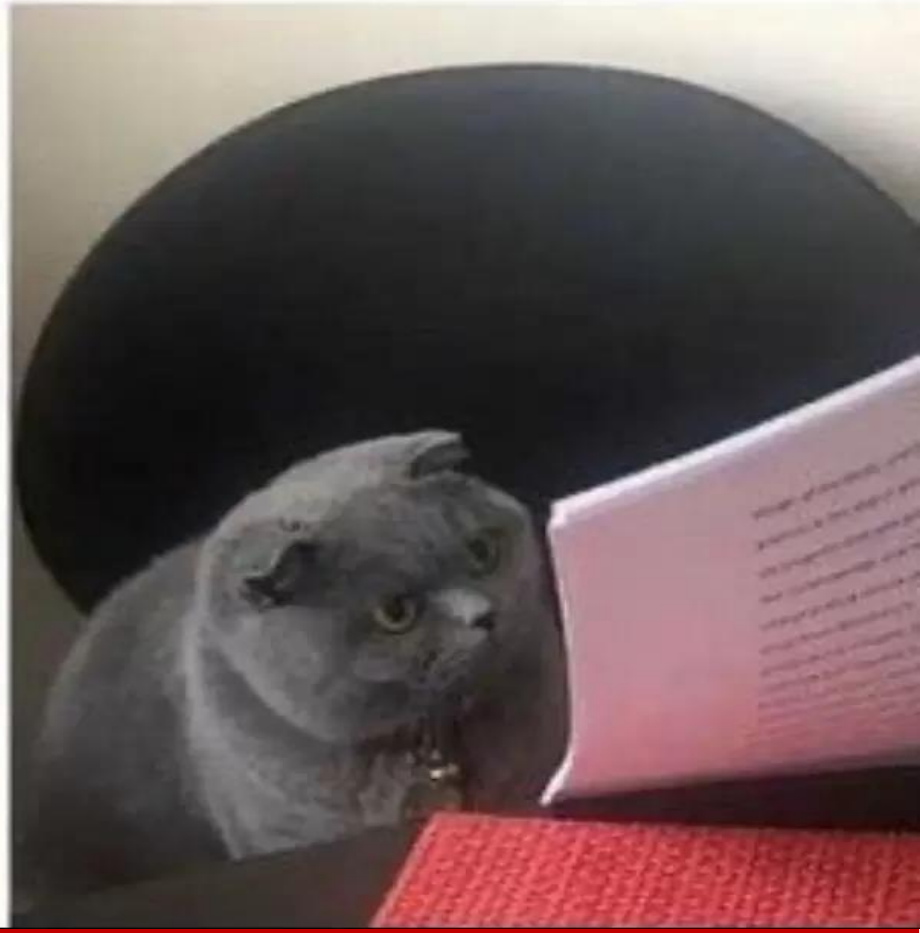
- ¿Cuál es la manera más segura para guardar tus contraseñas?

- Un gestor de contraseñas.

- ¿Y por qué pusiste “guardarlas en el bloc de notas”?

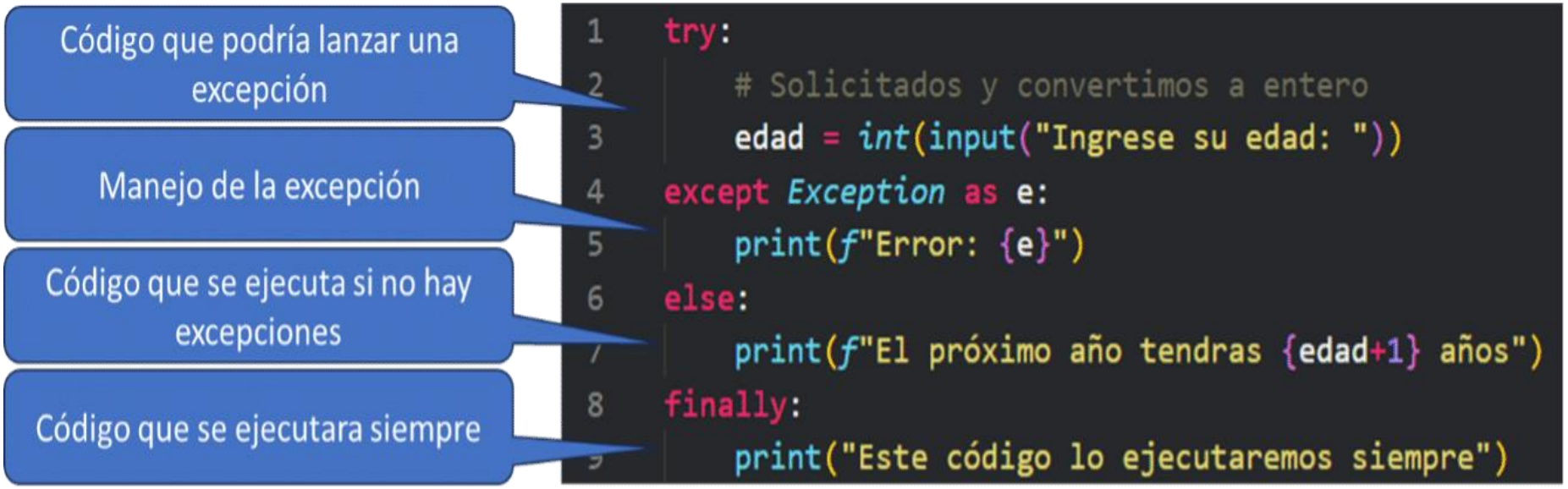


MANEJO DE ERRORES

Los errores, fallas y excepciones son situaciones en las que el programa no puede continuar su ejecución normal debido a problemas en el código. Estos pueden ocurrir por diversos motivos, como errores de sintaxis, problemas lógicos o situaciones excepcionales durante la ejecución.

Existen excepciones, que son situaciones anormales que pueden ocurrir durante la ejecución de un programa, como divisiones entre cero, acceso a índices inválidos en listas, etc.

Python proporciona un sistema de manejo de excepciones para capturar y manejar estas situaciones, evitando que el programa se detenga abruptamente.




```
Ingrese su edad: treinta
Error: invalid literal for int() with base 10: 'treinta'
Este código lo ejecutaremos siempre
```

```
Ingrese su edad: 30
El próximo año tendras 31 años
Este código lo ejecutaremos siempre
```

Fuente: Recursos Inacap

Ejemplo excepciones:

TypeError : Operación o función de tipo inapropiado.

•ZeroDivisionError : Dividir por cero.

•OverflowError : Cálculo excede el límite para un tipo de dato numérico.

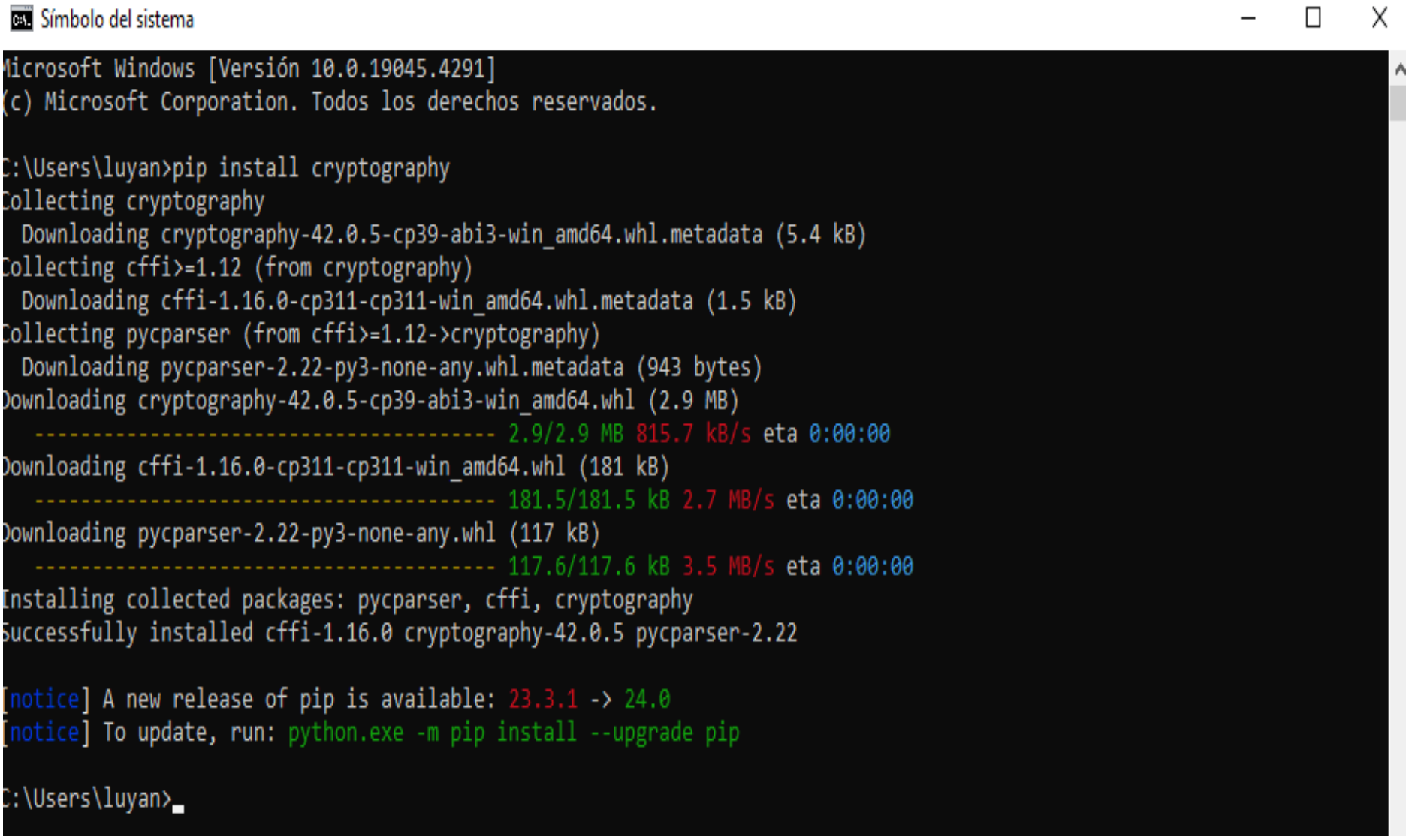
•IndexError : Acceder a una secuencia con un índice que no existe.

•KeyError : Acceder a un diccionario con una clave que no existe.

•FileNotFoundError : Acceder a un fichero que no existe.

•ImportError : Importación de un módulo que no existe.

Encriptación


Símbolo del sistema
Microsoft Windows [Versión 10.0.19045.4291]
(c) Microsoft Corporation. Todos los derechos reservados.
C:\Users\luyan>pip install cryptography
Collecting cryptography
Downloading cryptography-42.0.5-cp39-abi3-win_amd64.whl.metadata (5.4 kB)
Collecting cffi>=1.12 (from cryptography)
Downloading cffi-1.16.0-cp311-cp311-win_amd64.whl.metadata (1.5 kB)
Collecting pycparser (from cffi>=1.12->cryptography)
Downloading pycparser-2.22-py3-none-any.whl.metadata (943 bytes)
Downloading cryptography-42.0.5-cp39-abi3-win_amd64.whl (2.9 MB)
---------- 2.9/2.9 MB 815.7 kB/s eta 0:00:00
Downloading cffi-1.16.0-cp311-cp311-win_amd64.whl (181 kB)
---------- 181.5/181.5 kB 2.7 MB/s eta 0:00:00
Downloading pycparser-2.22-py3-none-any.whl (117 kB)
---------- 117.6/117.6 kB 3.5 MB/s eta 0:00:00
Installing collected packages: pycparser, cffi, cryptography
Successfully installed cffi-1.16.0 cryptography-42.0.5 pycparser-2.22
[notice] A new release of pip is available: 23.3.1 -> 24.0
[notice] To update, run: python.exe -m pip install --upgrade pip
C:\Users\luyan>

```
from cryptography.fernet import Fernet

#tipo de encriptado con algoritmo tipo AES
#método de cifrado simétrico, podremos usar esa misma clave,
#tanto para encriptar como para desencriptar

#El cifrado AES emplea un tamaño de clave variable de 128, 192 o 256 bits
#con un tamaño e bloque fijo de 128 bits.

#Los ataques como la fuerza bruta no pueden romper el cifrado AES

clave=Fernet.generate_key()
print ("clave generada:",clave)

mensaje="quiero encriptar esto".encode()
f=Fernet(clave)
encriptado=f.encrypt(mensaje)
print("Mensaje encriptado:",encriptado)

desencriptado=f.decrypt(encriptado)
print("Mensaje Desdencriptado:",desencriptado)
```

```python
import hashlib

salida = hashlib.sha256(b"El Libro De Python").hexdigest()
print("salida inicial:",salida)

print("salida 256:",hashlib.sha256(b"programacion segura").hexdigest())
print("salida 224:",hashlib.sha224(b"programacion segura").hexdigest())
print("salida 512:",hashlib.sha512(b"programacion segura").hexdigest())
```

```
salida inicial: f7b5c532807800c540f5e4476ea1f6d968294fc34c90f2e7e64435ea3c054ce
6
salida 256: 7292226db72b3c4be97004b91f298c963161351393e407869d660aef5e481e25
salida 224: ce3dc026e94c6b87ed15b7d2178cecc1450caf3998e35022dc55d3b0
salida 512: dcec6a96bea68592be67a3fac8146d82df0084898503c09dbf4bce250ac50f2a6fc
0d2da37855f86daec2ccb0fb4de9b4ce6452f5cdeb50d0b28d730fa0a5ef6
```

Crear un algoritmo que contenga en un diccionario el usuario y la contraseña De todos los perfiles con acceso al sistema.

Debe Validar el acceso indicando si el usuario y la contraseña existen en el diccionario para acceder a un algoritmo que permita ingresar un número y calcular el factorial de este.

Debe proteger los datos de acceso utilizando cifrado AES y HASH. El mismo ejercicio para ambos métodos.