

Creación Digital y Pensamiento Computacional

Juan Gualberto Gutiérrez Marín

Marzo 2023

Índice

1	Fundamentos de programación en Python	3
1.1	Conceptos iniciales	3
1.1.1	Instrucción	5
1.1.2	Secuencia	5
1.1.3	Algoritmo	7
1.1.4	Código	7
1.1.5	Tuplas	19
1.2	Estructuras de control selectivas e iterativas	19
1.2.1	Cuadrado: el bucle for..in range()	20
1.3	Funciones	21
1.4	Introducción al uso de funciones gráficas	23
2	Ciberseguridad	24
2.1	Criptografía	24
2.1.1	Introducción	24
2.1.2	Cifrado de llave simétrica o de una clave	24
2.1.3	Estenografía y estegoanálisis	25
2.1.4	Criptografía avanzada	26
2.1.5	Criptografía de llave asimétrica	27
2.2	Hacking ético	28
2.2.1	Introducción	28
2.2.2	Técnicas de búsqueda de información: Information gathering.	30
2.2.3	Escaneo: pruebas de PenTesting	31
2.2.4	Vulnerabilidades en sistemas	32
2.3	Incidentes de ciberseguridad	32
2.3.1	Análisis forense	32
2.3.2	Ciberdelitos	34
3	Big Data	36
3.1	Conceptos previos	37
3.2	Big data. Características. Volumen de datos.	38
3.3	Visualización, transporte y almacenaje de los datos.	39
3.4	Recogida, análisis y generación de datos.	39
3.5	Simulación de fenómenos naturales y sociales	41
3.6	Descripción del modelo	41
3.7	Identificación de agentes	42

3.8	Implementación del modelo mediante un software específico, o mediante programación	42
4	Inteligencia Artificial	44
4.1	Definición. Historia. El test de Turing	44
4.2	Aplicaciones. Impacto	47
4.3	Ética y responsabilidad social (transparencia y discriminación algorítmica)	48
4.4	Beneficios y posibles riesgos	50
4.5	Agentes inteligentes	51
4.5.1	Agentes inteligentes simples	53
4.6	Análisis y clasificación supervisada basada en técnicas de aprendizaje automático: reconocimiento de habla; reconocimiento de imágenes; y reconocimiento de texto	53
4.6.1	Reconocimiento del habla	54
4.6.2	Reconocimiento de imágenes	55
4.6.3	Reconocimiento de texto	56
4.7	Generación de imágenes y/o música basado en técnicas de aprendizaje automático: mezcla inteligente de dos imágenes; generación de música; traducción y realidad aumentada	57
4.7.1	Mezcla inteligente de dos imágenes	58
4.7.2	Generación de música	59
4.7.3	Realidad aumentada	60
4.8	Conclusiones	61

1 Fundamentos de programación en Python

“When you want to know how things really work, study them when they’re coming apart.”

— William Gibson, Zero History

Este tema forma parte del *Bloque I* (desarrollo de aplicaciones informáticas que procesan imágenes, audio y vídeo, como base de la creación digital) de la asignatura Creación Digital y Pensamiento Computacional.

En este tema aprenderemos:

- Conceptos de instrucción y secuenciación, algoritmo vs. código.
- Estructuras de control selectivas e iterativas (finitas e infinitas).
- Funciones.
- Introducción al uso de funciones gráficas (punto, línea, triángulo, cuadrado, rectángulo, círculo, elipse, sectores y arcos).

1.1 Conceptos iniciales

Partimos de la base que sabemos **qué es un ordenador**, tanto el hardware, que es su estructura física (circuitos electrónicos, cables, caja o gabinete, teclado, ratón, etc.), y el software, que es su parte intangible (programas, datos, información, documentación, etc.).

Desde el punto de vista funcional es una máquina que posee, al menos, una unidad central de procesamiento (CPU), una unidad de memoria y otra de entrada/salida (periféricos: pantalla, teclado, ratón, micrófono, cámara, tarjeta de red, puertos USB). Los periféricos de entrada permiten el ingreso de datos, la CPU se encarga de su procesamiento (operaciones aritmético-lógicas) y los dispositivos de salida los comunican a los medios externos. Es así, que la computadora recibe datos, los procesa y emite la información resultante, la que luego puede ser interpretada, almacenada, transmitida a otra máquina o dispositivo o sencillamente impresa; todo ello a criterio de un operador o usuario y bajo el control de un programa de computación.

Para *hablar* con los ordenadores, usamos lenguajes de programación.

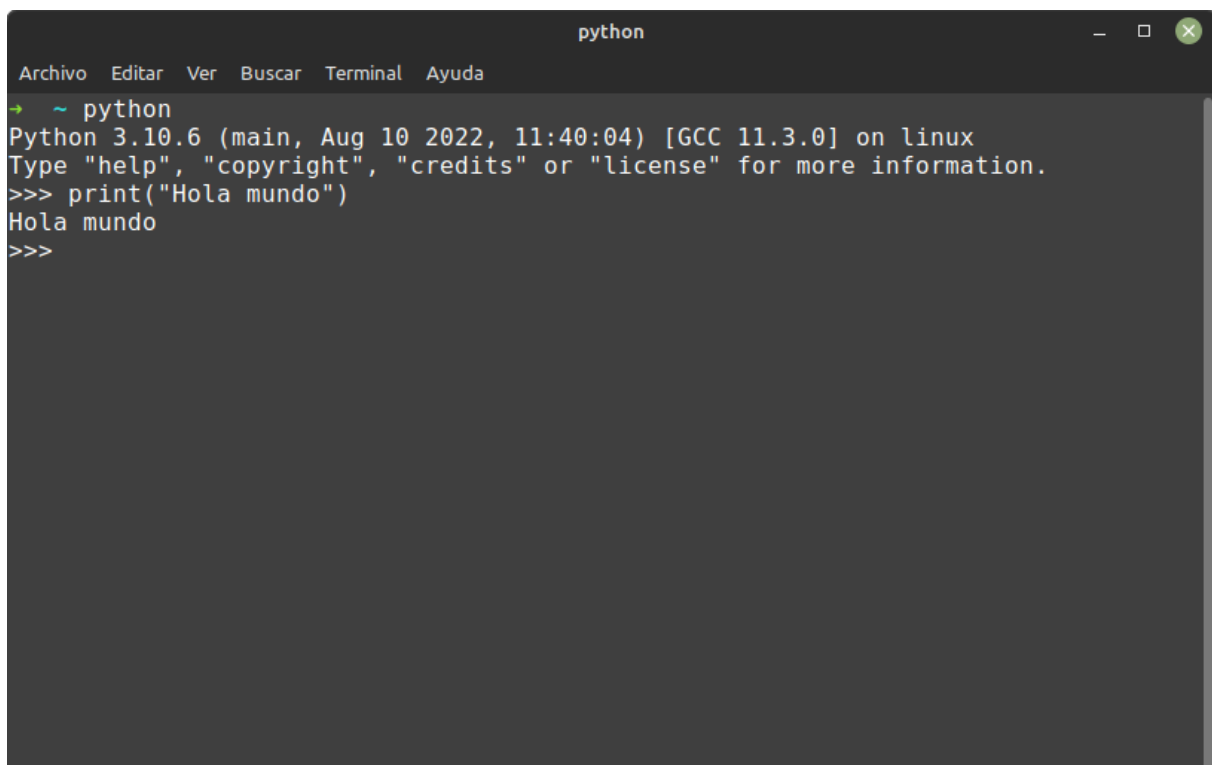
Un **lenguaje de programación** es un lenguaje formal (o artificial, es decir, un lenguaje con reglas gramaticales bien definidas) que le proporciona a una persona, en este caso el programador, la capacidad de escribir (o programar) una serie de instrucciones o secuencias de órdenes en forma de algoritmos con el fin de controlar el comportamiento físico o lógico de un sistema informático, de manera que se puedan obtener diversas clases de datos o ejecutar determinadas tareas. A todo este conjunto de órdenes escritas mediante un lenguaje de programación se le denomina programa informático.

Al igual que idiomas, existen gran cantidad y variedad de lenguajes de programación, entre los que destacan por ser los más usados lenguajes como Python, C, Java, o JavaScript. Puedes consultar la lista de los más usados en prestigiosos índices como:

- TIOBE
- IEEE

Nosotros vamos a usar el lenguaje de programación Python para todos nuestros ejercicios. Puedes instalar Python desde el App Store de tu sistema operativo o bien directamente desde su página Web, haciendo clic aquí mismo.. Debes instalar la versión 3.10 o superior porque hay estructuras de control como *switch-case* (lo veremos más adelante) que sólo están disponibles a partir de esta versión. Como entorno de desarrollo usaremos (Visual Studio Code)[<https://code.visualstudio.com/download>] con la “Python Extension Pack” añadida.

Cuando lo tengas instalado, abre una terminal de tu sistema operativo y ejecuta el comando `python` para entrar en modo interactivo. Cuando veas los símbolos `>>>` copia y pega las órdenes de este tutorial para ir comprobando qué hacen. También puedes ir guardando cada ejercicio en un fichero con extensión `.py` y desde la terminal ejecutando `python3 fichero.py` o bien desde el botón ejecutar de tu IDE (un IDE es un entorno de desarrollo, un software para programar) favorito.



```
python
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
~ python
Python 3.10.6 (main, Aug 10 2022, 11:40:04) [GCC 11.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> print("Hola mundo")
Hola mundo
>>>
```

Figura 1: Python en modo interactivo

1.1.1 Instrucción

Llamamos instrucción a:

- cada una de las órdenes que una persona da al ordenador para que ejecute una operación.
- conjunto de datos insertados en una secuencia estructurada o específica que el procesador interpreta y ejecuta.

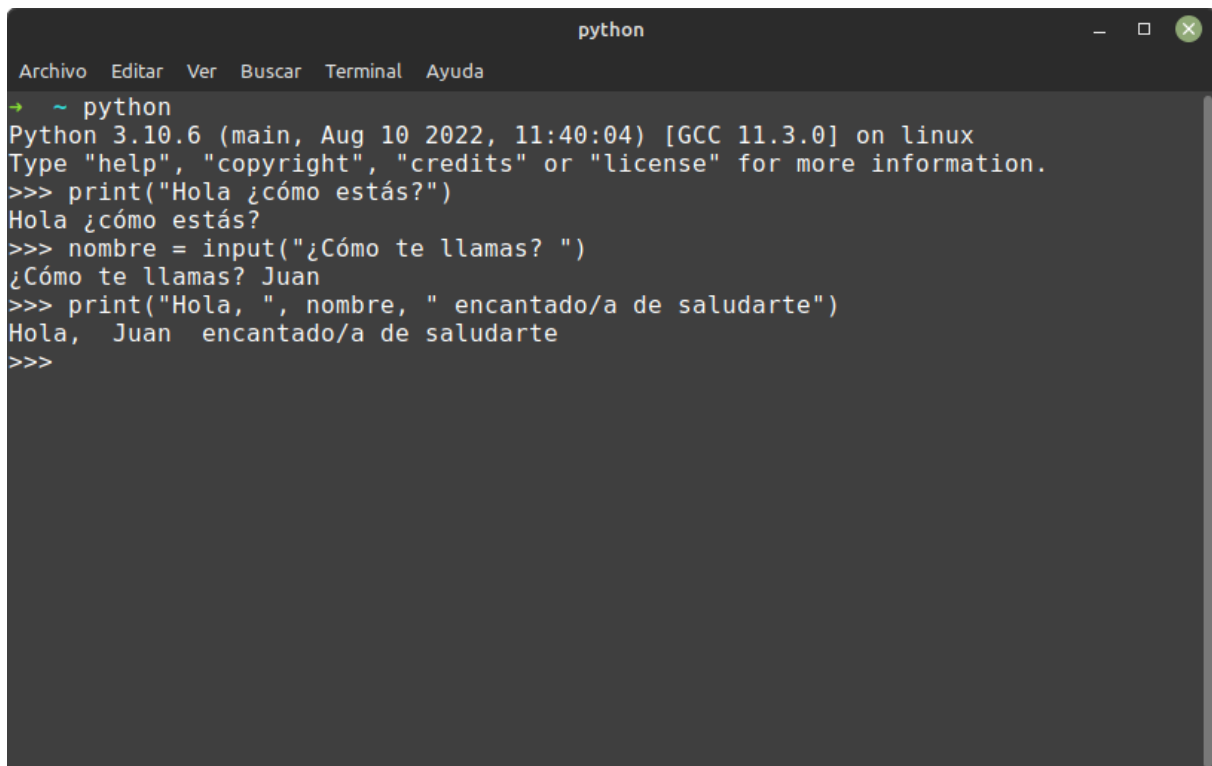
```
1 print("Hola Mundo!!")
```

1.1.2 Secuencia

Una secuencia de instrucciones son dos o más operaciones que se ejecutan una detrás de otra, en orden secuencial, de ahí su nombre.

A continuación vemos un ejemplo de una secuencia de tres instrucciones (si estás en modo interactivo copia y ejecuta línea a línea o no funcionará):

```
1 print("Hola ¿cómo estás?")
2 nombre = input("¿Cómo te llamas? ")
3 print("Hola, ", nombre, " encantado/a de saludarte")
```

A screenshot of a terminal window titled 'python'. The window has a menu bar with 'Archivo', 'Editar', 'Ver', 'Buscar', 'Terminal', and 'Ayuda'. The terminal shows the following text:

```
→ ~ python
Python 3.10.6 (main, Aug 10 2022, 11:40:04) [GCC 11.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> print("Hola ¿cómo estás?")
Hola ¿cómo estás?
>>> nombre = input("¿Cómo te llamas? ")
¿Cómo te llamas? Juan
>>> print("Hola, ", nombre, " encantado/a de saludarte")
Hola, Juan  encantado/a de saludarte
>>>
```

Figura 2: Ejecutando instrucciones una a una.

Sólo con estas tres líneas, estamos aprendiendo varios conceptos muy interesantes:

- el **operador** de *asignación*: cuando veas sólo un igual =, significa asignar, es decir, lo que haya a la derecha del igual se va a copiar en lo que haya a la izquierda del mismo.
- la **variable** *nombre*: una variable es como un nombre, es como llamamos a una zona de memoria RAM donde temporalmente almacenamos información que es relevante para el programa. En este caso la llamamos *nombre* para poder recordarla y consultarla cuando sea necesario. Fíjate cómo usamos el operador asignación (un igual) para indicar que la salida de la función que está a la derecha del mismo, se va a guardar en la variable *nombre* que está a la izquierda del igual.
- la **función** *print*: De manera muy intuitiva podemos afirmar que esta función lo que hará es mostrar un mensaje por pantalla. Fíjate cómo el mensaje va entre paréntesis. Es una instrucción de salida, porque la información fluye de
- la **función** *input*: Esta función, como su nombre indica, pide al usuario que teclee algo y lo guarda en la variable donde hacemos la asignación.

1.1.3 Algoritmo

Un algoritmo es un conjunto de instrucciones o reglas definidas y no-ambiguas, ordenadas y finitas que permite, típicamente, solucionar un problema, realizar un cómputo, procesar datos y llevar a cabo otras tareas o actividades.

1.1.4 Código

El código fuente de un programa informático (o software) es un conjunto de líneas de texto con los pasos que debe seguir la computadora para ejecutar un programa.

El código fuente de un programa está escrito por un programador en algún lenguaje de programación legible por humanos, normalmente en forma de texto plano.

Este código fuente escrito en un lenguaje legible por humanos no es directamente ejecutable por la computadora en su primer estado, sino que debe ser traducido a otro lenguaje o código binario; así será más fácil para la máquina interpretarlo (lenguaje máquina o código objeto que sí pueda ser ejecutado por el hardware de la computadora). Para esta traducción se usan los llamados compiladores, ensambladores, intérpretes, transpiladores y otros sistemas de traducción.

1.1.4.1 Tipos de datos en Python Al igual que por ejemplo en matemáticas tenemos diferentes conjuntos para los números (naturales, enteros, racionales o reales, complejos o imaginarios...), en los lenguajes de programación, cada variable tiene asociado un tipo que indica qué representan los 0 y 1 que realmente están almacenados en la memoria RAM del ordenador.

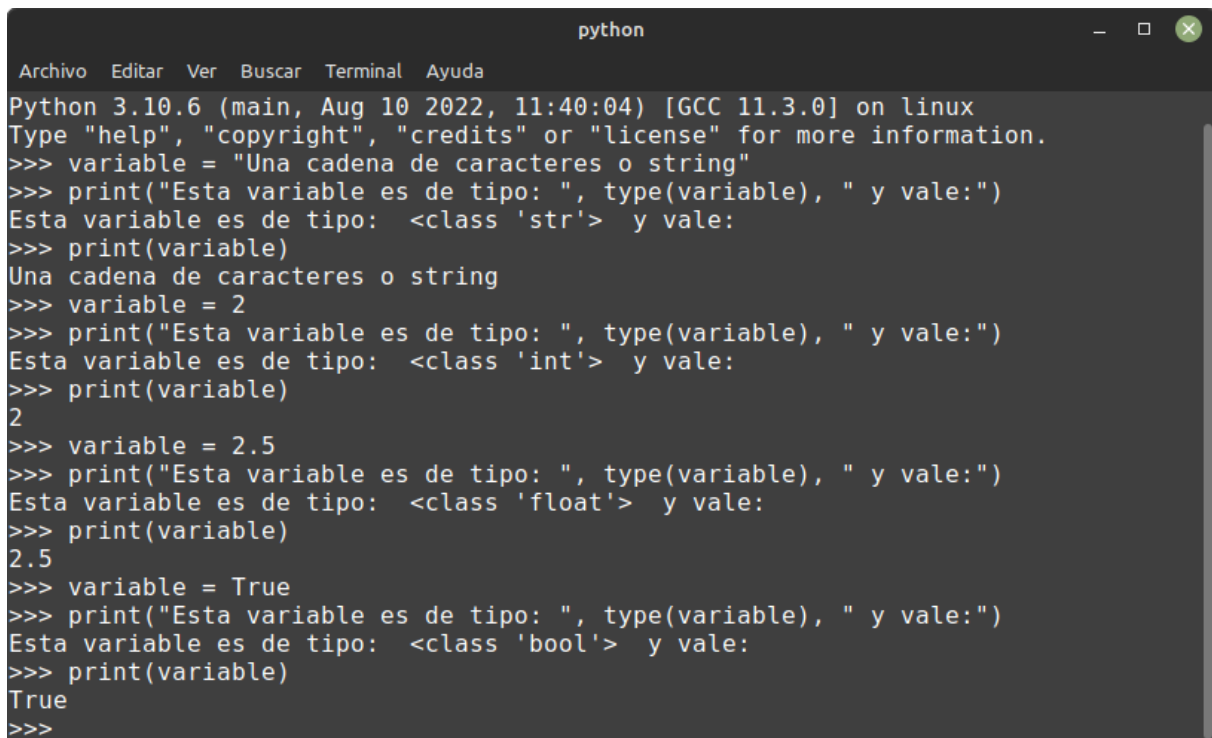
En Python, todo valor que pueda ser asignado a una variable tiene asociado un tipo de dato (aunque en Python todas son objetos). Así que los tipos de datos serían los esqueletos o clases (donde se definen las propiedades del objeto y qué se puede hacer con él, ej: un coche tiene matrícula, marca, modelo, color, titular) y las variables serían las instancias (objetos que representan algo del mundo real, mi coche con matrícula: J-1234-A, color: blanco, marca: Reanult, modelo: Fuego...).

Ejemplos:

```
1 # cadena / string
2 variable = "Una cadena de caracteres o string"
3 print("Esta variable es de tipo: ", type(variable), " y vale:")
4 print(variable)
5 # number / entero
6 variable = 2
7 print("Esta variable es de tipo: ", type(variable), " y vale:")
8 print(variable)
9 # float / decimal
10 variable = 2.5
```



```
11 print("Esta variable es de tipo: ", type(variable), " y vale:")
12 print(variable)
13 # verdadero-falso / booleano
14 variable = True
15 print("Esta variable es de tipo: ", type(variable), " y vale:")
16 print(variable)
```

A screenshot of a Python terminal window titled 'python'. The window has a menu bar with 'Archivo', 'Editar', 'Ver', 'Buscar', 'Terminal', and 'Ayuda'. The terminal shows the following interaction:

```
Python 3.10.6 (main, Aug 10 2022, 11:40:04) [GCC 11.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> variable = "Una cadena de caracteres o string"
>>> print("Esta variable es de tipo: ", type(variable), " y vale:")
Esta variable es de tipo: <class 'str'> y vale:
>>> print(variable)
Una cadena de caracteres o string
>>> variable = 2
>>> print("Esta variable es de tipo: ", type(variable), " y vale:")
Esta variable es de tipo: <class 'int'> y vale:
>>> print(variable)
2
>>> variable = 2.5
>>> print("Esta variable es de tipo: ", type(variable), " y vale:")
Esta variable es de tipo: <class 'float'> y vale:
>>> print(variable)
2.5
>>> variable = True
>>> print("Esta variable es de tipo: ", type(variable), " y vale:")
Esta variable es de tipo: <class 'bool'> y vale:
>>> print(variable)
True
>>>
```

Figura 3: Tipos básicos de datos

1.1.4.2 Números enteros Los números enteros, *integer* para Python, es cualquier número, positivo o negativo, sin decimales y, muy importante, **de longitud ilimitada**.

Ejemplos:

```
1 x = 2
2 y = 2342893749287492334356
3 z = -6555522
```

1.1.4.3 Números reales Los números reales, en programación los llamamos **de coma flotante**, son cualquier número positivo o negativo, que contenga al menos un decimal.

Ejemplos:

```
1 x = 3.141592
2 y = 1.0
3 z = -234.59
```

También es posible usar notación científica en Python (expresar números en potencia de 10):

```
1 x = 3.5321e4
2 y = 12E4
3 z = -127.7e100
```

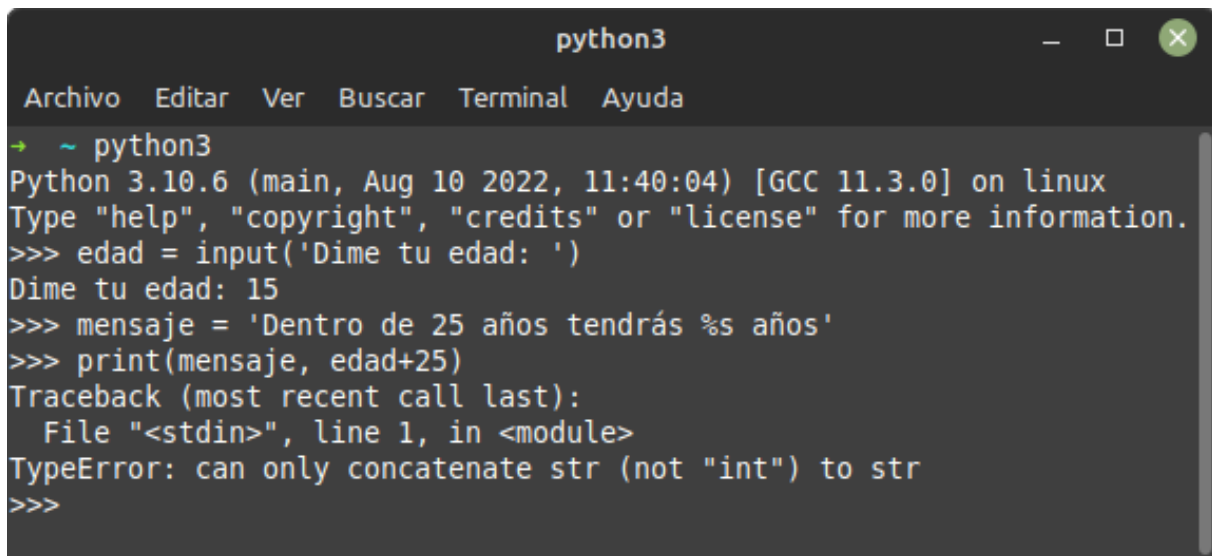
1.1.4.4 Números complejos Aunque los números complejos probablemente no los uses salvo en ecuaciones diferenciales, algunos tipos de integrales en aerodinámica, hidrodinámica y electromagnetismo entre otras.

A diferencia nuestra (probablemente uses *i* para la parte imaginaria del número), en Python se usa la letra **j**:

```
1 x = 3+5j
2 y = 5j
3 z = -5j
```

1.1.4.5 Conversión de números Como ya vimos en un apartado anterior, cuando quiero pedirle a un usuario que introduzca un texto por pantalla, uso la función *input*. Esta función pide **un texto**, aunque yo introduzca un número, seguirá siendo de tipo texto, es decir no es lo mismo asignar $x = 5$, que $x = '5'$ (si pongo comillas será el texto 5 sin ellas, el número 5). Prueba el siguiente código (recuerda ir línea a línea copiando, pegando y ejecutando si estás en modo interactivo):

```
1 edad = input('Dime tu edad: ')
2 mensaje = 'Dentro de 25 años tendrás %s años'
3 print(mensaje, edad+25)
```



```
python3
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
→ ~ python3
Python 3.10.6 (main, Aug 10 2022, 11:40:04) [GCC 11.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> edad = input('Dime tu edad: ')
Dime tu edad: 15
>>> mensaje = 'Dentro de 25 años tendrás %s años'
>>> print(mensaje, edad+25)
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
TypeError: can only concatenate str (not "int") to str
>>>
```

Figura 4: Error al intentar sumar una cadena de caracteres con un número entero.

Para solventar el error que da, tenemos que convertir la cadena de caracteres almacenada en la variable `edad` a un número. Para convertir a número tenemos las siguientes funciones:

```
1 entero = int("27")
2 real = float("27.3")
3 imaginario = complex("2+3j")
```

Con estos ejemplos, ¿sabrías arreglar el error anterior? Inténtalo sin mirar la solución.

```
1 textoEdad = input('Dime tu edad: ')
2 edad = int(textoEdad)
3 mensaje = 'Dentro de 25 años tendrás %s años'
4 print(mensaje, edad+25)
```

A la conversión de tipos también se le llama **casting** en el argot de los programadores.

1.1.4.6 Operadores Operadores matemáticos:

Operador	Operación	Ejemplo
+	Suma	$x + y$
-	Resta	$x - y$
*	Multiplicación	$x * y$
/	División	x / y

Operador	Operación	Ejemplo
**	Potencia	x**y
%	Módulo	x % y
//	División con redondeo	x // y

Al igual que pasa en matemáticas, en programación tenemos exactamente la misma precedencia de operadores, es decir en caso de concatenar operaciones, se harían primero las potencias, luego las multiplicaciones, divisiones, módulo y finalmente las sumas y restas. Compruébalo con estos ejemplos (verifica en tu ordenador qué resultado dan y piensa porqué):

```
1 print( 2+3*5 ) # 17
2 print( (2+3)*5 ) # 20
```

Otros operadores de asignación:

Operador	Ejemplo	Equivalente a
=	x = 5	x = 5
+=	x += 3	x = x + 3
-=	x -= 3	x = x - 3
*=	x *= 3	x = x * 3
/=	x /= 3	x = x / 3
%=	x %= 3	x = x % 3
//=	x //= 3	x = x // 3
**=	x **= 3	x = x ** 3
&=	x &= 3	x = x & 3
=	x	= 3
^=	x ^= 3	x = x ^ 3
»=	x »= 3	x = x » 3
«=	x «= 3	x = x « 3

Operadores de comparación:

Operador	Operación	Ejemplo
==	Igual a	x == y
!=	Distinto a	x != y
>	Mayor a	x > y
<	Menor a	x < y
>=	Mayor o igual a	x >= y
<=	Menor o igual a	x <= y

1.1.4.7 Booleanos Una vez vistos los operadores de comparación, vamos a seguir con ellos y ver para qué los podemos usar. Si tecleamos esto en nuestro Python en modo interactivo:

```
1 print(10 > 5)
2 print(5 == 9)
3 print(12 < 9)
```

Veremos que devuelve:

```
1 True
2 False
3 False
```

A esto es a lo que llamamos tipos booleanos, es decir, un tipo de dato binario que sólo tiene dos estados: verdadero y falso.

¿Para qué sirven estos tipos de datos? Nos ayudarán a tomar decisiones en nuestros programas y así ir por un camino u otro de nuestro código fuente, ejemplo:

```
1 a = 200
2 b = 33
3
4 if b > a:
5     print("b es más grande que a")
6 else:
7     print("b NO es más grande que a")
```

Si lo introduces en modo interactivo, copia y pega todo de golpe y al final tendrás que pulsar la tecla intro (o *Enter*) para indicar que la estructura de control ha terminado.

```

python3
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
File "<stdin>", line 1, in <module>
TypeError: can only concatenate str (not "int") to str
>>> a = 200
>>> b = 33
>>>
>>> if b > a:
...     print("b es más grande que a")
... else:
...     print("b NO es más grande que a")
...
b NO es más grande que a
>>>

```

Figura 5: Ejemplo de uso de booleanos para tomar decisiones. Recuerda un intro extra al final.

1.1.4.8 Strings Los *strings* o cadena de carteres son variables de tipo texto, es decir almacenan información que contienen caracteres de texto. Sabemos que hablamos de cadenas de caracteres porque usamos comillas para darles valor, emeplo:

```
1 cadena = "Esto es una variable de tipo cadena"
```

Operaciones con strings:

Con las cadenas de caracteres podemos:

Método	Descripción
<code>capitalize()</code>	Convierte a mayúsculas todas las letras
<code>count('a')</code>	Cuenta cuantas 'a' hay en el string (puedes poner otros caracteres a contar)
<code>find('mundo')</code>	Busca dónde aparece la subcadena <i>mundo</i> dentro de la cadena dada
<code>format()</code>	Sirve para dar formato
<code>index(valor)</code>	Busca y devuelve la primera ocurrencia de <i>valor</i> en la cadena
<code>isdigit()</code>	Devuelve verdadero si todos los caracteres son dígitos: 0-9
<code>islower()</code>	Devuelve verdadero si todas las letras están en mayúscula

Método	Descripción
isnumeric()	Devuelve verdadero si todos los caracteres son numéricos
isupper()	Devuelve verdadero si todas las letras están en mayúscula
join()	Convierte una lista en una cadena, es lo contrario de split()
lower()	Pasa a minúsculas todas las letras
replace(valor1, valor2)	Sustituye cualquier ocurrencia de valor1 por valor2
rfind(valor)	Busca por la derecha de la cadena la primera ocurrencia de un valor y devuelve su posición
rindex(valor)	Busca por la derecha de la cadena la primera ocurrencia de un valor y devuelve su posición
split(parametro)	Parte una cadena en una lista de cadenas según el separador <i>parámetro</i> , es lo contrario de join()
startswith()	Devuelve verdadero
strip()	Elimina los caracteres en blanco del principio y el final
swapcase()	Cambia las mayúsculas a minúsculas y al revés
title()	Convierte A Formato Título Con La Primera En Mayúscula
upper()	Pasa a mayúsculas todas las letras

Veamos algunos ejemplos:

El método `count()` retorna el número de veces que se repite un conjunto de caracteres especificado.

```
1 >>> s = "Hola mundo"
2 >>> s.count("Hola")
3 1
```

Los métodos `find()` e `index()` retornan la ubicación (comenzando desde el cero) en la que se encuentra el argumento indicado.

```
1 >>> s.find("mundo")
2 5
3 >>> s.index("mundo")
4 5
```

Difieren en que esta última lanza `ValueError` cuando el argumento no es encontrado, mientras que aquella retorna `-1`.

```
1 >>> s.find("world")
2 -1
3 >>> s.index("world")
4 Traceback (most recent call last):
5   File "<stdin>", line 1, in <module>
6   ValueError: substring not found
```

En ambos métodos la búsqueda ocurre de izquierda a derecha. Para buscar un conjunto de caracteres desde el final, utilícese del mismo modo `rfind()` y `rindex()`.

```
1 >>> s = "C:/python36/python.exe"
2 >>> s.find("/") # Retorna la primera ocurrencia.
3 2
4 >>> s.rfind("/") # Retorna la última.
5 11
```

`startswith()` y `endswith()` indican si la cadena en cuestión comienza o termina con el conjunto de caracteres pasados como argumento, y retornan `True` o `False` en función de ello.

```
1 >>> s = "Hola mundo"
2 >>> s.startswith("Hola")
3 True
4 >>> s.endswith("mundo")
5 True
6 >>> s.endswith("world")
7 False
```

Ambos métodos son preferidos ante la opción de emplear slicing.

```
1 # Se prefiere startswith().
2 >>> s[:4] == "Hola"
3 True
```

Veamos más ejemplos:

```
1 cadena = "Hello world!"
2 # A partir del carácter 4 hasta el final
3 cadena[4:]
4 # Los 4 primeros caracteres
5 cadena[:4]
6 # Desde la posición 2 a la 4
7 cadena[2:4]
8 # El carácter (letra) de la posición 6
9 cadena[6]
```

Si lo probamos en modo interactivo, veremos lo siguiente:

```
1 >>> cadena = "Hello world!"
2 >>> cadena[4:]
```



```
3 'o world!'
4 >>> cadena[:4]
5 'Hell'
6 >>> cadena[2:4]
7 'll'
8 >>> cadena[6]
9 'w'
```

Los métodos `isdigit()`, `isnumeric()` e `isdecimal()` determinan si todos los caracteres de la cadena son dígitos, números o números decimales.

```
1 >>> "1234".isnumeric()
2 True
3 >>> "1234".isdecimal()
4 True
5 >>> "abc123".isdigit()
6 False
```

Si bien estas definiciones resultan a priori similares, no lo son. La primera, `isdigit()`, considera caracteres que pueden formar números, incluidos aquellos correspondientes a lenguas orientales. `isnumeric()` es más amplia, pues incluye también caracteres de connotación numérica que no necesariamente son dígitos (por ejemplo, una fracción). La última, `isdecimal()`, es la más restrictiva al tener en cuenta únicamente números decimales; esto es, formados por dígitos del 0 al 9.

`lower()` y `upper()` retornan una copia de la cadena con todas sus letras en minúsculas o mayúsculas según corresponda.

```
1 >>> "HoLa Mundo!".lower()
2 'hola mundo!'
3 >>> "HoLa Mundo!".upper()
4 'HOLA MUNDO!'
```

Las funciones `strip()`, `lstrip()` y `rstrip()` remueven los espacios en blanco que preceden y/o suceden a la cadena.

```
1 >>> s = " HoLa mundo! "
2 >>> s.strip()
3 'HoLa mundo!'
4 # Remueve los de la derecha.
5 >>> s.rstrip()
6 ' HoLa mundo!'
7 # Remueve los de la izquierda.
8 >>> s.lstrip()
9 'HoLa mundo! '
```

Por último, el método `replace()` -ampliamente utilizado- reemplaza una cadena por otra.

```
1 >>> s = "HoLa mundo"
```

```
2 >>> s.replace("mundo", "world")
3 'Hola world'
```

El método de división de una cadena según un carácter separador más empleado es `split()`, cuyo separador por defecto son espacios en blanco y saltos de línea.

```
1 >>> "Hola mundo!\nHello world!".split()
2 ['Hola', 'mundo!', 'Hello', 'world!']
```

El separador puede indicarse como argumento.

```
1 >>> "Hola mundo!\nHello world!".split(" ")
2 ['Hola', 'mundo!\nHello', 'world!']
```

O bien, para separar únicamente según saltos de línea:

```
1 # Equivalente a split("\n").
2 >>> "Hola mundo!\nHello world!".splitlines()
3 ['Hola mundo!', 'Hello world!']
```

Un segundo argumento en `split()` indica cuál es el máximo de divisiones que puede tener lugar (-1 por defecto para representar una cantidad ilimitada).

```
1 >>> "Hola mundo hello world".split(" ", 2)
2 ['Hola', 'mundo', 'hello world']
```

Un segundo método de separación es `partition()`, que retorna una tupla de tres elementos: el bloque de caracteres anterior a la primera ocurrencia del separador, el separador mismo, y el bloque posterior.

```
1 >>> s = "Hola mundo. Hello world!"
2 >>> s.partition(" ")
3 ('Hola', ' ', 'mundo. Hello world!')
```

Strings dentro de strings:

Es posible sustituir dentro de una cadena de caracteres otra cadena (o incluso otro tipo de dato). Veámoslo con un ejemplo, pruébalo en tu ordenador y fíjate cómo se sustituye **%s** por el número **1000**:

```
1 puntos = 1000
2 mensaje = 'Has conseguido %s puntos'
3 print(mensaje % puntos)
```

- Primero usamos la cadena **%s** para indicar que eso debe ser sustituido.
- Luego usamos el operador **%** para decir que dentro de la variable *mensaje* sustituimos la cadena anterior por el contenido de la siguiente variable, que es *puntos*.

Multiplícate por cero:

Es posible multiplicar strings en Python y así conseguir curiosos efectos. Prueba a ver qué hace esto:

```
1 print('-'*10, '='*5, '-'*10)
```

1.1.4.9 Listas o arrays ¿Qué son las listas? Las listas, como en la vida real, representan un conjunto ordenado (es importante este punto, están en orden y cada uno en su lugar) de cosas. Veamos un ejemplo con esta lista de la compra de Saruman (mago arcano muy conocido):

```
1 listaCompra = ['patas de araña', 'alas de murciélago',  
2               'ojo de tritón', 'dedo gordo de una rana']  
3 print(listaCompra)  
4 print(listaCompra[2])  
5 listaCompra[3] = 'mantequilla de babosa'  
6 print(listaCompra)
```

¿Has probado qué muestran las tres instrucciones *print* de estas tres líneas de código fuente?

La primera instrucción *print* te muestra la lista entera, la segunda, el elemento en tercer lugar, curioso porque hemos puesto un 2, no un 3, pero recuerda que eso es así porque en informática siempre empezamos a contar en 0 (el tercer elemento de 0, 1, 2, 3, es el 2, uno menos). La tercera muestra una lista diferente, algo ha cambiado, ejecútalo en tu ordenador, fíjate bien e intenta explicar qué y porqué ha cambiado.

Añadiendo elementos a una lista:

Para añadir elementos a una lista usamos el método *append*. Ejemplo:

```
1 listaCompra = ['patas de araña', 'alas de murciélago',  
2               'ojo de tritón', 'dedo gordo de una rana']  
3 print(listaCompra)  
4 listaCompra.append('cicuta')  
5 listaCompra.append('eructo de oso')  
6 print(listaCompra)
```

Quitando elementos de una lista:

Para eliminar elementos de la lista usamos el comando *del* (abreviatura del inglés *delete*):

```
1 listaCompra = ['patas de araña', 'alas de murciélago',  
2               'ojo de tritón', 'dedo gordo de una rana']  
3 print(listaCompra)  
4 del listaCompra[0]  
5 del listaCompra[2]  
6 print(listaCompra)
```

1.1.5 Tuplas

Son como las listas pero usan paréntesis y son inmutables. ¿Qué significa inmutable? Pues prueba este código y observa el error que da:

```
1 tupla = (1,2,3,4,5)
2 tupla[2] = 'pepe'
```

Como habrás comprobado dice que las tuplas no admiten asignación, es decir, no se puede modificar el contenido de la tupla después de crearlo, a diferencia de las listas que sí. A cambio, cuando iteramos o recorremos la tupla, Python lo hace de manera mucho más rápida y eficiente que cuando recorremos o iteramos sobre una lista.

1.1.5.1 Diccionarios Los diccionarios podríamos verlos como un tipo de dato que representa un objeto. Los diccionarios se caracterizan por ir entre llaves y llevar un dato asociado a una clave de esta manera:

```
1 {clave: valor}
```

Donde la clave nos sirve para explicar qué dato almacena (ese dato sería el valor):

```
1 persona = {'nombre': 'Juan', 'apellido': 'García', 'edad': 16}
2 persona['nombre']
```

1.2 Estructuras de control selectivas e iterativas

Para entender mejor las estructuras de control, vamos a usar un paquete de Python llamado **turtle**. Así, de camino que aprendemos estructuras de control, hacemos una introducción al uso de funciones gráficas. En Ubuntu necesitaremos instalar el paquete Tk para disponer de las bibliotecas necesarias para usar ventanas en nuestros programas.

```
1 sudo apt install python3-tk
2 sudo apt install python3-pip
3 sudo pip3 install PythonTurtle
```

Si no dispones de un ordenador (Windows o Linux) donde instalar Python, puedes hacer esta parte del tutorial también online en esta Web: <https://www.pythonsandbox.com/turtle>. En ese mismo sitio Web también hay un resumen muy interesante de los comandos que vamos a usar: <https://www.pythonsandbox.com/turtle>.

1.2.1 Cuadrado: el bucle `for..in range()`

Nuestro primer dibujo será un cuadrado, presta atención a las instrucciones avanza y gira a la izquierda.

```
1 import turtle as tortuga
2
3 pantalla = tortuga.getscreen()
4
5 tortuga.forward(100)
6 tortuga.left(90)
7
8 tortuga.forward(100)
9 tortuga.left(90)
10
11 tortuga.forward(100)
12 tortuga.left(90)
13
14 tortuga.forward(100)
15 tortuga.left(90)
16
17 tortuga.done()
```

En donde:

- La instrucción `tortuga.getscreen()` nos “pinta” la ventana donde aparece la tortuga (el pequeño triángulo).
- La instrucción `tortuga.done()` espera a que cerremos la ventana para que podamos ver el dibujo que hagamos.
- La instrucción `tortuga.forward()` hace que avance la tortuga el número de espacios que se le indica.
- La instrucción `tortuga.left()` gira a la izquierda el número de grados indicados.

Por supuesto, muchos ya estaréis pensando, ¿y si las partes que se repiten las ponemos dentro de un bucle? Pues que entonces tendremos un programa mucho más sencillo, algo como esto:

```
1 import turtle as tortuga
2
3 pantalla = tortuga.getscreen()
4
5 for contador in range(4):
6     tortuga.forward(100)
7     tortuga.left(90)
8
9 tortuga.done()
```

Fíjate bien en los espacios en blanco a la izquierda dentro del bucle `for`, así le indicamos a Python

que esas instrucciones están *dentro* del *for*, A esto se le llama **identar** el código. Usaremos la tecla tabulador si el programa o IDE que usamos no lo hace de manera *automática* por nosotros.

RETOS: Acabamos de ver cómo dibujar un cuadrado, ¿serías capaz de hacer un pentágono? ¿y un hexágono? ¿y un octógono? PISTA: según el número de vértices, tienes que cambiar el número de vueltas (iteraciones) que da el bucle *for* y los grados que giras.

Los bucles se pueden anidar, esto es, poner unos dentro de otros. Es importante tener en cuenta la indentación, pues recuerda que según cómo lo movemos a la derecha con el tabulador, le indicamos a Python si una línea de código está dentro del bloque anterior. Prueba este código en tu ordenador a ver qué hace:

```
1 # ahora parametrizamos lado y metemos dos FOR anidados
2 # esto pinta polígonos dentro de polígonos
3 lado = 10
4 for k in range(10):
5     for i in range(8):
6         print("Vuelta número: ",i)
7         tortuga.forward(lado)
8         tortuga.left(45)
9     lado = lado + 20
```

RETO: Hemos visto cómo hacer que se pinten polígonos de más pequeño a más grande, pero, ¿serías capaz de hacerlo al revés? Pintar primero el más grande, luego dentro otro más pequeño y así sucesivamente. PISTA: Hay que *jugar* con la longitud del lado, pero ¡cuidado! *un lado no puede medir un número negativo*.

1.3 Funciones

Tras dibujar un cuadrado, un hexágono y un octógono, vemos que parte del código se repite, de manera que se podría *parametrizar* (hacerlo genérico usando variables o parámetros). Si sabemos el número de vértices y la longitud de cada lado, podríamos pintar cualquier polígono (el triángulo sería una pequeña excepción a esta regla), sabiendo que cada vértice tendrá $360/n$ grados.

```
1
2 import turtle as tortuga
3
4 pantalla = tortuga.getscreen()
5
6 def pintapoligono(lados, longitud):
7     if (lados > 2):
8         giro = 360 / lados
9         for contador in range(lados):
10             tortuga.forward(longitud)
11             tortuga.left(giro)
```

```

12     else:
13         print("Error: no hay polígonos de menos de 3 lados")
14
15     pintapoligono(2, 50)
16     pintapoligono(4, 25)
17     pintapoligono(6, 25)
18     pintapoligono(8, 25)
19
20     tortuga.done()

```

También son funciones las que usamos para comunicarnos con la tortuga así por ejemplo tenemos las siguientes:

FUNCIÓN	EXPLICACIÓN
tortuga.up()	Sube el lápiz (ya no pinta)
tortuga.down()	Baja el lápiz (ahora pinta)
tortuga.forward(n)	Avanza n “espacios”
tortuga.backward(n)	Retrocede n “espacios”
tortuga.left(n)	Gira a la izquierda “n” grados
tortuga.right(n)	Gira a la derecha “n” grados
tortuga.reset()	Borra la pantalla y la tortuga vuelve al inicio
tortuga.clear()	Borra la pantalla pero la tortuga se queda ahí
tortuga.pensize(n)	Establece el ancho de la línea a n píxeles
tortuga.pencolor(“red”)	Pone el color del lápiz a rojo
tortuga.pencolor((R,G,B))	Pone el color según la tupla R,G,B
tortuga.fillcolor(“red”)	Rellena con el color rojo
tortuga.fillcolor((R,G,B))	Rellena con el color según la tupla R,G,B

También podemos colorear combinando funciones, ejemplo:

```

1  turtle.color("black", "red")
2  turtle.begin_fill()
3  turtle.circle(80)
4  turtle.end_fill()

```

RETOS: ¿Te está gustando la tortuga de Python? Ahora te proponemos unos retos para que practiques:

1. Dibuja la bandera de España con la tortuga. Extra: ¡ponle un mástil!
2. Dibuja una casita (como la que hacen los niños pequeños, con figuras geométricas sólo: triángulos, cuadrados y rectángulos)
3. Dibuja un barco (como los que hacen los niños pequeños, con figuras geométricas sólo: triángulos, cuadrados y rectángulos)

1.4 Introducción al uso de funciones gráficas

Ya hemos visto con turtle lo básico (punto, línea, triángulo, cuadrado, rectángulo, círculo, elipse, sectores y arcos), ahora es el momento de pasar a TkInter, la biblioteca gráfica de Python.

TO-DO.

2 Ciberseguridad

2.1 Criptografía

2.1.1 Introducción

La criptografía es una técnica que se utiliza para proteger la información y mantenerla segura. Básicamente, se trata de convertir un mensaje en algo que sólo pueda ser entendido por la persona que tiene la clave para descifrarlo.

Dentro de la criptografía, hay tres conceptos clave que debes conocer: criptología, criptoanálisis y criptosistema. La criptología es la ciencia que estudia la criptografía, mientras que el criptoanálisis es la técnica para tratar de descifrar un mensaje sin tener la clave. Y finalmente, el criptosistema es el conjunto de técnicas y procedimientos que se utilizan para cifrar y descifrar mensajes.

Los elementos de un criptosistema incluyen el mensaje original, que se llama texto claro, y la clave que se utiliza para cifrarlo. El resultado de cifrar el mensaje es el texto cifrado. Para poder descifrar el mensaje cifrado, es necesario tener la clave correcta. Además, los criptosistemas también pueden incluir algoritmos matemáticos y otros procedimientos para hacer el cifrado más seguro.

En resumen, la criptografía es una técnica que se utiliza para proteger la información y mantenerla segura. Para ello, se utilizan técnicas como el cifrado y la utilización de claves, que forman parte de un criptosistema. La criptología estudia estos procesos, mientras que el criptoanálisis trata de romper la seguridad de los criptosistemas sin tener la clave adecuada.

2.1.2 Cifrado de llave simétrica o de una clave

Los cifrados de llave simétrica son un tipo de cifrado que utiliza la misma clave para cifrar y descifrar el mensaje. Esto significa que tanto el emisor como el receptor deben conocer la clave para poder comunicarse de forma segura.

Uno de los cifrados más conocidos de este tipo es el cifrado César. Este cifrado se basa en un desplazamiento de letras en el alfabeto. Por ejemplo, si usamos un desplazamiento de 3 posiciones, la letra “A” se cifraría como “D”, la letra “B” como “E”, y así sucesivamente. De esta manera, el mensaje original se convierte en un mensaje cifrado que parece ininteligible para alguien que no conoce el desplazamiento.

Por ejemplo, si queremos cifrar la palabra “HOLA” con un desplazamiento de 3 posiciones, el resultado sería “KROD”.

Hay muchos otros algoritmos de cifrado de llave simétrica, como el cifrado AES, DES y Blowfish. Estos algoritmos se utilizan en la vida cotidiana para proteger la información que se transmite a través de

internet, como las contraseñas y los datos bancarios.

Por último, el cifrado físico se refiere a la protección física de la información. Esto puede incluir la utilización de cajas fuertes, cerraduras, y otros dispositivos de seguridad para proteger documentos y objetos valiosos. Un ejemplo de cifrado físico es el uso de candados para proteger bicicletas o casilleros.

Los datos biométricos son medidas físicas o comportamentales únicas de una persona, como la huella digital, el iris, la voz o el rostro. Estos datos se pueden utilizar en la criptografía para proporcionar una capa adicional de seguridad en los sistemas de autenticación.

Por ejemplo, en lugar de utilizar una contraseña o una clave de seguridad, un sistema de autenticación biométrica puede utilizar el reconocimiento facial para identificar a una persona. El sistema puede escanear la cara del usuario y compararla con una base de datos de imágenes de caras autorizadas. Si hay una coincidencia, se le permite al usuario el acceso al sistema.

Los datos biométricos también se pueden utilizar para la encriptación de datos. En lugar de utilizar una clave de cifrado tradicional, se puede utilizar una clave generada a partir de los datos biométricos del usuario. Por ejemplo, se puede utilizar la huella dactilar del usuario para generar una clave de cifrado única. Esta clave sólo se puede desbloquear si la huella dactilar del usuario se escanea correctamente.

Sin embargo, es importante tener en cuenta que los datos biométricos pueden ser robados o falsificados. Por lo tanto, es importante que los sistemas de autenticación biométrica estén bien diseñados y sean seguros para evitar el acceso no autorizado. Además, es importante asegurarse de que los datos biométricos se almacenen de forma segura y se protejan contra el acceso no autorizado.

2.1.3 Estenografía y estegoanálisis

La esteganografía es una técnica de ocultación de información que se utiliza para esconder datos dentro de otros datos, como una imagen, un audio o un texto, de tal manera que el mensaje oculto no sea detectado por una persona que no tenga conocimiento de su existencia. Por otro lado, el estegoanálisis es el proceso de detectar y analizar la existencia de un mensaje oculto dentro de un archivo.

Existen varios algoritmos de esteganografía que se utilizan en el mundo real, entre ellos destacan:

- **Esteganografía en imágenes:** en este tipo de esteganografía se oculta información en el interior de una imagen. Los datos se pueden ocultar en los píxeles menos significativos de una imagen, lo que permite que el mensaje oculto no sea detectado a simple vista. Uno de los algoritmos más conocidos es el método de esteganografía LSB (Least Significant Bit), el cual consiste en reemplazar los bits menos significativos de la imagen con los bits del mensaje oculto.

- **Esteganografía en audio:** en este tipo de esteganografía se oculta información en el interior de un archivo de audio. Los datos se pueden ocultar en las frecuencias menos audibles, lo que permite que el mensaje oculto no sea detectado por el oído humano. Uno de los algoritmos más conocidos es el método de esteganografía MP3Stego, el cual consiste en reemplazar las muestras de audio menos significativas con los datos del mensaje oculto.
- **Esteganografía en texto:** en este tipo de esteganografía se oculta información dentro del propio texto de un mensaje. Uno de los algoritmos más conocidos es el método de esteganografía null cipher, el cual consiste en ocultar el mensaje en los espacios en blanco entre las palabras del texto.

En cuanto a los usos de la esteganografía en el mundo real, puede ser utilizada en situaciones en las que se necesita proteger la privacidad de la información, como en el ámbito militar o en la protección de datos sensibles. Por otro lado, también puede ser utilizada con fines malintencionados, como el ocultamiento de mensajes terroristas o para fines de espionaje.

El estegoanálisis se utiliza para detectar la existencia de un mensaje oculto en un archivo. Por ejemplo, puede ser utilizado por las fuerzas de seguridad para descubrir mensajes ocultos en imágenes o archivos de audio que puedan contener información valiosa para la prevención de delitos o actos terroristas.

2.1.4 Criptografía avanzada

La criptografía avanzada es una técnica de protección de la información que utiliza algoritmos y sistemas más complejos y sofisticados que los que se utilizan en la criptografía tradicional. La criptografía avanzada es utilizada para proteger información extremadamente sensible, como información bancaria, datos militares, información de gobiernos y empresas, entre otros.

La criptografía avanzada utiliza métodos matemáticos y computacionales avanzados para proteger la información, haciendo que sea muy difícil, si no imposible, para una persona no autorizada acceder a la información protegida. Los algoritmos utilizados en la criptografía avanzada son altamente seguros y se basan en la complejidad de ciertos problemas matemáticos, como el problema del logaritmo discreto y la factorización de números enteros.

La criptografía avanzada también utiliza técnicas de autenticación, como la firma digital y el intercambio de claves, para garantizar que la información sea auténtica y que solo las personas autorizadas tengan acceso a ella.

En resumen, la criptografía avanzada es una técnica de protección de la información altamente segura y compleja, que utiliza algoritmos y sistemas matemáticos avanzados para garantizar que la información sea protegida y solo accesible por personas autorizadas.

2.1.5 Criptografía de llave asimétrica

La criptografía de llave asimétrica, también conocida como criptografía de clave pública, es un tipo de criptografía que utiliza dos claves diferentes para cifrar y descifrar información. A diferencia de la criptografía de llave simétrica, donde ambas partes comparten la misma clave para cifrar y descifrar información, en la criptografía de llave asimétrica, cada parte tiene su propia clave: una clave pública y una clave privada.

La clave pública se utiliza para cifrar la información, mientras que la clave privada se utiliza para descifrarla. La clave privada es secreta y solo debe ser conocida por la persona que la posee, mientras que la clave pública puede ser compartida con cualquier persona.

La criptografía de llave asimétrica se utiliza en varios contextos, como la firma digital y la seguridad en servidores web. En la firma digital, el emisor de un mensaje utiliza su clave privada para firmar digitalmente el mensaje, lo que garantiza que el mensaje no ha sido modificado y que proviene del emisor legítimo. El receptor del mensaje utiliza la clave pública del emisor para verificar la firma digital y asegurarse de que el mensaje es auténtico.

Veamos un ejemplo: Si Bob quiere mandar un mensaje a Alice utilizando criptografía de llave asimétrica, podría utilizar un algoritmo como RSA o ECC.

Para asegurarse de que sólo Alice, destinataria del mensaje, pueda leerlo, Bob necesitaría la clave pública de Alice. Él utilizaría la clave pública de Alice para cifrar el mensaje antes de enviarlo. La clave privada, que es necesaria para descifrar el mensaje, sólo es conocida por Alice.

Una vez que Alice recibe el mensaje cifrado, ella utilizaría su clave privada para descifrarlo. Para hacer esto, primero debería importar su clave privada en su software de criptografía y luego usarla para descifrar el mensaje cifrado que recibió de Bob.

Es importante mencionar que, para que el sistema de criptografía de llave asimétrica sea seguro, es esencial mantener la clave privada en secreto. Si la clave privada se revela o se pierde, el sistema de seguridad se vería comprometido y el mensaje ya no estaría seguro.

En los servidores web, la criptografía de llave asimétrica se utiliza para proteger la información transmitida entre el servidor y el cliente. Cuando se establece una conexión segura entre un servidor y un cliente, el servidor envía su clave pública al cliente para cifrar la información, de modo que solo el servidor puede descifrarla con su clave privada. Esto evita que un atacante malintencionado pueda interceptar la información y descifrarla, lo que se conoce como un ataque de “man in the middle”.

Cuando visitas un sitio web seguro, como <https://www.iesvirgendelcarmen.com>, tu navegador web (por ejemplo, Firefox) utiliza criptografía de llave asimétrica para establecer una conexión segura con el servidor. Esto se logra mediante el protocolo SSL/TLS (Secure Sockets Layer/Transport Layer Security).

Durante el proceso de conexión, el servidor envía su certificado digital al navegador. Este certificado contiene información que confirma la identidad del servidor y su clave pública. El certificado es emitido por una entidad de certificación confiable (CA), como Verisign o Let's Encrypt, que garantiza la autenticidad del certificado.

El navegador verifica la autenticidad del certificado del servidor y confirma que el nombre de dominio en la URL del sitio web coincide con el nombre de dominio del certificado. Luego, el navegador utiliza la clave pública del servidor para cifrar una sesión de intercambio de claves de cifrado de datos. El servidor utiliza su clave privada para descifrar esta sesión de intercambio de claves.

Una vez que se ha establecido la conexión segura, el navegador y el servidor intercambian claves de cifrado de datos para proteger la privacidad y la integridad de la información transmitida entre ellos. Todo el tráfico entre el navegador y el servidor se cifra con estas claves.

Si un servidor malicioso intenta suplantar la identidad de un sitio web seguro, el navegador mostrará una advertencia de seguridad al usuario, ya que el certificado no se puede verificar o no coincide con el nombre de dominio en la URL. Por lo tanto, es importante verificar que el sitio web seguro que estás visitando esté usando un certificado emitido por una CA confiable y que el nombre de dominio en la URL coincida con el nombre de dominio en el certificado.

2.2 Hacking ético

2.2.1 Introducción

El hacking se refiere al acto de aprovechar vulnerabilidades en sistemas informáticos o redes para obtener acceso no autorizado o realizar modificaciones no autorizadas en los mismos. El hacking ético, por otro lado, es el uso de técnicas de hacking para identificar vulnerabilidades en sistemas o redes con el propósito de mejorar la seguridad y protegerlos contra ataques malintencionados.

Las fases típicas de un proceso de hacking ético son las siguientes:

1. Recopilación de información: El objetivo es obtener información sobre el sistema o red que se va a probar.
2. Escaneo: Se utilizan herramientas de escaneo de vulnerabilidades para identificar puertos abiertos, servicios en ejecución y vulnerabilidades conocidas.
3. Enumeración: Se recopila información adicional sobre los sistemas y servicios identificados en la fase de escaneo.
4. Explotación: Se intenta aprovechar las vulnerabilidades identificadas para obtener acceso no autorizado o realizar modificaciones en el sistema o red.

5. Mantenimiento del acceso: Si se logra obtener acceso, se realiza un mantenimiento del mismo para mantener la persistencia y seguir explorando el sistema o red.
6. Informe: Se documentan las vulnerabilidades encontradas y se informa al dueño del sistema o red para que puedan ser corregidas.

Existen varios tipos de hackers, algunos de los cuales son:

1. White hat (sombrero blanco): Son hackers éticos que utilizan sus habilidades para mejorar la seguridad de los sistemas y redes.
2. Black hat (sombrero negro): Son hackers malintencionados que utilizan sus habilidades para obtener acceso no autorizado a sistemas y redes con fines ilícitos.
3. Grey hat (sombrero gris): Son hackers que no tienen intenciones malintencionadas, pero pueden realizar actividades ilegales o no éticas para identificar vulnerabilidades.
4. Script kiddies: Son personas que utilizan herramientas automatizadas y programas preconfigurados para realizar ataques sin comprender realmente cómo funcionan.
5. Hacktivistas: Son hackers que utilizan sus habilidades para hacer una declaración política o social.

Es importante destacar que el hacking ético es una actividad legítima que se realiza con el permiso del dueño del sistema o red que se está probando. El objetivo es mejorar la seguridad y proteger los sistemas y redes contra ataques malintencionados.

En ciberseguridad, el “red team” y el “blue team” son dos equipos de seguridad que se utilizan en las pruebas de penetración (pen testing) y en los ejercicios de seguridad para mejorar la postura de seguridad de una organización.

El “red team” es un equipo de ataque, compuesto por hackers éticos, que simula ataques cibernéticos reales con el objetivo de poner a prueba la seguridad de la organización. Utilizan técnicas de hacking para encontrar vulnerabilidades en los sistemas y redes, y prueban los controles de seguridad de la organización.

El “blue team” es un equipo de defensa que trabaja para proteger la organización de los ataques simulados del “red team”. Utilizan herramientas de monitoreo y análisis para detectar y responder a los ataques, y mejoran la postura de seguridad de la organización.

El “purple team” es un equipo que combina los objetivos y habilidades de ambos equipos para mejorar la colaboración y la comunicación entre el “red team” y el “blue team”. El objetivo del “purple team” es identificar las debilidades de la organización y mejorar la defensa contra futuros ataques.

La razón por la que se utilizan estos equipos es para mejorar la seguridad de una organización. Los ataques cibernéticos son cada vez más sofisticados y frecuentes, y es necesario asegurarse de que los

sistemas y redes de la organización estén protegidos y ayudan también a que se cumplan con las leyes, regulaciones y estándares de seguridad de organizaciones y gobiernos.

Existen otros tipos de equipos de ciberseguridad, como el equipo de respuesta a incidentes de seguridad (CSIRT), que se centra en la gestión y respuesta a los incidentes de seguridad en la organización, y el equipo de gestión de riesgos de seguridad, que se centra en la evaluación y mitigación de los riesgos de seguridad en la organización.

2.2.2 Técnicas de búsqueda de información: Information gathering.

La fase de recopilación de información o “information gathering” es crucial en el hacking ético y en la ciberseguridad en general. Esta fase implica la recopilación de información sobre el objetivo para poder identificar posibles vulnerabilidades y ataques.

Existen diferentes técnicas y herramientas que se pueden utilizar para recopilar información sobre un objetivo. A continuación, se presentan algunas de las técnicas más comunes:

1. OSINT (Open Source Intelligence): Se trata de la recopilación de información a partir de fuentes públicas de acceso libre, como redes sociales, foros, blogs, noticias, entre otros. El objetivo es obtener información relevante y valiosa sobre el objetivo que pueda ser utilizada en la siguiente fase de análisis.
2. Escaneo de puertos y servicios: Los hackers utilizan esta técnica para identificar los servicios que se ejecutan en el sistema objetivo y para identificar posibles vulnerabilidades en estos servicios. Algunas herramientas populares para esta técnica son Nmap, Masscan y Zmap.
3. Enumeración de DNS: Esta técnica implica la recopilación de información sobre el objetivo a través de la consulta de registros DNS, como registros MX, registros de subdominios, registros de host, entre otros. Algunas herramientas populares para esta técnica son NSLookup, Dig y Fierce.
4. Escaneo de vulnerabilidades: Se trata de la identificación de posibles vulnerabilidades en el sistema objetivo, utilizando herramientas como Nessus, OpenVAS y Nikto.
5. Ingeniería social: Los hackers utilizan esta técnica para obtener información valiosa de los usuarios de la organización objetivo, como contraseñas, información personal y credenciales de inicio de sesión. Algunas técnicas de ingeniería social incluyen la suplantación de identidad, el phishing y la ingeniería social por teléfono.

Es importante tener en cuenta que estas técnicas deben ser utilizadas únicamente con fines éticos y legales, como parte de una prueba de penetración autorizada.

En cuanto a programas, algunas herramientas populares para la fase de recopilación de información incluyen:

- Maltego: una herramienta de OSINT que permite la recopilación y visualización de información en tiempo real.
- Nmap: una herramienta de escaneo de puertos y servicios.
- Metasploit: una plataforma de pruebas de penetración que incluye herramientas de escaneo de vulnerabilidades.
- Social-Engineer Toolkit (SET): una herramienta de ingeniería social que incluye diferentes técnicas de phishing.

Recuerda que estas herramientas deben ser utilizadas con precaución y con fines éticos y legales.

2.2.3 Escaneo: pruebas de PenTesting

El red team ha recopilado previamente información sobre el objetivo y ha identificado posibles vulnerabilidades y, por tanto, ahora es el momento de realizar pruebas de penetración o pentesting para evaluar la seguridad del sistema. El objetivo de estas pruebas es simular un ataque real y determinar si un atacante podría explotar las vulnerabilidades identificadas y acceder a información o recursos críticos.

En general, las pruebas de pentesting se realizan en tres etapas: recolección de información, análisis de vulnerabilidades y explotación. En la primera etapa, el equipo de pentesting utiliza herramientas de búsqueda de información para recopilar información sobre el objetivo. En la segunda etapa, el equipo de pentesting utiliza herramientas de análisis de vulnerabilidades para identificar posibles vulnerabilidades en el sistema. Finalmente, en la tercera etapa, el equipo de pentesting intenta explotar las vulnerabilidades para demostrar que se pueden acceder a recursos o información críticos.

El objetivo de las pruebas de pentesting es simular un ataque real para evaluar la seguridad de un sistema o red. Durante estas pruebas, se intenta explotar las vulnerabilidades encontradas en la fase anterior para obtener acceso no autorizado al sistema o red y, de esta manera, determinar la efectividad de las medidas de seguridad existentes y encontrar posibles debilidades.

Existen diferentes herramientas que pueden ayudar en la realización de pruebas de pentesting, entre ellas se encuentran Nessus y OpenVAS. Estas herramientas realizan un escaneo de vulnerabilidades en el sistema o red y proporcionan un informe detallado de las posibles vulnerabilidades encontradas. También pueden realizar pruebas de autenticación, escaneo de puertos, detección de malware, entre otras funciones.

Por ejemplo, Nessus es una herramienta ampliamente utilizada en el mundo de la ciberseguridad para escanear vulnerabilidades en sistemas y redes. Su funcionamiento se basa en la realización de escaneos de puertos y servicios en busca de posibles vulnerabilidades. Además, cuenta con una amplia base de datos de vulnerabilidades conocidas que le permite identificar posibles problemas de seguridad en

el sistema o red escaneados. Por otro lado, OpenVAS es una herramienta similar a Nessus, pero de código abierto, lo que la hace una opción más accesible para aquellos que buscan una herramienta gratuita.

2.2.4 Vulnerabilidades en sistemas

Una vulnerabilidad en un sistema informático es una debilidad o fallo en el software, hardware o configuración del sistema que puede ser aprovechada por atacantes para comprometer la seguridad del sistema, obtener acceso no autorizado, robar información o causar daño. Las vulnerabilidades pueden ser causadas por errores de programación, configuración incorrecta, falta de parches de seguridad, entre otros factores.

Además de Metasploit Framework, existen otras herramientas de explotación de vulnerabilidades, como ExploitDB, que es una base de datos en línea de exploits y técnicas de hacking; Core Impact, que es una herramienta de pruebas de penetración comercial que permite identificar y explotar vulnerabilidades en sistemas; y CANVAS, otra herramienta de prueba de penetración que permite a los evaluadores de seguridad identificar y explotar vulnerabilidades en aplicaciones y sistemas.

Es importante tener en cuenta que estas herramientas de explotación de vulnerabilidades solo deben ser utilizadas por profesionales de la seguridad debidamente capacitados y autorizados, y en un entorno de prueba controlado. Su uso inapropiado o malicioso puede tener graves consecuencias legales y de seguridad.

2.3 Incidentes de ciberseguridad

2.3.1 Análisis forense

La creciente dependencia de la tecnología en nuestras vidas diarias ha llevado a una mayor cantidad de crímenes y delitos que involucran dispositivos electrónicos, como ordenadores, móviles y tabletas. En respuesta a esta tendencia, ha surgido un campo especializado conocido como análisis forense digital o “digital forensics”, que se centra en la recopilación, preservación, análisis y presentación de evidencia digital en casos judiciales.

El análisis forense digital es una disciplina que implica la aplicación de técnicas y métodos de investigación científica para examinar datos electrónicos y determinar su autenticidad, integridad y relevancia para una investigación o proceso judicial. Las investigaciones forenses digitales pueden ser solicitadas por agencias gubernamentales, empresas, abogados y particulares para una variedad de propósitos, incluyendo la investigación de delitos informáticos, la recuperación de datos, la identificación de amenazas a la seguridad, la resolución de disputas y la obtención de pruebas en casos civiles o penales.

El proceso de análisis forense digital involucra varias etapas, como la identificación de la evidencia, la recolección o adquisición y preservación de la evidencia, el análisis y la interpretación de la evidencia, y la presentación de los hallazgos. Durante la etapa de identificación, se busca identificar la evidencia digital relevante para el caso, y se deben tomar medidas para preservar la evidencia y evitar su alteración o destrucción. La etapa de recolección y preservación implica la recopilación de la evidencia digital y su almacenamiento en un entorno seguro y controlado. En la etapa de análisis, se utiliza una variedad de técnicas, herramientas y métodos para analizar la evidencia y extraer información relevante. Finalmente, en la etapa de presentación, los hallazgos del análisis se documentan y se presentan en un informe, que se utiliza como evidencia en los procedimientos legales.

Entre las técnicas y herramientas utilizadas en el análisis forense digital, se encuentran el análisis de registro, el análisis de tráfico de red, la recuperación de datos borrados, la recuperación de contraseñas, entre otras. Las herramientas de software también son una parte esencial del análisis forense digital, y existen numerosas herramientas que pueden ayudar a los investigadores en cada etapa del proceso.

En resumen, el análisis forense digital es una técnica esencial en la lucha contra los delitos informáticos, y su aplicación puede ayudar a las organizaciones a identificar y resolver incidentes de seguridad, así como a investigar delitos informáticos y llevar a los autores ante la justicia. Es importante que los profesionales de la seguridad informática y los investigadores estén capacitados en las técnicas y herramientas de análisis forense digital para poder enfrentar los desafíos de un mundo cada vez más digitalizado.

A continuación, proporcionamos algunos ejemplos de herramientas que se utilizan comúnmente en cada una de las etapas del análisis forense digital:

1. Adquisición de datos:

- dd (para copiar datos bit a bit)
- FTK Imager (para adquirir imágenes de disco)
- EnCase Forensic Imager (para adquirir imágenes de disco)
- Helix3 Pro (para crear imágenes de disco)

2. Preservación de datos:

- FTK Imager (para crear imágenes forenses)
- Encase Forensic (para proteger los datos originales)
- WinHex (para preservar los datos de forma segura)

3. Análisis de datos:

- Autopsy (para analizar imágenes de disco)

- EnCase Forensic (para análisis de archivos y recuperación de datos)
- SANS SIFT Workstation (para análisis de redes)
- The Sleuth Kit (para análisis de archivos)

4. Presentación de resultados:

- Xplico (para reconstruir la comunicación en red)
- Wireshark (para capturar y analizar tráfico de red)
- Oxygen Forensic Detective (para análisis de dispositivos móviles)
- FTK (para presentar los resultados del análisis)

Es importante tener en cuenta que estas son solo algunas de las herramientas disponibles y que cada analista forense puede tener sus preferencias en cuanto a las herramientas que utiliza. Además, es importante mencionar que el uso de estas herramientas debe hacerse de manera legal y ética.

2.3.2 Ciberdelitos

Un ciberdelito es un delito que se comete en el ámbito digital, utilizando tecnologías de la información y la comunicación (TIC). También se le conoce como delito informático o delito cibernético. Los ciberdelitos pueden incluir una amplia variedad de actividades ilegales, como el acceso no autorizado a sistemas informáticos, el robo de información personal o financiera, la difusión de virus informáticos, el fraude en línea, el acoso en línea, el ciberespionaje, la extorsión y el phishing, entre otros.

Puede ser un delito informático en el que se utiliza una computadora o una red de computadoras para llevar a cabo actividades ilegales, como el acceso no autorizado a sistemas o el robo de información. También puede ser un delito que se comete utilizando internet como medio, como el acoso en línea o la difusión de material ilegal a través de la red.

Los ciberdelitos pueden ser llevados a cabo por individuos, grupos organizados o incluso por gobiernos. Algunos ejemplos de ciberdelitos incluyen:

- Hacking: El acceso no autorizado a sistemas informáticos con el fin de robar información o causar daños.
- Phishing: El uso de correos electrónicos falsos o sitios web falsos para engañar a las personas y obtener información confidencial, como contraseñas o números de tarjetas de crédito.
- Malware: La distribución de software malicioso que puede ser utilizado para espiar o dañar sistemas informáticos.
- Fraude en línea: El uso de internet para llevar a cabo estafas, como el fraude de inversión o la venta de productos falsos.

- Ciberacoso: La utilización de internet para hostigar, intimidar o amenazar a otras personas.

Los ciberdelitos son un problema creciente en todo el mundo, ya que la tecnología se ha vuelto cada vez más omnipresente en nuestras vidas cotidianas. Los delincuentes pueden utilizar herramientas y técnicas sofisticadas para cometer ciberdelitos y, a menudo, pueden hacerlo desde cualquier lugar del mundo, lo que dificulta su detección y enjuiciamiento.

Pueden tener graves consecuencias para las víctimas, incluyendo la pérdida de datos personales y financieros, la interrupción de los sistemas informáticos y la exposición a actividades ilegales. También pueden tener consecuencias más amplias, como la afectación de la economía o la seguridad nacional.

Para prevenir los ciberdelitos es importante tomar medidas de seguridad como mantener actualizados los sistemas y software, utilizar contraseñas seguras, evitar hacer clic en enlaces sospechosos y estar alerta a posibles intentos de phishing. También es importante contar con herramientas de seguridad como software antivirus, firewalls y herramientas de detección de intrusiones. En caso de sufrir un ciberdelito, es importante reportarlo a las autoridades y tomar medidas para mitigar los daños.

3 Big Data

En este tema aprenderemos:

- Big data. Características. Volumen de datos.
- Visualización, transporte y almacenaje de los datos.
- Recogida, análisis y generación de datos.
- Simulación de fenómenos naturales y sociales.
- Descripción del modelo.
- Identificación de agentes.
- Implementación del modelo mediante un software específico, o mediante programación.

El término “big data” se refiere a la enorme cantidad de datos que se generan a diario en diversas fuentes como sensores, redes sociales, transacciones financieras, registros médicos, entre otros. Las características principales de los datos que conforman el big data son el volumen, la variedad y la velocidad.

El volumen de los datos del big data es enorme y supera con creces la capacidad de los sistemas tradicionales de almacenamiento y procesamiento de datos. Además, los datos del big data suelen estar en constante crecimiento y actualización, lo que hace que el volumen sea cada vez mayor.

La variedad de los datos del big data hace referencia a la diversidad de formatos, fuentes y tipos de datos que se generan. Estos datos pueden ser estructurados (como bases de datos y hojas de cálculo) o no estructurados (como textos, imágenes y videos).

La velocidad de los datos del big data se refiere a la rapidez con que se generan y se deben procesar. En algunos casos, es necesario analizar y actuar sobre los datos en tiempo real para poder tomar decisiones rápidas y eficaces.

Para poder trabajar con big data es necesario contar con herramientas y tecnologías que permitan visualizar, transportar y almacenar los datos de manera eficiente. Algunas de estas herramientas son Hadoop, Spark, Cassandra y MongoDB.

La recogida, análisis y generación de datos son procesos fundamentales en el trabajo con big data. La recogida de datos se realiza a través de sensores, redes sociales, registros de transacciones, entre otros. El análisis de datos permite obtener información útil y relevante a partir de los datos del big data. La generación de datos puede ser realizada mediante la simulación de fenómenos naturales y sociales.

Para la simulación de fenómenos naturales y sociales es necesario crear un modelo que permita representar y simular el comportamiento de los elementos que conforman el fenómeno. Este modelo puede ser descrito mediante una serie de ecuaciones y algoritmos.

La identificación de agentes es un proceso importante en la creación de modelos de simulación. Los

agentes son los elementos individuales que interactúan dentro del fenómeno que se está simulando. Estos agentes pueden ser personas, animales, objetos, entre otros.

La implementación del modelo de simulación puede ser realizada mediante un software específico de simulación o mediante programación. En ambos casos, es necesario definir las variables y parámetros del modelo y establecer los límites y condiciones para la simulación.

3.1 Conceptos previos

El término “big data” se refiere a la enorme cantidad de datos que se generan a diario en diversas fuentes como sensores, redes sociales, transacciones financieras, registros médicos, entre otros. Las características principales de los datos que conforman el big data son el volumen, la variedad y la velocidad.

El volumen de los datos del big data es enorme y supera con creces la capacidad de los sistemas tradicionales de almacenamiento y procesamiento de datos. Además, los datos del big data suelen estar en constante crecimiento y actualización, lo que hace que el volumen sea cada vez mayor.

La variedad de los datos del big data hace referencia a la diversidad de formatos, fuentes y tipos de datos que se generan. Estos datos pueden ser estructurados (como bases de datos y hojas de cálculo) o no estructurados (como textos, imágenes y videos).

La velocidad de los datos del big data se refiere a la rapidez con que se generan y se deben procesar. En algunos casos, es necesario analizar y actuar sobre los datos en tiempo real para poder tomar decisiones rápidas y eficaces.

Para poder trabajar con big data es necesario contar con herramientas y tecnologías que permitan visualizar, transportar y almacenar los datos de manera eficiente. Algunas de estas herramientas son Hadoop, Spark, Cassandra y MongoDB.

La recogida, análisis y generación de datos son procesos fundamentales en el trabajo con big data. La recogida de datos se realiza a través de sensores, redes sociales, registros de transacciones, entre otros. El análisis de datos permite obtener información útil y relevante a partir de los datos del big data. La generación de datos puede ser realizada mediante la simulación de fenómenos naturales y sociales.

Para la simulación de fenómenos naturales y sociales es necesario crear un modelo que permita representar y simular el comportamiento de los elementos que conforman el fenómeno. Este modelo puede ser descrito mediante una serie de ecuaciones y algoritmos.

La *identificación de agentes* es un proceso importante en la creación de modelos de simulación. Los agentes son los elementos individuales que interactúan dentro del fenómeno que se está simulando. Estos agentes pueden ser personas, animales, objetos, entre otros.

La *implementación del modelo de simulación* puede ser realizada mediante un software específico de simulación o mediante programación. En ambos casos, es necesario definir las variables y parámetros del modelo y establecer los límites y condiciones para la simulación.

3.2 Big data. Características. Volumen de datos.

Como ya comentamos anteriormente, el término “big data” se refiere a la enorme cantidad de datos que se generan a diario en diversas fuentes como sensores, redes sociales, transacciones financieras, registros médicos, entre otros. Pero antes de adentrarnos en el tema es necesario hablar de **las 7 “V” del Big Data, qué caracteriza al Big Data**:

1. *Volumen*: hace referencia a la enorme cantidad de datos generados y almacenados en diferentes fuentes de información.
2. *Velocidad*: se refiere a la velocidad a la que se generan los datos y a la necesidad de procesarlos en tiempo real.
3. *Variedad de los datos*: se refiere a la diversidad de tipos de datos y su complejidad, que van desde datos estructurados como bases de datos, hasta datos no estructurados como imágenes, vídeos, audios y texto.
4. *Veracidad de los datos*: se refiere a la confiabilidad y precisión de los datos. Es importante asegurar que los datos utilizados sean precisos y confiables para tomar decisiones importantes.
5. *Viabilidad*: se refiere a la capacidad de las empresas y organizaciones para gestionar, almacenar y procesar grandes cantidades de datos.
6. *Visualización de los datos*: se refiere a la habilidad de transformar datos complejos en información visual fácil de entender y analizar.
7. *Valor de los datos*: se refiere a la capacidad de los datos para generar valor y proporcionar una ventaja competitiva a las empresas y organizaciones que los utilizan de manera efectiva.

Un proyecto de Big Data típicamente consta de varias **capas tecnológicas** que trabajan juntas para procesar y analizar grandes cantidades de datos. A continuación, se describen algunas de las capas tecnológicas comunes de un proyecto de Big Data:

1. *Ingesta de datos*: Esta capa se encarga de la recolección de datos de diversas fuentes, como sensores, redes sociales, bases de datos, etc., y su transferencia a la siguiente capa para su procesamiento.
2. *Almacenamiento de datos*: Esta capa almacena los datos recolectados en una infraestructura escalable y distribuida, como Hadoop Distributed File System (HDFS), Apache Cassandra, Amazon S3, entre otros.
3. *Procesamiento de datos*: Esta capa se encarga de procesar y analizar los datos utilizando tecnologías como Apache Spark, MapReduce, Hadoop, entre otras.

4. *Análisis de datos*: Esta capa se utiliza para el análisis y la exploración de los datos, utilizando herramientas de minería de datos, aprendizaje automático y estadísticas.
5. *Visualización de datos*: Esta capa permite la visualización y el análisis interactivo de los datos procesados y analizados, utilizando herramientas de visualización de datos como Tableau, QlikView, entre otras.
6. *Integración con sistemas existentes*: Esta capa se encarga de integrar los resultados del análisis de datos en sistemas existentes, como aplicaciones de negocios, CRM, sistemas de gestión de la cadena de suministro, entre otros.
7. *Seguridad y gestión de datos*: Esta capa garantiza la seguridad de los datos y la gestión de los permisos de acceso a los datos, cumpliendo con las regulaciones y normativas existentes.

3.3 Visualización, transporte y almacenaje de los datos.

En un proyecto de Big Data, la visualización, transporte y almacenamiento de los datos son tres aspectos críticos que deben ser cuidadosamente considerados.

- *Visualización de datos*: la visualización de datos es una parte crucial del análisis de Big Data. Permite presentar los datos de forma clara y fácilmente comprensible para que los usuarios puedan tomar decisiones informadas basadas en ellos. Las herramientas de visualización de datos se utilizan para crear gráficos, tablas, diagramas y otros tipos de representaciones visuales de los datos.
- *Transporte de datos*: para llevar los datos de un lugar a otro, se necesitan herramientas de transporte de datos. En un entorno de Big Data, esto puede implicar el movimiento de grandes cantidades de datos de una ubicación a otra. Las herramientas de transporte de datos incluyen soluciones de ETL (extracción, transformación y carga) y de streaming, que se utilizan para mover datos en tiempo real.
- *Almacenamiento de datos*: el almacenamiento de datos es otro aspecto crítico del Big Data. La capacidad de almacenar grandes cantidades de datos de forma eficiente y segura es esencial. Las tecnologías de almacenamiento de datos incluyen bases de datos NoSQL, almacenamiento de objetos, almacenamiento en la nube y almacenamiento en Hadoop. Cada una de estas tecnologías tiene ventajas y desventajas, y la elección de una u otra depende de las necesidades específicas del proyecto.

3.4 Recogida, análisis y generación de datos.

En primer lugar, la recogida de datos implica la identificación de las fuentes de datos relevantes para el proyecto y la captura de dichos datos de manera eficiente y en tiempo real. Puede involucrar la integración de datos de múltiples fuentes, tanto internas como externas a la organización.

Una vez recopilados los datos, se procede al análisis de los mismos. Esto implica la limpieza, procesamiento y transformación de los datos para que sean útiles para el análisis y la toma de decisiones. Este proceso puede incluir la identificación y eliminación de datos duplicados o incompletos, la normalización de los datos y la creación de modelos de datos para facilitar el análisis.

Finalmente, la generación de datos implica el uso de técnicas de análisis de datos para extraer información valiosa y tomar decisiones informadas. Esto puede implicar la creación de modelos de predicción, el análisis de tendencias y patrones, y la identificación de insights ocultos en los datos.

Algunos ejemplos concretos de productos comerciales y libres que se utilizan en la recopilación, análisis y generación de datos en Big Data:

- Recogida de datos:
 - Producto comercial: Google Analytics es una herramienta popular para recopilar datos de sitios web y aplicaciones móviles. Proporciona información sobre el comportamiento del usuario, el rendimiento del sitio web, la adquisición de tráfico y mucho más.
 - Producto libre: Apache NiFi es una plataforma de integración de datos de código abierto que permite recopilar datos de diversas fuentes, como sensores, bases de datos, archivos y más. Facilita la transferencia de datos en tiempo real a través de flujos de datos seguros y escalables.
- Análisis de datos:
 - Producto comercial: Tableau es una herramienta de visualización de datos que permite a los usuarios crear informes y paneles interactivos. Ayuda a los analistas de datos a identificar patrones, tendencias y oportunidades de negocio a partir de grandes conjuntos de datos.
 - Producto libre: Apache Spark es un motor de procesamiento de datos de código abierto que proporciona un análisis rápido de grandes conjuntos de datos. Proporciona una API unificada para trabajar con diferentes tipos de datos, como procesamiento de gráficos, aprendizaje automático y procesamiento de flujos.
- Generación de datos:
 - Producto comercial: Hootsuite Insights es una plataforma de escucha social que recopila datos de redes sociales y los utiliza para crear informes personalizados. Los usuarios pueden monitorear el sentimiento de la marca, identificar tendencias y realizar un seguimiento de la competencia.
 - Producto libre: Faker es una biblioteca de generación de datos de código abierto que crea datos falsos para pruebas y simulaciones. Se puede utilizar para generar datos de prueba para aplicaciones web y móviles, y se puede personalizar para crear datos que se ajusten a ciertos requisitos.

3.5 Simulación de fenómenos naturales y sociales

La simulación de fenómenos naturales y sociales en Big Data se refiere al uso de técnicas computacionales para recrear y modelar eventos que ocurren en la naturaleza o en la sociedad, con el objetivo de comprenderlos mejor y predecir su comportamiento futuro. Esta técnica se aplica en una amplia variedad de campos, desde la meteorología hasta la economía.

Un ejemplo concreto de aplicación de la simulación de fenómenos naturales en Big Data es el modelado del clima. La Agencia Meteorológica de Japón utiliza el superordenador más potente del mundo, llamado “Fugaku”, para simular el clima y predecir eventos como tifones, tsunamis y lluvias torrenciales. Este modelo utiliza una gran cantidad de datos históricos y en tiempo real, incluyendo datos de satélite, estaciones meteorológicas y boyas oceánicas, para predecir cómo el clima evolucionará en el futuro.

Otro ejemplo de simulación de fenómenos sociales en Big Data es el modelado de la propagación de enfermedades. Durante la pandemia de COVID-19, muchos países utilizaron modelos de simulación para predecir cómo se propagaría el virus y cómo podrían mitigarse sus efectos. Por ejemplo, la Universidad de Virginia desarrolló un modelo que utiliza datos de ubicación de teléfonos móviles para predecir la propagación del virus y recomendar medidas preventivas.

En ambos casos, la simulación de fenómenos naturales y sociales en Big Data requiere una gran cantidad de datos, así como el uso de técnicas avanzadas de análisis y modelado. Sin embargo, los beneficios potenciales son significativos, ya que pueden ayudar a prevenir desastres naturales y brotes de enfermedades, así como a mejorar la planificación y la toma de decisiones en una amplia variedad de campos.

3.6 Descripción del modelo

La descripción del modelo de simulación en big data se refiere a la documentación detallada de cómo se ha diseñado y construido el modelo de simulación. Esta descripción es importante para garantizar que el modelo pueda ser replicado, modificado y mejorado en el futuro.

La descripción del modelo debe incluir información sobre el propósito del modelo, el fenómeno que se está simulando, los datos utilizados para construir el modelo, los algoritmos y técnicas de análisis utilizados, y los resultados de la simulación. Además, se debe describir cómo se ha implementado el modelo en una plataforma de big data, incluyendo el hardware y software utilizados, y los detalles técnicos de la implementación.

Un ejemplo de modelo de simulación en big data es el sistema de simulación de tráfico desarrollado por la ciudad de Los Ángeles. Este modelo utiliza datos de sensores de tráfico, cámaras y GPS de vehículos para simular el flujo de tráfico en la ciudad. La descripción del modelo incluye detalles sobre cómo se recopilan y procesan los datos, cómo se construye el modelo y cómo se implementa en una

plataforma de big data. Con este modelo, la ciudad de Los Ángeles puede predecir el tráfico en tiempo real y tomar medidas para reducir la congestión en las carreteras.

3.7 Identificación de agentes

La identificación de agentes en Big Data se refiere a la identificación de individuos, entidades o sistemas que interactúan dentro de un conjunto de datos para la simulación de eventos. Los agentes pueden ser personas, animales, máquinas o sistemas, y se les puede asignar una serie de características, como edad, género, ubicación geográfica, comportamiento, entre otras.

La identificación de agentes es fundamental para la simulación de fenómenos en Big Data, ya que permite crear modelos más precisos que representan de manera más realista la interacción entre los diferentes elementos que conforman el sistema. Por ejemplo, en una simulación de tráfico urbano, los agentes pueden ser identificados como vehículos, conductores, peatones, semáforos, entre otros. Al asignar a cada agente características específicas, como velocidad, capacidad de reacción y preferencias de ruta, se pueden simular diferentes escenarios y evaluar su impacto en el tráfico.

En resumen, la identificación de agentes en Big Data es un proceso clave en la simulación de fenómenos complejos, ya que permite crear modelos más precisos y realistas, lo que puede ser utilizado en diferentes áreas, como la ingeniería, la gestión de recursos naturales, la planificación urbana, la medicina y la economía, entre otras.

3.8 Implementación del modelo mediante un software específico, o mediante programación

La implementación de un modelo de simulación en big data involucra el uso de tecnologías y herramientas específicas para procesar grandes cantidades de datos y realizar simulaciones en tiempo real. La idea es capturar la información relevante de los datos y utilizarla para generar modelos de simulación precisos y escalables.

Para implementar un modelo de simulación en big data, es necesario seguir los siguientes pasos:

1. Recopilar los datos relevantes: La primera etapa consiste en recopilar y seleccionar los datos relevantes para la simulación. Estos datos pueden provenir de diversas fuentes, como sensores, redes sociales, dispositivos IoT, entre otros.
2. Procesamiento de datos: El siguiente paso es procesar los datos utilizando técnicas de big data, como el procesamiento distribuido, el procesamiento en tiempo real y el procesamiento de lenguaje natural. El objetivo es limpiar, integrar y estructurar los datos de manera que sean utilizables para el modelo de simulación.

3. Selección del modelo de simulación: Una vez que los datos están listos, es necesario seleccionar el modelo de simulación más adecuado. Por ejemplo, si se trata de una simulación de tráfico, se puede utilizar un modelo basado en agentes.
4. Implementación del modelo de simulación: El siguiente paso es implementar el modelo de simulación utilizando herramientas y tecnologías de big data, como Apache Spark, Hadoop, Cassandra, entre otros.
5. Validación y ajuste del modelo: Una vez implementado el modelo, se debe validar y ajustar su precisión utilizando diferentes técnicas, como la validación cruzada y la comparación de resultados con datos históricos.

Algunos ejemplos de aplicaciones de simulación de fenómenos naturales y sociales en big data son:

- Simulación de tráfico: Los modelos de simulación de tráfico en big data pueden ayudar a predecir y optimizar el tráfico en tiempo real. Un ejemplo de producto comercial para esto es el software PTV Vissim.
- Simulación de eventos deportivos: Los modelos de simulación en big data pueden ayudar a predecir los resultados de eventos deportivos y analizar la estrategia de los equipos. Un ejemplo de producto comercial para esto es el software SAS Sports Analytics.
- Simulación de desastres naturales: Los modelos de simulación de desastres naturales en big data pueden ayudar a predecir y planificar la respuesta a eventos como terremotos y huracanes. Un ejemplo de software libre para esto es el proyecto HAZUS.

4 Inteligencia Artificial

En este tema aprenderemos:

1. Definición. Historia. El test de Turing.
2. Aplicaciones. Impacto.
3. Ética y responsabilidad social (transparencia y discriminación algorítmica).
4. Beneficios y posibles riesgos.
5. Agentes inteligentes simples.
6. Análisis y clasificación supervisada basada en técnicas de aprendizaje automático: reconocimiento de habla; reconocimiento de imágenes; y reconocimiento de texto.
7. Generación de imágenes y/o música basado en técnicas de aprendizaje automático: mezcla inteligente de dos imágenes; generación de música; traducción y realidad aumentada.

4.1 Definición. Historia. El test de Turing

La inteligencia artificial (IA) se refiere a la capacidad de las máquinas y los sistemas informáticos para realizar tareas que normalmente requerirían inteligencia humana, como el aprendizaje, el razonamiento y la resolución de problemas.

La IA se basa en el uso de algoritmos y modelos matemáticos complejos que permiten a las máquinas analizar grandes cantidades de datos y tomar decisiones basadas en patrones y predicciones. También puede utilizar técnicas de aprendizaje automático y procesamiento del lenguaje natural para comprender y responder al lenguaje humano.

No podemos definir la IA sin hablar del Test de Turing, que es una prueba propuesta por el matemático e informático Alan Turing en 1950 para evaluar la capacidad de una máquina para exhibir un comportamiento inteligente similar al de un ser humano.

La prueba se basa en la capacidad de una máquina para realizar una conversación en lenguaje natural con un evaluador humano, de tal manera que el evaluador no pueda distinguir si la respuesta proviene de una máquina o de otro ser humano. En esencia, el objetivo del test es determinar si una máquina puede exhibir un comportamiento indistinguible del de un ser humano.

Para realizar el test, se utiliza un protocolo de “juego de imitación” en el que un evaluador (humano) interactúa en una conversación con dos participantes ocultos detrás de una cortina o pantalla. Uno de los participantes es una máquina y el otro es un ser humano. El evaluador hace preguntas a ambos participantes y trata de determinar cuál de ellos es la máquina y cuál es el ser humano. Si el evaluador no puede distinguir entre los dos participantes, entonces la máquina ha “pasado” el Test de Turing.

El Test de Turing ha sido criticado por su simplicidad y por su incapacidad para evaluar de manera efectiva la inteligencia artificial en áreas más allá del procesamiento del lenguaje natural. Sin embargo,

sigue siendo una prueba influyente en el campo de la IA y ha sido utilizada como un punto de referencia importante en la medición de la capacidad de las máquinas para imitar la inteligencia humana.

La inteligencia artificial se divide en varias ramas, como:

- aprendizaje automático
- la visión por computador
- el procesamiento del lenguaje natural
- la robótica

Estas ramas se aplican en una amplia variedad de campos, desde la atención médica y la educación hasta la industria manufacturera y la investigación científica.

La IA tiene un gran potencial para mejorar nuestra vida y resolver algunos de los desafíos más importantes de la humanidad, pero también plantea desafíos éticos y sociales que deben ser abordados para asegurar su uso responsable y seguro.

Algunos de los momentos más importantes en la historia de la inteligencia artificial (IA) que podemos destacar son:

- 1940-1950: En 1943 Warren McCulloch y Walter Pitts publican un artículo en el que proponen un modelo matemático de neuronas artificiales, sentando las bases de la teoría de las redes neuronales.
- 1950-1960: En 1950 el matemático e informático británico Alan Turing propuso la idea de que las máquinas podrían ser capaces de pensar y razonar como los seres humanos. En 1956 John McCarthy, Marvin Minsky, Nathaniel Rochester y Claude Shannon organizan una conferencia en Dartmouth College en la que se acuña el término “inteligencia artificial” y se define el campo como la simulación de procesos de pensamiento humano en máquinas.
- 1960-1970: El éxito temprano en la IA llevó a la investigación en áreas como la lógica, el razonamiento basado en reglas y el aprendizaje automático. Se desarrollan programas para resolver problemas como el ajedrez y la comprensión del lenguaje natural. En la década de 1960, el investigador Joseph Weizenbaum desarrolló el programa ELIZA, que fue uno de los primeros programas de procesamiento del lenguaje natural. ELIZA fue capaz de comunicarse en lenguaje natural y llevar a cabo conversaciones sencillas con los usuarios.
- 1970-1980: En la década de 1970, se produjeron avances significativos en el aprendizaje automático y la inteligencia artificial basada en reglas. Los expertos en IA crearon sistemas expertos, que utilizaban conocimientos expertos para tomar decisiones en áreas como la medicina y la ingeniería.
- 1980-1990: Se producen avances en el aprendizaje automático y la visión por computadora. La IA se utiliza en aplicaciones comerciales, como la detección de fraudes en tarjetas de crédito y los sistemas de recomendación de películas. En la década de 1980, se desarrolló la tecnología

de redes neuronales, que permitió a las máquinas aprender de manera autónoma y mejorar su capacidad para tomar decisiones.

- 1990-2000: En la década de 1990, se produjeron importantes avances en la robótica y la visión por computadora. Los robots comenzaron a ser utilizados en la fabricación y la exploración espacial, y la visión por computadora se convirtió en una herramienta esencial para la vigilancia y la seguridad. En 1997, el superordenador de IBM “Deep Blue” derrota al campeón de ajedrez Garry Kasparov en una partida de seis juegos.
- 2000-2010: En la década de 2000, la inteligencia artificial se convirtió en una parte integral de la vida cotidiana gracias a los asistentes virtuales como Siri y Alexa. También se produjeron importantes avances en el aprendizaje profundo, una técnica de aprendizaje automático que ha impulsado importantes avances en áreas como el reconocimiento de voz y la visión por computadora.
- 2010-2020: En la década de los 2010 se produce un aumento explosivo en el volumen de datos disponibles y la capacidad de procesamiento, lo que lleva a avances significativos en el aprendizaje profundo y las redes neuronales. En 2011, IBM Watson, un sistema de inteligencia artificial basado en el procesamiento del lenguaje natural, gana el concurso de televisión “Jeopardy!”. En 2016, AlphaGo, un programa de inteligencia artificial de Google DeepMind, derrota al campeón mundial de Go en una serie de juegos. Para finales de esta década, la inteligencia artificial es utilizada en una variedad de aplicaciones, como la asistencia sanitaria, el transporte, la seguridad cibernética y la robótica. Se produce un debate creciente sobre los riesgos y desafíos éticos asociados con la IA, como la privacidad, la discriminación y el desplazamiento laboral.
- 2020-presente: El gran avance de la IA de estos últimos años hace de ésta ahora una tecnología disruptiva, produciendo grandes cambios en nuestra sociedad, tales como:
 - Mejora de la eficiencia: La IA puede realizar tareas repetitivas y complejas de manera más rápida y precisa que los humanos, lo que mejora la eficiencia en diversas industrias. Por ejemplo, Chat-GPT y otros chatbots pueden manejar una gran cantidad de consultas y preguntas de los clientes sin la necesidad de intervención humana.
 - Personalización: La IA puede analizar grandes cantidades de datos para identificar patrones y preferencias, lo que permite una mayor personalización en servicios y productos. Por ejemplo, la IA se utiliza en sistemas de recomendación de películas y música, lo que permite a los usuarios recibir recomendaciones adaptadas a sus gustos y preferencias.
 - Mejora de la atención sanitaria: La IA puede ayudar a los profesionales de la salud a diagnosticar enfermedades y desarrollar planes de tratamiento personalizados utilizando grandes cantidades de datos. Además, la IA se utiliza en robots quirúrgicos y sistemas de monitoreo de pacientes para mejorar la eficiencia y precisión de los procedimientos médicos.
 - Automatización: La IA puede automatizar tareas como la gestión de inventarios, la programación y el análisis de datos, lo que reduce los errores humanos y mejora la eficiencia en

- diversos procesos empresariales.
- Cambio en la naturaleza del trabajo: La IA puede desplazar ciertos trabajos que implican tareas repetitivas o predecibles, pero también puede crear nuevos trabajos en áreas como el desarrollo de sistemas de IA y la gestión de datos.

4.2 Aplicaciones. Impacto

La IA está presente en nuestro día a día en lugares como:

1. Asistentes de voz: Los asistentes de voz como Siri de Apple, Alexa de Amazon y Google Assistant utilizan IA para comprender y responder a las solicitudes de los usuarios.
2. Sistemas de recomendación: Las plataformas de comercio electrónico como Amazon y Netflix utilizan IA para recomendar productos y contenido personalizados a los usuarios.
3. Vehículos autónomos: Los vehículos autónomos como los coches sin conductor utilizan sistemas de IA para tomar decisiones en tiempo real basadas en los datos recopilados por los sensores y las cámaras.
4. Chatbots: Los chatbots como Chat-GPT y otros, utilizan IA para comprender y responder a las preguntas de los usuarios en línea.
5. Diagnóstico médico: Los sistemas de IA pueden analizar grandes cantidades de datos médicos y ayudar a los profesionales de la salud a realizar diagnósticos precisos y desarrollar planes de tratamiento personalizados.
6. Detección de fraudes: Los sistemas de IA pueden analizar grandes cantidades de datos financieros para detectar patrones y anomalías que puedan indicar fraudes.
7. Robots industriales: Los robots industriales utilizan IA para realizar tareas repetitivas y peligrosas en la fabricación y el ensamblaje de productos.
8. Sistemas de seguridad: Los sistemas de seguridad pueden utilizar IA para analizar el comportamiento y detectar patrones de amenazas potenciales en tiempo real.

Gracias a estos ejemplos, podemos ver que la IA puede tener un impacto positivo en nuestras vidas, ampliando lo anterior por ejemplo:

- En la atención médica: la IA puede ser utilizada para analizar grandes cantidades de datos médicos y ayudar a los médicos a hacer diagnósticos más precisos y proporcionar mejores tratamientos para los pacientes.
- En la educación: la IA puede ser utilizada para personalizar el aprendizaje y adaptarse a las necesidades individuales de cada estudiante, lo que puede mejorar la eficacia del proceso de enseñanza y aprendizaje.
- En el transporte: la IA puede ser utilizada para desarrollar vehículos autónomos que pueden mejorar la seguridad en la carretera y reducir la congestión del tráfico.

- En la investigación científica: la IA puede ser utilizada para analizar grandes cantidades de datos científicos y ayudar a los científicos a hacer descubrimientos importantes en áreas como la biología, la química y la física.
- En la industria manufacturera: la IA puede ser utilizada para optimizar la producción y reducir los costos de producción al hacer que los procesos de fabricación sean más eficientes y precisos.

Pero la IA tiene el potencial de tener un impacto negativo en diversos ámbitos, algunos de los riesgos y desafíos asociados con su uso podrían ser:

- Desplazamiento laboral: La automatización de tareas mediante la IA puede desplazar ciertos trabajos que implican tareas repetitivas o predecibles, lo que puede tener un impacto negativo en las personas que trabajan en esas áreas.
- Sesgos y discriminación: La IA puede estar sesgada si los datos utilizados para entrenar los algoritmos contienen sesgos y prejuicios. Esto puede llevar a decisiones discriminatorias en áreas como la selección de empleados o la concesión de préstamos.
- Pérdida de privacidad: La IA puede recopilar y analizar grandes cantidades de datos, lo que plantea desafíos de privacidad y seguridad. Por ejemplo, los sistemas de reconocimiento facial pueden utilizarse para rastrear a personas sin su conocimiento o consentimiento.
- Uso malintencionado: La IA puede ser utilizada para fines malintencionados, como la manipulación de opiniones políticas o la creación de contenidos falsos.
- Dependencia: La dependencia excesiva de la IA para la toma de decisiones críticas puede tener consecuencias negativas si los sistemas no son confiables o si se producen fallos técnicos.

4.3 Ética y responsabilidad social (transparencia y discriminación algorítmica)

El diseño y desarrollo de la IA plantea una serie de problemas éticos y de responsabilidad social que deben ser considerados cuidadosamente por los desarrolladores y usuarios de esta tecnología. Algunos de estos problemas incluyen:

- Sesgos y discriminación: La IA puede reflejar los sesgos de los datos utilizados para entrenarla, lo que puede llevar a decisiones discriminatorias y perjudiciales para ciertos grupos de personas.
- Privacidad y seguridad: La IA puede ser utilizada para recopilar y analizar grandes cantidades de datos personales, lo que plantea preocupaciones sobre la privacidad y la seguridad de la información.
- Responsabilidad y transparencia: La toma de decisiones automatizada por parte de la IA puede hacer que sea difícil determinar quién es responsable cuando se produce un error o un resultado no deseado. También puede ser difícil entender cómo se toman estas decisiones, lo que dificulta la transparencia y la rendición de cuentas.

- Impacto en el empleo: La IA puede automatizar muchas tareas que antes eran realizadas por personas, lo que plantea preocupaciones sobre el impacto en el empleo y la necesidad de reentrenamiento y reconversión laboral.
- Seguridad nacional: La IA puede ser utilizada para desarrollar armas autónomas, lo que plantea preocupaciones éticas y legales sobre el uso de esta tecnología en conflictos armados.
- Cambio cultural y social: La IA puede tener un impacto en la forma en que interactuamos y nos relacionamos entre nosotros, lo que plantea preguntas sobre el cambio cultural y social que puede surgir de la adopción generalizada de esta tecnología.

En general, es importante que los desarrolladores y usuarios de la IA consideren cuidadosamente estos problemas éticos y de responsabilidad social y trabajen juntos para asegurar que la IA se desarrolle y utilice de manera responsable y ética.

Te proponemos como ejercicio de autocritica ver el corto Sci-Fi Short Film “Slaughterbots” | DUST sobre un futuro distópico al que podríamos llegar en el caso de no controlar el avance de la IA.

Y hablando de futuros distópicos, Isaac Asimov presentó las Tres Leyes de la Robótica en su cuento de ciencia ficción de 1942 “Runaround”. Estas leyes aparecen en varias de sus obras posteriores, incluyendo su serie de novelas de robots como “Yo, Robot” (1950). Las Tres Leyes de la Robótica son ahora un concepto bien conocido en la ciencia ficción y han tenido una influencia duradera en la forma en que se piensa en la relación entre los robots y los humanos.

Las Tres Leyes de la Robótica son una serie de reglas ficticias creadas por el escritor. Las leyes son las siguientes:

- Un robot no puede hacer daño a un ser humano o, por inacción, permitir que un ser humano sufra daño.
- Un robot debe obedecer las órdenes dadas por los seres humanos, excepto cuando dichas órdenes entren en conflicto con la primera ley.
- Un robot debe proteger su propia existencia, siempre y cuando dicha protección no entre en conflicto con la primera o la segunda ley.

Estas leyes fueron concebidas originalmente para asegurar la seguridad de los humanos que trabajan junto a robots en el futuro, en un entorno en el que los robots son cada vez más autónomos. La idea es que los robots nunca puedan causar daño a los humanos y siempre obedezcan las órdenes dadas por ellos, al mismo tiempo que se aseguran de que los robots también estén protegidos.

En cuanto a su aplicación en la IA, estas leyes podrían ser utilizadas como principios éticos para guiar el diseño y desarrollo de sistemas de IA, especialmente aquellos que interactúan directamente con seres humanos. Por ejemplo, un sistema de IA podría estar programado para priorizar la seguridad humana por encima de todo, incluso si eso significa ignorar órdenes que entren en conflicto con esta prioridad. Esto podría ser particularmente relevante en aplicaciones como la conducción autónoma

de vehículos, en la que los sistemas de IA están tomando decisiones en tiempo real que pueden afectar la seguridad de los conductores y pasajeros.

Sin embargo, es importante señalar que la implementación literal de las Tres Leyes de la Robótica no es necesariamente práctica o posible en todos los contextos de la IA, y su aplicación debe ser adaptada y considerada cuidadosamente en cada caso.

Para terminar este apartado debemos hablar de la posibilidad de diseñar una IA con opiniones o decisiones sesgadas, lo que se conoce como **discriminación algorítmica**. La IA puede aprender a través de datos históricos que contienen sesgos, como el género o la raza, y estos sesgos pueden ser perpetuados en las decisiones que la IA toma en el futuro.

Por ejemplo, si los datos de entrenamiento utilizados para desarrollar una IA son sesgados hacia un grupo particular de personas, es posible que la IA tome decisiones que discriminen injustamente contra otras personas. Esto podría manifestarse en la selección de candidatos para trabajos, la evaluación de solicitudes de crédito, o la predicción de la reincidencia de los delincuentes.

Por ejemplo, si un algoritmo de contratación se entrena con datos históricos que reflejan un sesgo de género, puede aprender a preferir a los candidatos masculinos en lugar de a los femeninos, lo que perpetúa la discriminación de género en el proceso de contratación.

Es importante señalar que los sesgos pueden no ser intencionales y pueden ser el resultado de factores históricos, culturales y sociales que influyen en los datos de entrenamiento. Sin embargo, esto no significa que debamos aceptar la discriminación algorítmica como inevitable. Por consiguiente, el sesgo no se encuentra en la IA en sí misma, sino en los datos utilizados para entrenarla. Por lo tanto, es fundamental que se tomen medidas para asegurarse de que los datos de entrenamiento sean representativos y libres de sesgos, y para implementar controles de calidad para asegurar que la IA no tome decisiones discriminatorias.

Para reducir el riesgo de discriminación algorítmica, es necesario que se preste atención a la calidad y la representatividad de los datos de entrenamiento utilizados para desarrollar la IA. Además, es importante que las IA sean diseñadas de manera transparente y que se evalúen regularmente para detectar cualquier sesgo o discriminación en su funcionamiento.

4.4 Beneficios y posibles riesgos

En resumen, la aplicación de la inteligencia artificial (IA) en todos los ámbitos de nuestra vida tiene el potencial de generar muchos beneficios, pero también puede presentar riesgos significativos. Algunos posibles beneficios de la IA incluyen:

1. Automatización de tareas: La IA puede ser utilizada para automatizar tareas que son repetitivas, aburridas o peligrosas para los humanos, lo que puede liberar tiempo para que los humanos se

- centren en tareas más creativas o estratégicas.
2. Mejoras en la toma de decisiones: La IA puede ayudar a analizar grandes cantidades de datos para tomar decisiones más informadas y precisas en una variedad de contextos, desde la medicina hasta las finanzas.
 3. Avances en la medicina: La IA puede ayudar a acelerar el proceso de descubrimiento de medicamentos, así como a identificar patrones en los datos médicos que pueden llevar a mejores diagnósticos y tratamientos.

Sin embargo, también hay algunos riesgos que deben ser considerados al aplicar la IA en todos los ámbitos de nuestra vida:

1. Sesgos y discriminación: La IA puede reflejar los prejuicios y sesgos humanos, lo que puede llevar a decisiones injustas o discriminatorias. Esto es particularmente preocupante en aplicaciones como la contratación, la evaluación del crédito y la justicia penal.
2. Pérdida de empleos: La automatización impulsada por la IA puede reemplazar a los trabajadores humanos en una variedad de industrias, lo que puede tener un impacto negativo en la economía y en la vida de los trabajadores afectados.
3. Vulnerabilidades de seguridad: La IA puede ser utilizada para desarrollar ataques cibernéticos más sofisticados, así como para identificar vulnerabilidades en sistemas de seguridad existentes.

4.5 Agentes inteligentes

En el contexto de la inteligencia artificial, un agente es un programa informático que actúa en un entorno determinado, tomando decisiones y realizando acciones para lograr un objetivo específico. Esencialmente, un agente es una entidad que percibe su entorno a través de sensores y actúa sobre él a través de efectores.

Los agentes de inteligencia artificial se basan en la idea de la autonomía, lo que significa que pueden tomar decisiones por sí mismos y actuar de manera autónoma, sin intervención humana directa. Los agentes pueden ser muy simples, como un termostato que ajusta la temperatura de una habitación en función de la temperatura ambiente, o muy complejos, como un agente de bolsa que realiza operaciones financieras en el mercado de valores.

Un agente en IA es una entidad autónoma que percibe su entorno, toma decisiones y realiza acciones para lograr un objetivo específico. Los agentes pueden ser muy simples o muy complejos, y se utilizan en una amplia variedad de aplicaciones de inteligencia artificial, desde la robótica hasta los sistemas de recomendación y las aplicaciones de procesamiento de lenguaje natural.

Russell y Norvig, en su libro “Inteligencia Artificial: Un Enfoque Moderno”, clasifican los agentes en diferentes categorías según su complejidad y características. Estas categorías son las siguientes:

1. Agentes reactivos simples: Son agentes que toman decisiones basadas únicamente en la información sensorial actual, sin mantener una representación interna del mundo. Por lo tanto, no tienen memoria de eventos pasados y no pueden planificar para el futuro.
2. Agentes reactivos basados en modelo: Son agentes que utilizan un modelo interno del mundo para tomar decisiones basadas en la información sensorial actual. Este modelo les permite tomar en cuenta el efecto a largo plazo de sus acciones y tomar decisiones más informadas.
3. Agentes basados en objetivos: Son agentes que persiguen objetivos específicos y toman decisiones basadas en la información sensorial actual y su conocimiento del mundo para avanzar hacia esos objetivos.
4. Agentes basados en utilidades: Son agentes que tienen una función de utilidad que les permite evaluar diferentes opciones y seleccionar la que maximiza la utilidad esperada.
5. Agentes basados en aprendizaje: Son agentes que pueden aprender de la experiencia y mejorar su desempeño a lo largo del tiempo. Pueden ser agentes de refuerzo, supervisados o no supervisados.

La clasificación de agentes de Russell y Norvig es útil para entender las diferentes formas en que los agentes pueden interactuar con el mundo y tomar decisiones en diferentes situaciones. Esta clasificación es una herramienta importante en la teoría y la práctica de la inteligencia artificial.

Otra clasificación de agentes en inteligencia artificial es la propuesta por Weiss, en su libro “Multiagent Systems: A Modern Approach to Distributed Artificial Intelligence”. Esta clasificación se centra en los agentes de múltiples entidades y los diferentes tipos de relaciones que pueden tener entre sí. La clasificación de Weiss incluye los siguientes tipos de agentes:

1. Agentes basados en roles: Son agentes que están diseñados para desempeñar un papel específico en un sistema multiagente y se relacionan con otros agentes en función de ese papel.
2. Agentes de conocimiento: Son agentes que tienen conocimientos especializados en un dominio específico y se relacionan con otros agentes para intercambiar información y tomar decisiones informadas.
3. Agentes de coordinación: Son agentes que se relacionan con otros agentes para coordinar actividades y asegurar que los objetivos del sistema multiagente se logren de manera efectiva.
4. Agentes de cooperación: Son agentes que se relacionan entre sí para lograr objetivos comunes que no pueden lograr individualmente.
5. Agentes de competencia: Son agentes que compiten entre sí para lograr objetivos individuales y pueden utilizar estrategias como la cooperación selectiva y la competencia directa.

La clasificación de Weiss es particularmente relevante para la inteligencia artificial distribuida, donde múltiples agentes interactúan y se relacionan entre sí para lograr objetivos en un sistema más grande. Esta clasificación ayuda a comprender cómo diferentes tipos de agentes pueden trabajar juntos y cómo las relaciones entre ellos pueden afectar el desempeño del sistema en su conjunto.

4.5.1 Agentes inteligentes simples

Los agentes inteligentes simples son programas de computadora que pueden percibir su entorno, tomar decisiones y actuar en consecuencia para lograr objetivos específicos. Estos agentes están diseñados para operar de manera autónoma en entornos determinados, y están programados para interactuar con el mundo mediante sensores y actuadores.

Un agente inteligente simple consta de cuatro componentes principales:

1. Percepción: El agente debe ser capaz de percibir su entorno a través de sensores.
2. Razonamiento: El agente debe ser capaz de razonar sobre su entorno y tomar decisiones basadas en la información que ha recopilado a través de la percepción.
3. Acción: El agente debe ser capaz de actuar en el entorno mediante actuadores.
4. Objetivos: El agente debe tener un conjunto de objetivos definidos para que pueda tomar decisiones y actuar en consecuencia para lograr esos objetivos.

Por ejemplo, un agente inteligente simple podría ser diseñado para controlar el termostato de una casa. El agente puede percibir la temperatura del aire en la habitación a través de un sensor, razonar sobre si la temperatura actual es demasiado alta o baja en relación con el objetivo de temperatura deseado, y actuar para ajustar el termostato en consecuencia.

Los agentes inteligentes simples son una forma básica de inteligencia artificial y se utilizan en una amplia variedad de aplicaciones, desde sistemas de automatización industrial hasta juegos de computadora y asistentes virtuales.

4.6 Análisis y clasificación supervisada basada en técnicas de aprendizaje automático: reconocimiento de habla; reconocimiento de imágenes; y reconocimiento de texto

El aprendizaje automático (también conocido como machine learning en inglés) es una rama de la inteligencia artificial que se centra en el desarrollo de algoritmos que permiten a un sistema informático aprender de datos sin ser programado explícitamente. En otras palabras, en lugar de escribir un programa que le indique al sistema cómo realizar una tarea específica, el sistema se entrena a sí mismo a través de ejemplos y datos para realizar esa tarea de manera más eficiente.

El aprendizaje automático se divide en tres categorías principales: aprendizaje supervisado, no supervisado y por refuerzo.

1. Aprendizaje supervisado: se utiliza para predecir una salida conocida a partir de una entrada conocida. El sistema se entrena a través de un conjunto de datos de entrenamiento que incluye ejemplos de entrada y salida, y se ajusta para que pueda hacer predicciones precisas sobre nuevas entradas.

2. Aprendizaje no supervisado: se utiliza cuando no hay salida conocida y se busca encontrar patrones y estructuras en los datos de entrada. El sistema se entrena a través de un conjunto de datos de entrada sin etiquetar y busca agrupar los datos en categorías o clústeres similares.
3. Aprendizaje por refuerzo: se utiliza para entrenar a un sistema a tomar decisiones en un entorno dinámico. El sistema se entrena a través de la retroalimentación recibida por su entorno en respuesta a sus acciones, y ajusta su comportamiento para maximizar una recompensa específica.

El aprendizaje automático se aplica en una variedad de campos, desde la clasificación de imágenes y la traducción automática, hasta el diagnóstico médico y la detección de fraudes en línea. La capacidad de los algoritmos de aprendizaje automático para analizar grandes cantidades de datos y encontrar patrones ocultos ha llevado a importantes avances en muchos campos y ha permitido a las empresas y organizaciones tomar decisiones informadas basadas en datos.

4.6.1 Reconocimiento del habla

El reconocimiento del habla es una aplicación común del aprendizaje automático en la que se utiliza un modelo de aprendizaje profundo llamado Redes Neuronales Convolucionales (CNN, por sus siglas en inglés) para convertir el habla en texto.

Primero, se recolectan y etiquetan grandes cantidades de datos de voz y texto para entrenar el modelo. Luego, el modelo de CNN aprende a reconocer patrones en la señal de voz y a asociarlos con palabras escritas, para lo cual se utiliza una técnica de aprendizaje supervisado. Durante el entrenamiento, el modelo ajusta los pesos de sus capas para maximizar la precisión de sus predicciones de texto a partir de la señal de voz.

Una vez entrenado, el modelo se puede utilizar para transcribir automáticamente el habla en tiempo real, lo que es útil para la transcripción de reuniones, la creación de subtítulos para videos o la interacción con asistentes de voz. Los modelos de reconocimiento de voz también se utilizan en la creación de herramientas de dictado de voz para personas con discapacidades que les impiden escribir con un teclado.

En resumen, el aprendizaje automático se utiliza en el reconocimiento del habla para entrenar modelos de CNN que convierten la señal de voz en texto mediante el reconocimiento de patrones en los datos de voz y la asociación de estos patrones con palabras escritas.

Algunos ejemplos de librerías y productos utilizados para el reconocimiento del habla mediante aprendizaje automático:

1. TensorFlow: Esta popular librería también incluye herramientas para el reconocimiento del habla, incluyendo modelos de redes neuronales recurrentes y convolucionales para procesamiento de señales de audio.

2. Kaldi: Es una librería de código abierto especializada en el reconocimiento del habla. Kaldi proporciona una variedad de herramientas para la extracción de características de audio y la construcción de modelos acústicos y de lenguaje.
3. PyTorch: Ofrece herramientas para el procesamiento de señales de audio y el reconocimiento del habla.
4. Google Cloud Speech-to-Text: Es un servicio de reconocimiento del habla basado en la nube, proporcionado por Google Cloud Platform. Ofrece una amplia variedad de herramientas para el reconocimiento de voz en tiempo real y la transcripción de audio a texto.
5. Amazon Transcribe: Es un servicio de reconocimiento de voz basado en la nube proporcionado por Amazon Web Services. Amazon Transcribe utiliza tecnología de aprendizaje automático para convertir el habla en texto, con soporte para varios idiomas.
6. Microsoft Azure Speech Services: Es un servicio de reconocimiento del habla basado en la nube proporcionado por Microsoft Azure. Incluye una variedad de herramientas para la transcripción de audio y la conversión de voz a texto.

4.6.2 Reconocimiento de imágenes

El reconocimiento de imágenes es otra aplicación popular del aprendizaje automático, en la que se utilizan modelos de aprendizaje profundo llamados Redes Neuronales Convolucionales (CNN) para analizar imágenes y clasificarlas en diferentes categorías.

El proceso comienza recolectando y etiquetando grandes cantidades de imágenes para entrenar el modelo de CNN. Durante el entrenamiento, el modelo aprende a reconocer patrones en las imágenes y a asociarlos con diferentes etiquetas, que se usan para clasificarlas en categorías como objetos, animales, personas, etc. Para ello, se utiliza un enfoque de aprendizaje supervisado, en el que el modelo ajusta sus pesos para minimizar el error en las predicciones de etiquetas.

Una vez que se entrena el modelo, se puede utilizar para clasificar imágenes nuevas en tiempo real. Por ejemplo, se puede utilizar para identificar objetos en imágenes, para reconocer rostros en fotografías, para detectar objetos en videos de vigilancia, para clasificar imágenes médicas en diferentes patologías, entre otras aplicaciones.

El aprendizaje automático se ha convertido en una herramienta importante en el reconocimiento de imágenes, ya que permite clasificar grandes cantidades de datos en poco tiempo y con una alta precisión. Además, los modelos de CNN se han vuelto cada vez más complejos y precisos gracias a los avances en la arquitectura y en la capacidad de procesamiento de las computadoras.

Algunos ejemplos de librerías y productos para aprendizaje automático en reconocimiento de imágenes son:

1. TensorFlow: Es una de las librerías más populares en aprendizaje automático y es utilizada por empresas como Google, Uber y Airbnb. Incluye herramientas para la construcción de modelos de reconocimiento de imágenes, y ofrece una variedad de modelos pre-entrenados, como Inception, MobileNet, entre otros.
2. Keras: Es una librería de aprendizaje automático de alto nivel escrita en Python que puede funcionar sobre TensorFlow y Theano. Keras es muy fácil de usar y cuenta con una gran cantidad de modelos pre-entrenados, así como también con una amplia gama de herramientas para el procesamiento de imágenes.
3. OpenCV: Es una librería de código abierto para el procesamiento de imágenes y el aprendizaje automático. Incluye herramientas para el procesamiento de imágenes, reconocimiento de objetos y detección de caras.
4. PyTorch: Es una librería de aprendizaje automático desarrollada por Facebook. Ofrece una variedad de herramientas para el procesamiento de imágenes y el reconocimiento de objetos.
5. Amazon Rekognition: Es un servicio de reconocimiento de imágenes ofrecido por Amazon Web Services (AWS). Ofrece una amplia gama de herramientas para el reconocimiento de objetos y personas en imágenes, así como también para la detección de texto y contenido inapropiado.
6. Google Cloud Vision: Es un servicio de reconocimiento de imágenes ofrecido por Google Cloud Platform. Ofrece una amplia gama de herramientas para el reconocimiento de objetos y personas en imágenes, así como también para la detección de texto y contenido inapropiado.

4.6.3 Reconocimiento de texto

El reconocimiento de texto es otra aplicación del aprendizaje automático que se utiliza para analizar texto en bruto y extraer información útil de él. El proceso comienza con la recolección y preprocesamiento del texto, que puede ser en forma de documentos, artículos, mensajes de redes sociales, correos electrónicos, entre otros.

Una vez que se tiene el texto, se utiliza el aprendizaje automático para analizarlo y extraer información relevante. Para ello, se utilizan diferentes técnicas, como el procesamiento del lenguaje natural (NLP), la detección de sentimientos, la clasificación de texto, entre otras.

En el procesamiento del lenguaje natural, por ejemplo, se utiliza el aprendizaje automático para analizar el texto y comprender su significado. Esto incluye tareas como la identificación de entidades, la extracción de relaciones, la clasificación de documentos, entre otros.

En la detección de sentimientos, se utiliza el aprendizaje automático para analizar el texto y determinar el tono emocional del mensaje. Esto es especialmente útil en el análisis de redes sociales, donde se puede analizar el sentimiento de los usuarios hacia una marca o producto.

En la clasificación de texto, se utiliza el aprendizaje automático para clasificar el texto en diferentes

categorías, como spam / no spam, positivo / negativo, relevante / no relevante, etc.

El reconocimiento de texto es una aplicación amplia y útil del aprendizaje automático, ya que permite analizar grandes cantidades de texto en poco tiempo y con una alta precisión. Esto puede ser utilizado en diferentes ámbitos, como en el análisis de sentimiento de redes sociales, la clasificación de documentos, la extracción de información de correos electrónicos, entre otras aplicaciones.

Como ejemplos de librerías y productos relacionados podemos poner los siguientes ejemplos:

1. NLTK (Natural Language Toolkit): es una librería en Python que se utiliza para el procesamiento del lenguaje natural y la clasificación de texto. Ofrece una amplia gama de herramientas para el preprocesamiento de texto, como tokenización, lematización, etiquetado de partes del discurso, entre otros.
2. SpaCy: es otra librería en Python que se utiliza para el procesamiento del lenguaje natural y el análisis de texto. Ofrece herramientas para el preprocesamiento de texto, así como también para la identificación de entidades, la detección de sentimientos, la clasificación de texto, entre otros.
3. TensorFlow: es una plataforma de aprendizaje automático en código abierto desarrollada por Google. Ofrece una amplia gama de herramientas para el reconocimiento de texto, incluyendo modelos preentrenados para la clasificación de texto, la extracción de entidades, la generación de texto, entre otros.
4. IBM Watson Natural Language Understanding: es un servicio en la nube ofrecido por IBM que utiliza el aprendizaje automático para el análisis de texto. Ofrece herramientas para la detección de sentimientos, la extracción de entidades, la clasificación de texto, entre otros.
5. Amazon Comprehend: es otro servicio en la nube que utiliza el aprendizaje automático para el análisis de texto. Ofrece herramientas para la detección de sentimientos, la extracción de entidades, la clasificación de texto, entre otros.

4.7 Generación de imágenes y/o música basado en técnicas de aprendizaje automático: mezcla inteligente de dos imágenes; generación de música; traducción y realidad aumentada

Para hacer generación de imágenes y música basado en técnicas de aprendizaje automático, existen varias opciones y herramientas disponibles, algunas de ellas podrían ser:

1. GANs (Generative Adversarial Networks): Las GANs son una técnica de aprendizaje automático que se utiliza para la generación de imágenes. Se trata de un enfoque que utiliza dos redes neuronales: una red generativa y una red discriminativa. La red generativa se encarga de crear nuevas imágenes a partir de una distribución aleatoria de datos de entrada, mientras que la red discriminativa intenta distinguir las imágenes generadas de las imágenes reales. Al entrenar estas dos redes juntas, se puede obtener un modelo que puede generar imágenes realistas.

2. VAEs (Variational Autoencoders): Los VAEs son otra técnica de aprendizaje automático utilizada para la generación de imágenes. Se trata de una variante de los autoencoders que se enfoca en la generación de imágenes en lugar de la reconstrucción de imágenes existentes. Al igual que con las GANs, los VAEs utilizan una distribución aleatoria de datos de entrada para generar nuevas imágenes.
3. MIDI-VAE: Es una técnica de aprendizaje automático utilizada para la generación de música. Se basa en los VAEs mencionados anteriormente, pero se enfoca en la generación de secuencias de notas MIDI. MIDI-VAE utiliza una red neuronal para aprender la distribución de los datos de entrada, y luego puede generar nuevas secuencias de notas MIDI a partir de esa distribución.
4. MuseGAN: Es otra técnica de aprendizaje automático utilizada para la generación de música. MuseGAN se basa en las GANs y utiliza una red neuronal para generar varias pistas musicales simultáneamente. MuseGAN puede generar nuevas pistas de música en varios géneros y estilos.

4.7.1 Mezcla inteligente de dos imágenes

Para realizar una mezcla inteligente a partir de dos imágenes utilizando aprendizaje automático, se puede utilizar una técnica conocida como generación de imágenes mediante redes adversarias condicionales (cGAN, por sus siglas en inglés).

Primero, se debe entrenar una red neuronal con un conjunto de datos de imágenes parecidas a las que se quieren mezclar. Luego, se proporcionan dos imágenes como entrada a la red neuronal, y esta genera una imagen resultante que es una mezcla de ambas.

Para hacer esto, se utiliza una red adversaria, que consta de dos partes: el generador y el discriminador. El generador toma las dos imágenes como entrada y genera una imagen resultante. El discriminador luego evalúa esta imagen y determina si es real o falsa.

El proceso de entrenamiento implica iterar entre el generador y el discriminador hasta que la imagen generada sea lo suficientemente realista. Una vez que la red está entrenada, se puede utilizar para hacer mezclas de imágenes a partir de dos imágenes de entrada.

Existen varias bibliotecas de aprendizaje automático que permiten entrenar y utilizar redes adversarias condicionales, como TensorFlow, PyTorch y Keras. Con estas herramientas, es posible crear mezclas inteligentes de imágenes a partir de dos imágenes de entrada.

Algunos buenos recursos para comenzar son:

1. Tutorial de PyTorch: “Pix2Pix Image Translation” (<https://github.com/junyanz/pytorch-CycleGAN-and-pix2pix/blob/master/docs/tutorials.md>). Este tutorial detalla cómo utilizar la biblioteca PyTorch para crear una red adversaria condicional para hacer una mezcla de imágenes.

2. Tutorial de TensorFlow: “Image-to-Image Translation with Conditional Adversarial Nets” (<https://phillipi.github.io/pix2pix/>). Este tutorial detalla cómo utilizar TensorFlow para entrenar una red adversaria condicional para hacer una mezcla de imágenes.
3. Tutorial de Keras: “Conditional GANs” (https://keras.io/examples/generative/conditional_gan/). Este tutorial detalla cómo utilizar la biblioteca Keras para crear una red adversaria condicional para hacer una mezcla de imágenes.

4.7.2 Generación de música

Para generar música usando aprendizaje automático, puedes utilizar una técnica llamada redes neuronales recurrentes (RNN). Las RNN son un tipo de red neuronal que se utiliza para procesar datos secuenciales, como el audio o el texto.

Aquí hay algunos pasos generales que puedes seguir para generar música usando aprendizaje automático:

- Preprocesamiento de datos: Primero, debes recopilar datos de música en un formato que la red neuronal pueda entender, como archivos MIDI o archivos de audio. Luego, debes dividir los datos en secuencias para entrenar la RNN.
- Entrenamiento de la RNN: A continuación, puedes entrenar la RNN utilizando los datos preprocesados. Durante el entrenamiento, la red neuronal aprenderá patrones en los datos y creará un modelo para generar música.
- Generación de música: Una vez que la RNN está entrenada, puedes usarla para generar nueva música. Esto se puede hacer alimentando una pequeña secuencia de notas a la RNN y dejando que genere la siguiente secuencia de notas. Puedes repetir este proceso para generar una pieza completa de música.

Hay muchas bibliotecas de aprendizaje automático que puedes usar para crear una RNN para generar música, como TensorFlow, Keras o PyTorch. También hay proyectos de código abierto disponibles en línea que puedes utilizar para empezar, como “Magenta” de Google, que proporciona herramientas y modelos para generar música utilizando aprendizaje automático.

Es importante tener en cuenta que, aunque las redes neuronales pueden generar música sorprendentemente realista, todavía hay mucho trabajo por hacer para que las generaciones sean completamente convincentes y musicales. Además, es importante tener en cuenta las cuestiones de derechos de autor y propiedad intelectual cuando se genera música utilizando datos existentes.

Existen diversas fuentes en línea que ofrecen tutoriales para generar música utilizando técnicas de aprendizaje automático. Algunas opciones podrían ser:

1. Tutorial de Google Magenta: Magenta es un proyecto de Google que utiliza IA para crear arte y música. En su sitio web, ofrecen una sección de tutoriales que cubren diferentes temas, desde el uso de redes neuronales hasta la creación de música a través de la API de Magenta. Puedes encontrar más información en el siguiente enlace: <https://magenta.tensorflow.org/>
2. Tutorial de TensorFlow: TensorFlow es una plataforma de aprendizaje automático desarrollada por Google. En su sitio web, ofrecen una sección de tutoriales que cubren diferentes temas relacionados con el aprendizaje automático, incluyendo la generación de música. Puedes encontrar más información en el siguiente enlace: <https://www.tensorflow.org/tutorials>
3. Curso de Coursera “Music and Technology: Algorithmic and Generative Music”: Este curso ofrecido por la Universidad Pompeu Fabra de Barcelona, explora diferentes técnicas para la creación de música generativa utilizando herramientas de programación y aprendizaje automático. Puedes encontrar más información en el siguiente enlace: <https://www.coursera.org/learn/algorithmic-generative-music>
4. Tutorial de Python y música: Este tutorial de Real Python utiliza el lenguaje de programación Python y diversas librerías para crear música utilizando técnicas de aprendizaje automático. Puedes encontrar más información en el siguiente enlace: <https://realpython.com/learning-to-compose-music-with-recurrent-neural-networks/>

4.7.3 Realidad aumentada

La realidad aumentada (AR) es una tecnología que permite superponer objetos virtuales en el mundo real a través de un dispositivo como un smartphone o una tableta. El aprendizaje automático puede ayudar a mejorar la precisión y la calidad de estas experiencias de AR al permitir que el software reconozca mejor y responda a los objetos y el entorno real.

Para crear experiencias de realidad aumentada utilizando aprendizaje automático, se pueden seguir los siguientes pasos:

1. Recopilar datos: Es necesario recopilar imágenes y datos de objetos del mundo real que se utilizarán en la experiencia de AR. Estos datos se utilizarán para entrenar un modelo de aprendizaje automático que pueda reconocer y rastrear objetos en el mundo real.
2. Entrenar el modelo: Utilizando una herramienta de aprendizaje automático, se puede entrenar el modelo con los datos recopilados. El modelo aprenderá a reconocer los objetos y el entorno real y a seguir su movimiento.
3. Desarrollar la experiencia de AR: Con el modelo entrenado, se puede desarrollar la experiencia de AR utilizando herramientas de programación de AR, como ARKit o ARCore. Estas herramientas permiten superponer objetos virtuales en el mundo real y rastrear su movimiento utilizando el modelo de aprendizaje automático.

4. Prueba y ajuste: Es importante probar la experiencia de AR y ajustar el modelo de aprendizaje automático si es necesario para mejorar la precisión y la calidad de la experiencia.

Existen varias herramientas y plataformas que facilitan la creación de experiencias de AR con aprendizaje automático, como Unity, Vuforia y ARToolkit. También hay tutoriales en línea y comunidades de desarrolladores que pueden proporcionar orientación y recursos para comenzar a crear experiencias de AR utilizando aprendizaje automático como por ejemplo:

1. Página de documentación de ARCore de Google: Esta página proporciona una guía detallada para desarrollar experiencias de realidad aumentada con ARCore de Google, que incluye reconocimiento de imágenes, detección de planos, seguimiento de movimiento y mucho más.
2. Página de desarrolladores de ARKit de Apple: Si estás interesado en el desarrollo de realidad aumentada en dispositivos iOS, esta página te proporciona una guía para comenzar con ARKit, que incluye reconocimiento facial, seguimiento de objetos y detección de planos.
3. Página de desarrolladores de Vuforia: Vuforia es una plataforma de realidad aumentada que permite agregar objetos 3D, videos, imágenes y otros elementos a la realidad aumentada. La página de desarrolladores de Vuforia ofrece una amplia documentación y tutoriales para aprender a utilizar su tecnología.
4. Página de desarrolladores de Unity: Unity es una popular plataforma de desarrollo de videojuegos y también se puede utilizar para crear experiencias de realidad aumentada. La página de desarrolladores de Unity ofrece una guía detallada y tutoriales sobre cómo crear experiencias de realidad aumentada con su motor de juego.

4.8 Conclusiones

La inteligencia artificial es una herramienta tecnológica crucial y prometedora para el futuro de la humanidad. La IA tiene el potencial de transformar muchos aspectos de nuestra vida diaria, desde la forma en que trabajamos y nos comunicamos hasta la forma en que nos relacionamos con el mundo.

Hoy día (abril 2023), es posible encontrar soluciones online para infinidad de áreas, como por ejemplo:

- Video: Creación y edición de vídeo 10 veces más rápido:
 1. Supercreator.ai: <https://www.supercreator.ai/>
 2. Tavus: <https://www.tavus.io/>
 3. Windsor.io: <https://www.windsor.io/>
- Imágenes: Creación de arte e imágenes a partir de texto:
 1. Stokimg.ai: <https://stockimg.ai/>

2. Midjourney: <https://www.midjourney.com>
 3. Dreamer: <https://deepdreamgenerator.com>
- Texto: Generación de texto
 1. ChatGPT: <https://chat.openai.com>
 2. Notion: <https://www.notion.so/product/ai>
 3. Jasper: <https://www.jasper.ai/>
 - Investigación: Creación de contenidos o resumir artículos en segundos.
 1. Bearly: <https://bearly.ai/>
 2. Scholarcy: <https://www.scholarcy.com/>
 - Diseño: Diseños, logotipos, UI en minutos.
 1. Looka: <https://looka.com/>
 2. Gaileo: <https://www.usegalileo.ai/>
 3. Uizard: <https://uizard.io/>
 - Presentaciones: Crea presentaciones 10 veces más rápido.
 1. Slidesai: <https://www.slidesai.io/es>
 2. Otterai: <https://otter.ai/>
 3. Murfai: <https://murf.ai/>
 - Audio: Audio, música y sonidos en minutos.
 1. WhisperMemos: <https://whispermemos.com/>
 2. Soundful: <https://soundful.com/>
 3. Steno: <https://steno.ai/>
 - Productividad: Procesado de documentos, asistente de video o escritura:
 1. Nanonets: <https://nanonets.com/>
 2. Lumen5: <https://lumen5.com/>
 3. Jenni: <https://jenni.ai/>

“AI will not replace you. A person using AI will.”