



Tecnológico  
de Monterrey

Uso de álgebras modernas para seguridad y criptografía  
(Gpo 601)

**Profesores:** Dr. Luis Miguel Méndez Díaz  
y Dr. Daniel Otero Fadul



# Protección de Datos **CRPTOGRÁFÍA** **Y SEGURIDAD**

Kevin Antonio González Díaz (A01338316)  
Luis Maximiliano López Ramírez (A00833321)  
Adrian Pineda Sanchez (A00834710)  
Ana Paola Almeida Pérez (A00833937)  
Hendrik Steven Arias López (A0138065)

# RESUMEN

En este proyecto, desarrollamos un sistema de seguridad integral que se enfoca en proteger la información sensible de los migrantes.

Implementamos un esquema criptográfico en Python utilizando el cifrado Fernet para cifrar y descifrar archivos de manera segura.

Además, creamos una aplicación en Power Apps para recolectar información en bases de datos SQL y un dashboard en Power BI para mostrar estadísticas importantes del negocio.





# INTRODUCCIÓN

01

En la era digital actual, la implementación de medidas de ciberseguridad y criptografía es esencial para proteger la integridad de los datos sensibles de individuos y organizaciones.

02

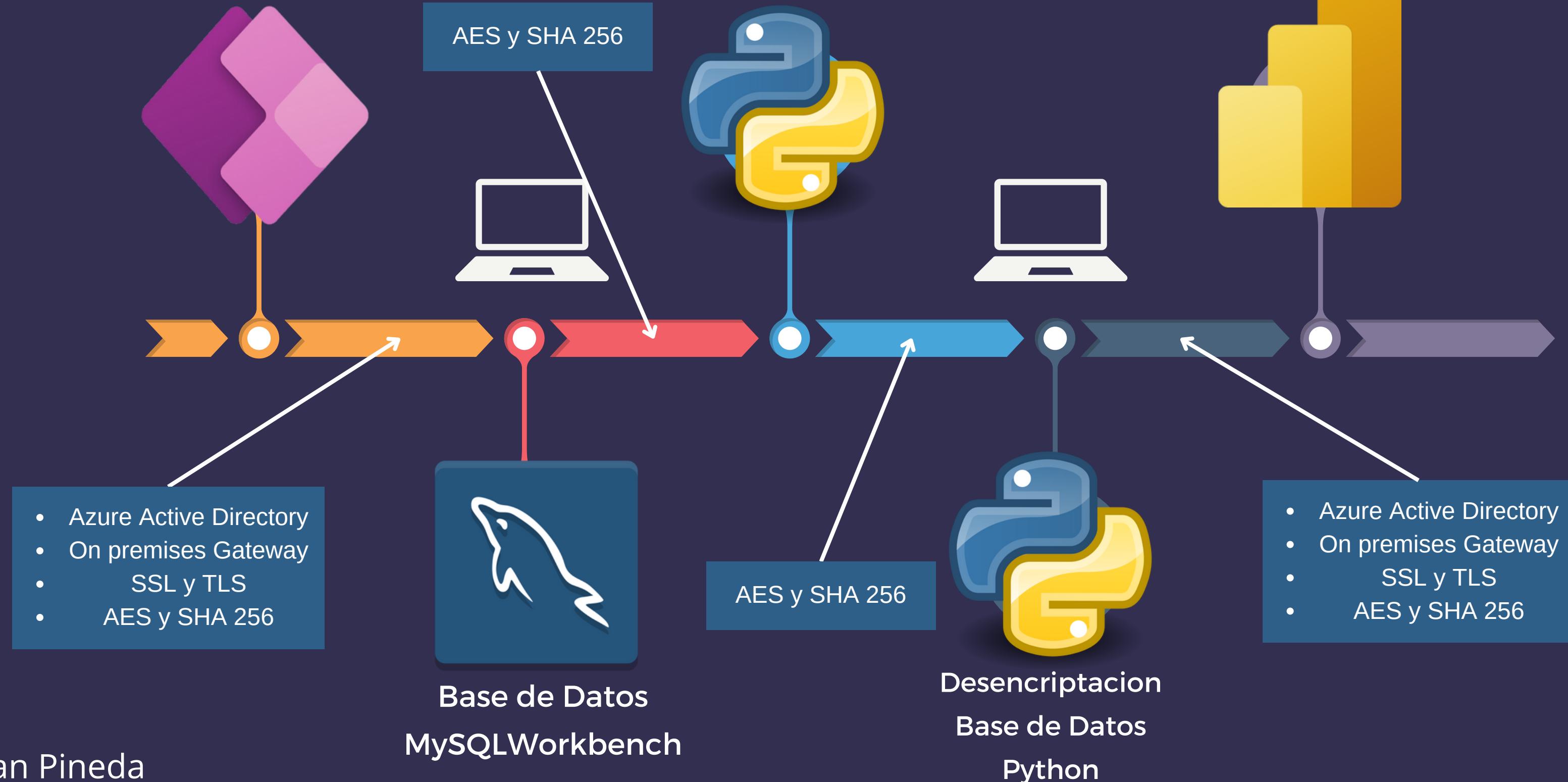
En México, la protección de datos personales está regulada por la Ley de Protección de Datos Personales en Posesión de Particulares, que promueve la privacidad y el derecho a la autodeterminación informativa.

03

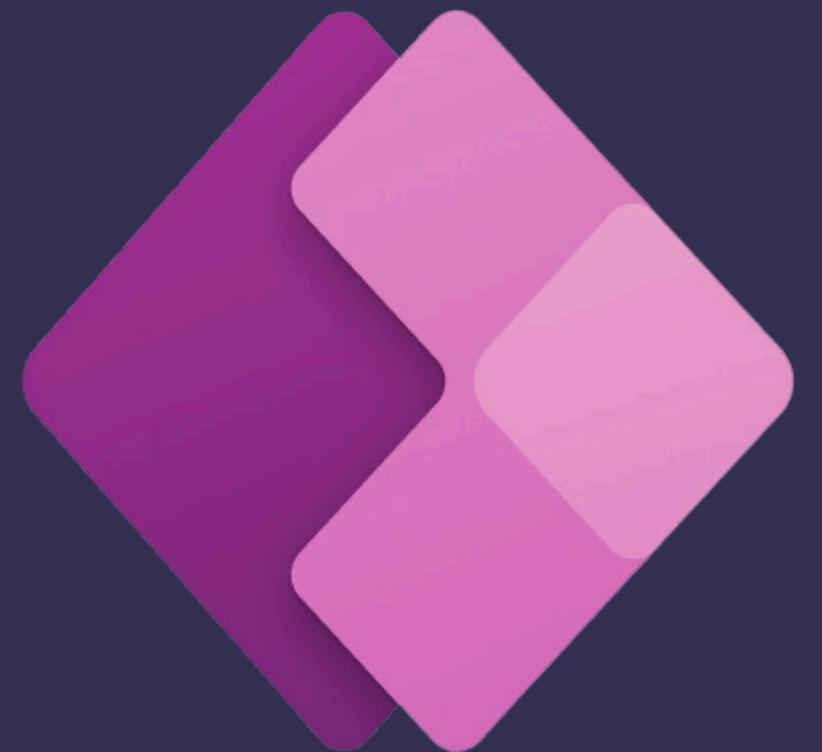
La organización Casa Monarca en Monterrey, busca implementar criptografía de clave pública para la gestión de contraseñas y reforzar el cumplimiento legal en protección de datos,

# Diagrama de Flujo

Recolección Datos  
Power apps



# POWER APPS Y BASE DE DATOS





# Power Apps

Menu Inicio      2024-06-12 23:33:22

Adrian Pineda Sanchez  
adrian.pineda@ext.cemex.com

**¡Bienvenido!**

**Nuevo Registro**

**Face ID**

**CASA MONARCA**  
AYUDA HUMANITARIA AL MIGRANTE, A.B.P.

X DatosGeneradosCriptoIn... ✓

Fecha de atencion

Adulto, NNA, NNAnA

Nombre completo

Numero Telefonico o de contacto

Sexo

Fecha de nacimiento

31/12/2001    00    00 : 00

Edad

Llenado del formulario

Base de Datos Local en MySQL  
mediante un Gateway con SSL/TLS

Datos

Buscar

+ Agregar datos

DatosGeneradosCriptoInventa... SharePoint - adrian.pineda@ext.cemex.c...

basedatosmigrantes.datosgen... MySQL - BaseDatosMigrantes local...

Nombre del conjunto de datos  
default

Conexión  
MySQL

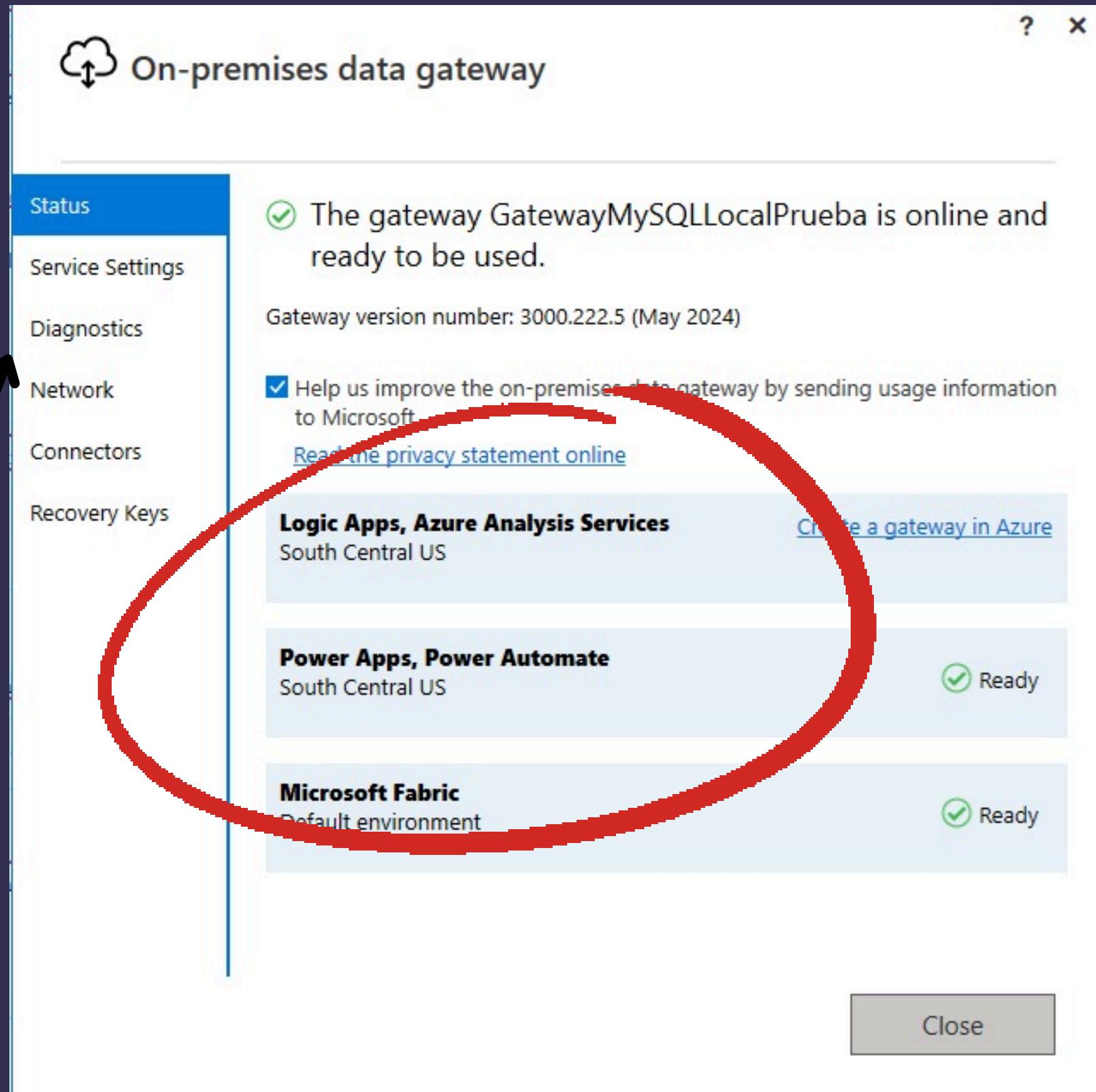
Premium

Detalles de la conexión  
BaseDatosMigrantes localhost



# Power Apps Gateway

Se configura el Gateway desde local a traves de un .exe introduciendo las credenciales de Power Apps



Debe configurarse el acceso del Gateway a las instancias locales de MySQL

El status del Gateways esta listo y funcionando para todos estos servicios incluyendo Power Apps

# MySQL Workbench

Connect to MySQL Server

Please enter password for the following service:

Service: Mysql@localhost:3306  
User: root  
Password:

Save password in vault

OK Cancel

Usuario root y el servicio local son los unicos autorizados (pueden agregarse mas desde root)

pruebabasedatoslocal SQL File 1\* Administration - Server Status

1 • SELECT \* FROM DatosGeneradosCriptoInventados1;

2 Ver Base de Datos

Result Grid Filter Rows: Export: Wrap Cell Content:

Fecha_de_atencion	Adulto_NNA_NNAnA	Nombre_completo	Numero_telefonico_de_contacto	Sexo	Fecha_de_nacimiento	Edad	Pais_de_origen	Departamento_Estado	Estado_Civil	Tipo_poblacion	Documento_identidad	Hijos
2023-01-15	Niño no acompañado	Juan Perez	555-1234	Hombre	2005-08-12	17	México	CDMX	Soltero	Niño	INE123456	No
2023-01-16	Niña acompañada	Maria Gonzalez	555-5678	Mujer	2008-03-25	15	Honduras	Tegucigalpa	Soltera	Niña	INE654321	Sí
2023-01-17	Adolescente acompañado	Luis Lopez	555-8765	Hombre	2003-05-30	20	El Salvador	San Salvador	Soltero	Adolescente	INE987654	No
2023-01-18	Adulto	Ana Martinez	555-4321	Mujer	1985-11-11	38	Guatemala	Guatemala City	Casada	Adulto	INE456789	Sí

# MySQL Workbench Status

Ubicacion Local

The screenshot shows the MySQL Workbench Status window. On the left, there's a sidebar with sections for 'Ubicacion Local' (Local Location), 'Server Directories', 'Replica', 'Authentication', and 'SSL'. A red circle highlights the 'Server Directories' section, which lists paths for Base Directory, Data Directory, Disk Space in Data Dir, Plugins Directory, Tmp Directory, Error Log, General Log, and Slow Query Log. Another red circle highlights the 'Authentication' section, showing SHA256 Password Private Key and SHA256 Password Public Key. A third red circle highlights the 'SSL' section, showing SSL CA, SSL CA Path, SSL Cert, and SSL Cipher. In the center, a large blue box contains the text 'Numero de Conexiones Realizadas' (Number of Connections Made). To the right, there's a summary of server status with metrics like CPU Load (2%), Connections (5), Traffic (5.05 KB/s), Key Efficiency (0.0%), Selects per Second (0), InnoDB Buffer Usage (12.3%), InnoDB Reads per Second (0), and InnoDB Writes per Second (0). A red circle highlights the 'Connections' bar chart in the summary.

Connection Name  
**Local instance MySQL80**

Host: Adrian  
Socket: MySQL  
Port: 3306  
Version: 8.0.37 (MySQL Community Server - GPL)  
Compiled For: Win64 (x86\_64)  
Configuration File: C:\ProgramData\MySQL\MySQL Server 8.0\my.ini  
Running Since: Fri May 24 05:22:07 2024 (19 days 18:12)

Refresh

**Server Directories**

Base Directory: C:\Program Files\MySQL\MySQL Server 8.0\  
Data Directory: C:\ProgramData\MySQL\MySQL Server 8.0\Data\  
Disk Space in Data Dir: Could not determine  
Plugins Directory: C:\Program Files\MySQL\MySQL Server 8.0\lib\plugin\  
Tmp Directory: C:\Windows\SERVICE~1\NETWOR~1\AppData\Local\Temp  
Error Log: On .\ADRIAN.err  
General Log: Off  
Slow Query Log: On ADRIAN-slow.log

**Replica**

: this server is not a replica in a replication setup

**Authentication**

SHA256 Password Private Key: private\_key.pem  
SHA256 Password Public Key: public\_key.pem

**SSL**

SSL CA: ca.pem  
SSL CA Path: n/a  
SSL Cert: server-cert.pem  
SSL Cipher: n/a

Numero de Conexiones Realizadas

Server Status: Running  
CPU/Load: 2%  
Connections: 5

Traffic: 5.05 KB/s  
Key Efficiency: 0.0%

Selects per Second: 0  
InnoDB Buffer Usage: 12.3%

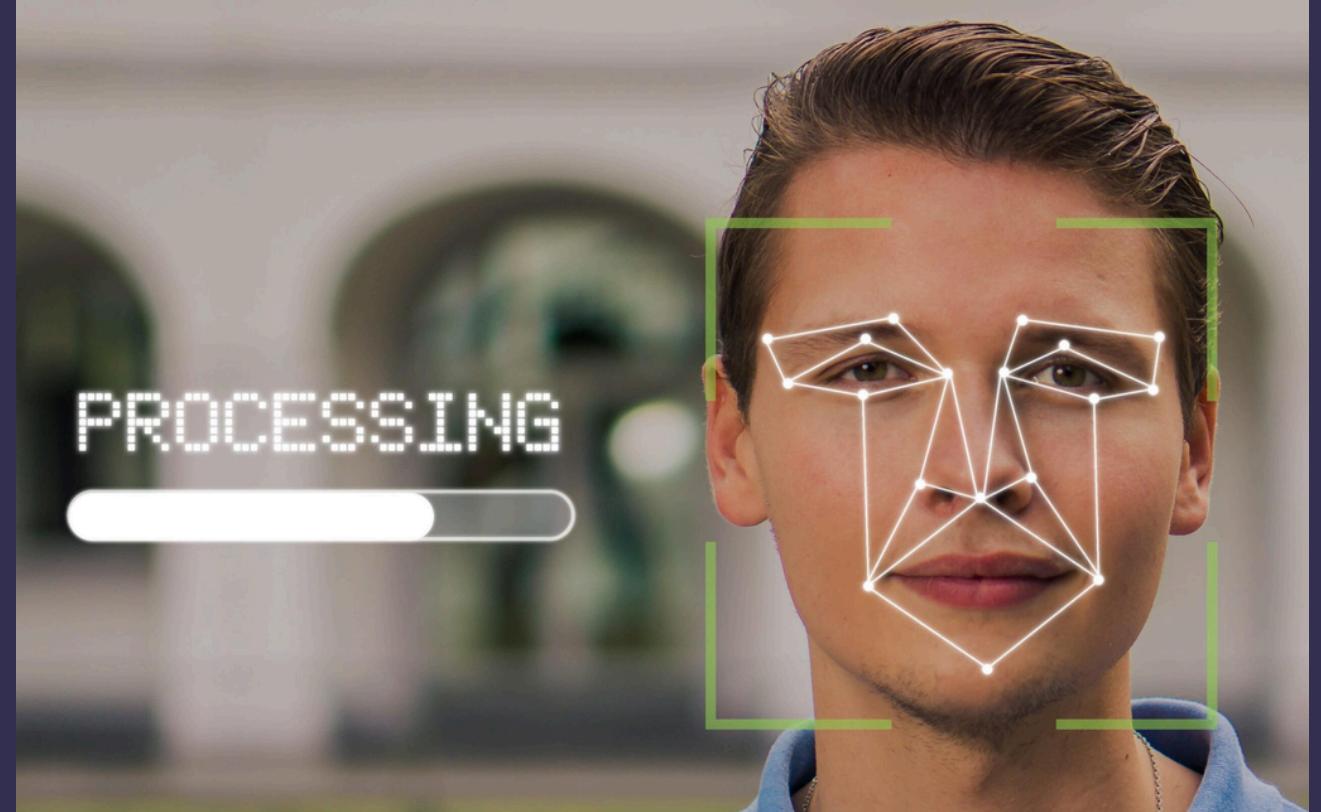
InnoDB Reads per Second: 0  
InnoDB Writes per Second: 0

# FACE ID



# LOBE AI

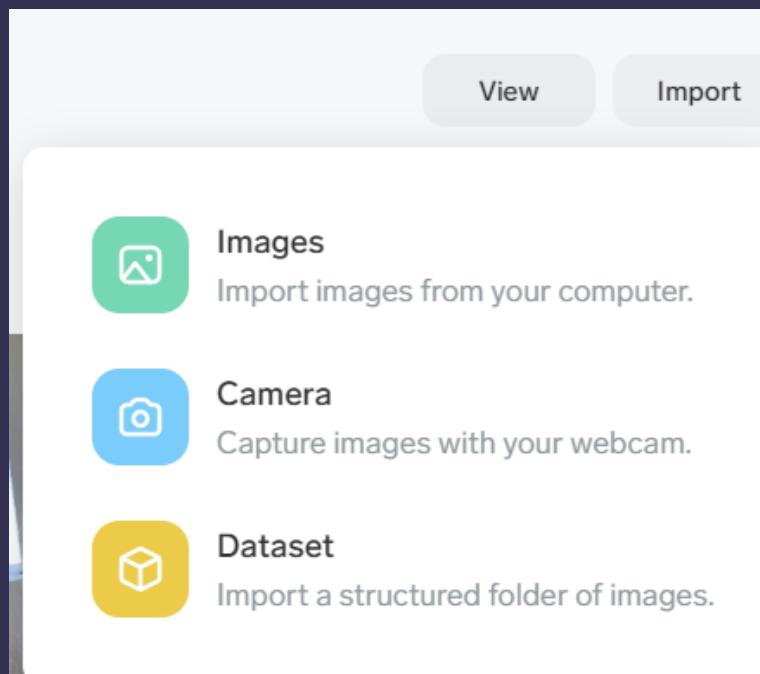
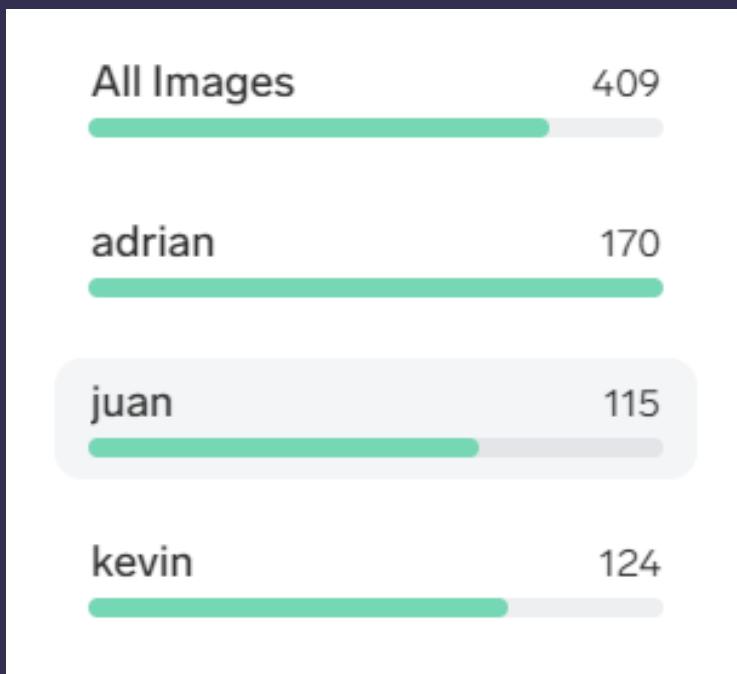
Lobe AI es una herramienta de Microsoft diseñada para facilitar la creación, el entrenamiento y la implementación de modelos de aprendizaje automático (Machine Learning) mediante CNN.



## Ventajas:

- Creacion de Modelos de IA gratuitos
- Versatilidad y Ergonomía
- Compatibilidad con IOS, Android, Web y Power Platform
- Robustez en seguridad y presicion
- Local y exportable

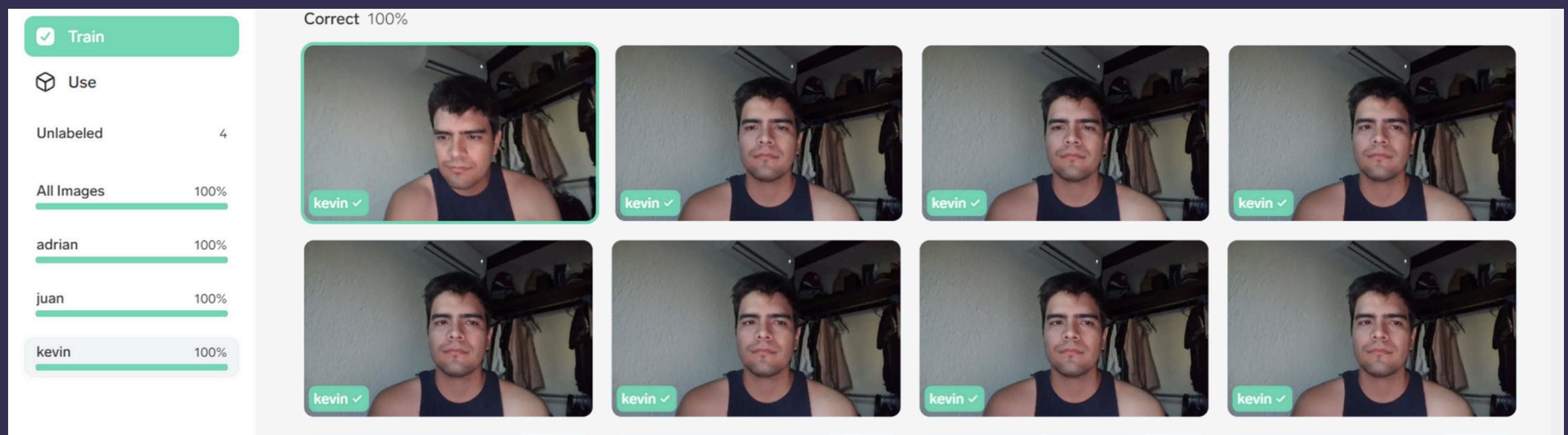
# CAPTURA



En menos de 10-15 segundos podemos tener una muestra suficiente para la captura del perfil mediante una toma flash de imágenes, con su label

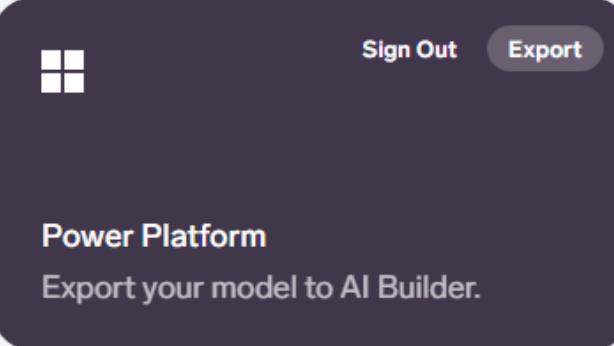
# ENTRENAMIENTO

CNN realiza un entrenamiento iterativo en base a cada iteración nueva, detectando fallas y errores del modelo de predicción



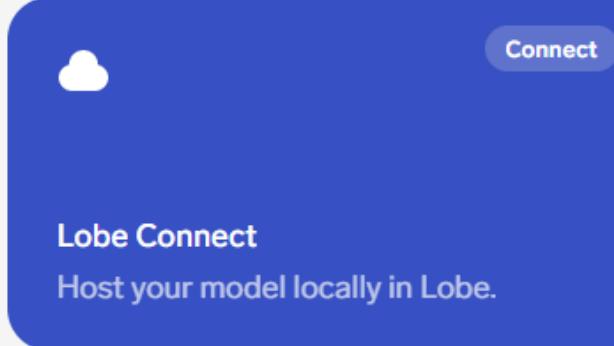
# EXPORTACIONES

**Integrations**



Sign Out Export

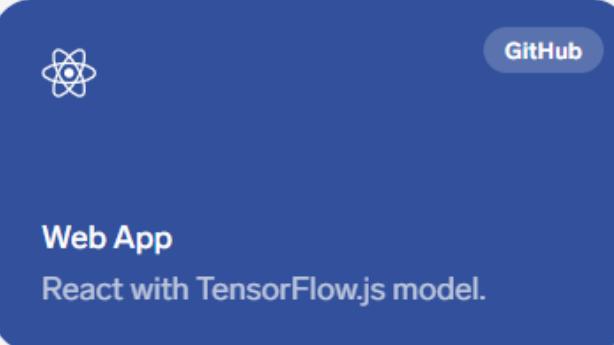
**Power Platform**  
Export your model to AI Builder.



Connect

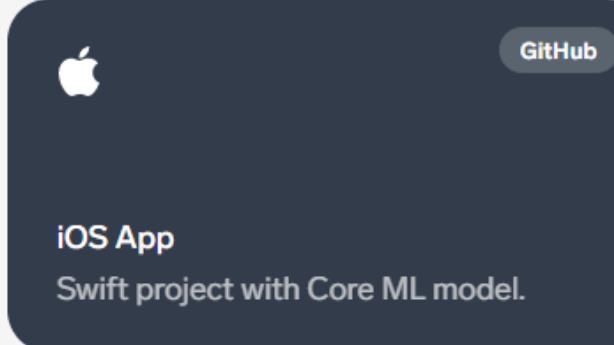
**Lobe Connect**  
Host your model locally in Lobe.

**Starter Projects**



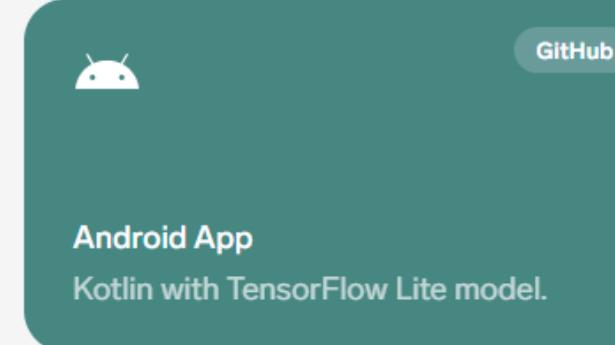
 GitHub

**Web App**  
React with TensorFlow.js model.



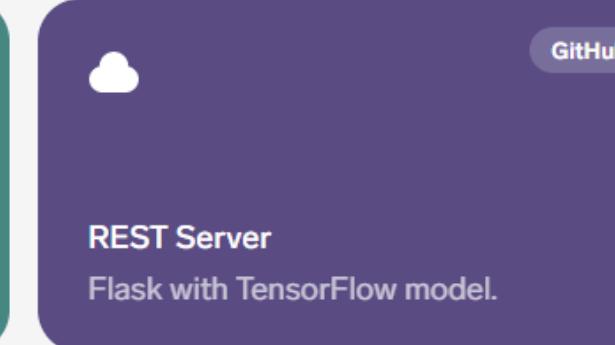
 GitHub

**iOS App**  
Swift project with Core ML model.



 GitHub

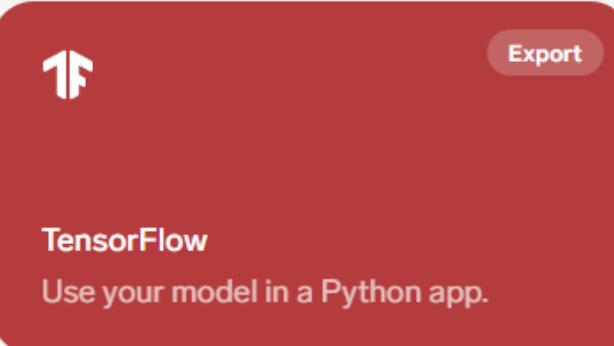
**Android App**  
Kotlin with TensorFlow Lite model.



 GitHub

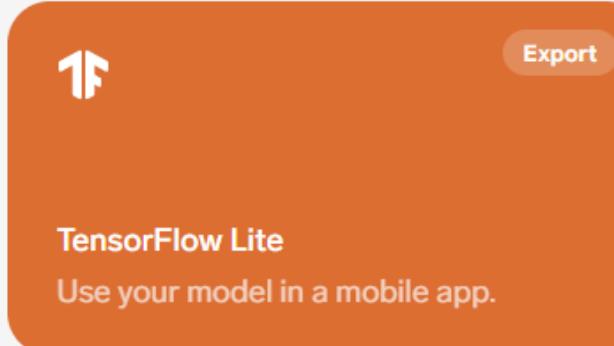
**REST Server**  
Flask with TensorFlow model.

**Model Files**



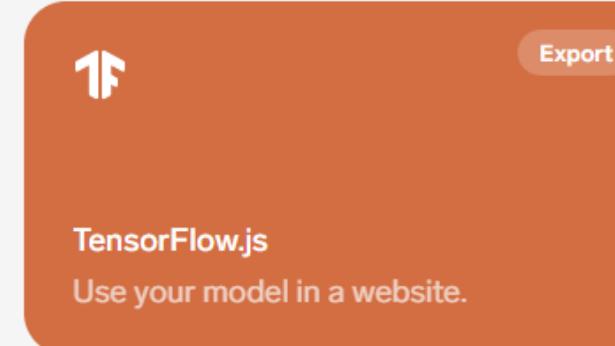
 Export

**TensorFlow**  
Use your model in a Python app.



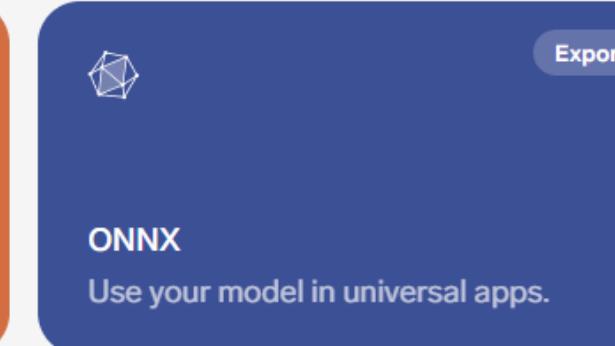
 Export

**TensorFlow Lite**  
Use your model in a mobile app.



 Export

**TensorFlow.js**  
Use your model in a website.



 Export

**ONNX**  
Use your model in universal apps.

# APLICACIÓN LOCAL



# MÉTODO FERNET

## Cifrado con Fernet

Se implementó el uso del algoritmo Fernet, parte del módulo `cryptography` de Python, para implementar cifrado simétrico.

El cifrado simétrico es crucial para asegurar la confidencialidad e integridad de los datos utilizando una clave secreta compartida.

Objetivo: Proteger archivos dentro de una carpeta mediante técnicas de cifrado avanzadas.

## Características del Algoritmo Fernet

Fernet es una especificación de cifrado simétrico autenticado que utiliza:

- AES en modo CBC para cifrado.
- HMAC con SHA256 para garantizar la integridad de los datos.

Proporciona una comprobación de integridad robusta, asegurando que los datos cifrados no hayan sido alterados.

# MÉTODO HASH

## SHA256

SHA256 Es un algoritmo HASH seguro que posee 256 bits.

El cifrado Hash es de vital importancia para la protección de claves. ya que es un método que puede transformar caracteres a una clave única donde no se puede sacar inversa. haciendo que dentro del sistema

El método HASH sigue siendo vulnerable a ataques de fuerza bruta o ingeniería social.



# GENERACIÓN DE CLAVES

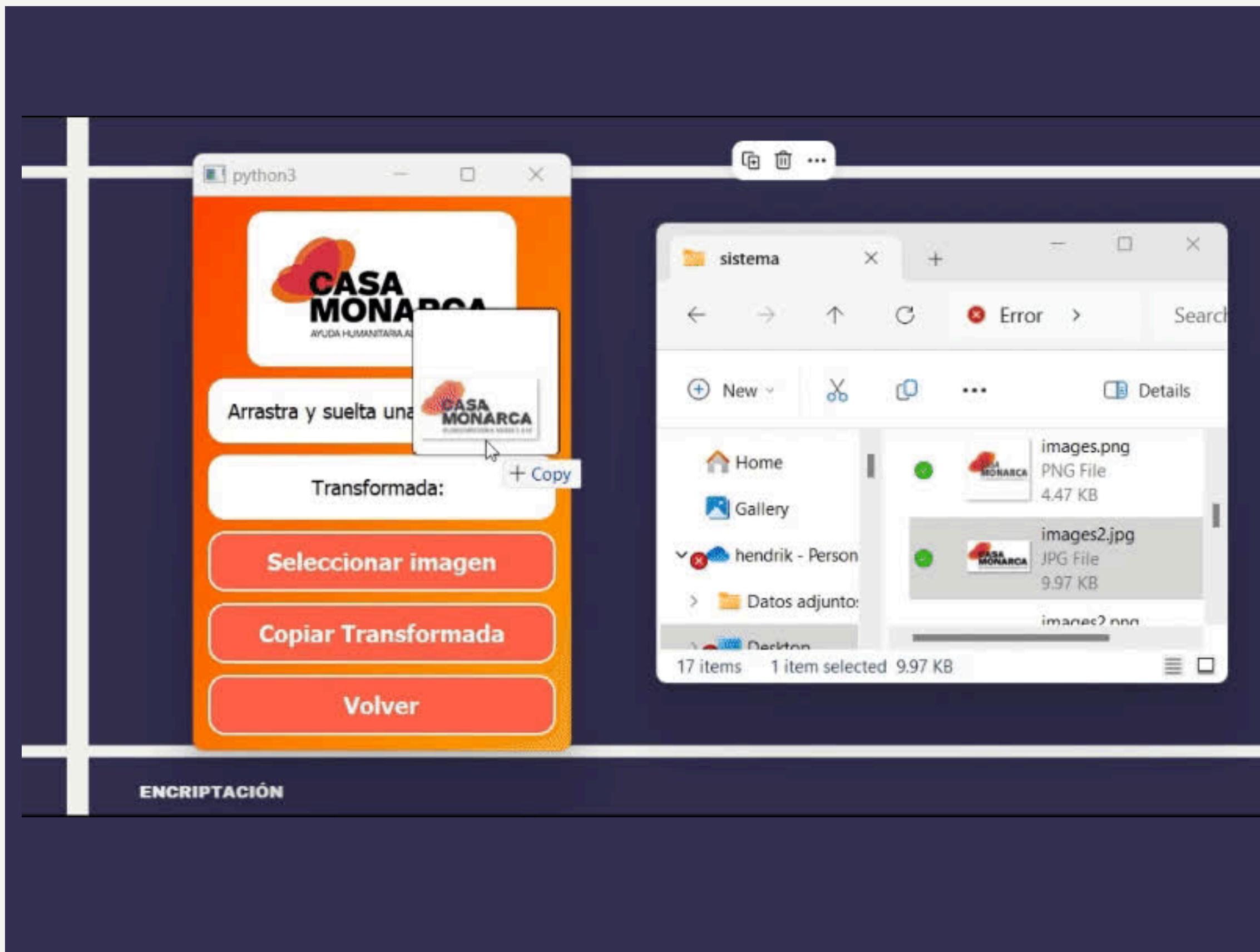


- Utilización de la función `generate_key` para crear una clave segura a partir de una contraseña proporcionada por el usuario.
- Empleo de PBKDF2HMAC con SHA256, que es un método recomendado para derivar claves de contraseñas robustas.
- Importancia de la sal (salt) en la generación de claves:
  - Protege contra ataques de diccionario y rainbow tables.
  - Se genera de manera aleatoria para cada sesión, aumentando la seguridad.

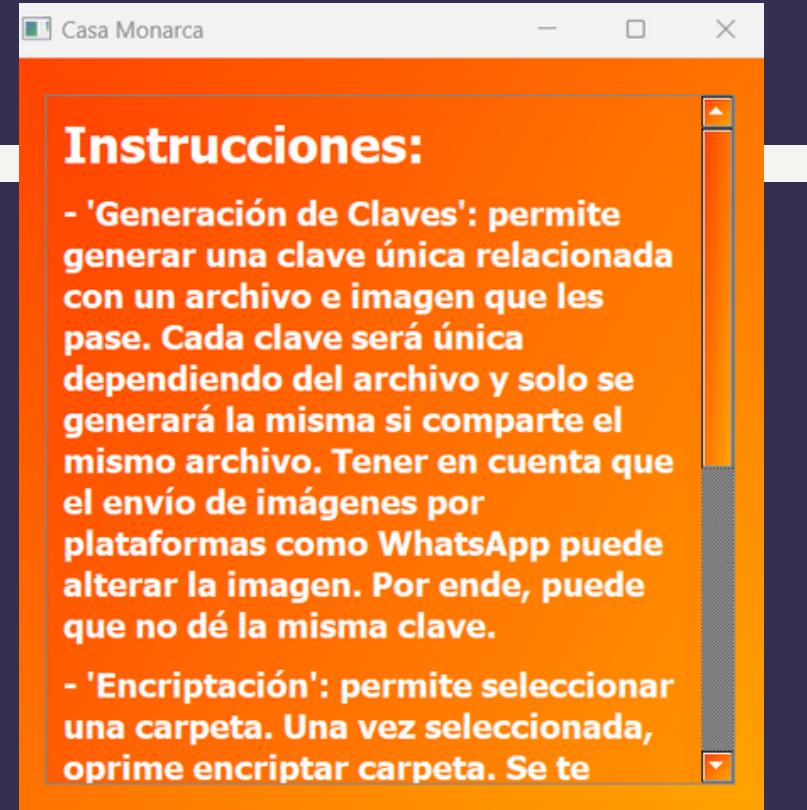
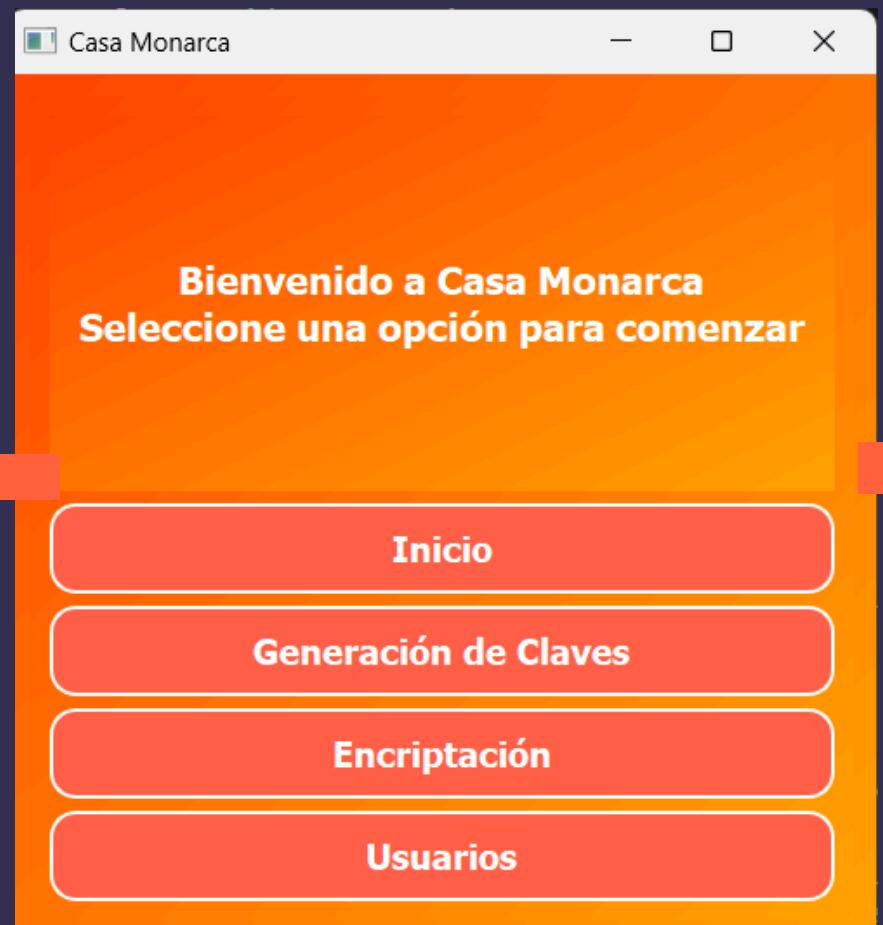
# Metodología

- 1 Importar módulos  
Se importan los módulos necesarios: `os`, `base64`, `Fernet` de `cryptography` y componentes de tkinter.
- 2 Función `generate\_key`  
Genera una clave de cifrado a partir de una contraseña y una sal opcional.
- 3 Función  
`process\_directory`  
Cifra o descifra archivos dentro de un directorio dado.
- 4 Clase `App`  
Define la interfaz gráfica de la aplicación.
- 5 Método `open\_folder`  
Abre un cuadro de diálogo para seleccionar una carpeta.
- 6 Método  
`process\_folder`  
Procesa la carpeta seleccionada (cifra o descifra) con una contraseña.
- 7 Inicialización de la aplicación  
Crea y muestra la ventana principal de la interfaz de usuario.

# GENERACIÓN DE CLAVES

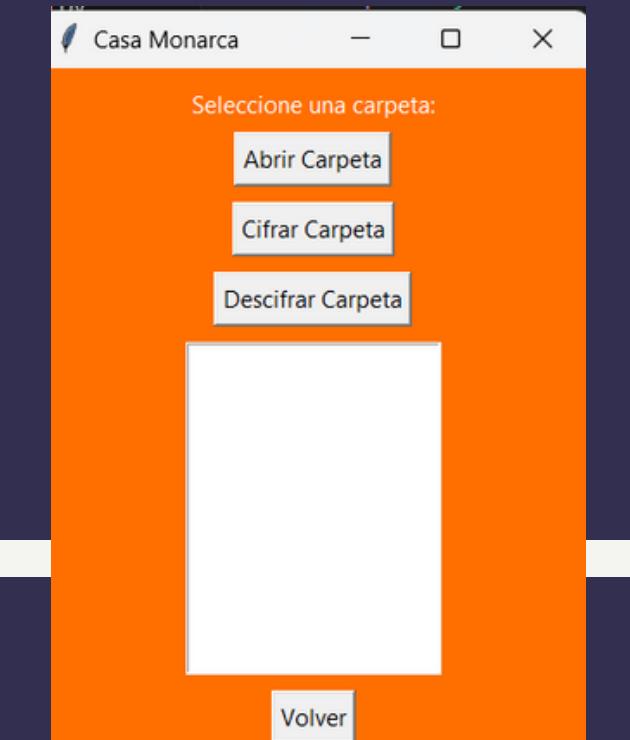


# APP Local



INICIO

ENCRYPTACIÓN

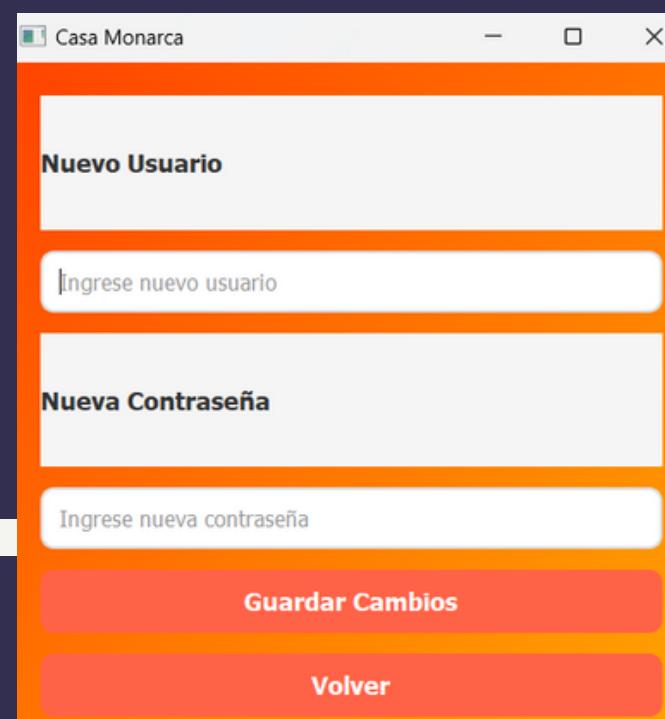


Volver



GENERACIÓN DE CLAVES

USUARIO



Volver

HENDRIK STEVEN  
ARIAS LÓPEZ

# IMPLEMENTACIÓN

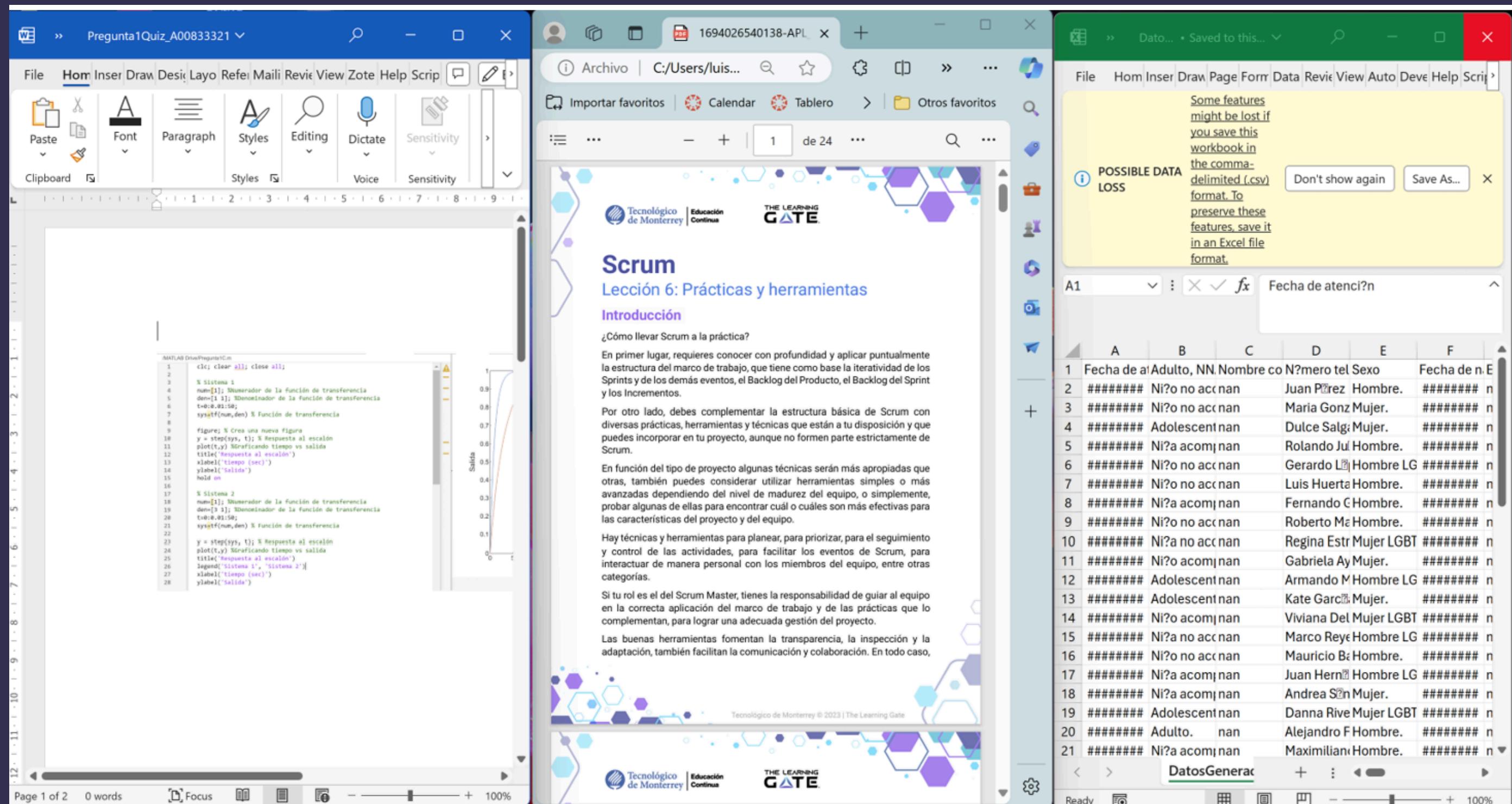
## PRUEBA ENcriptación

The screenshot shows a Windows desktop environment. In the foreground, there is a standard file explorer window titled "Prueba" containing various files and folders. One folder, "DatosGeneradosCriptoInventados", is highlighted. In the background, two Microsoft Office applications are open: a "Casa..." application (likely OneNote) and an Excel spreadsheet titled "DatosGeneradosCriptoInventados". The Excel window displays a table with columns A through F. Column A contains dates, column B contains gender status, column C contains names, column D contains ages, column E contains sex, and column F contains dates. A warning message box from Excel is visible, stating "POSSIBLE DATA LOSS" and providing instructions to save the file as an Excel file to preserve features.

This screenshot shows the same desktop environment after attempting to open the encrypted file. The file explorer window now shows an error message: "No podemos abrir este archivo" (We can't open this file) with the sub-message "Se ha producido un error." (An error has occurred). In the background, the Excel application still displays the warning about possible data loss. A separate Microsoft Word application window is also open, showing an error message: "Word experienced an error trying to open the file. Try these suggestions." It lists three troubleshooting steps: "Check the file permissions for the document or drive.", "Make sure there is sufficient free memory and disk space.", and "Open the file with the Text Recovery converter." The file path shown in the Word window is "C:\...\Pregunta1Quiz\_A00833321.docx".

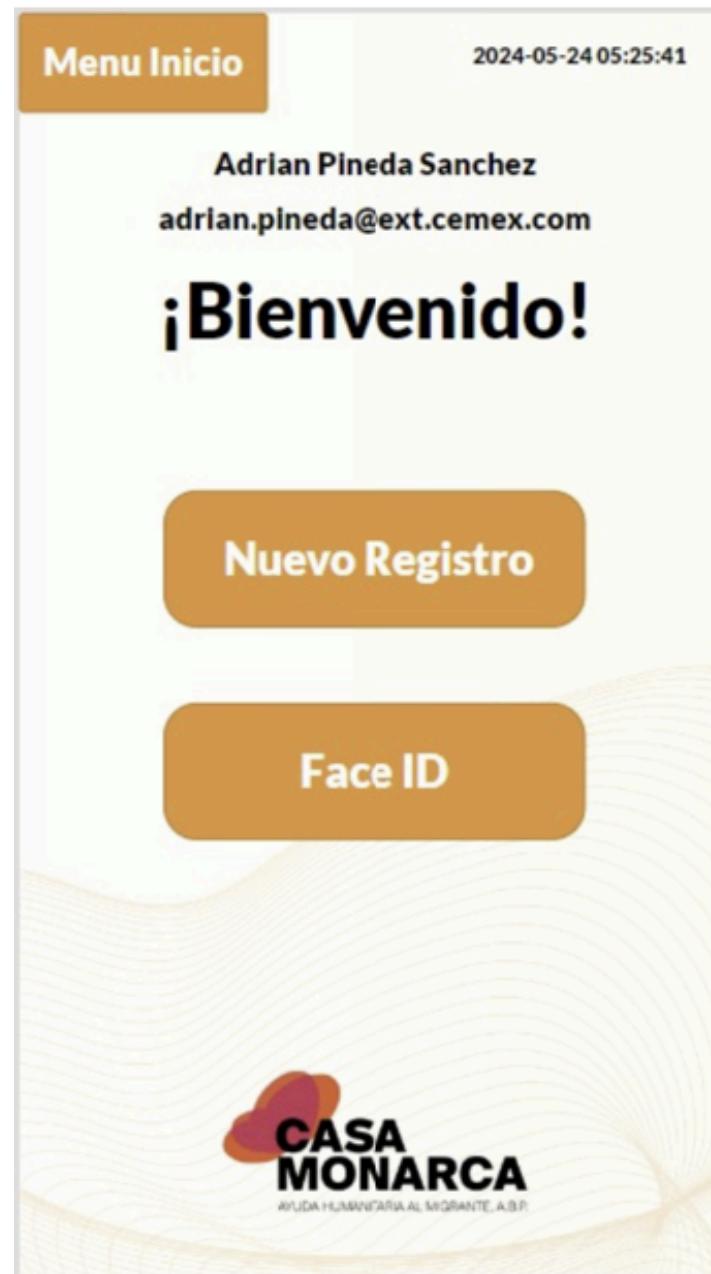
# IMPLEMENTACIÓN

## PRUEBA DESCRIPCION



# RESULTADOS

## Power Apps



## Power BI



# CONCLUSIONES

Hicimos una implementación que no solo garantiza la protección de datos sensibles de los migrantes, sino que también ofrece una solución económica y práctica para Casa Monarca.

La solución de cifrado de datos es segura, eficiente y de fácil implementación, permitiendo a la organización proteger la información sensible de los migrantes de manera económica y práctica.

La integración de Power Apps y Power BI mejora la capacidad de Casa Monarca para servir a la comunidad permitiendo un análisis detallado de sus datos



# RECOMENDACIONES

- Continuar investigando y actualizando los métodos de cifrado para asegurar que sigan siendo seguros frente a nuevas amenazas.
- Implementar pruebas automatizadas para validar continuamente la seguridad y la eficiencia de la solución.
- Capacitar al personal de Casa Monarca en el uso de las nuevas herramientas y en mejores prácticas de seguridad informática.
- Mantener una colaboración estrecha con socios formadores y expertos en seguridad para recibir retroalimentación y mejorar la solución.

