente. Es información que la computadora no necesita de manera inmediata para su funcionamiento. Puede almacenar archivos de todo tipo (documentos, imágenes, videos, audios, etc.). El dispositivo de almacenamiento secundario interno es el disco rígido o disco duro.</p>
<h3>COMPONENTES EXTERNOS</h3>	
<p>Son todos aquellos dispositivos que utiliza la computadora, pero que no son imprescindibles para su funcionamiento.</p>	

	<p>Dispositivos periféricos:</p> <p>Son aquellos que se conectan a la CPU para añadir funciones u operaciones a la computadora, pero no son parte esencial de la misma.</p> <p>Pueden ser:</p> <ul style="list-style-type: none"> • De entrada: que introducen los datos a la computadora. • De salida: que extraen los datos de la computadora. • Mixtos: que cumplen ambas funciones. • De almacenamiento: que permiten almacenamiento permanente y se conectan de manera externa. • De comunicación: que permiten la conexión entre computadoras.
--	---

¿QUIÉN PIENSA? – LA CPU:

La CPU es también conocida como unidad central de procesamiento, microprocesador o procesador.

Es el componente más importante de la computadora, ya que su función principal es procesar todas las tareas de la computadora a través de la resolución de instrucciones lógicas y matemáticas que se encuentran almacenadas en la memoria RAM. Para realizar cualquier tarea, CPU necesita saber en qué paso está, que hay que hacer en ese paso, y cuál es el resultado de ese paso. Por lo tanto, la base del funcionamiento de los dispositivos electrónicos es:

- 1) Buscar el próximo paso.
- 2) Leer y ejecutar las instrucciones.
- 3) Obtener el resultado.

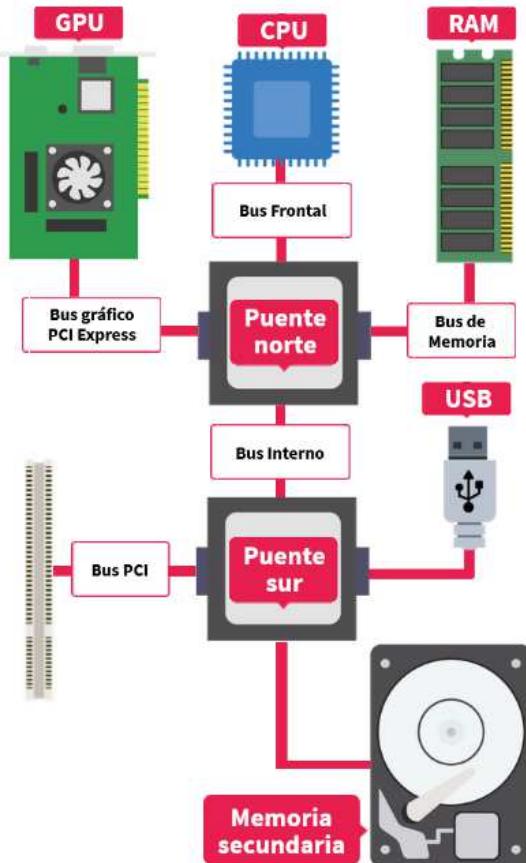
Las características de la CPU que determinan la velocidad en la cual se ejecutan los procesos son:

- **Frecuencia:** velocidad en la cual la CPU estuvo trabajando. Cada tic del reloj esta medido en ciclos por segundos y se expresan en hertz.
- **Núcleos:** Nos permiten tener a disposición más de un procesador para que ejecute tareas a la vez. Dual core, quad core u octa core, hacen referencia a la cantidad de núcleos que el procesador posee.
- **Subprocesos o hilos:** son las cosas que el procesador puede hacer al mismo tiempo.
- **Memoria caché:** nos permite almacenar temporalmente un conjunto de instrucciones que están en la RAM en una memoria interna del procesador. De modo que no debe ir a buscarlas a la memoria, y accede con mayor rapidez.

Arquitectura de Von Neumann:

El procesador necesita comunicarse con muchos elementos. Lee datos e instrucciones de la memoria RAM, requiere de información desde periféricos de entrada y se comunica con periféricos de salida para mostrar los resultados. La arquitectura de comunicación de los componentes se ve de la siguiente manera:

Arquitectura de comunicación entre componentes



GPU:

Una unidad de procesamiento gráfico es un coprocesador dedicado al procesamiento de gráficos para aligerar la carga de trabajo del procesador central en aplicaciones, como los videojuegos o aplicaciones 3D interactivas.

CPU:

La unidad central de procesamiento es el hardware dentro de un ordenador u otros dispositivos programables, su trabajo es interpretar las instrucciones de un programa informático.

RAM:

En la memoria de acceso aleatorio donde se cargan todas las instrucciones que ejecuta la CPU y otras unidades del computador, además de contener los datos que manipulan los distintos programas.

PUENTE NORTE:

Es el chip que controla las funciones de acceso desde y hasta el CPU, PCI-Express, memoria RAM, vídeo integrado (dependiendo de la placa) y el puente sur.

PUENTE SUR:

Es un chip que se encarga de coordinar los diferentes dispositivos de entrada y salida y algunas otras funcionalidades de baja velocidad. No está conectado a la CPU y se comunica con ella indirectamente a través del puente norte.

USB:

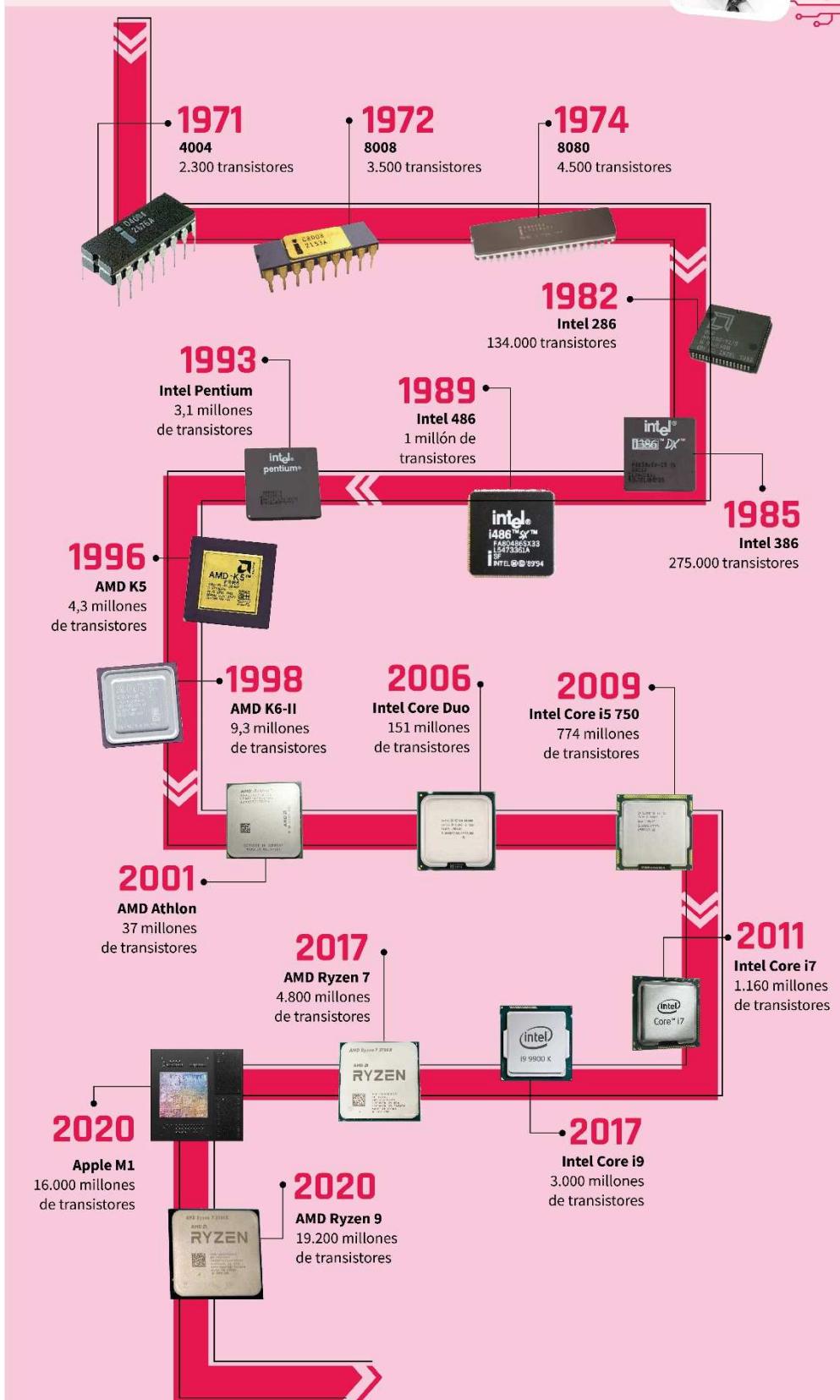
El bus universal en serie es utilizado como estándar para conexión de periféricos. Se puede conectar con el teclado, el mouse, la memoria USB, el joystick, el escáner, la cámara digital, el celular, el reproductor multimedia, la impresora, el módem, la grabadora de DVD externa, el disco duro externo, entre otros.

MEMORIA SECUNDARIA:

Es un tipo de almacenamiento masivo y permanente con mayor capacidad para almacenar datos e información que la memoria primaria (RAM) que es volátil, aunque la memoria secundaria es de menor velocidad.

Evolución de los microprocesadores en el tiempo

La Ley de Moore, establecida en 1965 y reformulada en 1975, afirma que el número de transistores en circuitos integrados se duplicará cada dos años y que la tendencia continuará durante las siguientes décadas.



CLASE 6 – MEMORIAS:

INTRODUCCION A LAS MEMORIAS:

La memoria es la encargada de guardar y procesar información. Está dividida en dos partes:

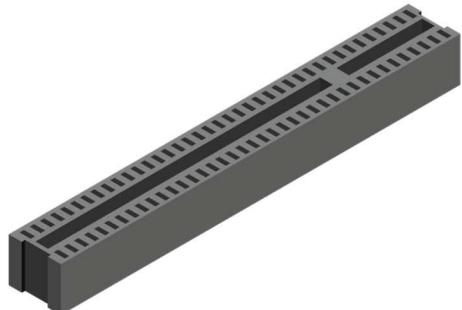
Memoria primaria o principal	Memoria secundaria
Prioriza la velocidad ante el procesamiento. Cuando el procesador desea ejecutar una operación, primero debe cargarla dentro de la memoria principal (la memoria RAM). Estos datos son alojados de manera temporal hasta que el procesador los haya ejecutado. En este caso, al ser una memoria volátil, si pierde energía, todo lo que no se haya pasado a memoria secundaria se pierde. Dentro de esta memoria se encuentra la memoria caché, que es la más veloz, pero tiene muy poca capacidad de almacenamiento.	Lo más importante es la capacidad de almacenamiento no volátil. Es decir, que cuando no hay energía, la información sigue existiendo y no se pierde. Es el conjunto de dispositivos que complementan al sistema de memoria. Para almacenar información, utilizamos 3 tipos de tecnologías: Magnética. Óptica. Estado Solido (SSD).
Características	
Como su nombre lo indica, es la memoria principal de la computadora, se utiliza para almacenar datos o información de forma temporal.	Se refiere a los dispositivos de almacenamiento secundario, donde se puede almacenar información de manera permanente.
El procesador puede acceder directamente a los datos almacenados.	El procesador no puede acceder a los datos de forma directa. Estos deben primero copiarse en la memoria principal para que el procesador pueda leerlos.
Puede ser de tipo volátil o no volátil. En el primer caso, la información solamente se guarda mientras la computadora esté encendida. En el segundo caso, la información permanece, aunque la computadora se apague.	Siempre son de tipo no volátil.
Su capacidad es limitada. Actualmente su capacidad puede llegar hasta los 64 gigabytes.	Puede guardar una gran cantidad de datos e información. Su capacidad llega hasta los terabytes.
El acceso a la memoria principal se realiza a través del bus de datos.	A la memoria secundaria únicamente puede accederse a través de los buses de entrada y salida.
Su velocidad es mayor que la memoria secundaria.	Su velocidad es menor que la primaria.
La memoria primaria tiene un mayor costo que la memoria secundaria.	Su costo es menor que la primaria.
Tipos	
ROM: Es el acrónimo de “read only memory” o memoria de solo lectura. Como el nombre lo sugiere, solo puede ser leída, no escrita. Guarda las instrucciones necesarias para que la computadora pueda iniciarse. CACHÉ: La memoria caché se sitúa entre la CPU y la memoria RAM. La CPU copia en ella los datos más relevantes que va a utilizar de la memoria RAM para acceder a ellos más rápidamente.	MAGNETICOS: Es un dispositivo de almacenamiento que emplea un sistema de grabación magnética para almacenar información. Está formado por uno o más discos que giran a velocidad constante. De este tipo son los discos rígidos o disquetes. OPTICOS: Los datos almacenados en una unidad óptica, pueden ser guardados o leídos a través de un láser. Son dispositivos ópticos los CD y DVD. DE ESTADO SOLIDO:

RAM: Es el acrónimo de “read only memory” o memoria de solo lectura. Como el nombre lo sugiere, solo puede ser leída, no escrita. Guarda las instrucciones necesarias para que la computadora pueda iniciarse.	Es un dispositivo de almacenamiento que no posee partes móviles y que permiten la escritura y lectura en múltiples posiciones en la misma operación mediante pulsos eléctricos. Tipos: discos de estado sólido y memorias.
--	--

La memoria RAM se conecta a la CPU a través de una ranura llamada slot. Este slot posee múltiples pines que conectan la ranura a los módulos de memoria. Una placa madre puede tener más de un slot.

La CPU puede acceder a la memoria RAM a través del:

- **Single channel:** para el acceso a la información en la RAM se utiliza una única señal a un ancho de banda y frecuencia determinada.
- **Dual channel:** Permite el acceso simultáneo a dos módulos de memoria. Para ello, todos los módulos de memoria deben tener la misma capacidad, velocidad, frecuencia, latencia y fabricante.



Características de las memorias RAM:

- **Velocidad:** las computadoras electrónicas digitales no tenían sistema operativo. Los programas, por lo regular, manejaban un bit a la vez, en columnas de switchs mecánicos. Los programas de lenguaje máquina manejaban tarjetas perforadas.
- **Capacidad:** es la cantidad de datos que se pueden almacenar en una RAM. La capacidad se mide en gigabytes (GB).
- **Latencia:** es la cantidad de ciclos de reloj que transcurren entre una petición y su respuesta.
- **Voltaje:** El voltaje hace referencia a la energía consumida por el módulo de RAM.

Dual channel: ¿Cómo se mide la velocidad y capacidad en las memorias?

- Las velocidades se suman > Si la velocidad de cada módulo es de 1600 Mhz, la velocidad total será de 3200 Mhz.
- La capacidad se suma > Si cada módulo tiene una capacidad de 8 GB, la capacidad total será de 16 GB.

¿Cómo afecta la latencia al tiempo total de ejecución de una tarea?

Comparemos la velocidad de acceso a distintos componentes al tiempo humano y a la distancia.

Acción de la computadora	Latencia	Tiempo humano	Distancia
CPU 3Ghz	0,3 nanosegundos	1 segundo	10 centímetros
Caché L1	0,9 nanosegundos	3 segundos	30 centímetros
Caché L2	2,8 nanosegundos	9 segundos	85 centímetros
Caché L3	12,9 nanosegundos	43 segundos	4 metros
RAM	70 - 100 nanosegundos	3,5 a 5,5 minutos	20 a 30 metros
SSD (disco sólido)	7-150 microsegundos	2h a 2 días	2 a 45 kilómetros
Disco rígido	1-10 milisegundos	11 días a 4 meses	304 a 3000 kilómetros

Internet de San Francisco a Australia	183 milisegundos	6 años	24 veces la distancia a la Luna.
Reboot sistema completo	90 segundos	3 milenios	2 veces la distancia a Marte

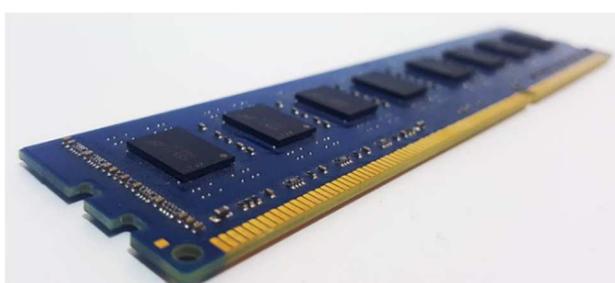
UNIDADES DE MEDIDA:

Todo dispositivo de almacenamiento o incluso la memoria principal de la computadora tiene cierto tamaño.



MEMORIA PRINCIPAL:

RAM es el acrónimo de random access memory (memoria de acceso aleatorio). La información almacenada en este tipo de memoria se pierde cuando se desconecta la alimentación del PC o del portátil. Se conoce generalmente como memoria principal o memoria temporal o volátil del sistema informático. Es el lugar donde se almacenan temporalmente tanto los datos como los programas que la CPU está procesando, o va a procesar, en un determinado momento.



La Random Access Memory (RAM), es la memoria de acceso aleatorio y forma parte de la memoria principal. Es un circuito integrado que almacena los datos, programas o información mientras la usamos, y cuando dejamos de hacerlo pasan a una memoria secundaria liberando el espacio que ocupaba.

Al ser una memoria aleatoria puede saber dónde se encuentran los datos e ir directamente a ellos.

Es volátil, por lo tanto, si se queda sin energía, pierde toda la información y se inicia desde cero.

¿Por qué el proceso con la memoria RAM es tan veloz?

A través de los buses se envían datos en binario, los cuales se transmiten con una cierta frecuencia. El ritmo de los mensajes es manejado por el reloj, que le dice a la RAM cada cuánto se envían los datos.

Cuando constantemente le solicitamos a la memoria RAM el mismo tipo de datos e instrucciones, la información se almacena en una memoria intermedia llamada **caché**. La información de esta memoria se guarda en niveles de la cache: L1, L2, L3 y L4. Cada uno de estos niveles es más grande que el anterior, y pueden o no guardar la misma información que el nivel anterior. Es decir que cuando el procesador necesita información empieza buscando en las memorias más cercanas y rápidas que tenga, y si no lo encuentra, buscará en la memoria RAM.

Las memorias caché son muy caras de fabricar y entre más veloces sean más costosas son de producir.

Dentro del procesador, la información se carga dentro de celdas muy diminutas, y la unión de éstas forma un registro, el cual es el primer y más pequeño paso en el eslabón de las memorias y la información.

El ordenador tiene varias memorias y componentes funcionando al mismo tiempo, y la comunicación entre ellas es la que condiciona el rendimiento. Cuando una de las memorias o componentes frena el rendimiento de la computadora, se produce un **cuello de botella** que implica que el sistema no tiene la suficiente cantidad de memoria o la velocidad necesaria. Esta situación recorta la velocidad a la que la **RAM** puede servir de información al procesador, lo que ralentiza el funcionamiento global.

Registros de la CPU:

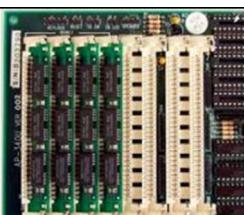
Un registro es una memoria de muy alta velocidad, que se utiliza en los procesadores para acceder a información importante de manera rápida. La CPU tiene 5 registros internos:

- 1) PC: program counter.
- 2) IR: instructions register.
- 3) MAR: memory address register.
- 4) MDR: memory data register.
- 5) Accumulator.

Caché de la CPU:

Es un apoyo importante para el procesador que se divide en un total de tres niveles generales al que podemos sumar un cuarto que no resulta nada común. La diferencia entre memoria caché L1, L2 y L3 obedece a un orden de jerarquía establecido por cercanía al procesador, velocidad y capacidad.

Tipos de RAM:



FPM RAM (Fast Page Mode): el modo de página rápida es un tipo de memoria RAM que espera durante todo el proceso de localización de un bit de datos por columna y fila; y luego lee el bit antes de comenzar con el siguiente. La velocidad máxima de transferencia es de unos 176 Mbps.

	SDR RAM (Single Data Rate): es una forma completa de memoria de acceso dinámico sincrónico. Tiene tiempos de acceso entre 25 y 10 ns (nanosegundos) y están en módulos DIMM (módulo de memoria dual en línea) de 168 contactos.
	RD RAM (Rambus): la memoria dinámica de acceso aleatorio rambus es una forma completa de RDRAM. Este tipo de chips de RAM funciona en paralelo, lo que permite alcanzar una velocidad de datos de 800 Mhz o 1600 Mbps. Genera mucho más calor al funcionar a tan altas velocidades.
	V RAM (Video): es la memoria RAM optimizada para adaptadores de video. Tiene dos puertos para que los datos de video puedan escribirse al mismo tiempo que el adaptador de video lee regularmente la memoria para refrescar la pantalla actual del monitor.
	EDO RAM (extended data output): en castellano su sigla significa salida de datos extendida. No espera a que finalice el procesamiento del primer bit para continuar con el siguiente. En cuanto se localiza la dirección del primer bit, la EDO RAM comienza a buscar el siguiente.
	DDR RAM: lanzada en el año 2000, aunque no empezó a usarse hasta casi el año 2002. Operaba a 2.5V y 2.6V y su densidad máxima era de 128 Mb (por lo que no había módulos con más de 1 GB) con una velocidad de 266 MT/s (100-200 Mhz).
	DDR2 RAM: lanzada en 2004, funcionaba a un voltaje de 1.8 voltios, un 28% menos que DDR. Se dobló su densidad máxima hasta los 256 Mb (2 GB por modulo). Lógicamente la velocidad máxima también se multiplicó, llegando a 533 Mhz.
	DDR3 RAM: se lanzó en 2007 y supuso toda una revolución porque aquí se implementaron los perfiles XMP. Para empezar los módulos de memoria operaban a 1.5V y 1.65V, con velocidades base de 1066 Mhz pero que llegaron mucho más allá, y la densidad llegó hasta 8GB por módulo.
	DDR4 RAM: lanzada en 2014. Se reduce el voltaje a 1.05V y 1.2V, aunque muchos módulos operan a 1.35V. La velocidad se ha visto notablemente incrementada pero su base comenzó en los 2133 Mhz. Actualmente ya hay módulos de 32 GB, pero esto también se va ampliando poco a poco.
	DDR5 RAM: lanzada a mediados del 2020, llega a anchos de banda de hasta 6.4 Gbps en sus modelos iniciales. Es la primera memoria DDR de doble canal en un solo chip. Su frecuencia base es de 4800 Mhz, y además su consumo baja por la clásica reducción de voltaje, esta vez a 1.1V. Su capacidad de almacenamiento máxima en un módulo de memoria es de 128 GB.

MEMORIA SECUNDARIA:

¿Cómo funciona la memoria de la computadora?

El dígito binario o bit es la mínima unidad de información donde se puede guardar un dato, y solo puede aceptar valores 0 y 1. A su vez, los bits se pueden agrupar en estructuras de 8 celdas conocidas como byte,

que constituyen una unidad direccional de memoria. Esta agrupación ayuda a interpretar lo que es el archivo en sí.

La memoria secundaria es la más lenta, pero más segura a la hora de almacenar información. En sus inicios era conocida como memoria ROM (Read Only Memory), ya que su función era contener información que no podía modificarse, es decir, contenía archivos solo de lectura.

En la actualidad, la memoria secundaria sigue trabajando bajo ese concepto, pero con los avances se permitió borrar o sobrescribir la información que tenía guardada, aunque siga resultado muy costoso en cuestión de tiempo para el procesador en comparación con la memoria primaria, y es por esta razón que se evita utilizarla a menos que sea necesaria.

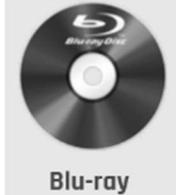
Dentro de la memoria secundaria existen 3 tipos principales de tecnologías que permiten guardar información a largo plazo:

- 1) **Magnética (HDD):** los datos se guardan según un patrón magnético en un disco giratorio que se encuentra cubierto por una membrana magnética. Son las más baratas en construir, pero son las más lentas debido a sus limitaciones físicas.
- 2) **Óptica:** los bits se codifican como puntos de luz y puntos sin luz, elevando la velocidad de lectura, aunque sean limitados por su capacidad de almacenamiento.
- 3) **Sólida (SSD):** trabajan a través de transistores que atrapan o eliminan cargas eléctricas dentro de su estructura. Son las más veloces, pero las más costosas de fabricar.

Los dispositivos de memoria, al ser dispositivos físicos, tienden a desgastarse, por lo cual es importante tener la información más importante respaldada y segura ante cualquier eventualidad.

Dentro de los tipos de memoria secundaria principales, existen diferentes dispositivos que fueron apareciendo a medida que la tecnología avanzaba. A continuación, vamos a ver algunos de los que causaron mayor impacto:

MAGNETICO	 Cinta magnética	Es un tipo de medio o soporte de almacenamiento de datos que se graba en pistas sobre una banda plástica con un material magnetizado, generalmente óxido de hierro o algún cromato. El tipo de información que se puede almacenar en las cintas magnéticas es variado, puede ser vídeo, audio o datos.
	 Diskette	Dispositivo de almacenamiento utilizado para transportar información de una PC a otra, su capacidad podía llegar hasta 2,88 Mb. Los más utilizados eran los de 3 1/2 —llamados así debido a su apariencia física—. Destacaban los discos ZIP. Eran muy utilizados hasta la aparición de la memoria flash.
	 Discos duros	El disco duro está formado por uno o varios platos rígidos introducidos en una caja hermética y unidos por un eje común que gira a gran velocidad. Sobre cada uno de los patos, que normalmente tienen sus dos caras destinadas al almacenamiento, se sitúan sendos cabezales de lectura/escritura.
OPTICO	 CD	El disco compacto (compact disc) es un medio óptico que se usa para almacenar datos en formato digital, ya sean imágenes, videos, audio, documentos, como otros datos. En un principio esta tecnología fue usada para el CD audio, pero más tarde se expandió y adaptó para el almacenamiento de datos (lo que conocemos como CD-ROM), de video (conocido como VCD Y SVCD), la grabación doméstica (llamada CD-R y CD-RW). El CD puede almacenar hasta 80 minutos de audio o, lo que es igual, 700 MB de datos.

		Significa "disco digital versátil". Es un disco óptico capaz de almacenar contenidos de medios. Los DVDs vienen en múltiples tipos y capacidades de almacenamiento; pueden tener uno o dos lados, una sola capa o dos capas, todas dictando la cantidad de contenidos de medios que el DVD puede almacenar. Las capacidades de almacenamiento de los DVDs van desde 1,46 GB en un DVD de un solo lado y una capa a 17,08 GB en un DVD de dos lados y dos capas. Las variaciones de DVD también consisten en DVD-R, DVD+R, DVD-RW, DVD+RW y DVD-Ram que describen la manera en la que el contenido de medios se almacena en el disco. DVD-R y DVD+R son capaces de ser escritos con datos (audio, video, entre otros) solamente una vez, mientras que DVD-RW, DVD+RW y DVD-Ram son capaces de ser escritos, borrados y reescritos múltiples veces.
		Es un formato de disco óptico, una evolución del CD y el DVD. Al igual que estos, tiene el mismo tamaño y aspecto externo, pero multiplica la capacidad del disco. En un Blu-ray de una sola capa podemos almacenar unos 25 GB de información. En un volumen como este pueden caber unos 27.000 minutos de música en formato MP3. Esto en una sola capa porque otra de las virtudes más interesantes de este formato es que puede admitir varias, multiplicando su capacidad. Así, podemos encontrar discos Blu-ray de hasta 100 GB de capacidad.
SOLIDO		Es un dispositivo en forma de tarjeta, que se encuentra orientado a realizar el almacenamiento de grandes cantidades de datos en un espacio reducido, permitiendo la lectura y escritura de múltiples posiciones de memoria en la misma operación. Todo esto gracias a impulsos eléctricos.
		Es un dispositivo portátil de almacenamiento, compuesto por una memoria flash, accesible a través de un puerto USB. Su capacidad varía según el modelo, y en la actualidad podemos encontrar en el mercado pendrives con una capacidad de hasta 256 Gb en un mínimo espacio. Es considerado la sucesión de los viejos diskettes dada su gran capacidad de almacenamiento y compatibilidad con diferentes dispositivos.
		Es un dispositivo que almacena datos. Su nombre significa disco de estado sólido, haciendo alusión a dispositivos que no tienen ni un solo movimiento mecánico en su interior, al contrario que los HDD. Los SSD de hoy en día utilizan el bus SATA o el PCIe del ordenador (discos ssd M2), siendo los últimos más rápidos que los primeros dado que un SSD normal encuentra un cuello de botella en el bus SATA ya que un SSD ofrece velocidades superiores a las que ofrece el bus SATA 3.

FORMAS DE ALMACENAMIENTO DE DATOS:

Sistema numérico:

El sistema de numeración es un conjunto de símbolos y reglas de generación que permiten construir todos los números validos en el sistema.

Dentro del sistema numérico se pueden hacer dos grandes divisiones:

- 1) **Sistema numérico no posicional:** son aquellos en los cuales el valor de los símbolos que componen el sistema es fijo, no depende de la posición, por ejemplo: el sistema romano.
- 2) **Sistema numérico posicional:** son aquellos donde el valor del símbolo depende del valor que se les ha asignado y de la posición que ocupa el símbolo.

El **dígito** es cada uno de los símbolos diferentes que constituyen el sistema de numeración.

Definimos como base del sistema de numeración a la cantidad de dígitos que lo conforman.

Ejemplo: Este sistema está formado por diez símbolos, los dígitos del 0 al 9. Por lo tanto, estaremos frente a una base 10. Una vez agotada la cantidad de dígitos que forman al sistema de numeración, las cantidades mayores a la base se obtienen combinando en forma adecuada los diferentes dígitos del sistema. Esto hace que cada uno de los dígitos adopte distintos valores según la posición que ocupe.

$$3434_{10} = 3000 + 400 + 30 + 4$$

Una forma más clara es si expresamos en número en función de su base 10.

$$3434_{10} = 3 \cdot 10^3 + 4 \cdot 10^2 + 3 \cdot 10^1 + 4 \cdot 10^0$$

También podemos representar números decimales en sistema posicional.

$$3434.25_{10} = 3 \cdot 10^3 + 4 \cdot 10^2 + 3 \cdot 10^1 + 4 \cdot 10^0 + 2 \cdot 10^{-1} + 5 \cdot 10^{-2}$$

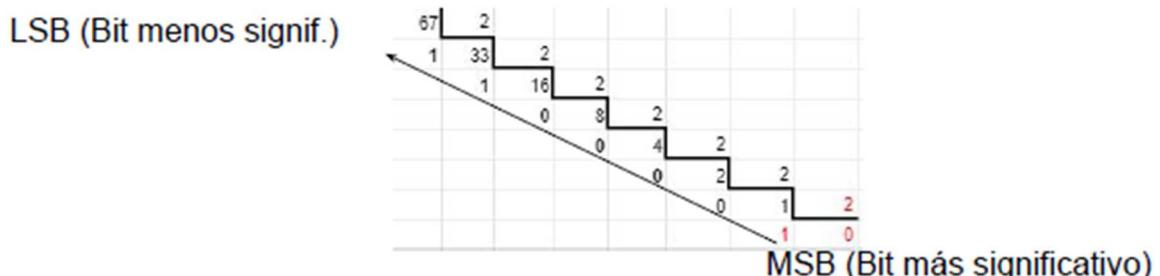
Sistema binario:

El **sistema binario** es un sistema de numeración que está formado por dos símbolos, los dígitos son representados utilizando dos cifras: 0 y 1.

Conversión de base 10 a binario:

Podemos convertir cualquier número decimal a otra base mediante el siguiente método, lo veremos con un ejemplo 67_{10} a base 2 (binario).

Tomamos el número y calculamos los residuos de sucesivas divisiones enteras por la base de llegada:



Al tener en cuenta el sentido (der. a izq.), tenemos: $67 = 10000112$

Podemos verificarlo:

$$1000011_2 = 1 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 67$$

Conversión a otras bases

Siguiendo el ejemplo anterior podemos convertir el 67_{10} a base 16 (Hexadecimal) y base 8 (octal).

$$10000011_2 = 001 - 000 - 011 = 103_{10}$$

1 0 3

$$10000011_2 = 0100 - 0011 = 43_{16}$$

4 3 |

Decimal	Binario	Hexadecimal	Octal
0	0000	0	0
1	0001	1	1
2	0010	2	2
3	0011	3	3
4	0100	4	5
5	0101	5	6
6	0110	6	7
7	0111	7	
8	1000	8	
9	1001	9	
10	1010	A	
11	1011	B	
12	1100	C	
13	1101	D	
14	1110	E	
15	1111	F	

FRAGMENTACION, SEGMENTACION Y PAGINACION:

1. ¿Qué es la fragmentación?

Llamamos fragmentación al espacio que queda desperdiciado al momento de usar los métodos de partición de memoria.



Se genera cuando, durante el reemplazo de procesos, quedan huecos entre dos o más procesos de manera no contigua y cada hueco no se puede ocupar con algún proceso de la lista de espera. Quizás, si unimos todos los huecos, sí sea espacio suficiente, pero se requeriría de un proceso de desfragmentación de memoria o compactación para lograrlo. Esta fragmentación se denomina fragmentación externa.

La fragmentación interna es generada cuando se reserva más memoria de la que el proceso va realmente a usar. Se debe de esperar a la finalización del proceso para que se libere el bloque completo de la memoria.

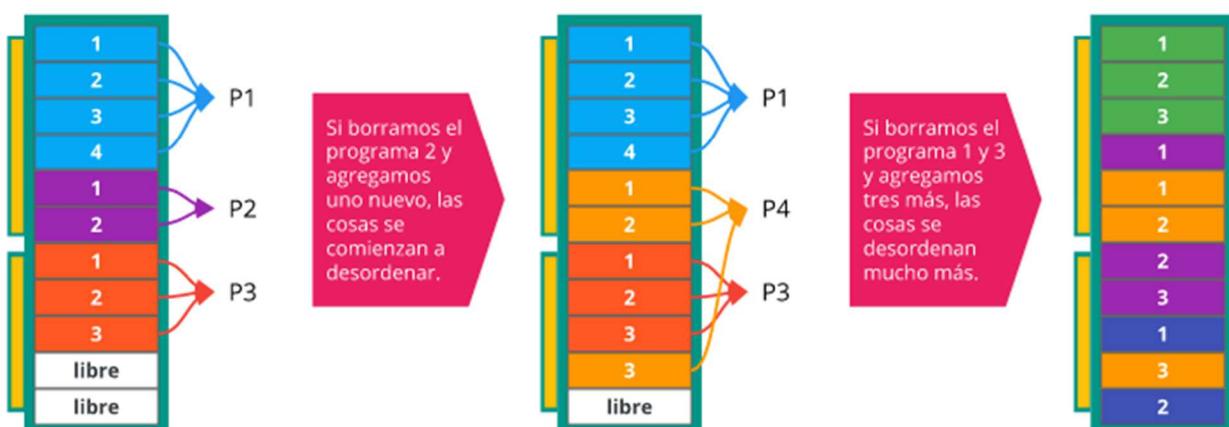
2. ¿Qué es la segmentación?

Es otra técnica de gestión de memoria que pretende acercarse más al punto de vista del usuario.

Los programas se desarrollan en torno a un núcleo central desde el que se bifurca a otras partes o se accede a zonas de datos. Desde este punto de vista, un programa es un conjunto de componentes lógicos de tamaño variable o un conjunto de segmentos, es decir, el espacio lógico de direcciones se considera como un conjunto de segmentos, cada uno definido por su tamaño y un número.

La segmentación de un programa la realiza un compilador y en ella cada dirección lógica se expresará mediante dos valores: **número de segmento (s)** y **desplazamiento dentro del segmento (d)**.

¿Qué es la segmentación?



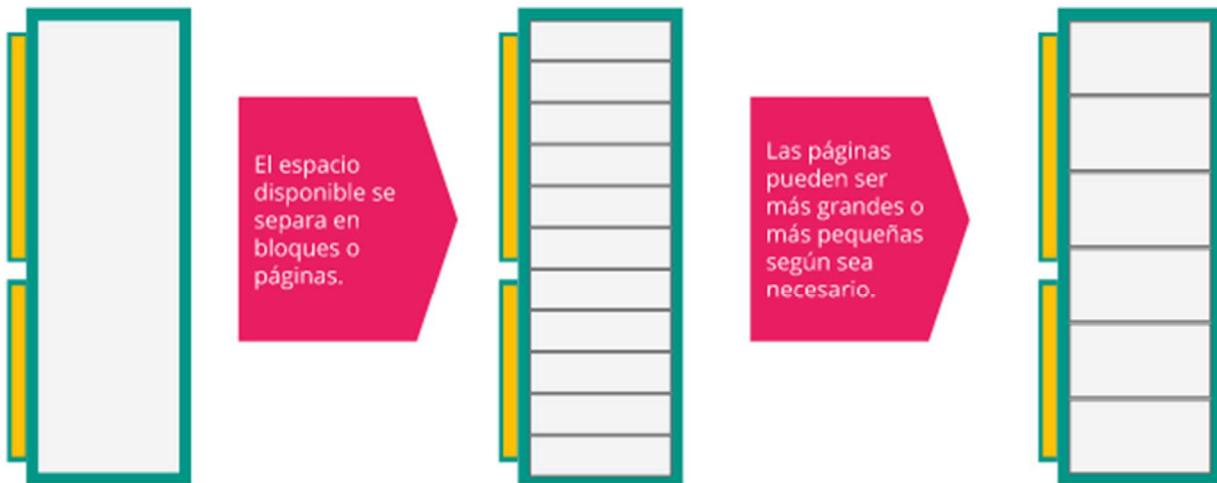
3. ¿Qué es la paginación?

La paginación es una técnica de gestión que permite asignar la memoria de forma discontinua. Con este fin, se divide la memoria en trozos de tamaño fijo llamados **armazones** o **frames** y la lógica en bloques de igual tamaño denominados **páginas**. El sistema operativo mantiene internamente una tabla de páginas donde se relaciona cada página cargada en memoria con el frame que la contenga, es decir, su dirección inicial en memoria real.

El sistema operativo analizará cada nuevo trabajo que se disponga a entrar para conocer el número de páginas que ocupa y buscará en su lista de frames libre un número igual de ellos. Si estos existen, cargará en ellos las páginas del programa y construirá la correspondiente tabla de páginas, actualizando la lista de frames libres. Cada trabajo en memoria tendrá su propia tabla de páginas apuntada por el bloque de control del proceso.

De esta manera, se logra evitar la fragmentación externa ya que cualquier frame libre es assignable a un trabajo que lo necesite. Por otro lado, seguirá existiendo fragmentación interna puesto que, los trabajos no ocuparán un tamaño múltiplo del tamaño de la página.

¿Qué es la paginación?



CLASE 7 – SISTEMAS OPERATIVOS:

SISTEMAS OPERATIVOS:

El **sistema operativo** es el soporte lógico que controla el funcionamiento del equipo físico. Es decir, el sistema de comunicación usuario-dispositivo que comprende un conjunto de programas. Se encarga de administrar los recursos ofrecidos por el hardware, y actúa como intermediario entre la computadora y usuario ofreciendo un ambiente amigable y sencillo de interpretar.

El SO empieza a funcionar en el momento en que encendemos nuestro dispositivo y deja de funcionar cuando lo apagamos. Podemos encontrarlo en gran parte de los aparatos tecnológicos que utilizan microprocesadores para funcionar, como ser computadoras, celulares o heladeras inteligentes.

Recursos administrados por el SO:

- Gestiona la **memoria** de acceso aleatorio y ejecuta las aplicaciones, designando los recursos necesarios.
- Administra la **CPU** gracias al algoritmo de programación.

- Direcciona las **entradas y salidas de datos** (a través de drives), por medio de los periféricos de entrada y salida.
- Administrar la **información** para el buen funcionamiento de la PC.
- Dirigir las **autorizaciones** de uso para el usuario.
- Administrar los **archivos**.

En el caso de los servidores, también se encuentran sistemas operativos mayormente heredados de UNIX como Red Hat, también está Windows Server diseñado específicamente para computadoras.

Los sistemas operativos de servidores son multiusuarios, lo cual significa que varios usuarios están conectados al mismo tiempo trabajando sobre el mismo núcleo, en cambio en las computadoras domésticas tienden a ser monousuarios.

Clasificación de los SO:

- **Open source:** permiten usar, modificar y adaptar un sistema operativo a voluntad de usuario. Por ejemplo: Ubuntu y Red Hat.
- **Proprietary software:** son de propietario y posee limitaciones que no permiten modificaciones. Por ejemplo: Windows.
- Según los usuarios:
 - ✓ **Multiusuario:** SO que permite que varios usuarios ejecuten simultáneamente sus programas.
 - ✓ **Monousuario:** SO que permite ejecutar los programas solamente de un usuario por vez.
- Según la gestión de tareas:
 - ✓ **Multitarea:** SO que puede ejecutar varios procesos al mismo tiempo.
 - ✓ **Monotarea:** SO que permite ejecutar un solo proceso a la vez.
- Según la gestión de recursos:
 - ✓ **Centralizado:** SO que permite utilizar los recursos de un solo ordenador.
 - ✓ **Distribuido:** SO que permite ejecutar los procesos de más de un ordenador al mismo tiempo.

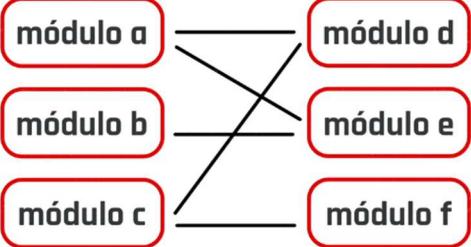
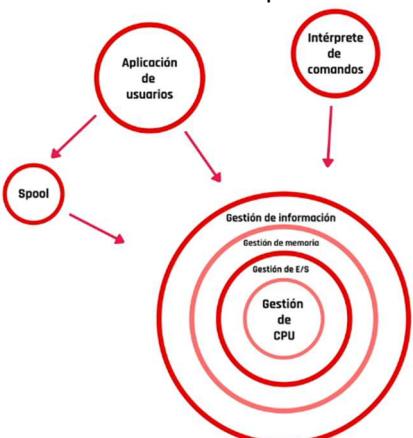
Generaciones de sistemas operativos:	
Generación Cero (década de 1940)	 Las computadoras electrónicas digitales no tenían sistema operativo. Los programas, por lo regular, manejaban un bit a la vez, en columnas de switchs mecánicos. Los programas de lenguaje máquina manejaban tarjetas perforadas.
Primera generación (1945-1955)	 Tubos de vacío y tableros enchufables: Se lograron construir máquinas calculadoras usando tubos de vacío. Estas máquinas eran enormes y ocupaban cuartos enteros con decenas de miles de tubos de vacío, pero eran mucho más lentas que incluso las computadoras personales más baratas de la actualidad. Toda la programación se realizaba en lenguaje de máquina absoluto.

<p>Segunda generación (1955-1965)</p> 	<p>Transistores y sistemas de lote: Estas máquinas se encerraban en cuartos de computadora con acondicionamiento de aire especial. Para ejecutar un programa, un programador escribía primero el programa en papel (en FORTRAN o ensamblador) y luego lo perforaba en tarjetas. Después, llevaba el grupo de tarjetas al cuarto de entrada y lo entregaba a uno de los operadores. Cuando la computadora terminaba el trabajo que estaba ejecutando en ese momento, se separaba la salida impresa y se llevaba al cuarto de salida donde el programador podía buscarla. Luego, el operador tomaba uno de los grupos de tarjeta traídos del cuarto de entrada y lo introducía en el lector. Si se requería el compilador de FORTRAN, el operador tenía que traerlo de un archivero e introducirlo en el lector. Dado el alto costo del equipo, la solución que se adoptó generalmente fue el sistema por lotes. El principio de este modo de operación consistía en juntar una serie de trabajos en el cuarto de entrada, leerlos y grabarlos en una cinta magnética usando una computadora pequeña y (relativamente) económica. Después de cerca de una hora de reunir un lote de trabajos, la cinta se rebobinaba y se llevaba al cuarto de la máquina, donde se montaba en una unidad de cinta. El operador cargaba entonces un programa especial, que leía el primer trabajo de la cinta y lo ejecutaba. La salida se escribía en una segunda cinta, en lugar de imprimirse. Cada vez que terminaba un trabajo, el sistema operativo leía automáticamente el siguiente trabajo de la cinta y comenzaba a ejecutarlo.</p>
<p>Tercera generación (1965-1970)</p> 	<p>Circuitos integrados (CI) y multiprogramación: Las máquinas diferían solo en el precio y el rendimiento (memoria máxima, velocidad del procesador, número de dispositivos de E/S permitidos, entre otros). IBM trató de resolver simultáneamente ambos problemas introduciendo la System/360, puesto que todas las máquinas tenían la misma arquitectura y conjunto de instrucciones, los programas escritos para una máquina podían ejecutarse en todas las demás, al menos en teoría. Los 360 y los sistemas operativos de tercera generación parecidos a él producidos por otros fabricantes de computadoras lograron satisfacer a sus clientes en un grado razonable y también popularizaron varias técnicas clave que no existían en los sistemas operativos de la segunda generación. Tal vez la más importante de ellas haya sido la multiprogramación. El problema era el tiempo de espera, la solución a la que se llegó fue dividir la memoria en varias secciones, con un trabajo distinto en cada partición. Mientras un trabajo estaba esperando que terminara su E/S, otro podía estar usando la CPU. Si se podían tener en la memoria principal suficientes trabajos a la vez, la CPU podía mantenerse ocupada casi todo el tiempo. También, tenían la capacidad de leer trabajos de las tarjetas al disco tan pronto como se llevaban al cuarto de computadoras. Luego, cada vez que un trabajo terminaba su ejecución, el sistema operativo podía cargar uno nuevo del disco en la partición que había quedado vacía y ejecutarlo.</p>

Cuarta generación (1980- a nuestros días) 	<p>Computadoras personales:</p> <p>Con la invención de los circuitos integrados a gran escala (LSI), chips que contienen miles de transistores en un cm² de silicio, nació la era de la computadora personal.</p> <p>Dos sistemas operativos dominaron inicialmente el campo de las computadoras personales y las estaciones de trabajo: MS-DOS de Microsoft y UNIX. MS-DOS se usaba ampliamente en la IBM PC y otras máquinas basadas en la CPU Intel 8088 y sus sucesoras. Más tarde, la Pentium y Pentium Pro. Aunque la versión inicial de MS-DOS era relativamente primitiva, versiones subsecuentes han incluido características más avanzadas, muchas de ellas tomadas de UNIX. El sucesor de Microsoft para MS-DOS, Windows, originalmente se ejecutaba encima de MS-DOS, pero a partir de 1995 se produjo una versión autosuficiente de WINDOWS.</p> <p>El otro competidor importante es UNIX, que domina en las estaciones de trabajo y otras computadoras del extremo alto, como los servidores de red. UNIX es popular sobre todo en máquinas basadas en chips RISC de alto rendimiento.</p>
---	--

CLASIFICACION Y COMPARACION:

CLASIFICACION Y CARACTETRISTICAS DE LOS SISTEMAS OPERATIVOS		
Gestión de usuario	Multiusuario	<p>Pueden brindar servicios a varios usuarios al mismo tiempo, ya sea por medio de terminales conectadas a la computadora o por sesiones remotas en una red de comunicación. Ejemplos:</p> <ul style="list-style-type: none"> • Windows (a partir de XP). • Unix. • Linux. • Mac OSX. • Solaris.
	Monousuario	<p>Soportan solo a un usuario a la vez sin importar cuantos procesadores tiene la computadora, o cuantas tareas realice el usuario, solo podrá dar servicio a uno. Ejemplos:</p> <ul style="list-style-type: none"> • Windows (hasta Me). • DOS.
Gestión de tareas	Multitarea	<p>Son SO que permiten realizar varias tareas al mismo tiempo, son mucho más comunes. Ejemplos:</p> <ul style="list-style-type: none"> • Windows. • Unix. • Linux. • Mac OSX.
	Monotarea	<p>Sistemas operativos que realizan solo una tarea a la vez sin que se pueda interrumpir. Son los más primitivos. Por ejemplo: si queremos imprimir un archivo en estos SO, no vamos a poder realizar ninguna otra tarea hasta que la computadora imprima y pueda recibir otra instrucción. Ejemplos:</p> <ul style="list-style-type: none"> • DOS. • Windows Me. • Windows Vista.
Gestión de recursos	Centralizado	Es aquel que utiliza los recursos de una sola computadora, es decir, su memoria, CPU, disco y periféricos. Ejemplos:

		<ul style="list-style-type: none"> • Windows • Linux • Mac OSX • Unix
	Distribuido	<p>Según Tanenbaum, un sistema distribuido es "una colección de computadoras independientes que aparecen ante los usuarios del sistema como una única computadora. De eso podemos entender que las máquinas son autónomas y los usuarios siempre piensan que el sistema es como una única computadora. Un sistema distribuido se caracteriza por comportarse frente al usuario como una sola máquina; el usuario desconoce sobre qué procesador se está ejecutando sus procesos y dónde residen sus ficheros. Ejemplos:</p> <ul style="list-style-type: none"> • Novell Netware • Windows Server • Cisco IOS • Unix • Linux
	Monolítica	<p>Están constituidos por un solo programa compuesto por una serie de rutinas entrelazadas entre sí, de tal forma que pueden comunicarse entre ellas. Suelen ser SO hechos a medida, con lo cual son muy rápidos, pero no tienen flexibilidad para soportar distintos tipos de aplicaciones.</p>  <pre> graph TD a[módulo a] --- d[módulo d] b[módulo b] --- e[módulo e] c[módulo c] --- f[módulo f] d --- e d --- f e --- f </pre> <p>Ejemplos:</p> <ul style="list-style-type: none"> • VMS. • Linux. • Multics. • Windows (hasta Me).
Estructura interna	Jerárquica	<p>A medida que fueron creciendo las necesidades de los usuarios y se perfeccionaron los sistemas, fue necesario una mayor organización del software del SO, donde una parte del sistema contenía sub-partes y se organizaba en forma de niveles.</p> <p>La estructura jerárquica subdivide en capas o anillos perfectamente definidos y con una clara interfaz con respecto al resto de los recursos.</p>  <pre> graph TD A[Aplicación de usuarios] --> Spool((Spool)) A --> I[Intérprete de comandos] Spool --> G[Gestión de información] I --> G G --> GM[Gestión de memoria] G --> GE[Gestión de E/S] G --> GC[Gestión de CPU] </pre>

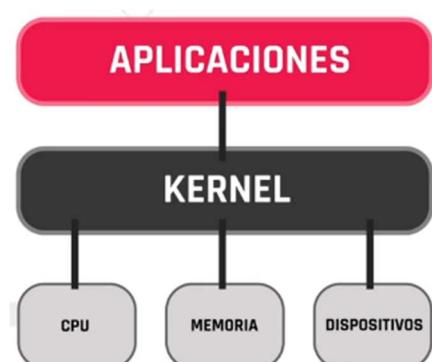
		<p>Ejemplos:</p> <ul style="list-style-type: none"> • Unix. • Multics.
	Máquina virtual	<p>En estos sistemas operativos se separan la multiprogramación y la maquina extendida, que suelen estar unidas en otros sistemas. El objetivo de esos sistemas es integrar distintos sistemas operativos dando la sensación de ser varias máquinas diferentes.</p>
	Cliente - servidor	<p>Ejemplos:</p> <ul style="list-style-type: none"> • Microsoft Hyper-V • VMware • VirtualBox • QEMU • Kernel-Based Virtual machine <p>Es un sistema operativo es de propósito general, ya que sirve para toda clase de aplicaciones, y cumple con las mismas actividades que los sistemas operativos convencionales. Mantiene la visión que tiene un usuario de su computador personal, pero la red le permite compartir el espacio del disco con el fin de economizar los recursos. La desventaja que tienen es que no resuelven el problema de compartir información, lo que dificulta el trabajo en grupo.</p>

El sistema operativo lo elegimos en base a las necesidades, pero siempre teniendo en cuenta el hardware, ya que algunos sistemas operativos se limitan a las capacidades de este último.

KERNEL Y LLAMADAS AL SISTEMA:

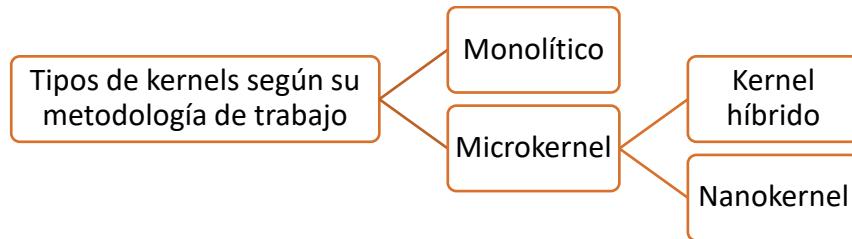
El **kernel o núcleo** (cerebro del sistema), es la parte esencial del sistema operativo que se encarga de interactuar entre las aplicaciones y de las necesidades de recursos que posee el dispositivo para ejecutarlos, decidiendo cuando asignar o quitar recursos de hardware a las aplicaciones que se ejecutan en el software, como así también de asignar prioridades según las necesidades del sistema operativo.

Es decir, comunica y administra los recursos de la computadora.

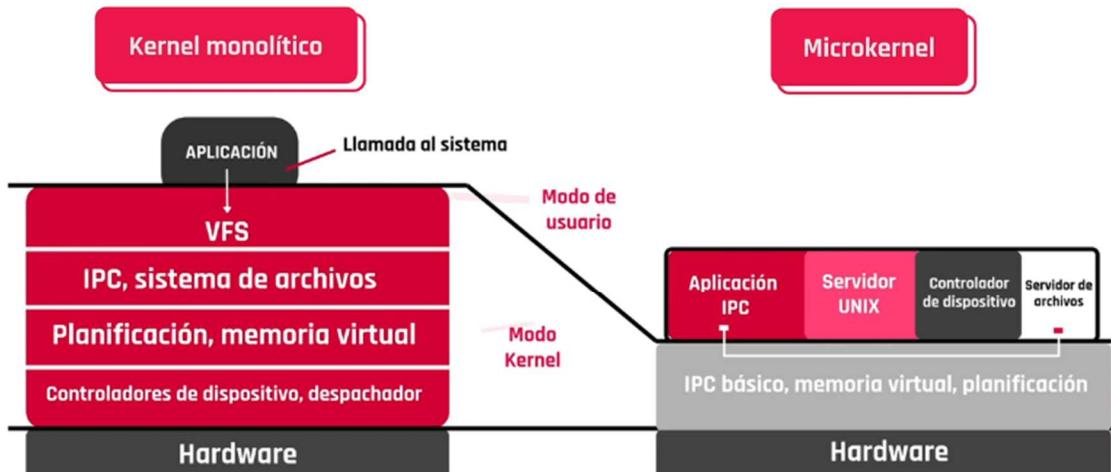


Las interacciones se llevan a cabo a través de las **llamadas al sistema**, que son el método que tienen las aplicaciones para solicitar un servicio o un recurso. Por ejemplo: solicitar a la impresora la impresión de un documento.

Existen varios modelos de kernels que varían según el creador del sistema operativo. Por ejemplo: Mac, Linux y Windows poseen su propio kernel, pero existen otros sistemas operativos como Android que utilizan kernels ya creados.



- 1) **Kernel monolítico:** es un código de muchas líneas que está alojado en un solo espacio de memoria, y posee todos los drivers, servicios y métodos de administración de recursos. Su ventaja es que es más veloz porque se comunica con las llamadas al sistema. Las desventajas de este diseño son, que se desperdicia mucho espacio de memoria porque se deben cargar los drivers y métodos para todo tipo de dispositivos, casi el 70% del kernel no se utiliza; y que si un sistema falla, todo el núcleo falla. Linux trabaja con este tipo de kernel.
- 2) **Microkernel:** solo posee las instrucciones básicas de administración en un pequeño espacio de memoria, y deja a los diferentes dispositivos su propio manejo. Su principal ventaja es que resulta más fácil agregar nuevas funcionalidades. Las desventajas de este modelo son, que un microkernel posee únicamente a un dispositivo, y al ser parte fundamental del sistema operativo, hay que diseñar un sistema operativo por cada dispositivo con su microkernel determinado, lo cual requiere más líneas de código; y es más lento ya que se comunica con paso de mensajes.



Luego aparecen como una segunda generación de kernels, versiones mejoradas de las originales, donde encontramos:

- 3) **Kernel híbrido:** es un microkernel con más código no esencial, pero, de todas formas, menor cantidad que el de un monolítico puro. También es un poco más ágil que un microkernel. Es compatible para una gran cantidad de dispositivos. Algunos ejemplos son: XNU y DragonFlyBSD.
- 4) **Nanokernel:** poseen menos código que un microkernel, pero son más difíciles de crear. En este caso todos los servicios se comunican con paso de mensaje, y son de fácil modificación del sistema operativo. Por ejemplo:

Cuando un dispositivo o proceso falla, la función del kernel es interrumpir todo lo que está haciendo la computadora para evitar un daño en el sistema operativo.

Llamadas al sistema:

Las llamadas al sistema son la manera en que un programa solicita una acción al sistema operativo con el que interactúa. Es el punto de enlace entre el modo usuario y el modo privilegiado del sistema operativo, lo cual permite a las aplicaciones utilizar los recursos del hardware.

El objetivo de las llamadas al sistema es diferenciar que acciones puede hacer o no un usuario en modo usuario, en comparación a las que puede hacer un usuario en modo privilegiado para evitar que se ejecuten acciones que puedan resultar peligrosas para el sistema operativo.

Las llamadas al sistema se clasifican en:

- **Gestión de control:** Supervisa el inicio, creación, detención y finalización de los procesos.
- **Gestión de archivos:** Incluyen la creación, eliminación, apertura, cierre, escritura y lectura de archivos.
- **Gestión de dispositivos:** Administra los recursos disponibles, como ser el almacenamiento.
- **Gestión de información:** Asegura la puntualidad e integridad de la información.
- **Comunicación entre procesos:** Coordina la interacción entre los distintos procesos y aplicaciones.

CLASE 8 – PROCESOS:

¿QUÉ ES UN PROCESO?

Los **procesos** son la ejecución de los programas o instrucciones.

Todos los softwares se organizan en procesos que quieren utilizar la CPU, y el sistema operativo es quien los administra para determinar el orden en que se ejecutaran. El cambio de un proceso a otro es denominado **cambio de contexto**.

Los procesos se ejecutan uno por vez, y son efímeros (se crean y se terminan). No son almacenados en la memoria principal para que no ocupen espacio y llenen la memoria RAM.

Se pueden crear:

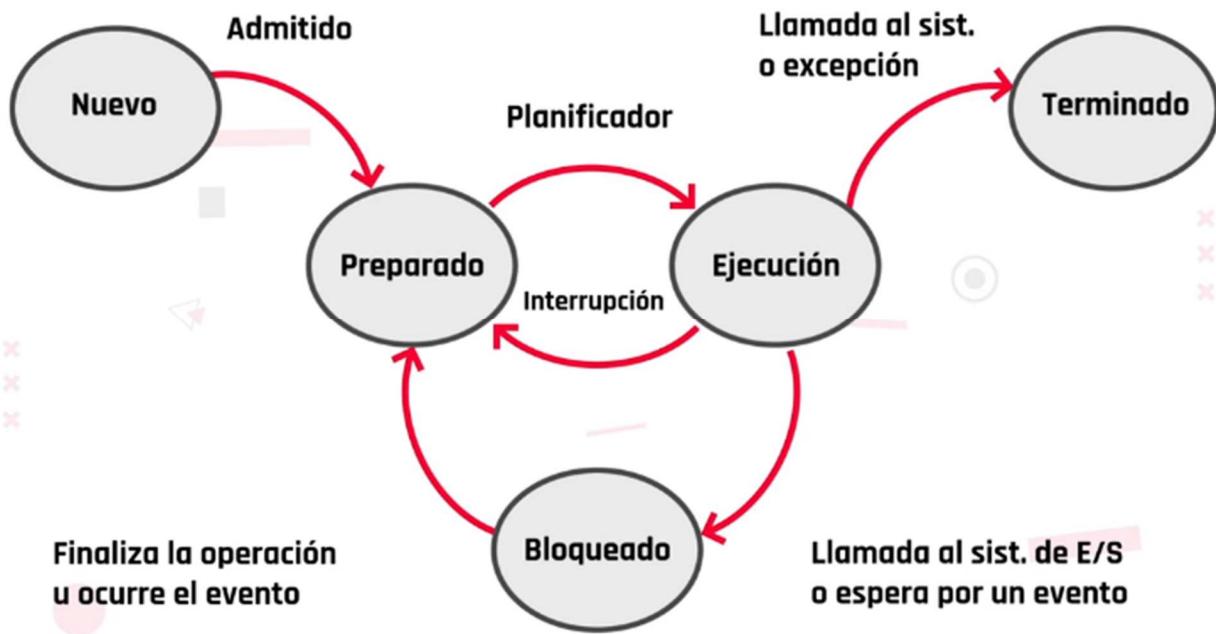
- **De manera interactiva con el usuario.** Por ejemplo: cuando exportamos un archivo, estamos creando un proceso.
- **Proceso de llamada al sistema operativo.** Se crean en segundo plano. Por ejemplo: cuando un software no puede acceder directamente a un recurso y le solicita el sistema operativo que lo gestione.

Los estados de los procesos pueden ser:

- **Nuevo:** cuando el proceso se crea.
- **Listo:** cuando el proceso está en condiciones de ser ejecutado.
- **Ejecución:** cuando su turno de utilizar el proceso comenzó.
- **Bloqueado:** cuando está esperando que un proceso o recurso pueda ser utilizado.
- **Salida:** cuando ha sido ejecutado y su ciclo de vida finaliza.

Cuando el proceso se crea, se encuentra en estado **nuevo**, y pasa a **listo** cuando el sistema operativo lo carga en la memoria. Luego cuando se comienza a ejecutar, ingresa al estado de **ejecución** donde se pueden presentar dos situaciones:

- 1) Cambiar el contexto, es decir que se produzca una interrupción y sea suspendido cuando hacemos un llamado. Es **bloqueado**.
- 2) Puede ser ejecutado y cumplir con su objetivo, donde pasa al estado de **salida**, dando lugar a que otro proceso sea ejecutado.



Mecanismos de comunicación entre procesos (IPC):

- **Señales:** son avisos que puede enviar un proceso a otro. Luego el sistema operativo se encarga de que el proceso que recibe la señal tome una acción para gestionarla.
- **Memoria compartida:** es un recurso compartido a disposición de los softwares para que puedan intercambiar información. Entonces, dos procesos pueden estar realizándose con la memoria compartida y al mismo tiempo pueden estar intercambiando información.

Cuando se da un proceso que no puede resolverse instantáneamente, como por ejemplo cuando ocurre una llamada al sistema, se crean otros procesos que se denominan **hijos** cuya función es realizar subtareas para lograr que el proceso padre pueda cumplir su objetivo. Los procesos padres pueden tener varios procesos hijos, pero los procesos hijos pueden tener un solo proceso padre. Esos procesos hijos también pueden convertirse en procesos padres.

COMUNICACIÓN DE LOS PROCESOS:

Existen dos tipos de procesos que se ejecutan de manera concurrente:

- 1) **Procesos independientes:** tienen completa autonomía, por lo tanto, no pueden ser afectados ni afectar a otros procesos que se estén ejecutando en el sistema.
- 2) **Procesos cooperativos:** pueden afectar y ser afectados por otros procesos. De hecho, son todos los procesos que comparten datos o recursos con otros procesos.

Motivos para que los procesos sean cooperativos:

- Compartir información: algunos procesos carecen de información, entonces deben consultarla para poder ejecutarse.
- Eficiencia del CPU: gracias a que los procesos comparten información, el CPU es más eficiente y veloz. Lo cual, da como resultado la **modularidad**, que es la ejecución independiente y simultánea de varios pasos de una tarea. Es decir, cuando una tarea contiene varios pasos, el CPU puede ejecutarlos de manera independiente y simultánea.

La comunicación puede traernos problemas si un proceso ejecuta una tarea de forma errónea o no hay planificación, y hay procesos que su inicio dependen de la finalización de procesos anteriores.

Existen dos métodos de intercomunicación (IPC) para que los procesos logren comunicarse, que constan de dos modelos:

- 1) **Memoria compartida:** se establece un espacio en memoria que es compartido por los procesos. Sería como prestarle un resumen a alguien, que le saca fotocopia y trabaja en su resumen en base al nuestro, pero sin modificar nuestro trabajo. Ventajas: la memoria compartida generalmente es más económica que utilizar un multiprocesador.
- 2) **Pasos de mensaje:** en este método de comunicación existe un intermediario que comunica los procesos. Ese intermediario es el kernel. Ventajas: no existen los errores como exclusión mutua, y con compatibles con cualquier tipo de arquitectura de computadora.

A la hora de elegir, es importante entender y analizar qué tipo de trabajo vamos a realizar y que características disponemos.

SINCRONIZACION DE LOS PROCESOS:

El estado de los procesos indica en que parte del ciclo de vida están, y en base a este ciclo el sistema operativo toma decisiones con los semáforos.

Mientras un proceso se está ejecutando y aparece la llamada de espera pasa a una lista de bloqueado, y permanece ahí hasta que un proceso diferente le envía la señal de avance y el proceso que permanecía bloqueado se coloca en una fila de espera para utilizar el CPU.



Área crítica: está compuesta por el procesador, los procesos y las operaciones.

Es importante llevar una planificación del uso del CPU, sino la cola de procesos puede colapsar o tener una inanición, que significa que funciona de manera tan deficiente porque le niega recursos a otros procesos que necesitan ejecutarse.

Técnicas de planificación de CPU:

- 1) **First in, first out (FIFO):** se asigna tiempo de ejecución del CPU al primer proceso que lo solicite. El proceso se realiza por completo antes de pasar al siguiente.
- 2) **Shortest Job First (SJF):** la prioridad de ejecución la tiene el proceso que menor tiempo de ejecución tiene.
- 3) **Shortest Remaining Time (SRTF):** si un proceso largo se está ejecutando, y llega uno de menor tiempo, se interrumpe el primero, ejecutándose el segundo. Una vez terminado este segundo proceso, se vuelve al primer proceso en el sector donde quedó cortado, excepto que aparezca uno más corto. En este caso, si se inició un proceso de 5 tiempos de ejecución, se cumplió el primer tiempo y aparece un proceso de 3 tiempos, se cambia al de 3 tiempos y luego se termina con los 4 tiempos restantes del primer proceso. En el caso de que queden procesos de misma cantidad de tiempos, tiene prioridad aquel que llegó primero.
- 4) **Round Robin:** en este caso existe una porción de tiempo establecido en donde los procesos, a medida que van llegando a la fila de espera se ejecutan en el CPU, hasta que esa porción de tiempo se cumple. Una vez que eso pasa, se interrumpe el proceso y se pasa al siguiente en la lista. Si aún no estuviera terminado el proceso, ingresa nuevamente a la fila, pero ubicándose al final. Aquí, se establece que todos los procesos tienen un tiempo de ejecución equitativo.

Existen otras planificaciones que combinan de forma híbrida las 4 anteriores, o presentan algoritmos diferentes. Algunos ejemplos son: la retroalimentación multinivel, o la planificación por comportamiento.

HILOS DE EJECUCION (THREAD):

Los procesos pueden dividirse en secuencias de tareas denominadas **hilos**, que son porciones de código que pueden ejecutarse de forma simultánea en cooperación con otros subprocessos. Los subprocessos simultáneos proporcionan mayor eficiencia.

Pueden existir múltiples hilos dentro de un proceso ejecutándose de forma concurrente, compartiendo recursos y memoria. En cambio, los procesos no comparten de esta manera.

Es muy importante la sincronización al momento en que trabajan los hilos, ya que un subprocesso puede bloquear un recurso y negarle el acceso a otro hilo.

Hasta la década del 2000 los procesadores eran monolíticos, por lo tanto, podían trabajar con un solo hilo a la vez. Luego aparecieron los procesadores multinúcleo, los cuales comenzaron con esta metodología de trabajo de varios hilos en ejecución, lo cual aumentó la velocidad de procesamiento.

Procesador	Ventajas	Desventajas
Monolítico	<ul style="list-style-type: none">No presenta los errores que podrían aparecer en un sistema multinúcleo.Poseen menor cantidad de problemas de bloqueo de recursos.	<ul style="list-style-type: none">Tienen una capacidad de respuesta menor.Su comportamiento es más predecible.
Multinúcleo	<ul style="list-style-type: none">Excelente capacidad de respuesta.Buen trabajo en paralelo de las tareas.	<ul style="list-style-type: none">Sincronización compleja de planificar.Su comportamiento es difícil de predecir, ya que puede presentar errores.

PLANIFICACION DE PROCESOS:

La planificación son las políticas y mecanismos que poseen los sistemas operativos actuales para realizar la gestión del procesador. Su objetivo es dar un buen servicio a todos los procesos que existan en un momento dado en el sistema.

CRITERIOS A TENER EN CUENTA A LA HORA DE ELEGIR O DISEÑAR UN ALGORITMO DE PLANIFICACION	
Rendimiento	Es el número de trabajos o procesos realizados por unidad de tiempo, que debe ser lo mayor posible.
Tiempo de respuesta	Es la velocidad con que el ordenador da la respuesta a una petición. Depende mucho de la velocidad de los dispositivos de entrada y salida.
Tiempo de servicio	Es el tiempo que tarda en ejecutarse un proceso, donde se incluye el tiempo de carga del programa en memoria, el tiempo de espera en la cola de procesos separados, el tiempo de ejecución en el procesador y el tiempo consumido en operaciones de entrada/salida.
Tiempo de procesador	Es el tiempo que un proceso está utilizando el procesador sin contar el tiempo que se encuentra bloqueado por operaciones de entrada/salida.

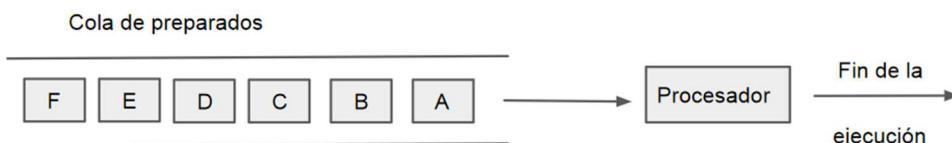
Tiempo de ejecución	Es idéntico al tiempo de servicio menos el tiempo de espera en la cola de procesos separados; es decir, es el tiempo teórico que necesitaría el proceso para ser ejecutado si fuera el único presente en el sistema.
Tiempo de espera	Es el tiempo que los procesos están activos, pero sin ser ejecutados, es decir, los tiempos de espera en las distintas colas.
Eficiencia	Se refiere a la utilización del recurso más caro en un sistema, el procesador, que debe estar el mayor tiempo posible ocupado para lograr así un gran rendimiento.

Algoritmos de planificación de CPU:

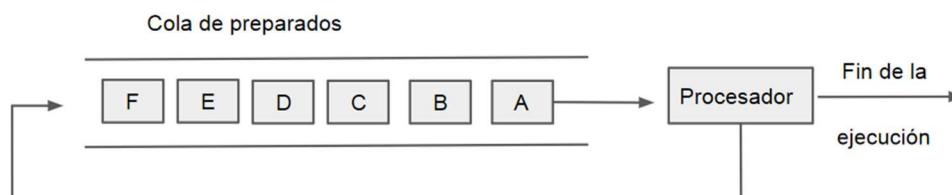
El planificador del procesador tiene como misión la asignación del mismo a los procesos que están en la cola de procesos preparados.

Políticas de planificación:

- 1) **Primero en llegar, primero en salir (FIFO):** en esta política de planificación, el procesador ejecuta cada proceso hasta que termina; por lo tanto, los procesos que entran en cola de procesos preparados permanecerán encolados en la orden en que lleguen hasta que les toque su ejecución. También se conoce como “primero en entrar, primero en salir”.



- 2) **Round Robin (RR):** consiste en conceder a cada proceso de ejecución un determinado periodo de tiempo “q” (quantum), transcurrido el cual, si el proceso no ha terminado, se le devuelve al final de la cola de procesos preparados, concediéndose el procesador al siguiente proceso por su correspondiente quantum.



- 3) **El siguiente proceso, el más corto (SJF):** esta política toma de la cola de procesos preparados el que necesite menos tiempo de ejecución para realizar su trabajo. Para ello, debe saber el tiempo de ejecución que necesita cada proceso, lo cual no es tarea fácil, pero es posible a través de diversos métodos como puede ser la información suministrada por el propio usuario o por el propio programa, basándose en la historia anterior.
- 4) **Próximo proceso, el de tiempo restante más corto (SRTF):** esta técnica cambia el proceso que está en ejecución cuando se ejecuta un proceso con una exigencia de tiempo de ejecución total menor que el que se está ejecutando en el procesador.
- 5) **Colas múltiples:** cuando los procesos que van a ser ejecutados en una computadora se pueden agrupar en distintos grupos, podemos asignarlos a diferentes colas, cada una con distinta planificación, para darle a cada una de ella la que realmente necesite. Esta política divide la cola en procesos preparados en varias colas separadas, de manera que los procesos se asignan a una determinada cola según sus necesidades y tipo.

CLASE 9 – EVALUACION PARCIAL.

MODULO 3: HERRAMIENTAS DE TRABAJO

CLASE 10 – LENGUAJES Y PARADIGMAS DE PROGRAMACION:

LENGUAJES DE PROGRAMACIÓN:

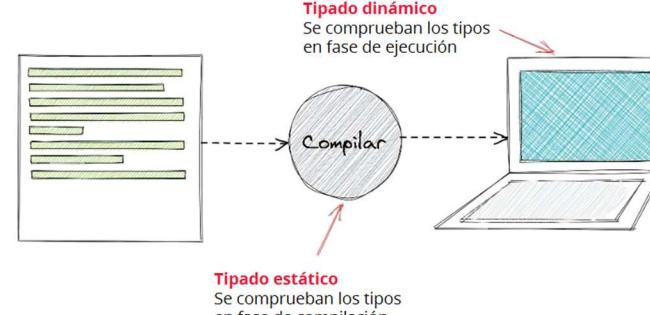
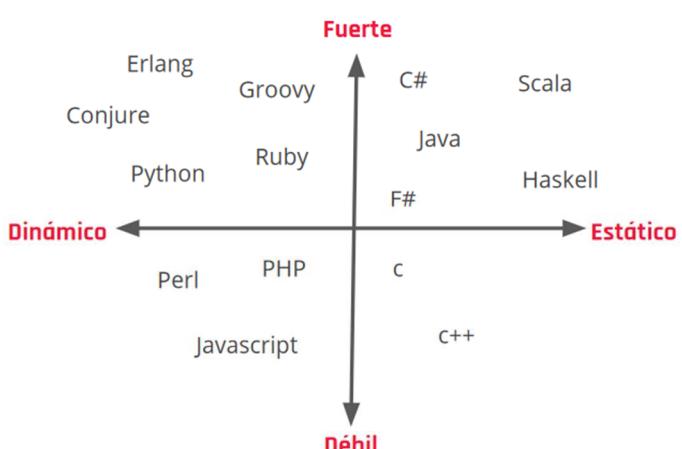
Son los lenguajes formales que nos permiten darle instrucciones a la computadora.

Pueden ser:

- **Específicos:** son aquellos que resuelven problemas puntuales, por ejemplo, un lenguaje de programación para realizar gráficos matemáticos.
- **Generales:** permiten desarrollar un montón de aplicaciones distintas casi independientes de contexto, como por ejemplo un sitio web de mascotas o un comercio electrónico.
- **Bajo nivel:** son utilizados para dar instrucciones muy específicas y utilizar al máximo los recursos disponibles. Pero debemos estar atentos no solo a la funcionalidad que queremos desarrollar, sino también en que hardware.
- **Alto nivel:** son aquellos que se encuentran mas cercanos al lenguaje natural que al lenguaje binario o de máquina. Es decir, permiten abstraernos de las cosas internas de la máquina, permitiendo enfocarnos en desarrollar funcionalidades y sistemas de manera más sencilla. Un ejemplo es JavaScript.

No es necesario saber todos los lenguajes disponibles. Los desarrolladores suelen tener dominio de algunos lenguajes.

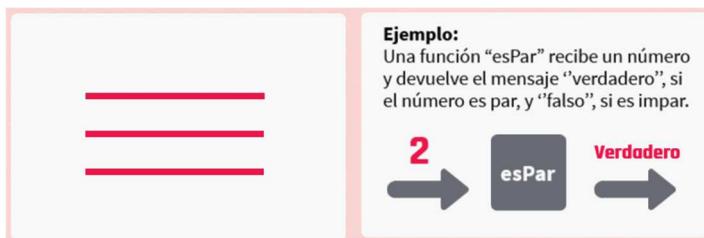
TIPADOS DE LENGUAJE Y FRAMEWORKS		
Los lenguajes tipados fuerte y débil se distinguen según si permiten o no violaciones de los tipos de datos una vez declarados.	Tipado débil	<p>En estos lenguajes no indicamos, la mayoría de las veces, el tipo de variable. Aquí podemos asignar, por ejemplo, un valor entero a una variable que anteriormente tenía una cadena. Pero, no solo eso, también podemos operar con variables de distintos tipos. Su principal ventaja es que es mucho más rápido de desarrollar, pero una clara desventaja es que podemos cometer muchos más errores si no tenemos cuidado.</p> 
	Tipado fuerte	<p>En estos lenguajes se nos obliga a indicar el tipo de dato al declarar la variable. Además, dicho tipo no puede ser cambiado una vez definida la variable. La ventaja es que, al ser código más expresivo, cometaremos menos errores. La desventaja es que son mucho más estrictos a la hora de programar y que hay que escribir mucho más código.</p> 
Tipado estático		<p>En el tipado estático, la comprobación de tipificación se realiza durante la compilación y no durante la ejecución. Comparado con el tipado dinámico, el estático permite que los errores de tipificación sean detectados antes y que la ejecución del programa sea más eficiente y segura.</p> 
Tipado dinámico		<p>La comprobación de tipificación se realiza durante su ejecución en vez de durante la compilación. Comparado con el tipado estático, este es más</p>

	<p>flexible, a pesar de ejecutarse más lentamente y ser más propenso a contener errores de programación.</p> 
	 <p>Tipado dinámico Se comprueban los tipos en fase de ejecución</p> <p>Tipado estático Se comprueban los tipos en fase de compilación</p>
	<h2>Posicionamiento de cada lenguaje de programación</h2> 
Frameworks o marcos de trabajo	<p>Es una estructura previa / esqueleto que se puede aprovechar para desarrollar un proyecto. El Framework es una especie de plantilla, un esquema conceptual, que simplifica la elaboración de una tarea, ya que solo es necesario complementarlo de acuerdo a lo que se quiere realizar.</p> 

PARADIGMAS DE PROGRAMACIÓN:

Un paradigma es una forma de pensar bajo un modelo preestablecido. En programación tenemos:

- **Paradigma estructurado:** sigue una línea de pensamiento donde se suele ejecutar una instrucción a la vez y uno se rige en un acotado set de instrucciones. Es muy utilizado para el desarrollo de sistemas.



- **Paradigma de programación orientada a objetos:** el código puede agruparse de tal forma que llegue a representar una entidad y que interprete mensajes. La fortaleza del paradigma de la programación orientada a objetos yace en utilizar abstracciones y crear entidades.

Ejemplo:

Un código representa un carrito de compra.



Otro código representa un producto con su precio.



Luego, puedo agregarle la responsabilidad al carrito que vaya agregando productos para luego preguntarle el costo total.



- **Paradigma funcional:** se basa en un concepto muy simple, el de las funciones matemáticas. La fortaleza de este paradigma radica en que siempre que a la función X se le pasa el valor A, está siempre va a devolver el valor B. Esta propiedad de devolver el mismo valor es conocida como inmutabilidad.

Ejemplo:

La solución funcional al problema de si un número es par o no es muy similar al estructurado, debemos crear una función "esPar" que reciba un número y nos diga si es par o impar.



- **Paradigma lógico:** en lugar de desarrollar pasos e instrucciones, utiliza reglas lógicas para consultar al sistema y el mismo infiere que hacer en base a las reglas lógicas establecidas.

Paradigma de programación lógica → Instrucciones → Reglas lógicas

Ejemplo:

Reglas lógicas:

Toda persona cuyo saldo sea negativo es deudor.

A todo deudor se le aplica una tasa de interés del 10%

Con este set lógico podríamos preguntar:

¿Cuál es la tasa de interés de Juan?

El sistema responde analizando si Juan es una persona, si es deudor o no y si aplica o no la tasa de interés.



- **Paradigma de programación con lenguaje específico de dominio:** los lenguajes que encontramos acá tratan de resolver problemáticas específicas.

Ejemplo:

Cuando queremos consultar una base de datos de un supermercado para saber qué productos tenemos en la categoría de electrodomésticos.



- **Multiparadigma:** a lo largo de la evolución de la programación, con nuevos desafíos y paradigmas ha habido lenguajes que han modificado su estructura para poder permitir dar soluciones a distintos paradigmas.

Ejemplo:



En JavaScript se puede escribir código tanto con el paradigma estructurado como con programación orientada a objetos e incluso utilizar el paradigma funcional.

¿Mientras más paradigmas tenga un lenguaje es mejor?

No, un lenguaje es una herramienta y hay distintas herramientas para distintas soluciones. Siempre debemos analizar el contexto, tiempos, con qué equipo contamos, si hay presupuesto, cuales son las herramientas que disponemos para trabajar y que queremos lograr.

La mejor manera de conocer un paradigma de programación es investigar y programar en un lenguaje característico de ese paradigma. No hace falta ser un experto. Solo el hecho de conocerlo nos brinda más herramientas a la hora de desarrollar.



DEL CODIGO AL EJECUTABLE:

TIPOS DE CODIGO	
Código fuente	Es una colección de instrucciones de computadora escritas usando un lenguaje de programación legible por humanos.
Código maquina	Es una secuencia de sentencias en lenguaje de máquina o binario. Es el resultado obtenido después de que el compilador convierta el código fuente en un lenguaje que pueda ser comprendido por el procesador
Compilador	Es una aplicación traduce (compila) el código fuente en un código que el procesador puede comprender y ejecutar. Este código de máquina se almacena en forma de archivo ejecutable.

Diagrama del proceso de compilación:

El diagrama ilustra el proceso de compilación:

- código fuente**: Representado por un icono de documento.
- resultado**: Representado por un icono de flecha naranja.
- Compilador**: Representado por un cuadro rojo.
- ejecutar en**: Representado por un icono de terminal.
- .exe**: Representado por un icono de archivo.
- ejecutar!**: Representado por un icono de laptop.

Los flujos de datos son:

- Un flecha verde apunta desde el "código fuente" al "Compilador", etiquetada como "compilado".
- Una flecha naranja apunta desde el "Compilador" al "resultado", etiquetada como "resultado".
- Una flecha azul apunta desde el "resultado" al "ejecutar en", etiquetada como "ejecutar en".
- Una flecha azul apunta desde el "ejecutar en" al ".exe", etiquetada como "ejecutar!".
- Una flecha azul apunta desde el ".exe" al "ejecutar!", etiquetada como "ejecutar!".

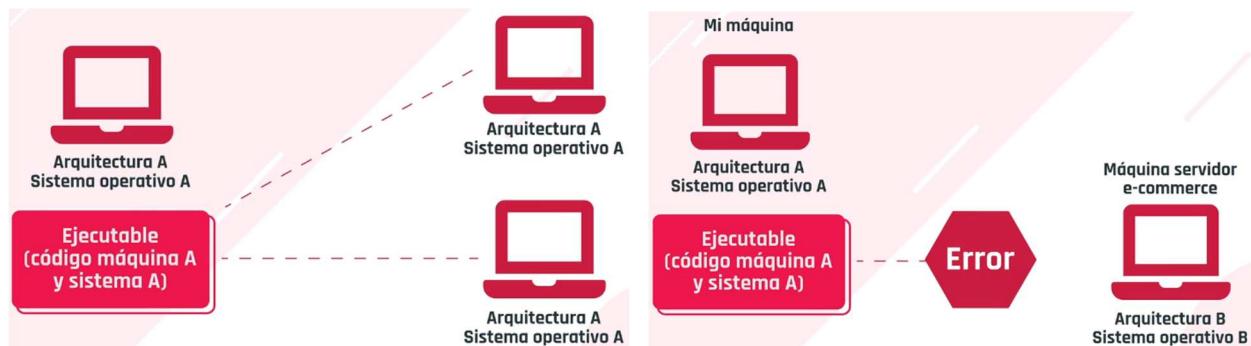
Interprete	<p>Traduce el código fuente línea a línea y lo ejecuta directamente. El proceso de traducción funciona mucho más rápido que en un compilador, pero la ejecución es más lenta y se necesita una gran cantidad de memoria.</p>
-------------------	--

Escribimos programas utilizando los lenguajes de programación, pero usualmente los programas suelen estar conformados por muchos archivos escritos en distintos lenguajes.

Para que la maquina interprete todos esos lenguajes distintos, las instrucciones deben pasar del código que escribimos a un código que la maquina entienda. Esa traducción se denomina **compilación**, y lo que hace es tomar todo el código fuente y lo transformarlo en código máquina para que pueda ser ejecutado en el dispositivo.

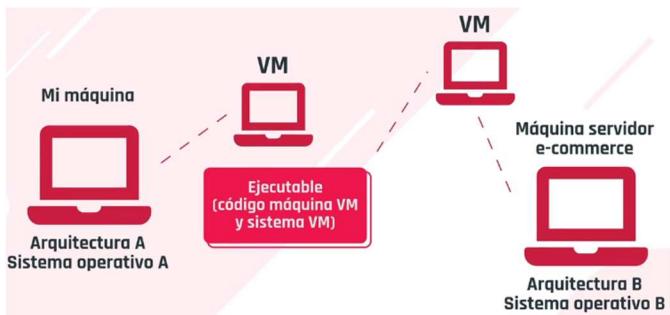
El resultado de la compilación (el ejecutable), debería poder ejecutarse correctamente siempre y cuando la maquina donde se compile sea similar a donde se ejecute, lo que implica tener similares arquitecturas de CPU y sistemas operativos.

Si la arquitectura y el sistema operativo de la maquina donde se ejecuta el código son diferentes a los de la maquina donde se compilo, el código no va a funcionar. Entonces debemos llevar el código fuente a una maquina similar a la B (donde queremos ejecutar) para que se compile correctamente y obtener un programa ejecutable para esa máquina.



Existen otras dos formas para que los programas sean entendidos y ejecutados por una máquina, independientemente de la arquitectura.

- 1) **Máquinas virtuales:** en estos casos, al momento de realizar la compilación, lo que hacemos es compilar el código fuente a un código que entienda la VM (Virtual Machine). Este código va a poder ser interpretado por cualquier VM, y aquella que tenga la versión para una computadora B (donde se quiere ejecutar) será la que traduzca el código. Es decir, Virtual Machine funciona como un traductor para los distintos tipos de sistemas operativos y arquitecturas.



Existen empresas que se encargan de mantener estas VM actualizadas ante cambios en la arquitectura.

- 2) **Intérpretes:** Este proceso hace un análisis línea por línea en cada sistema donde se ejecuta el código fuente, así traduce el código maquina a un lenguaje que la misma entienda.

Estos métodos permiten que un código programa pueda ser independiente de la arquitectura, ya que el código fuente no es compilado previamente a código máquina para crear el ejecutable.

Nosotros no podemos elegir como se va a ejecutar nuestro código (si va a ser compilado, interpretado o traducido por una VM) porque viene de la mano de como el lenguaje de programación fue diseñado.

Diferencias radicadas en la performance y rendimiento		
Formas de interpretación del código	Pros	Contras
Compilación	Se ejecuta velozmente	
Máquinas virtuales (VM)	Portabilidad. Nos permiten escribir códigos que sabemos que van a funcionar independientemente de donde corran.	El código, en vez de ejecutarse en la máquina específica, se ejecuta en la máquina virtual que hace de intermediaria.
Interpretación		La traducción se realiza línea por línea cada vez que se ejecuta, lo cual ralentiza la ejecución del código.

CLASE 11 – MAQUINAS VIRTUALES:

ESCRITORIOS REMOTOS:

Son programas que nos permiten acceder e interactuar con una computadora a distancia a través de una conexión a internet, permitiendo que podamos trabajar desde cualquier parte. Estos programas no requieren una conexión de red física, ni un hardware adicional para vincular las computadoras, lo único que se necesita es acceso a internet, que ambas computadoras tengan la misma aplicación de escritorio remoto, y que permanezcan encendidas de manera simultánea.

La computadora a la que se accede de forma remota recibe el nombre de host, y aquella desde la que trabajamos de manera física se denomina cliente.

Varios clientes pueden acceder a un mismo host, mientras este cuente con la capacidad suficiente para soportar todas las conexiones simultáneas.

Existen distintos tipos de aplicaciones de escritorios remotos. La más utilizada es teamviewer por su facilidad de uso, compatibilidad de múltiples plataformas y una opción gratuita para uso personal. Otros ejemplos son: Anydesk, Chrome remote desktop, Windows remote desktop, etc.

La ventaja de los escritorios remotos es que permite el ahorro de recursos. Dentro de las desventajas encontramos:

- Si el programa que brinda el servicio de escritorio remoto no posee la seguridad necesaria, puede ser objeto de ciberataques.
- El rendimiento del sistema depende enteramente de la calidad de conexión a internet. Si esta no es confiable puede comprometer a todo el sistema.

MAQUINAS VIRTUALES:

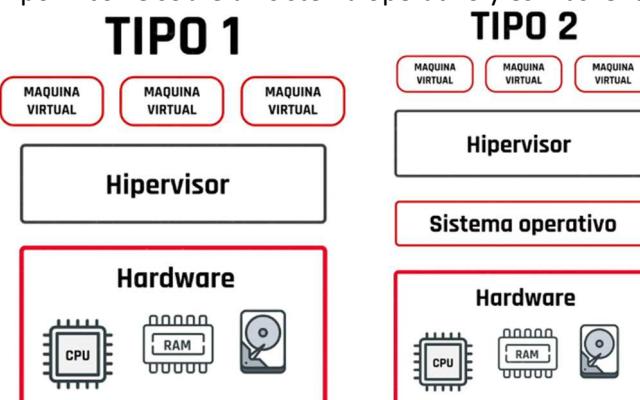
Una máquina virtual es un software capaz de contener en su interior un sistema operativo haciéndole creer que es una computadora de verdad. Y ese sistema operativo, puede a su vez albergar otro más, como si fueran mamushkas.

Existen dos tipos de máquinas virtuales:

- 1) **De sistemas:** emula una computadora completa. Es decir, es un software que nos permite ejecutar otro sistema operativo en su interior.

El lugar donde la máquina virtual es creada se llama **hipervisor**, que es una capa de software que se instala sobre la parte física de la computadora y se encarga de asignar parte de la memoria, disco rígido, CPU y demás recursos físicos. Existen dos tipos de hipervisor:

- ✓ Tipo 1: es el más utilizado por ser más rápido y seguro. Corre directamente sobre la parte física de la computadora, y sobre él se crearán una o más máquinas virtuales.
- ✓ Tipo 2: corre sobre un sistema operativo y es más lento que el tipo 1.



Sobre el hipervisor se pueden crear tantas máquinas virtuales como queramos, y cada una funciona como una computadora real.

- 2) **De procesos:** no emula una computadora completa, sino solo un proceso en concreto, como por ejemplo una aplicación, permitiendo que cada una se comporte de la misma manera independientemente del sistema operativo sobre el que se ejecute. Esto puede ser de gran utilidad al momento de desarrollar aplicaciones que van a ejecutarse en distintos sistemas operativos.

MAQUINAS VIRTUALES	
Ventajas	<ul style="list-style-type: none">• Podemos probar otros sistemas operativos sin cambiar el hardware.• Permite ejecutar programas antiguos.• Permite utilizar aplicaciones disponibles para otros sistemas operativos.• Nos ofrece un entorno de seguridad para saber cómo funcionan virus y malwares.• Su uso permite mejorar el aprovechamiento del hardware (equipo físico) al utilizar recursos que de otra forma estarían ociosos.

Desventajas	<ul style="list-style-type: none"> • Son menos eficientes que las maquinas reales porque acceden al hardware de forma indirecta ya que el software se ejecuta sobre el sistema operativo. • Tiene que solicitar acceso al hardware de la maquina física, lo cual ralentiza el proceso. • Cuando varias máquinas virtuales se ejecutan en la misma maquina física, el rendimiento puede verse afectado si la computadora carece de los recursos necesarios.
--------------------	---

Las ventajas de las máquinas virtuales, permitió llevar la virtualización a otras áreas como el almacenamiento o las redes.

CONTENEDORES:

Es un concepto de empaquetación de software que incluye la aplicación y todas sus dependencias de ejecución.

Un contenedor es un espacio virtual donde podemos agregar nuestros productos (software que desarrollamos), todas las herramientas necesarias para armarlo y ponerlo en funcionamiento (librerías), y el sistema operativo donde pruebo que funcione correctamente.

De esta manera, los clientes solo deben abrir el contenedor en cualquier sistema operativo y podrá ejecutar nuestro software sin problema.

Los contenedores funcionan de manera conjunta con el sistema operativo y no requieren de un hipervisor, por lo que son mucho más rápidos. A su vez, trabajan en capas por lo que cada vez que agreguemos, modifiquemos o quitemos dependencias vamos a generar una nueva versión de nuestro contenedor, es decir una capa que irá por encima de la anterior. Esto se diferencia de un sistema de versionado (GIT o Google Docs).

Para poder implementar un contenedor, lo primero que necesitamos hacer es crear una imagen. Sería encontrar una imagen base del software donde mostrar el sistema. Las imágenes bases que forman parte de nuestro build inicial del contenedor pueden ser el sistema operativo, la base de datos de nuestra aplicación software.

Luego deberemos hacer un publish (publicar) al contenedor para que este se suba al repositorio y cualquier persona pueda utilizarla haciendo un pull, y ejecutar el programa haciendo un run (para correr el contenedor).

Esto permite que las implementaciones de nuevas versiones, que antes tardaban días, se puedan realizar en segundos.

Configuración:

La mejor característica de contenedores es que podemos configurar el sistema fácilmente y también más rápido. Es posible desplegar nuestro código en menos tiempo y esfuerzo con la ayuda de contenedores. Los requisitos de la infraestructura ya no están vinculados con el entorno de la aplicación, ya que se puede utilizar en una amplia variedad de entornos.

Tamaño:

Al proporcionar una huella más pequeña del sistema operativo a través de contenedores, un contenedor tiene la capacidad de reducir el tamaño del desarrollo.

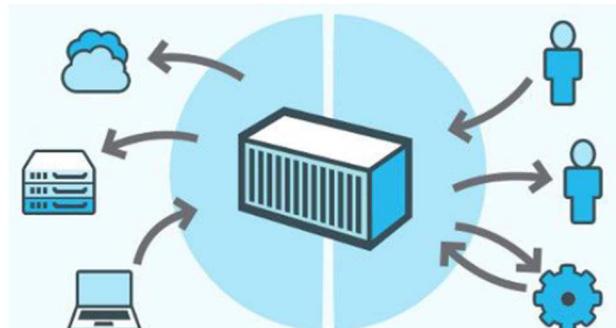
Productividad:

Utilizar contenedores equivale a aumentar la productividad. Esto facilita la configuración técnica y el despliegue rápido de la aplicación. Además, ayuda a ejecutar la aplicación en un entorno aislado y reduce los recursos.



Gestión múltiple:

Existen herramientas de programación y clustering para contenedores. Algunos contenedores exponen una web y otros ofrecen API como su front end, que nos permite utilizar varias herramientas para controlarlo. Además, nos ayuda a controlar un clúster de hosts contenedores como un único host virtual.



Servicios:

La lista de tareas que nos permite especificar el estado del contenedor dentro de un cluster y los servicios. Básicamente, cada tarea representa una instancia de un contenedor que debe estar en ejecución y que puede ser programada sobre los nodos (cada instancia que lo ejecuta).

La isolación:

Los contenedores se utilizan para ejecutar aplicaciones en un entorno aislado (isolado). Lo mejor de esta característica de los contenedores es que aquí cada contenedor es independiente de otro y además, nos permite ejecutar cualquier tipo de aplicación requerida.

Seguridad:

Los contenedores proporcionan configuraciones por defecto que ofrecen una mayor protección para las aplicaciones que se ejecutan sobre ellos y a través de orquestadores. La plataforma establece valores predeterminados seguros, al tiempo que deja los controles en manos del administrador para cambiar las configuraciones y las políticas según sea necesario.

ADMINISTRADOR DE CONTENEDORES:

Los orquestadores son sistemas de automatización del despliegue, ajuste de escala y manejo de aplicaciones en contenedores.

Un orquestador es una herramienta que automatiza el despliegue, administración, escalamiento, comunicación, y disponibilidad de nuestro software ejecutándose en contenedores.

Utilizar contenedores es muy fácil y ventajoso, pero hay entornos en los que necesitamos que no existan tiempos de inactividad, por lo que, si un contenedor se cae, otro debe iniciarse automáticamente, y la mejor forma es que sea empleado por un orquestador.

Características más importantes de los orquestadores:

- 1) **Auto-reparación:** el orquestador puede recuperar los contenedores que fallen reemplazándolos o dando de baja a los que no responden.
- 2) **Retroceso automatizado:** es la capacidad de retroceder (sería como un ctrl z, pero a nivel de sistema). Esto implicaría cambiar toda la configuración y datos del sistema. Si quisieramos hacerlo de forma manual, deberíamos detener el sistema, hacer un back up, y luego iniciar el sistema desde el mismo.
- 3) **Auto-escalado:** cuando se producen picos de demanda se requieren muchos más recursos de computación de los servidores. El auto-escalado es una gran ventaja, especialmente en la nube moderna donde los costos se basan en los recursos consumidos.
- 4) **Balance de carga:** en el caso de que un contenedor reciba mucha demanda, el orquestador es capaz de distribuir el tráfico de red de manera que sea estable y balanceada.

Un *orquestador de contenedores* se ocupa de cuestiones como:

- Configuración automática.
- Despliegue y "levantado" automático de servicios basados en contenedores.
- Balanceado de carga.
- Autoescalado y autoreinicio de contenedores.
- Control de la "salud" de cada contenedor.
- Intercambio de datos y networking.
- Mantenimiento de parámetros "secretos" y configuraciones.



El orquestador permitió que funciones que antes costaban mucho esfuerzo humano de planificación, tiempo y dinero, ahora sean automatizadas. Por esta razón, es que los contenedores y orquestadores deben implementarse conjuntamente.

Kubernetes:

Es el motor de orquestación de contenedores más popular que existe en el mercado. Comenzó siendo un proyecto de Google. Actualmente, miles de equipos de desarrolladores lo usan para desplegar contenedores en producción. La herramienta funciona agrupando contenedores que componen una aplicación en unidades lógicas para una fácil gestión y descubrimiento.

Docker swarm:

Swarm es la solución que propone Docker ante los problemas de los desarrolladores a la hora de orquestar y planificar contenedores a través de muchos servidores. Viene incluido junto al motor de Docker y ofrece muchas funciones avanzadas integradas —como el descubrimiento de servicios, balanceo de carga, escalado y seguridad—.

Mesosphere DC/OS:

El sistema operativo Mesosphere Datacenter (DC/OS) es una plataforma de código abierto, integrada para datos y contenedores desarrollados sobre el kernel de sistema distribuido Apache Mesos. Se ha diseñado para gestionar múltiples máquinas dentro de un centro de datos con uno o más clústeres, ya sea en la nube o usando software en servidores en local. DC/OS puede desplegar contenedores y gestionar tanto aplicaciones sin estado como protocolos con estado en el mismo entorno. Es capaz de funcionar con Docker Swarm y Kubernetes.

Hashicorp Nomad:

Soportada por Linux, Mac y Windows, Nomad es una herramienta binaria única capaz de planificar todas las aplicaciones virtualizadas en contenedores o independientes. Nomad ayuda a mejorar la densidad, a la vez que reduce costos, ya que es capaz de distribuir de manera eficiente más aplicaciones en menos servidores.

Amazon ECS:

El servicio de AWS es un sistema de gestión muy escalable que permite a los desarrolladores ejecutar aplicaciones en contenedores. Está formado por muchos componentes integrados que permiten la fácil planificación y despliegue de clústeres, tareas y servicios del contenedor.

Amazon Elastic Kubernetes Service:

Amazon EKS facilita la implementación, la administración y el escalado de aplicaciones en contenedores mediante Kubernetes en AWS. Ejecuta la infraestructura de administración de Kubernetes por el usuario en varias zonas de disponibilidad de AWS para disminuir errores. Las aplicaciones que se ejecutan en cualquier entorno estándar de Kubernetes son totalmente compatibles y pueden migrar fácilmente a Amazon EKS.

Azure Kubernetes Service (AKS):

El servicio de Azure es código abierto y está optimizado para su uso en las máquinas virtuales de Azure, denominadas Azure Virtual Machines. Proporciona las herramientas necesarias para crear, configurar y gestionar la infraestructura de contenedores Docker abiertos. AKS ofrece desarrollo simplificado de aplicaciones basadas en contenedores y despliegue con soporte para Kubernetes, Mesosphere DC/OS o Swarm para la orquestación.

Google Kubernetes Engine (GKE):

Montado sobre Kubernetes, permite desplegar, gestionar y escalar aplicaciones de contenedores en la nube de Google. El objetivo de GKE es optimizar la productividad del departamento de desarrollo al mejorar la gestión de las cargas de trabajo basadas en contenedores. Oculta tanto las tareas de gestión simple como aquellas más complejas detrás de herramientas de líneas de comando, usando interfaces transparentes y fáciles de usar. Obviamente, Kubernetes es la columna vertebral de GKE. Aunque no es estrictamente necesario dominar Kubernetes para usar GKE, ayuda mucho si al menos conocemos sus fundamentos básicos.

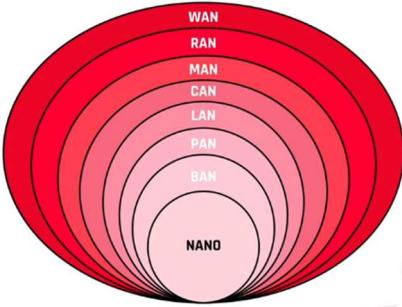
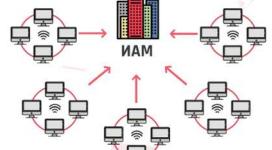
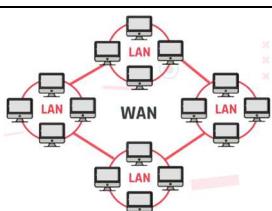
MODULO 4: SURFEANDO INTERNET

CLASE 12 – REDES:

REDES

Una red de informática es un conjunto de dispositivos informáticos independientes conectados entre sí, capaces de comunicarse electrónicamente entre sí, que se envían y reciben datos para compartir información y recursos.

La finalidad de su creación fue acortar las distancias, asegurar la confiabilidad y disponibilidad de la información, aumentar la velocidad de transmisión de los datos, y reducir los costos.

CLASIFICACION	
	
Redes por alcance	<p>Red de área personal (PAN – Personal Area Network): es la utilizada por los dispositivos personales como, por ejemplo: aquellos inalámbricos conectados por bluetooth los auriculares, parlantes, Smart TV, etc.</p> 
	<p>Red de área local (LAN – Local Area Network): es una red que cubre áreas geográficas pequeñas, con un alcance de 1 a 5 kilómetros. Son áreas que incluyen hogares, oficinas, un grupo de edificios, etc.</p> 
	<p>Red de área metropolitana (MAN – Metropolitan Area Network): son redes que normalmente se emplean en ciudades, y que cubren un rango de 50 a 60 kilómetros. Son redes de conexión de alta velocidad, que interconectan a varias redes de área local en una sola gran red, en una zona geográfica específica.</p> 
	<p>Red de área amplia (WAN – Wide Area Network): cubre una zona geográfica de gran escala, con un diámetro aproximado de 100 a 1000 kilómetros. Requieren atravesar rutas de acceso público y utilizan, al menos parcialmente, circuitos proporcionados por una entidad proveedora de servicios de telecomunicación.</p> 
Por grado de autentificación	<p>Redes de acceso privadas: solo puede ser usada por algunas personas que cuenten con la clave de acceso personal con la que esté configurada.</p> <p>Redes de acceso públicas: puede ser utilizada por cualquier persona ya que no requiere una clave para poder acceder a ella.</p>
Por tipo de conexión	<p>Cableadas o por métodos guiados: utilizan componentes físicos y sólidos para la transmisión de datos. Dentro de los más utilizados tenemos el par trenzado, el cable coaxial, y fibra óptica.</p>

	<p>La ventaja de esto es que pierden menos señal y existen menos ruidos, en cambio, la desventaja está dada por la incomodidad que resulta toda su instalación en cada área.</p> <p>Inalámbricas o por métodos no guiados: los datos se propagan libremente a través del aire. Las más utilizadas son el infrarrojo, bluetooth, y wifi. Su conexión se establece mediante sistemas dispersos y de alcance de área, como ondas de radio, señal infrarroja o microondas. Son un poco más lentas, pero mucho más cómodas y prácticas.</p>
Por su grado de difusión	<p>Intranet: red privada de ordenadores que utiliza tecnología de Internet para compartir dentro de una organización parte de sus sistemas de información y sistemas operacionales.</p> <p>Es decir, es una red informática que utiliza la tecnología del protocolo de Internet para compartir información, sistemas operativos o servicios de computación dentro de una organización. Suele ser interna, en vez de pública como internet, por lo que solo los miembros de esa organización tienen acceso a ella.</p> <p>Extranet: red privada que se utiliza para compartir de forma segura parte de la información propia de una organización con proveedores, compradores, socios, clientes o cualquier otro negocio u organización.</p> <p>Es decir, es parte de la Intranet de una organización que se extiende a usuarios fuera de ella, usualmente utilizando Internet y sus protocolos.</p> <p>Internet: es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial.</p>

MEDIOS DE TRANSMISION:

El medio de transmisión constituye el soporte físico a través del cual el emisor y receptor pueden comunicarse en un sistema de transmisión de datos.

	Están constituidos por cables que se encargan de la conducción de las señales desde un extremo a otro. La velocidad de transmisión depende directamente de la distancia entre las terminales.	
Medios guiados	<p>Pares trenzados: Conjunto de pares de hilos de cobre conductores, cruzados entre sí. La forma trenzada del cable se utiliza para reducir la interferencia eléctrica con respecto a los pares cercanos que se encuentran a su alrededor. La velocidad máxima de transmisión es de 1 Gbps y la distancia entre repetidores es de 2 a 10 km.</p>	
	<p>Cable coaxial: Tiene un alambre de cobre duro en su parte central. La velocidad máxima de transmisión es de 2 Gbps y la distancia entre repetidores es de 10 a 100 km.</p>	
	<p>Fibra óptica: Es un enlace hecho con un hilo muy fino de material transparente y recubierto de un material opaco que evita que la luz se disipe. Por el núcleo, es una hebra fina hecha de vidrio o plásticos, se envían pulsos de luz, no eléctricos. La velocidad máxima de transmisión es mayor a 10 Gbps y la distancia entre repetidores es mayor a 100 km.</p>	

	La transmisión y la recepción de información se lleva a cabo por antenas. A la hora de transmitir, la antena irradia energía electromagnética en el medio y la antena lo receptiona cuando capta las ondas electromagnéticas del medio que la rodea.	
Medios no guiados	<p>Señales de bluetooth: Hacen posible la transmisión de los datos mediante un enlace por radiofrecuencia.</p>	
	<p>Señales de infrarrojo: Son ondas direccionales incapaces de atravesar objetos sólidos.</p>	
	<p>Señales de wifi: Permiten la interconexión inalámbrica de dispositivos electrónicos.</p>	

VELOCIDADES DE INTERNET:

Internet es una red global donde es posible acceder a casi cualquier tipo de información, mediante la comunicación con cualquier persona o dispositivo en el mundo. Posee las mismas características que las otras redes de comunicaciones de datos.

Características de una red de datos:

Nombre	Descripción
Velocidad	Es el tiempo en el que se transmiten los datos, la rapidez de subida y bajada depende del medio y estándares que utilicemos para comunicarnos, se mide generalmente en megabits por segundo.
Seguridad	Su objetivo está en evitar que intrusos accedan a la información transmitida.
Confiabilidad	Mide la relación de fallos en la transmisión: menos fallos, más confiable.
Escalabilidad	Evita que el servicio no decaiga si el número de usuarios aumenta.
Disponibilidad	Es la capacidad de la red para estar siempre funcionando.

Bajada de datos	Es la capacidad que tiene Internet para navegar entre la red, es decir, la velocidad con la cual podemos descargar elementos —por ejemplo, páginas web—.
Subida de datos	Es la capacidad de cargar datos en la Web, por ejemplo, podríamos verlo en el tiempo que demora en subir un video a YouTube.
Paquetes	Son los bloques en lo que se divide la información al viajar por la red. El ping es el tiempo exacto que demora un paquete de datos en ser enviado de un dispositivo a otro, se mide en milisegundos.

Test de velocidad:

Un test de velocidad, o speedtest, es una herramienta utilizada para evaluar la performance de nuestra de red datos o de Internet. En ella podemos ver nuestra velocidad de subida, bajada y ping.

Desde aquí podemos ingresar a un test sencillo, que evaluará estos aspectos:

<https://www.speedtest.net/es>

Luego de ingresar, hacemos clic en “Inicio”, se realiza el test y, a continuación, nos mostrará una pantalla como la siguiente:



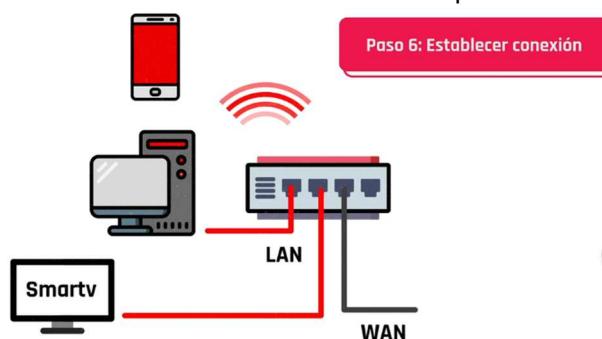
ARMANDO NUESTRA PROPIA RED:

Pasos:

- 1) Listar todos los dispositivos que vamos a conectar a la red.
- 2) Analizar cuales dispositivos necesitan conexión cableada, y cuales inalámbrica. Debemos recordar que la red cableada tendrá mejor performance y será más segura que una red inalámbrica.
- 3) Hacer un croquis de la casa con la ubicación de los distintos dispositivos que se conectarán a través de cableado.
- 4) Diseñar la red y decidir estratégicamente donde ubicar al router. Las compañías de internet normalmente nos entregan un router que trae un modem integrado capaz de transmitir datos por cable y por wifi. Si solo nos proveen de un modem, debemos conseguir un router wifi; en cambio si nos proveen un router con modem integrado, pero sin wifi, debemos adquirir un punto de acceso wifi.

El router cumplirá la función de separar la red pública que llega desde el exterior y la red privada de nuestra casa.

- 5) Ubicar el router. Lo ideal es ubicarlo lo más cerca posible del centro de la casa, para poder tener en cuenta la distancia de los dispositivos que van conectados por cable, sino también encontrar la mejor cobertura para la conexión wifi.
- 6) Tomar las medidas necesarias entre el router y los dispositivos que se conectarán a través de cables, y comprar el cable red para hacer la conexión. El cable debe ser UTP categoría 5E o 6. Cada tramo de cable debe tener dos fichas RJ45 en sus extremos.
- 7) Conectar los cables que llegan del exterior (de la red WAN) al router, y en cada una de las bocas del router conectamos uno a uno los cables que compramos. Si son más de 4 dispositivos los que queremos conectar, vamos a necesitar un switch para conectar los cables que faltan. En el otro extremo del cable conectamos los dispositivos.



Para la red wifi debemos tener en cuenta que la cobertura de la conexión dependerá de la ubicación del router. En el caso de estar en una casa muy amplia o con muchas paredes, podemos instalar extensores de red wifi o PLC para cubrir todos los espacios necesarios. El extensor debe estar en un punto intermedio entre el router y la zona donde queremos que llegue la señal.

¿Qué sucede cuando nos conectamos a una red?

Ya sea por un medio guiado o inalámbrico, siempre que nos conectamos a una red, el router nos identifica para reconocernos y, cuando necesitamos, interactuar con los demás dispositivos conectados.

Dirección IP:

La dirección IP o simplemente IP es un número único, el cual reconoce a cada dispositivo conectado en una red. Podríamos comparar a las IP con los números telefónicos que identifica a cada una de las personas en una agenda.

Puerta de enlace:

De la misma forma que cada dispositivo conectado a la red posee una IP. El router, dispositivo que administra la red, también posee una conocida como puerta de enlace.

La puerta de enlace es utilizada por los dispositivos de una red cuando se comunican con un dispositivo de una red diferente a la que se encuentran, esto sucede por ejemplo cuando navegamos en Internet.

IP dinámica o estática:

La asignación IP de nuestro dispositivo puede ser de dos maneras:

- 1) **Dinámica**: si permitimos que el router designe de forma automática nuestra IP.
- 2) **Estática**: cuando nosotros desde el sistema operativo la definimos.

Comandos básicos:

```
>_ ipconfig
```

En Windows y Mac nos muestra la dirección IP y puerta de enlace de nuestra pc.

```
>_ ifconfig
```

En Linux nos muestra una descripción de la dirección Ip y puerta de enlace de nuestra Pc.

```
>_ ping www.digitalhouse.com (URL o dirección IP)
```

Este comando envía paquetes a la dirección especificada. Es utilizado para comprobar conectividad entre dispositivos.

CLASE 13 – PROTOCOLOS DE INTERNET:

¿CÓMO FUNCIONA LA INTERNET?

Los protocolos son reglamentos o instrucciones que se fijan por tradición o convenio.

Los protocolos de internet fueron diseñados para encaminar confiabilidad y eficiencia a la transferencia de distintos datos específicos en las redes.

El modelo más importante de protocolos que hacen posible internet es el **Modelo de protocolo TCP/IP**. El TCP/IP —protocolo de control de transmisión/protocolo de Internet— consiste en una combinación de los protocolos previamente mencionados y son la piedra angular de las redes informáticas modernas.

Y algunos de los más importantes y usados son:

- **TCP (Transmission Control Protocol)**: hace referencia al protocolo de control de transmisión que permite la comunicación confiable entre computadoras, garantizando el establecimiento de la conexión, la transferencia de datos y la finalización de la conexión.

El TCP garantiza que los datos sean entregados al lugar de destino, sin ningún error y en el mismo orden que se transmitieron. Se encuentra en una capa intermedia entre el protocolo IP y la aplicación y, esta ubicación se debe a que la aplicación necesita que la comunicación de la red sea confiable. El protocolo TCP da soporte a muchas de las aplicaciones más populares de Internet —navegadores, intercambio de ficheros, etcétera— y protocolos de aplicación HTTP, SSH, FTP, entre otros.

- **IP (Internet Protocol):** el protocolo de internet, permite enviar los datos en paquetes direccionables a las distintas computadoras de la red.

IP es un protocolo de comunicación de datos digitales clasificado funcionalmente en la capa de red —que es la que nos proporciona conectividad y la selección de ruta entre dos sistemas hosts—. La función principal es conseguir que los datos lleguen desde origen al destino, aunque no tenga una conexión directa. Estos datos se transfieren mediante paquetes conmutados —método de agrupar los datos transmitidos a través de una red digital en paquetes, estos están compuestos por los datos en sí y la información de control que nos indicará cual es la ruta que debe tomar para que los datos lleguen a destino—.

Este protocolo se encargará de buscar el mejor método de enrutamiento, sin garantías de alcanzar el destino final, pero aun así trata de buscar la mejor ruta entre las conocidas por la máquina que esté usando IP.

- **DHCP (Dynamic Host Configuration Protocol):** el protocolo de configuración dinámica de host es el encargado de asignar las direcciones IP.
- **HTTP (Hypertext Transfer Protocol):** es un protocolo cliente-servidor que gestiona las transacciones web entre esas dos entidades. Nos permite navegar en sitios web a través de direcciones www y enlaces.

El protocolo de transferencia de hipertexto es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor. El cliente —normalmente un navegador web— realiza una petición enviando un mensaje, con cierto formato al servidor. El servidor —se le suele llamar un servidor web— le envía un mensaje de respuesta, permitiendo la comunicación entre ambos. Tiene como desventaja que no está protegida y podríamos pensar que toda la información está en texto puro. Si alguien intercepta una comunicación, podría ver nuestros datos.

- **HTTPS (Hypertext Transfer Protocol Secure):** el protocolo seguro de transferencia de hipertexto está destinado a la transferencia segura de datos de hipertexto. Lo que hace es encriptar los datos que son enviados entre clientes y servidores utilizando algoritmos de encriptación, de este modo toda la información sensible, como números de tarjetas, números de teléfono, claves de acceso, entre otros, pueden ser enviados de manera segura. Si alguien intercepta una comunicación, no podría ver nuestros datos sensibles, solamente obtendría un mensaje encriptado y este va a ser muy difícil de desencriptar.
- **URI (Uniform Resource Identifier):** una dirección www, comúnmente conocida como dirección web y técnicamente llamada como URI, es un bloque de texto que se escribe en la barra de navegación de un navegador, y puede ser identificada de dos maneras:
 - 1) URL: indica donde se encuentra el recurso que deseamos obtener, y siempre comienza con un protocolo (el http).
 - 2) URN: es el nombre exacto del recurso uniforme. El nombre del dominio, y en ocasiones el nombre del recurso. Son las que como usuarios ingresamos en el navegador, pero por detrás se redireccionan a direcciones IP gracias al protocolo DNS.
- **DNS (Domain Name System):** el sistema de nombre de dominio permite a un servidor encargarse de la transformación URL a dirección IP.

El sistema de nombres de dominio, es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados tanto a Internet como a redes privadas, que asocia información con el nombre del dominio. Su función principal es “traducir” los nombres de los dominios que estamos acostumbrados, como youtube.com, en identificadores binarios asociados con los equipos conectados a la red o direcciones IP, como 84.78.754.20.

Para acceder a Internet los usuarios utilizan el nombre de dominio, en lugar de los complejos números de IP, pero ¿de dónde obtiene Internet las direcciones IP correspondientes a los nombres de dominio solicitados? Para ello, Internet utiliza su “agenda grande” llamada DNS. El servidor DNS proporciona este servicio a Internet.

- **UDP (User Datagram Protocol):** el protocolo de datagramas de usuario es un protocolo del nivel de transporte basado en el intercambio de datagramas —un datagrama es un paquete de datos y un paquete de datos es cada uno de los bloques en que se divide la información para enviar—. Su función es permitir el envío de datagramas a través de la red sin que se haya establecido previamente una conexión ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera.

El protocolo UDP es más ligero ya que no utiliza tantas capas como el protocolo TCP/IP porque no existe un control sobre el envío de los paquetes. Al ser orientada a la no conexión lo único que le interesa a este protocolo es enviar los datagramas lo más rápido posible, sin tener en cuenta si el paquete llegó completo o no. Se utiliza comúnmente para la transmisión de datos de alta velocidad, por ejemplo, para streaming, juegos online, entre otros.

- **FTP:** el protocolo de transferencia de archivos es utilizado para el envío y recepción de archivos entre dispositivos de la red.
- **SSH:** es el protocolo para acceder a equipos remotos.
- **SMTP:** el protocolo para transferencia simple de correo sirve para la transferencia de correos electrónicos.
- **POP3 e IMAP:** sirven para la recepción de los correos desde una casilla.

Protocolo IP:

El protocolo de Internet, conocido por sus siglas en inglés IP —Internet Protocol—, es el protocolo principal de la familia de protocolos de Internet y su importancia es fundamental para el intercambio de mensajes en redes informáticas. Es decir, son normas que nos van a regir el intercambio de información a través de una red de computadoras o dispositivos.

El protocolo IP junto al protocolo de control de transmisiones —TCP o Transmission Control Protocol— sientan las bases de Internet. Para que el remitente pueda enviar un paquete de datos al destinatario, el protocolo IP define una estructura de paquetes que agrupa los datos que se tienen que enviar. Así, el protocolo IP cómo se describe la información sobre el origen y el destino de los datos y los separa de los datos útiles en la cabecera de cada paquete de información enviado.

El protocolo IP identifica cada dispositivo que se encuentre conectado a la red mediante su correspondiente dirección IP. La dirección IP se utiliza para identificar de manera única tanto al dispositivo como a la red a la que pertenece, dividiéndose así en dos partes:

- Una dirección que identifica la red.
- Una dirección que identifica al dispositivo dentro de esa red.

No puede haber en una misma red y, por lo tanto, tampoco en Internet, dos dispositivos conectados con una misma dirección IP. La dirección IP es única y exclusiva para cada equipo conectado a Internet.

Pero, normalmente, no solemos memorizar las direcciones IP, sería casi imposible memorizar las IP de las webs a las que queremos acceder. Con este objetivo, se crearon los nombres de dominio. Entonces cada

vez que queremos acceder a una página web utilizamos su nombre de dominio, por ejemplo, google.com en vez de utilizar su dirección de IP 78.45.789.03

Quien se encarga de estas traducciones entre nombres de dominio y direcciones IP será el protocolo de sistema de nombres de dominio —Domain Name System o DNS— que tenga configurado nuestro dispositivo.

El protocolo de control de transmisión/protocolo de Internet —TCP/IP— consiste en un par de protocolos que permiten la comunicación entre los dispositivos o computadoras pertenecientes a una red sin importar si el software o el hardware de cada uno es diferente. Este protocolo funciona de la siguiente forma: cuando se transfiere información de un dispositivo a otro —por ejemplo, mensajes de correo electrónico o cualquier otro tipo de datos— esta información no es transmitida de una sola vez, sino que se divide en pequeñas partes. El modelo TCP/IP es usado para comunicaciones en redes y, como todo protocolo, describe un conjunto de guías generales de operación para permitir que un equipo pueda comunicarse en una red. TCP/IP provee conectividad de extremo a extremo especificando cómo los datos deberían ser formateados, direccionados, transmitidos, enrutados y recibidos por el destinatario.

LA FAMOSA DIRECCION IP:

Una dirección IP es un número único que representa la ubicación de un dispositivo dentro de Internet o de una red. Ninguna página web puede estar online si no tiene una IP asociada.

IP (Internet Protocol) significa “protocolo de Internet”, lo cual representa unas series de reglas y formatos mediante la cual los datos son enviados a través de una red.

Cuando ingresamos a una página web, por ejemplo google, escribimos en el navegador “www.google.com” y el navegador traduce ese texto a una dirección IP para conectarse a la página de google y acceder a su contenido. De la misma manera, si quiero enviar información desde mi computadora hacia otro dispositivo (este ubicado en mi domicilio o en otro lado) debo conocer su dirección IP, y esta dirección debe ser única para que al enviar información llegue hasta la dirección correcta.

IPv4:

Una dirección IP es una cadena de números separados por puntos, donde cada conjunto se llama octeto:



Las direcciones IPv4 se expresan como un conjunto de cuatro números, un ejemplo podría ser la dirección 192.158.1.38.

Cada número del conjunto puede oscilar entre 0 y 255. Por lo tanto, el rango de direccionamiento IP completo va desde 0.0.0.0 a 255.255.255.255.

255 no es un numero al azar, cada octeto se llama así porque está formado por 8 bits (bit = 0 o 1). Entonces cada octeto es un numero formado por 8 dígitos que pueden ser ceros o unos:

192.168.32.01 =11000000.10101000.100000.00000001

255 es el número más grande que puede ser formado por un numero de 8 bits.

00000000 = 0
00000010 = 2
00011000 = 24
01110011 = 115
11111111 = 255

Los números IP poseen una parte que corresponde a la red y otra que corresponde al host (o dispositivo):

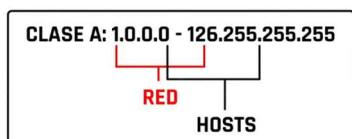
192.168.80.1

RED

HOST

La porción del número que identifica a la red varía en base a las clases. Las más importantes son las A, B y C.

La clase A se distingue porque su número de red solo contiene un octeto, y el resto corresponde a números de host:



La clase B tiene dos octetos habilitados para host. Y la clase C solo posee un octeto habilitado para host.

Existen dos tipos de direcciones IP:

- **Las públicas:** son todas aquellas que sirven para identificarnos en Internet, es decir, para identificar dispositivos en la gran red.

Desde		A	
	Identificador de red	Identificador de host	Identificador de red
Clase A		0.0.0	127.255.255.255
Clase B		128.0.0	191.255.255.255
Clase C		192.0.0	223.255.255.255
	Dirección de grupo		Dirección de grupo
Clase D	224.0.0.0		239.255.255.255
	Indefinido		Indefinido
Clase E	240.0.0.0		247.255.255.255

- **Las privadas:** son el número asignado a un dispositivo dentro de una red privada. Es decir, para identificar, por ejemplo, nuestro celular, notebook, tablet, entre otros dispositivos, dentro de una misma red wifi en nuestro hogar. Se reservan para ello determinados rangos de

Desde		A	
	Identificador de red	Identificador de host	Identificador de red
Clase A		10.0.0.0	10.255.255.255
Clase B		172.16.0.0	172.31.255.255
Clase C		192.168.0.0	192.168.255.255

La dirección IP será estática o dinámica en función de si es siempre la misma o va cambiando. Dependiendo del caso, será asignada por el proveedor de acceso a Internet, un router o el administrador de la red privada a la que esté conectado el equipo.

- **Estática:** un número IP asignado de manera fija, es decir, aunque el dispositivo con la IP asignada esté apagado, este continuará manteniendo la misma dirección.

- **Dinámica:** se asignan cuando el dispositivo está funcionando, dependiendo de las IP que están libres, a diferencia de las estáticas si el dispositivo se apaga, cuando vuelva a encenderse podría llegar a tener otra IP diferente.

Máscara de subred:

Una subred es una combinación de números que sirve para delimitar el ámbito de una red de computadoras. El protocolo TCP/IP usa la máscara de subred para determinar si un host está en la subred local o en una red remota.

Su función es indicar a los dispositivos que parte de la dirección IP es el número de la red, incluyendo la subred y qué parte es la correspondiente al host.

Los números IP, como vimos anteriormente, poseen una parte que corresponde a la red y otra que corresponde al host (o dispositivo):

192.168.80.1

RED

HOST

¿Cómo distingue el sistema que parte es la red y que parte es el host?

192.168.80.1 → Número de IP

A través de una máscara de subred: **255.255.255.0** → Máscara de subred

¿Para qué sirve una máscara de subred?

En nuestra casa tenemos tres dispositivos conectados: La IP del primero es 192.168.1.2, la del segundo 192.168.1.3 y la del tercero 192.168.1.4. Podemos ver que los tres primeros números son iguales mientras que el último cambia. Lo que hace la máscara de subred es identificar esa parte fija de la IP de la parte variable. La máscara le asignará el 225 a la posición de nuestra IP que no varía y le pone un 0 a la variable.

192.168.1.2

192.168.1.3

192.168.1.4

Números de IP

255.255.255.0

Máscara de subred

Se pueden separar la dirección IP y la máscara de subred, la red y las partes de host de la dirección, podemos verlo transformando las direcciones a binario:

Dirección IP:

192.168.1.2 = 11000000.10101000.00000001.00000010

Máscara de subred:

255.255.255.0 = 11111111.11111111.11111111.00000000

Los primeros 24 bits se identifican como la dirección de red. Los últimos 8 bits se identifican como la dirección de host. Esto nos proporciona los siguientes números:

Dirección de Red

192.168.1.0 = 11000000.10101000.00000001.00000000

Dirección de Host

0.0.0.2 = 00000000.00000000.00000000.00000010

Si el router tiene la dirección IP 192.168.1.1 y máscara 255.255.255.0, todo lo que se envía a una dirección IP con formato 192.168.1.X se manda hacia la red local, mientras que direcciones con distinto formato de dirección IP serán enviadas hacia otra red, como Internet.

Direcciones IP importantes:

Existen algunas IP dentro de las redes que solo un dispositivo puede tener y por lo que, si otro dispositivo se asigne una de estas direcciones, la red podría no funcionar correctamente.

- **Router:** la primera dirección disponible (por ejemplo 192.168.1.1) corresponde al router, el dispositivo que hace enlace con las otras redes, como Internet. De este modo, todos los dispositivos que quieran consultar algo en Internet lo primero que deben hacer es enviar la petición a la dirección del router, el cual se encargará de redirigir la petición.
- **Broadcast:** es la dirección más alta de la red a la que pertenezca el dispositivo, y es utilizada por el router para enviar un mensaje de difusión a todos los dispositivos que tengan una IP asignada dentro de la red, en redes hogareñas generalmente es 192.168.1.255.

IPv6:

IPv6 es la versión 6 del protocolo de Internet. Está destinada a sustituir al estándar IPv4 ya que la anterior versión cuenta con un límite de direcciones de red que impide el crecimiento de la misma.

Ventajas de IPv6:

- **Número casi ilimitado de IPs únicas:** este nuevo protocolo permite que cada dispositivo conectado a Internet tenga su propia dirección IP. Una ventaja que poco a poco se va convirtiendo en un requisito con el continuo avance del Internet de las cosas.
- **Autoconfiguración:** el nuevo protocolo consta de mejores métodos para realizar la configuración automática, lo que supone una mejora significativa respecto al clásico DHCP utilizado en IPv4.
- **Más seguridad:** el protocolo IPv6 puede ser mejorado con IPsec (Internet Protocol Security, en inglés) para gestionar la encriptación y autenticación entre hosts. Proporciona un sólido marco de seguridad de punto a punto en la transferencia de datos.
- **Más eficiencia:** la gestión de paquetes es mucho más eficiente en IPv6.

¿Cómo podemos conocer nuestra IP privada y pública?

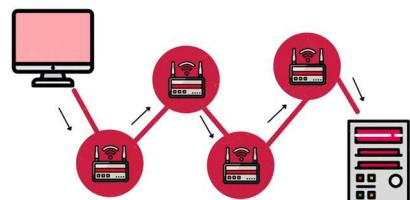
- Pública: desde <https://whatismyip.com>.
- Privada: desde la terminal con el comando “ipconfig” para Windows, o “ifconfig” en Linux y Mac.

CLASE 14 – PROTOCOLOS AVANZADOS:

REDES INTERNAS:

¿Cómo se transmite la información que enviamos a través de internet?

Una de las formas es el **routing o enrutamiento** que es la acción de mover datos de una red a otra. Este proceso es llevado a cabo por el router, que permite interconectar computadoras estableciendo que ruta seguirán mis datos.



Cada vez que enviamos un mail, ingresamos a un sitio de internet, reprodujimos un video, etc., la información viaja desde mi computadora hasta su destino en cualquier parte del mundo a través de cientos o miles de routers.

Por ejemplo:

Mi computadora, posee la siguiente red y dirección IP:



Dirección IP

192.168.1.0

192.168.1.5

Cuando queremos ingresar a una página web, google por ejemplo, la computadora envía una solicitud a través del navegador. Primero traduce la dirección www.google.com en una dirección IP, y esa será la dirección a la que viajara la solicitud de visualización de una pagina web.

Esa solicitud sale como un mensaje hacia el router de mi red local, y este será quien nos comunicara con el exterior. Cuando el mensaje llega al router, este busca cual es la dirección de destino y reconoce que no pertenece a nuestra red local, verifica en la tabla de enrutamiento que tiene configurada cual es la mejor ruta posible para que el mensaje (los paquetes de datos) llegue a destino. En esa ruta habrá más routers que irán pasando el mensaje hasta que llega a destino.

Una vez que llega a la computadora de destino, esta responde con la información que satisface la solicitud, la cual viaja a través de los routers hasta llegar a mi computadora.

La conexión entre dos computadoras siempre se establece de la misma forma, a través de direcciones IP. Si queremos obtener diferentes servicios de la otra computadora dentro de la misma conexión (por ejemplo: conectarnos a la página web y al servicio de mails que provee) las diferenciamos a través de puertos. Cada dispositivo tiene 65536 puertos, cada uno destinado a enviar o recibir cierto tipo de información. Los más conocidos van del 0 al 1023, y son los que están reservados para el sistema operativo y los protocolos de red más importantes. El puerto 21 le corresponde al FTP, el 25 al SMTP, y el 80 al HTTP. Los puertos del 1024 al 49151 son los que utilizan las aplicaciones y juegos que utilizan nuestras computadoras; y los superiores al 49151 le pertenecen a los puertos dinámicos o privados.

Entonces, cuando solicitamos una página web hicimos una petición de tipo HTTP, lo que quiere decir que solicitaremos esa información al puerto 80 de la computadora que contiene la página. Esta información viaja junto a la dirección IP:



142.251.33.100 : 80

Al mismo tiempo se genera un puerto aleatorio en mi computadora, en el que recibirá la información de respuesta. Una vez que el mensaje llega a la computadora de destino, esta sabe que debe responder con una página web, porque la petición ingreso por su puerto 80. La respuesta vuelve hacia nuestra PC por los routers, ingresa por el puerto aleatorio y la página web se puede visualizar.

¿Cuál es la función de un router en la red?

El router realiza las siguientes acciones:

- 1) Recibe el paquete de datos.
- 2) Busca cuál es la dirección de destino.
- 3) Verifica la tabla de enrutamiento que tiene configurada.
- 4) Procede a enviar el paquete a destino por la mejor ruta posible

Tabla de enrutamiento:

Son un conjunto de reglas que sirven para determinar qué camino deben seguir los paquetes de datos.

Las tablas de enrutamiento contienen toda la información necesaria para hacer que uno o varios paquetes de datos puedan viajar a través de la red utilizando el mejor camino.

Algunos componentes importantes de una tabla de enrutamiento son:

- Red de destino: corresponde a la red de destino donde deberá ir el paquete de datos.

- Siguiente salto: es la dirección de IP de la interfaz de red por donde viajará el paquete de datos para seguir con su camino hasta el final.
- Interfaz de salida: es la interfaz de red por donde deben salir los paquetes para llegar posteriormente a destino.

Tipos de enrutamiento:

Enrutamiento estático	Enrutamiento dinámico
<p>Las tablas se crean de forma manual. El administrador de red las configura con la información de cómo alcanzar las diferentes redes remotas. Este es responsable de que las redes sean accesibles y estén libres de bugs e inconsistencias.</p> <ul style="list-style-type: none"> • Consume menos ancho de banda. • Consume menos memoria. • Se utiliza para redes pequeñas. • No es escalable. <p>Ventajas: Aunque el mantenimiento es complicado, no se consume ancho de banda de red para enviar mensajes entre routers.</p> <p>Desventajas: Cualquier cambio en la red requiere que el administrador agregue o elimine las rutas afectadas por dichos cambios.</p>	<p>La información necesaria para crear y mantener actualizadas las tablas se obtienen de los demás routers de la red. Estos utilizan protocolos de enrutamiento para intercambiar información con sus routers vecinos.</p> <ul style="list-style-type: none"> • Alto consumo de ancho de banda. • Alto consumo de memoria. • Se utiliza para redes grandes. • Es automático. <p>Ventajas: El administrador solo pone en marcha el enrutamiento dinámico, luego las tablas de enrutamiento se ajustan automáticamente ante cambios en la red.</p> <p>Desventajas: Consumo mucho ancho de banda, debido a los mensajes que se intercambian los routers para configurarse automáticamente.</p>

Puertos:

Los puertos son puntos de conexión para el intercambio de información y la transmisión de datos.

Cuando enviamos datos desde nuestra red local a la externa el router utiliza una serie de canales o puertas en las que se organiza el contenido que enviamos. Estos son los puertos. Funcionan como puertas que se abren y cierran y permiten el paso de la información que enviamos o recibimos en la red.

Todos los routers tienen un total de 65536 puertos que van desde el 0 al 65535. La IANA, entidad que supervisa la asignación global de direcciones IP y otros recursos relativos a los protocolos de internet tiene establecido un estándar de asignación de puertos.

Existen 3 grupos de puertos que tienen una función específica:

- 1) **Puertos del 0 al 1023:** Son los que están reservados para el sistema operativo de la computadora y los protocolos más importantes para su funcionamiento.
- 2) **Puertos del 1024 al 49151:** Son los puertos registrados, los que se utilizan por las aplicaciones y los juegos que instalas en la computadora.
- 3) **Puertos del 49152 al 65535:** Puertos dinámicos o privados, corresponden a las aplicaciones que necesitan conectarse a un servidor.

REDES EXTERNAS (HTML):

Cuando nuestros datos salen de router, viajan fuera de nuestra red local y van directamente a parar al ISP (Proveedor de Servicios de Internet), que es la empresa que nos brinda conexión a internet a través de diferentes tecnologías (fibra óptica, banda ancha, cable modem, 3G, 4G, etc.).

Actualmente la mayoría de nuestros paquetes de datos viajan protegidos y solo es visible a donde viajan (no el contenido). Los ISP reciben todos los paquetes de datos que enviamos y los envían a su destino,

pudiendo aplicar filtros de normativa referentes a bloquear páginas de piratería, contenido protegido geográficamente o políticas gubernamentales (según lo que determine cada gobierno).

En internet existen distintos protocolos que hacen esto llamado direccionamiento externo. Algunos métodos son:

- **Proxy:** se trata de un equipo informático que intercepta conexiones de red hechas desde un cliente a un servidor de destino, eludiendo así el ISP.
- **VPN o Red Privada Virtual:** es una tecnología que permite una extensión segura de la red local sobre una red pública como internet, permitiendo que nuestra computadora envíe y reciba datos conectándose a otras redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada.
- **TOR:** es una red de anonimato que se encuentra distribuida y superpuesta sobre internet, en la que el direccionamiento de los mensajes intercambiados entre los usuarios no revela su dirección IP. Además, mantiene la integridad y el secreto de la información que viaja por ella. Para utilizarla, primero el usuario accede a un intermediario de la red TOR, quien sabe la identidad del usuario, pero no con quien se comunicará, y el último intermediario sabe con quién se comunica, pero no quién es el usuario que envía el mensaje. De este modo, nadie puede saber con quién se comunica.

VPN:

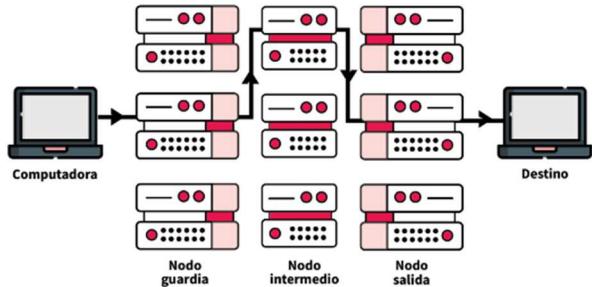
Una red privada virtual, o por sus siglas en inglés también llamada VPN, es una tecnología que protege nuestra privacidad cuando utilizamos Internet dirigiendo nuestra conexión a través de un servidor que oculta la dirección IP y encripta la comunicación online. Cuando se utiliza una VPN, la información enviada desde la computadora pasa a través de uno de los servidores del proveedor de VPN antes de llegar a su destino.



Ventajas			
Son fáciles de instalar y utilizar.	Velocidad	Compatibilidad con la mayoría de los dispositivos.	
Desventajas			
Encriptación débil	Fallos del software	Políticas de registro variadas	

TOR:

A primera vista, la red Tor es similar a una VPN. Los mensajes hacia y desde su computadora pasan a través de la red Tor en lugar de conectarse directamente a los recursos de Internet. Pero donde las VPN brindan privacidad, Tor brinda anonimato.



Ventajas	Difíciles de apagar La red está distribuida por lo que no hay un lugar central para hacerlo.	Anonimato casi completo	
Desventajas	Lentitud Los mensajes pasan por tres o más servidores y se cifran y descifran al menos 3 veces.	Dirigida por voluntarios Por lo tanto, no hay ingresos para actualizaciones y mantenimiento.	Baja compatibilidad con dispositivos

CLASE 15 – SEGURIDAD INFORMATICA:

La seguridad informática, o ciberseguridad, es una disciplina que se encarga de proteger la integridad y la privacidad de los datos y toda la información que se encuentre alojada en un sistema informático. La idea principal es que se pueda evaluar la seguridad de los sistemas de cómputo y redes para, posteriormente, protegerlos de los ataques informáticos que se pueden llevar a cabo a los sistemas.

CIBERSEGURIDAD Y TIPOS DE AMENAZAS:

La seguridad informática se enfoca en la protección de la infraestructura computacional y todo lo vinculado con la misma, especialmente, en la información que se transmite a través de las redes de computadoras. Para minimizar todos los riesgos a la infraestructura y a la información se han creado a lo largo de la historia múltiples métodos, como estándares, protocolos, reglas, herramientas y obviamente leyes informáticas.

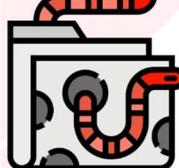
Debemos tener en cuenta que la seguridad informática únicamente se va a centrar en el medio de comunicación por el cual va a viajar la información. No debemos confundir este término con el de seguridad de la información, ya que esta última puede estar en diferentes medios y no solo en los medios informáticos.

Bajo este último concepto, la **seguridad informática** va a identificar, eliminar vulnerabilidades y proteger de ataques maliciosos a los equipos de cómputo, servidores, redes informáticas y todo aquel medio informático por el cual se transmita información.

Tipos de amenazas informáticas:

Malware significa “Malicious Software”, y es el término que se utiliza para definir a todos los softwares maliciosos que tienen como objetivo infiltrarse o dañar un sistema de información sin el consentimiento del usuario. Para que el malware pueda completar su objetivo es primordial que este oculto al usuario, porque es lo que le permite seguir actuando. Si el usuario nota que existe algún tipo de malware, hará lo posible por eliminarlo.

Es un concepto amplio que incluye virus, troyanos, gusanos, etc.

AMENAZAS TECNOLOGICAS MAS COMUNES	
Virus 	<p>Es el primero y más antiguo de todos. Es un malware con el objetivo de permanecer en el sistema copiándose a sí mismo en varios lugares desde el momento que se ejecuta en el sistema, así cuando intentamos eliminar un archivo o programa infectado, el virus seguirá en la memoria porque habrá infectado otras partes del sistema.</p> <p>El objetivo de un virus puede variar, pero en esencia busca destruir o inhabilitar archivos o programas que tengamos en el dispositivo, además de afectar el funcionamiento del mismo.</p> <p>La mayoría de los virus se adhieren a archivos ejecutables o al registro maestro de arranque. Son de poca afección, no tienen capacidad por si mismos de afectar a otros dispositivos a menos que lo pasemos por medio de un hardware, como por ejemplo un USB.</p>
Gusano 	<p>Es un malware que se copia a sí mismo en el sistema, y utiliza la red para copiarse a otras máquinas a través de las vulnerabilidades de la red o agujeros de seguridad, lo cual le da mayor capacidad de infección.</p> <p>El objetivo del gusano es replicarse a sí mismo hasta saturar el funcionamiento del sistema.</p> <p>Cuando ataca un gusano, se debe apagar toda la red para que no se propague y pasar un antimalware.</p>
Troyanos 	<p>No causan daños en sí mismos, pero funcionan como una estructura para cargar malwares ocultos. Por lo general son los programas sin licencias que instalamos en nuestras computadoras.</p> <p>Requieren de la ejecución del usuario, porque no pueden duplicarse por sí mismos. Los troyanos pueden generar “backdoors” que son puertas traseras para que un dispositivo pueda ser controlado de forma remota por alguien más.</p> <p>Pueden ser utilizados como servidores proxys para ocultar ataques o introducir spam.</p>
Adwares 	<p>El objetivo que tienen es bombardear los dispositivos con publicidades. No son dañinos, y usualmente vienen dentro de los troyanos.</p>

Todos estos malwares atacan el sistema operativo, por lo tanto, una vez que se reinstala el sistema desaparece el malware.

Existen algunos especialmente peligrosos, que cuentan con un modo de ataque más sutil para robar:

Spywares	Son softwares espías que no dañan el dispositivo pero que roban información del sistema.
-----------------	--

	<p>El objetivo es permanecer oculto para poder robar todo tipo de datos. También puede acceder a la cámara o micrófono del dispositivo sin que el usuario lo note. Este tipo de malwares suelen ingresar en troyanos, o también pueden ser instalados. Este malware también ataca el sistema operativo, por lo tanto, una vez que se reinstala el sistema desaparece.</p> <p>Permanecen ocultos al usuario.</p>
Rootkits	<p>Son malwares más complejos formados por un conjunto de softwares. Está dirigido a los programas de usuarios, por lo tanto, tienen acceso al dispositivo en modo sistema o kernel, que les permite realizar modificaciones a los procesos internos del sistema operativo, a los archivos del sistema, e incluso a las cuentas de usuario.</p> <p>Estos malwares logran esconderse de los softwares antimalwares y antivirus. Permanecen ocultos al usuario.</p>
Botnets	<p>Bot = robot – Net = red.</p> <p>Son una red de robots puesto por un atacante en una red de computadoras para ser todas controladas al mismo tiempo. Suelen ser enviados a través de troyanos.</p> <p>Por lo general se usan para cometer crímenes digitales (crimewares) como robos de identidad o información bancaria.</p> <p>Permanecen ocultos al usuario.</p>
Ransomware	<p>Los softwares de secuestro suelen ser utilizados para atacar empresas y secuestrar su información de servicios y productos, y luego pedir un rescate.</p> <p>El ciber-atacante hace evidente el chantaje por secuestro y generalmente suele pedir una contraseña para ingresar de nuevo al sistema. Este tipo de malwares se pueden encontrar en archivos adjuntos de correos electrónicos no deseados, o al hacer click en vínculos que aseguran venir de bancos o instituciones legales.</p>

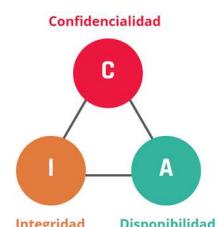
Consejos:

- ✓ Tener cuidado con las descargas que realizamos en nuestros dispositivos y el uso de aplicaciones no autorizadas.
- ✓ Evitar el uso de páginas peligrosas.
- ✓ Usar un software antimalware.

PROTECCION DE LA INFORMACION:

Principios de la seguridad de la información:

La información es recurso clave para tomar decisiones, dimensionar cosas, y disminuir riesgos. La misma cuenta con tres dimensiones conocidas como: integridad, disponibilidad y confidencialidad, también llamadas CIA por sus siglas en inglés. Los atacantes de un sistema van a tratar de vulnerar algunas de esas dimensiones.



- **Integridad:** consiste en que la información se encuentre completa, entera y que los datos que están dentro del sistema sean los que deberían ser. Un ejemplo de esta dimensión sería el ataque a una base de datos y la modificación de los datos que hay en la misma, con lo cual podemos seguir viendo la información, pero la misma es errónea debido a que la original fue alterada.
- **Disponibilidad:** significa que la información una persona/usuario debe poder tener acceso a la información en el momento que lo necesita, es decir, en tiempo y forma. Un típico ataque a este tipo de dimensión es el ataque de denegación de servicio.

- **Confidencialidad:** refiere a que la información tiene que estar disponible únicamente para las personas que tienen acceso a esta información y bloqueada para el acceso a terceros. Por ejemplo, los datos personales e historiales médicos.

Protección de la información:

La protección de la información se basa en garantizar el completo y total funcionamiento de las 3 dimensiones, para ello, debemos implementar medidas preventivas y reactivas.

Medidas preventivas se refiere a todas las acciones que pueden tomarse para evitar problemas no deseados. Por otro lado, las medidas reactivas son aquellas donde ya se ocasionó un problema de seguridad y hay que solventarlo.

Protección de la confidencialidad:

La confidencialidad puede romperse de varias maneras, tanto directas (hackeando la seguridad) como indirectas a través de errores humanos. Algunas técnicas para asegurar la confiabilidad pueden ser:

Nombre	Descripción
Encriptación	Significa cambiar el formato de los datos con la razón de que si estos son interceptados solo las personas autorizadas sepan cómo leerlos (medida preventiva).
Controles de acceso	Asegurar que solo las personas autorizadas puedan acceder a la información (medida preventiva).
Borrado remoto	Se refiere al esfuerzo de mantener los datos siempre privados, en el caso de que se perdiera el acceso, la capacidad de bloquear el dispositivo o borrar la información (medida reactiva).
Capacitación al personal	Existe un concepto llamado ingeniería social, el cual es la denominación que se le da a cómo los usuarios son engañados para otorgar sus accesos, la capacitación en estos problemas es una acción preventiva para evitarlos.

Protección de la integridad:

La integridad puede romperse de varias maneras similares a la de la confiabilidad, por lo cual, varias de sus acciones de seguridad son reutilizadas. Algunas técnicas para asegurar la integridad pueden ser:

Nombre	Descripción
Auditorias	Se utilizan para comprobar que la información coincide con lo que debería ser correcto (medida reactiva)
Control de versiones	Si ha ocurrido un inconveniente con la información, diversas herramientas de control de versiones ayudan a “volver a un estado anterior” (medida reactiva).
Firmas digitales	Esta medida permite asegurar la autenticidad del documento (medida preventiva).
Detección de intrusos	Diseñados para detectar problemas cuando un acceso no autorizado se ha cometido (medida reactiva).

Protección de la disponibilidad:

La disponibilidad debe tenerse en cuenta para cuando ocurra un problema de seguridad como de forma preventiva al mismo. Algunas técnicas para asegurar la disponibilidad pueden ser:

Nombre	Descripción
Tolerancia a fallos	La capacidad de los sistemas o servidores a que si algún tipo de fallo sucede, la información pueda ser utilizada (preventiva o reactiva dependiendo la situación).

Redundancia	De esta forma la información y las validaciones de acceso se repitan tanto que la información está segura de no perderse en su totalidad (preventiva).
Parches de seguridad	Cuando se detecta una falla, debe solucionarse el problema para que no vuelva a ocurrir, igualmente si la falla fue por un software, actualizarlo con la vulnerabilidad resuelta

Falla:

Una falla, también conocida como bug, es un error en un programa o sistema operativo que desencadena un resultado indeseado.

El término bug viene desde 1947 cuando Grace Hopper, mientras estaba programando el Mark II, descubrió que un insecto (bug) había provocado un error en uno de sus relés electromagnéticos.

En el desarrollo del software existen muchos tipos de fallas, pero en general se pudieron establecer unos tipos generales de bugs según su comportamiento.

Tipo de fallas	Descripción
Heisenbug	Basados en el principio de incertidumbre de Heisenberg se denominan a aquellos bugs que alteran o desaparecen su comportamiento al tratar de depurarlos.
Bohrbug	Nombrados así por el modelo atómico de Bohr, es una clasificación de un error de software inusual que siempre produce una falla al reiniciar la operación que causó la falla.
Mandelbug	Llamado así por el matemático Benoit Mandelbrot, un mandelbug es un fallo con causas tan complejas que su comportamiento es totalmente caótico.
Schroedingerbugs	Son errores que no aparecen hasta que alguien lee el código y descubre que, en determinadas circunstancias, el programa podría fallar. A partir de ese momento, el "Schroedingerbug" comienza aparecer una y otra vez.

Vulnerabilidades:

Una vulnerabilidad es una debilidad o fallo de un sistema informático que puede poner en riesgo la integridad, confidencialidad o disponibilidad de la información.

La evaluación o detección de vulnerabilidades permite reconocer, clasificar y caracterizar los agujeros de seguridad.

Pasos para detectar una vulnerabilidad:

Si bien no existe un método único para detectar vulnerabilidades, es posible armar una serie de ítems a tener en cuenta para considerar nuestra información segura.

- Evaluar cómo está constituida la red e infraestructura de la empresa.
- Delimitar quién puede y debe acceder a la información confidencial.
- Probar que las copias de seguridad realizadas funcionen.
- Identificar las partes más sensibles y esenciales del sistema.
- Realizar auditorías del estado de la seguridad informática.

INGENIERIA SOCIAL:

La ingeniería social es el método de obtener información confidencial a través de usuarios legítimos del sistema a atacar.

Se basa en distintos métodos o acciones para **engañar al usuario**, así de esta forma conseguir la información buscada, como ser contraseñas o datos sensibles.

Técnicas más comunes de ingeniería social:

El arte del engaño digital consiste en obtener información de los usuarios a través de medios como teléfonos, emails, correo tradicional o contacto directo.

TECNICAS	
Pretexting	Se presenta cuando un supuesto representante de algún servicio pregunta por información de la cuenta del cliente
Baiting	Consiste en colocar pendrives o memorias externas con malwares en lugares de personas escogidas puedan infectar sus computadoras
Phishing	Consiste en engañar a un grupo de personas mediante correos electrónicos, páginas web, perfiles de redes sociales o sms falsos con el fin de robar información
Vishing	Llamadas telefónicas mediante las cuales se busca engañar a la víctima suplantando a personas del gobierno o empresas para que la víctima revele información privada
Redes sociales	Esta técnica tiene dos grandes objetivos, obtener información de la víctima y por otro lado generar una relación con la misma por otro lado para poder así ser estafada
Ciberbullying	Esto puede o no limitarse al uso de internet, se utiliza para amenazar con difundir textos o imágenes que dañen o avergüencen a la víctima
Grooming	Conjunto de estrategias en la que una persona adulta busca ganarse la confianza de un menor, para que a través de la tecnología poder abusar o explotar sexualmente de la víctima
Sexting	Comprende el envío o recepción de contenido sexual a través de medios electrónicos, el mismo consiste en el intercambio de imágenes o videos sexuales, en especial a través de celular.
Sextortion	Forma de extorsión en la que se chantajea a una persona por medio de una imagen o video de sí misma desnuda.

Todas estas técnicas varían según la interacción con la víctima, en las cuales pueden ser de manera **pasiva, no presenciales, presenciales no agresivas y agresivas**, todas con el mismo fin de chantajear a la persona.

CLASE 16 – EVALUACION FINAL.

CLASE 17 – SEGURIDAD INFORMATICA:

COMPONENTES BASICOS DE LA SEGURIDAD:

La seguridad de la información consiste en todas las acciones que llevamos adelante para proteger la integridad, la privacidad de los datos y toda la información que se encuentre alojada en un sistema informático. Para poder proteger a nuestra computadora tenemos dos tipos de seguridad: seguridad activa y seguridad pasiva.

SEGURIDAD ACTIVA	SEGURIDAD PASIVA
Los elementos denominados activos contienen información, pueden tener muchas formas: servidores, dispositivos móviles, bases de datos, entre otros. Esos activos contienen información que alguien quiere	Es un conjunto de acciones o técnicas de seguridad que entran en acción para minimizar los daños a los sistemas informáticos. Estas acciones se activan

vulnerar, obtener, destruir, etcétera. Como su intención es acceder a una información, lo va a hacer a través de una vulnerabilidad —problema que tienen los sistemas que contienen información—. La amenaza aprovecha esa vulnerabilidad para ingresar de forma indebida a la información y hacer lo que quería hacer. La seguridad activa protege y evita daños en los sistemas informáticos.

Buenas prácticas:

- Uso y empleo adecuado de contraseñas. Una de las técnicas para que una contraseña sea segura consiste en la combinación entre letras, números, mayúsculas y otros caracteres. No se debe usar nombre de mascotas o fechas de nacimiento, entre otros datos que pueden ser de conocimiento público.
- Uso de software de seguridad informática, como antivirus, anti-espías y cortafuegos.
- Encriptar los datos importantes: La encriptación consiste en cifrar los datos o la información mediante un algoritmo de cifrado con una clave para que el dato/información solo pueda ser leído si se conoce la clave de cifrado.

cuando se ha introducido un malware o cualquier otra amenaza en los sistemas.

Buenas prácticas:

- La realización de copias de seguridad de los datos en más de un dispositivo y/o en distintas ubicaciones físicas.
- Escanear y limpiar continuamente los equipos para controlar y evitar ataques de malware.
- Crear particiones en el disco duro para almacenar archivos y backups/copia de seguridad en una unidad distinta a donde tenemos nuestro sistema operativo.
- Frente a un ataque, desconectar el equipo de la red hasta que se pueda solucionar.
- Es importante que cuando haya una infección por un virus, comprobar que el antivirus funcione correctamente.

MEDIDAS DE PROTECCION:

¿Qué es el control?

Cuando hablamos de control solemos encontrar muchas definiciones. Sin embargo, en este curso nos vamos a referir a control como un proceso que consiste en una paridad entre un resultado con otro.

Muchas veces se piensa que la seguridad de la información consiste solo en implementar controles técnicos. Pero para que esta seguridad sea integral sobre los equipos y software informáticos se deben implementar también algunos controles de tipo administrativo y físicos. A continuación, veremos algunas de esas clases de controles.

CLASES DE MEDIDAS DE SEGURIDAD		
PROACTIVAS	Directivas	Nos dicen qué podemos o no hacer. Intentan que las actividades de los sistemas se realicen de una manera específica con el fin de que se produzcan ciertos resultados esperados.
	Disuasivas	Pueden desviar la intención del atacante potencial a un sistema o el uso indebido por parte del personal. Se diferencian con las directivas en que estas no nos restringen directamente, sino que nos hacen una advertencia, la cual se puede o no tener en cuenta a la hora de ejecutar la acción indebida.
	Preventivas	Buscan que no se produzca un accidente o cualquier tipo de acción indebida en los sistemas. La diferencia con las disuasivas es que estas buscan informar y prevenir una acción indebida.

REACTIVAS	 Detectivas	Se basan en la búsqueda de potenciales ataques o peligros a los que puede estar expuesto un sistema informático.
	 Correctivas	Una vez se ha encontrado el riesgo o ha sucedido un incidente que ha puesto en peligro a los datos o información, se activan estas medidas de seguridad. Su objetivo es solucionar el sistema luego que ha sucedido el desvío.

Auditoria:

Auditar es la acción de analizar de manera exhaustiva y profunda las distintas características y áreas de una organización. En informática, el auditor es el encargado de analizar y determinar que toda la informática de la organización trabaje de manera eficiente.

Objetivos	Descripción	Conocimientos necesarios del auditor
Eficiencia	Se debe trabajar de manera tal que la información recabada sea útil para la toma de decisiones.	Experiencia en gestión de proyectos.
Normativa	Se deben cumplir las normativas determinadas para certificar que la empresa trabaja bajo las normas estándares.	Conocimiento de softwares y normativas.
Gestión de recursos	Recursos utilizados de manera correcta.	Conocimiento de Infraestructura.

El auditor:

La mayoría de los auditores trabajan en **pequeños grupos** de hasta 4 personas y son el nexo directo con los distintos departamentos y dirección. El auditor informático **plasmará** en un **informe final** todas las debilidades, oportunidades de mejora y recomendaciones para que la organización **sin carácter obligatorio** decida si aceptarlas o no.

Las herramientas más comunes son:

- **Entrevistas:** a través de entrevistas al personal determinar si son conscientes y utilizan las normas establecidas por la empresa en su día a día.
- **Encuestas:** sirven para tener un panorama general del estado de la empresa.
- **Análisis de los procesos:** las empresas deberían tener documentado sus distintos procesos para que el auditor revise que cumplan los estándares pautados.
- **Análisis del código de software:** mediante distintas pruebas o análisis de la sintaxis los auditores aseguran que las pautas para el desarrollo de software sean cumplidas.

SEGURIDAD FISICA Y SEGURIDAD LOGICA:

Seguridad física:

Consiste en el establecimiento de técnicas que permiten resguardar de cualquier tipo de daños a los equipos en los cuales se almacena los activos de una organización (sus datos).

Incluye aspectos como:

- **Dispositivos físicos de protección:** pararrayos, extintores, detectores de humo, alarma contra intrusos, entre otros.
- **Uninterruptable Power Supply (UPS):** es un dispositivo electrónico que almacena energía por medio de una batería interna. Esto les permite a los dispositivos que están conectados al mismo, frente a un apagón eléctrico, seguir almacenando la información por un determinado tiempo.
- **Respaldo de datos:** es importante saber que los datos son los activos más importantes dentro de una organización, por tal motivo, es de suma importancia el manejo y cuidado de los mismos ya que pueden estar expuestos a muchos factores como hurto, alteración, virus, entre otros. Por tal motivo, se deben realizar copias de seguridad o backups de los datos completos e incrementales. El backup es un proceso por el cual se realiza la copia de los datos originales con el fin de prevenir cualquier tipo de pérdida de los mismos.
- **Sistemas redundantes:** son la copia de datos de mayor importancia. Cuando uno de los sistemas falla, no se pierde la información, sino que se recupera del otro lugar donde se encuentra.

Seguridad lógica:

La seguridad lógica es un tipo de software que impide que malware o hackers puedan ingresar a nuestra computadora a través de Internet o de una red. Está conformada por un conjunto de procesos que se encargan de garantizar la seguridad de los datos y sistemas, además controlan el acceso a los mismos.

Incluye aspectos como:

- **Control de acceso:** impide el acceso a personas no autorizadas mediante el uso de usuarios y contraseñas.
- **Cifrado de datos:** el cifrado es la acción de transformar un mensaje de tal forma que no pueda ser comprendido por otra persona distinta al receptor. Por lo tanto, el cifrado de datos consiste en la aplicación de un algoritmo de cifrado acompañado de una clave, con el objetivo de transformar el mensaje, para que únicamente pueda ser leído por el destinatario.
- **Antivirus:** permite escanear, detectar y eliminar malwares en un sistema informático.
- **Firewalls:** impide que un malware o hackers puedan ingresar a nuestra computadora a través de internet o de una red.

SEGURIDAD EN INTERNET:

Ataques de denegación de servicio (DoS):

Cuando hablamos de la dimensión de disponibilidad nos referimos a que la persona debe tener acceso a la información en el momento en que la necesite, en tiempo y forma.

La denegación de servicio consiste en la interrupción del acceso a los servicios (computadoras y redes) por parte de los usuarios legítimos.

En un DoS lo que sucede es que se produce una gran cantidad de peticiones desde solamente una máquina o una dirección IP al servicio, produciendo una saturación de los puertos, hasta que llega un momento en que el servidor no tiene capacidad de respuesta a todos los servicios solicitados y comienza a rechazar peticiones, es aquí donde se produce la denegación del servicio. Por otro lado, un DoS no solo puede ocurrir desde la red. El incremento del uso de recursos de manera sintética o forzada (como CPU o memoria) también puede producir un DoS. Es decir, no solo puede ocurrir saturando la red, sino que también se puede saturar otros recursos y producir el mismo efecto. Y esto podría ocurrir desde la red o internamente en el servidor con algún agente instalado programado para tal fin.

Ataques de denegación de servicio distribuido (DDoS):

En un DDoS lo que sucede es que se produce una gran cantidad de peticiones al servicio, pero en este tipo se lleva a cabo desde varios puntos o direcciones IPs de conexión produciendo la saturación del puerto de destino, hasta que llega un momento en que el servidor no tiene capacidad de respuesta a todos los servicios solicitados y comienza a rechazar peticiones, es aquí donde se produce el ataque de denegación de servicio distribuido.

Bot	Es una aplicación de software que se encarga de realizar las tareas que tienen la característica de ser simples y repetitivas. Las mismas se realizarán a través de Internet. Estos bots trabajan mucho más rápido de lo que trabajaría una persona
Botnet	Es un conjunto de dispositivos que están conectados a Internet y que cuya seguridad ha sido comprometida por un atacante para instalar un bot programado para efectuar un ataque de DoS. Los dispositivos comprometidos quedan a la espera de que el atacante envíe una señal para comenzar el ataque.
Computadora zombie	Una computadora zombie es una computadora que ha sido infectada por un virus, troyano o un gusano, y se utiliza de forma remota por un tercero, para realizar ataques maliciosos (entre ellos está el ataque de denegación de servicio distribuido DDoS).

Diferencia entre DoS y DDoS:

En DoS las peticiones se realizan desde solo una máquina o una dirección IP, como también puede ser desde algún agente instalado programado para tal fin. En DDoS las peticiones se realizan desde varios puntos o direcciones IPs.

Métodos de ataque:

- Consumen el ancho de banda.
- Alteran las tablas de enrutamiento —la ruta por donde debe ir la información—. Por tal motivo, la información que se envía no llega a destino.
- Fallas en los componentes físicos de una red.

Hacking y Cracking:

Un sistema de información es un conjunto de elementos que están orientados al tratamiento y la administración de los datos para obtener información en base a ellos.

Un hacker es una persona a la cual le apasiona el conocimiento, descubrir o aprender nuevas cosas e indagar más sobre ellas. Toda aquella persona que hackea cualquier tipo de sistema descubre sus vulnerabilidades con el objetivo de poder encontrar alguna herramienta que la minimice o suprima —en el caso de un white hat— o utilizar esta vulnerabilidad a su favor —en el caso de un black hat— y esto lo logra en base a su conocimiento.

Y por qué no nombrar a aquellas personas que han sido hackers, por ejemplo, Rene Favaloro, un hacker en medicina, al descubrir una vulnerabilidad en el sistema cardiaco y realizar el primer bypass cardiaco.

Tipos de hacker:

- **Sombrero blanco (white hats):** utilizan los conocimientos en informática y seguridad informática con el fin de defender los sistemas de información.
- **Sombrero gris (gray hats):** tienen conocimientos tanto de la parte defensiva como ofensiva y pueden trabajar en cualquiera de los ámbitos.
- **Sombrero negro (black hats):** tienen conocimientos informáticos y recurren a hacer actividades maliciosas o ilegales. También conocidos como crackers.

Las diferencias entre hacker y cracker

El **hacker** es un experto en varias ramas técnicas relacionadas con las tecnologías de información de las comunicaciones, como son: programación, redes, sistemas operativos e ingeniería de software.

El **cracker** es también un experto, pero además es quien viola la seguridad de un sistema informático con fines ilícitos o con un objetivo deshonesto y no ético.