Instituto Tecnológico y de Estudios Superiores de Monterrey
Escuela de Ingeniería y Ciencias

Ingeniería en Ciencias de Datos y Matemáticas

Uso de álgebras modernas para seguridad y criptografía (MA2006B.601)

Implementación segura de esquemas de protección de datos personales con criptografía de clave pública

Secure implementation of personal data protection schemes with public key cryptography

Equipo 3:

Adrian Pineda Sánchez (A00834710)

Luis Maximiliano López Ramírez (A00833321)

Kevin Antonio González Díaz (A01338316)

Ana Paola Almeida Pérez (A00833937)

Hendrik Steven Arias López (A01378065)

Docentes:

Dr. Luis Miguel Méndez Díaz y Dr. Daniel Otero Fadul

Monterrey, Nuevo León, México. 13 de marzo 2024

Índice

1. Resumen

En este trabajo se examina la creciente relevancia de la ciberseguridad y la criptografía en el entorno contemporáneo. Además, se subraya la necesidad de comprender los conceptos criptográficos modernos y de explorar medidas de protección eficaces. Se sugiere la adopción de criptografía de clave pública en Casa Monarca como un importante medio para asegurar la confidencialidad de la información sensible. Se detallan opciones de implementación y se resaltan medidas adicionales recomendadas, tales como el control de acceso y la auditoría de actividades. Se enfatiza la importancia de un enfoque holístico para fortalecer el cumplimiento legal y contribuir al desarrollo sostenible.

2. Abstract

This paper examines the growing relevance of cybersecurity and cryptography in the contemporary environment. Furthermore, it emphasizes the need to understand modern cryptographic concepts and explore effective protective measures. The adoption of public key cryptography at Casa Monarca is suggested as a significant means to ensure the confidentiality of sensitive information. Implementation options are detailed, and additional recommended measures, such as access control and activity auditing, are highlighted. The importance of a holistic approach to strengthen legal compliance and contribute to sustainable development is emphasized.

3. Introducción

En la era digital actual, la implementación de medidas de ciberseguridad y criptografía es crucial para individuos y organizaciones, con el fin de proteger la integridad de los datos sensibles. A pesar de los esfuerzos por asegurar los algoritmos criptográficos, la evolución tecnológica y nuevas técnicas analíticas han incrementado su vulnerabilidad. Es imperativo revisar y mejorar continuamente estos algoritmos para asegurar la seguridad de los datos intercambiados [1].

La ciberseguridad y la criptografía se apoyan en álgebras modernas para comprender su

funcionamiento y, mediante análisis de literatura, identificar áreas susceptibles de mejora. Esta revisión busca asegurar tanto la eficiencia matemática como la aplicabilidad operativa de los algoritmos, contribuyendo a la industrialización inclusiva y sostenible, y a la protección de infraestructuras y tecnologías innovadoras.

En México, la protección de datos personales se rige por la Ley de Protección de Datos Personales en Posesión de Particulares, que establece normativas para un tratamiento legítimo, controlado e informado de los datos, garantizando así la privacidad y el derecho a la autodeterminación informativa [1].

La organización Casa Monarca en Monterrey, que apoya a migrantes, busca reforzar su cumplimiento legal en protección de datos y asegurar la integridad de su información. El principal objetivo es implementar criptografía de clave pública para la gestión de contraseñas, lo cual permitirá fortalecer la seguridad de la información sensible y cumplir con los estándares legales y recursos disponibles adaptados a sus necesidades específicas [2].

4. Método

4.1. Uso de recursos disponibles

Considerando las condiciones iniciales que observamos en torno al presupuesto de la organización socioformadora para la implementación de esquemas criptográficos para el salvaguardar los datos, debemos considerar únicamente herramientas de software abierto y gratuito, de preferencia intuitivas de usar, o en su defecto, software que requiera una preparación y conocimiento ligero a moderado para capacitar a los miembros encargados de dicha tarea pertenecientes a la organización socioformadora, y en términos del hardware, software asi como bases de datos locales y recursos en la nube tenemos:

Recursos de Hardware y Software disponible

4.1.1. Servidores de Base de Datos

Instalación de MySQL Workbench

MySQL Workbench es una herramienta de desarrollo SQL y cliente de base de datos que permite a los usuarios interactuar con varios sistemas de gestión de bases de datos (DBMS) como MySQL, PostgreSQL, Oracle, SQL Server, entre otros. Esta herramienta facilita la ejecución de scripts SQL, la edición de datos y la exploración de estructuras de bases de datos.[28]

Figura 1: Pantalla Inicial MySQL Workbench

Configuración

Instalación:

- **Descarga:** Se puede descargar desde el sitio oficial de SQL Workbench.
- **Requisitos:** Asegurarse de tener los drivers JDBC correspondientes a los DBMS con los que se va a trabajar.

Configuración de la conexión:

- **Apertura:** Abrir SQL Workbench y seleccionar "File» Çonnect Window".

- **Detalles de conexión:** Proporcionar los siguientes detalles:
  - **Driver:** Seleccionar el driver JDBC del DBMS correspondiente.
  - **URL del servidor:** Introducir la URL del servidor de la base de datos. En caso de no tener un servidor externo, la misma computadora puede actuar como servidor utilizando `localhost` o `127.0.0.1` como URL.
  - **Credenciales:** Ingresar el nombre de usuario y la contraseña para acceder a la base de datos.
- **Guardar y probar:** Guardar la configuración y probar la conexión para asegurarse de que está funcionando correctamente.

Ventajas en Criptografía y Seguridad

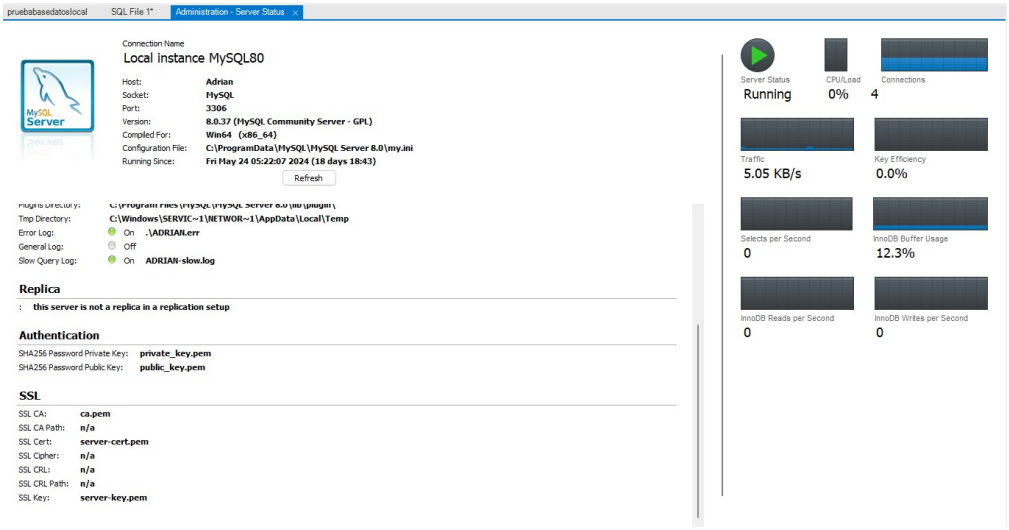

Figura 2: Administration Status Server MySQL Workbench

Cifrado de Datos:

- Utiliza protocolos TLS/SSL para cifrar la comunicación entre SQL Workbench y el servidor de base de datos, protegiendo los datos en tránsito.

Autenticación Segura:

- Soporta autenticación robusta mediante credenciales de usuario, incluyendo métodos de autenticación como SHA256 para asegurar las contraseñas de administrador.

Control de Acceso:

- Proporciona control granular sobre el acceso a la base de datos, asegurando que solo usuarios autorizados puedan interactuar con los datos.

Gestión de Certificados:

- Facilita la configuración y gestión de certificados SSL para validar la identidad de los servidores y asegurar las conexiones.

Auditoría y Monitoreo:

- Mantiene registros detallados de las conexiones y actividades para auditorías de seguridad y cumplimiento.

Creación de Tablas y Datos Sintéticos

En el entorno de SQL Workbench, se pueden crear las tablas SQL necesarias para los formularios de Casa Monarca y también instaurar datos sintéticos. Esto permite visualizar y probar la aplicación en Power Apps, asegurando que todos los componentes funcionen correctamente antes de utilizar datos reales.

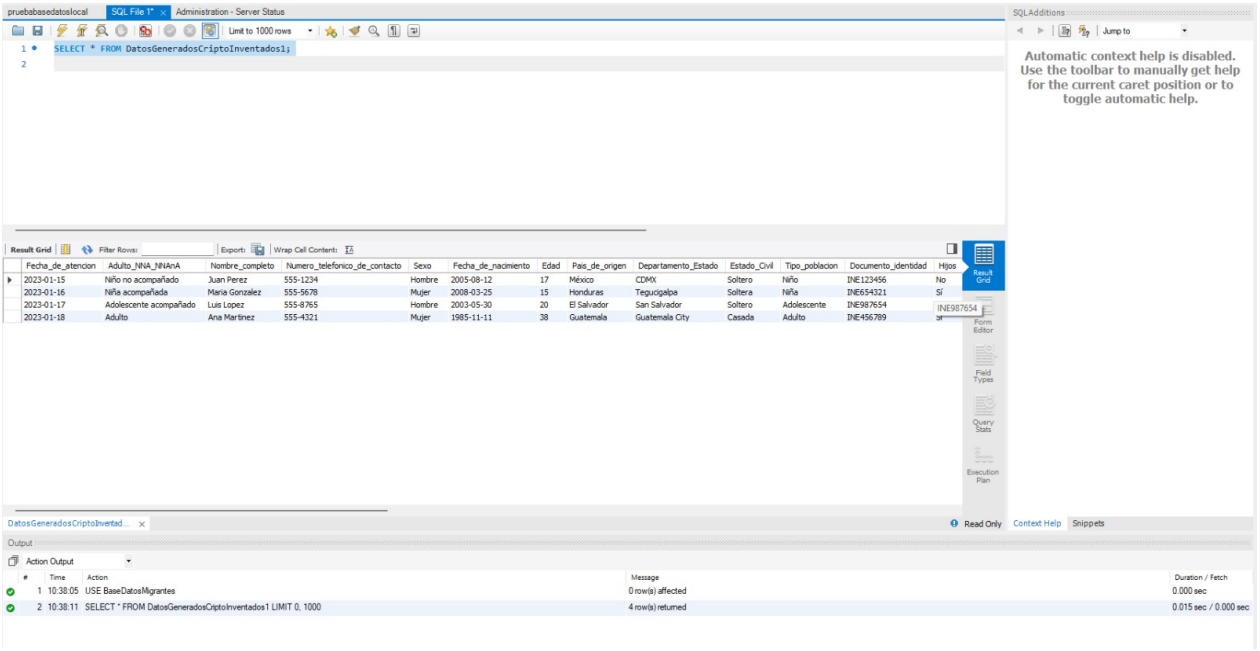

Figura 3: Tabla obtenida de la base de datos en MySQL Workbench `BaseDeDatosMigrantes`

4.2. Implementación del proyecto

4.2.1. Aplicación Local

El código desarrollado implementa un esquema criptográfico para cifrar y descifrar archivos dentro de una carpeta utilizando criptografía simétrica con el algoritmo **Fernet** del módulo **cryptography** en Python. Este algoritmo garantiza la confidencialidad e integridad de los datos mediante el uso de una clave secreta.

El esquema criptográfico utiliza el algoritmo **Fernet**, que es parte de la biblioteca **cryptography**. Fernet es una especificación que proporciona cifrado simétrico autenticado. Utiliza AES en modo CBC con una clave de 128 bits y HMAC con SHA256 para garantizar la integridad de los datos cifrados.

La generación de claves se realiza mediante el uso de la función `generate_key` que emplea **PBKDF2HMAC** con SHA256 para derivar una clave de una contraseña proporcionada por el usuario. Se utiliza una sal (salt) para proteger contra ataques de diccionario y rainbow tables.

El proceso de cifrado y descifrado se implementa en la función `process_directory`, que

recorre todos los archivos en un directorio y aplica el cifrado o descifrado con la clave generada.

Para verificar la correcta implementación, se pueden utilizar vectores de prueba estándar proporcionados por la documentación de **cryptography** y **NIST** para asegurar que los algoritmos funcionan como se espera.

Por ejemplo, para PBKDF2HMAC:

- **Password**: `"password"`
- **Salt**: `"salt"`
- **Iterations**: 1
- **Output**: SHA256 hash correspondiente

Para Fernet:

- **Key**: `b'mysecretpassword'`
- **Plaintext**: `b'secret data'`
- **Ciphertext**: Resultado esperado del cifrado.

Estos vectores se pueden encontrar en la documentación oficial de NIST.

El esquema utilizado es de **clave simétrica**, específicamente el cifrado Fernet. Este método es apropiado para aplicaciones donde la misma clave se utiliza tanto para cifrar como para descifrar la información. Fernet garantiza que el mensaje cifrado no ha sido manipulado, ya que incluye una comprobación de integridad.

Para proteger la información sensible en memoria:

1. La clave generada y utilizada debe ser manejada cuidadosamente, asegurando que no permanezca en memoria más tiempo del necesario. Se pueden utilizar bibliotecas como **keyring** para almacenar claves en un almacén seguro del sistema operativo.

2. Inmediatamente después de usar datos sensibles (como contraseñas y claves), se deben sobrescribir esos datos en memoria para evitar fugas.

Los datos cifrados se almacenan directamente en los mismos archivos de entrada, sobrescribiendo los datos originales. Esto es una medida para garantizar que los datos no queden expuestos.

Aunque en este caso se utiliza criptografía simétrica, la administración de claves es crítica. Las claves deben ser generadas, almacenadas y distribuidas de manera segura. Se recomienda el uso de almacenes de claves seguros y el intercambio de claves mediante canales seguros para evitar la interceptación.

El montaje del prototipo debe incluir la implementación de la solución en un entorno de prueba controlado para generar un escenario de *proof of concept*.

Otro punto importante del código local es la parte de hash.py, la cual transforma una imagen y devuelve una clave de 20 dígitos con mayúsculas, minúsculas y símbolos. Esto emula el comportamiento de un administrador de claves.

El funcionamiento de este sistema es sencillo. Se basa en un código donde transformamos una imagen en una función hash, por lo cual, tiene las características del hash, que es una función que no tiene inversa. Usando la librería de hashlib [25], podemos transformar una imagen o prácticamente cualquier documento en una función hash. A este resultado podemos hacerle pequeñas alteraciones que generan las mayúsculas y simbología. Esto nos devuelve una clave de 20 dígitos que es lo suficientemente segura para poder durar 6 meses o más sin necesidad de cambiarse.

4.2.2. Power Apps

La aplicación de Power Apps para Casa Monarca está diseñada para registrar datos de migrantes de manera eficiente y segura. La pantalla de inicio de la aplicación muestra opciones para realizar un nuevo registro y utilizar la identificación facial (Face ID) para acceder a los datos. La interfaz es intuitiva y fácil de usar, con botones claramente etiquetados y una apariencia moderna.[27]

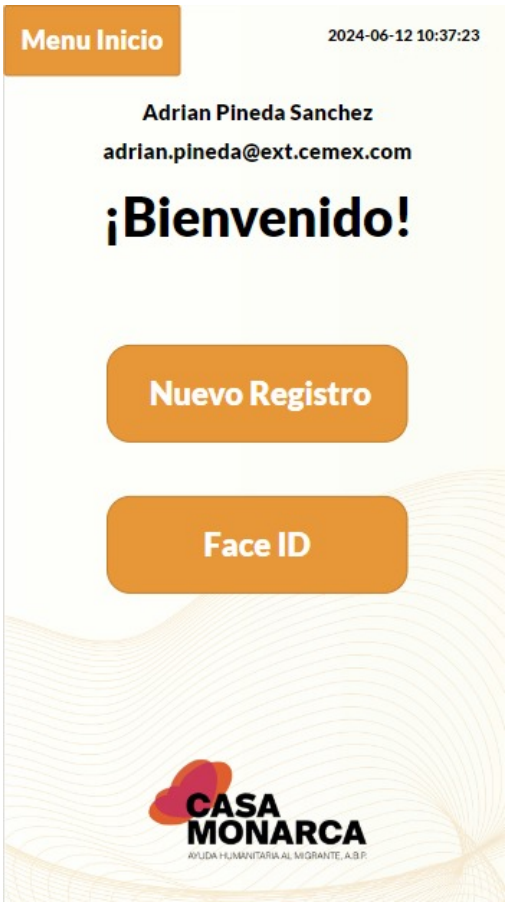

Figura 4: Pantalla de inicio de Power Apps

Pantalla de Inicio:

- **Bienvenida Personalizada:** Muestra el nombre del usuario y su dirección de correo electrónico, junto con la fecha y hora actuales.
- **Opciones de Navegación:** Dos botones principales para "Nuevo Registroz "Face ID".

Nuevo Registro:

- Permite a los usuarios ingresar nuevos datos de migrantes en la base de datos.
- Formularios diseñados para capturar información relevante de manera estructurada.

Face ID:

- Utiliza reconocimiento facial para identificar y verificar a los migrantes registrados.
- Aumenta la seguridad al asegurar que solo los usuarios autorizados puedan acceder a los datos sensibles.

Marca de la Organización:

- Incluye el logo de Casa Monarca y su lema de ayuda humanitaria, reforzando la identidad y misión de la organización.

Ventajas de Power Apps en Seguridad para el Registro de Datos

Seguridad Integrada:

- Power Apps ofrece autenticación multifactor (MFA) y soporte para autenticación robusta mediante Active Directory, garantizando que solo usuarios autorizados accedan a la aplicación.

Cifrado de Datos:

- Los datos en tránsito y en reposo están cifrados utilizando protocolos estándar de la industria como TLS/SSL, protegiendo la información contra accesos no autorizados.

Control de Acceso:

- Power Apps permite definir roles y permisos granulares, asegurando que solo los usuarios adecuados tengan acceso a determinadas funcionalidades y datos.

Auditoría y Monitoreo:

- Registros detallados de acceso y actividad, permitiendo auditorías y revisiones de seguridad para detectar y responder a posibles incidentes.

Facilidad de Integración:

- Se integra fácilmente con otras herramientas de Microsoft como Power BI para análisis de datos y SharePoint para almacenamiento seguro, proporcionando un ecosistema seguro y eficiente.

Flexibilidad y Escalabilidad:

- La capacidad de personalizar y escalar la aplicación según las necesidades de la organización, asegurando que puede crecer y adaptarse sin comprometer la seguridad.

Conexión Power Apps y MySQL mediante un Gateway

Un gateway en Power Apps, específicamente el On-premises Data Gateway, permite la conexión segura entre los servicios de Power Apps y las bases de datos locales, como las gestionadas mediante SQL Workbench. Este gateway actúa como un puente seguro, permitiendo la transferencia de datos sin necesidad de almacenarlos en la nube, lo cual es ideal para cumplir con políticas de seguridad y regulaciones.[26]

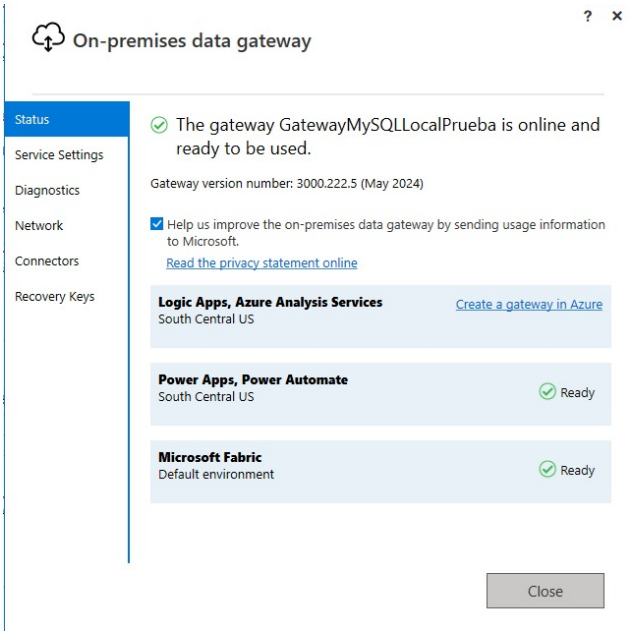

Figura 5: Configuración Exitosa del Gateway con la base de Datos Local

Pasos para la Configuración

Descarga e Instalación del Gateway:

- **Descarga:** Descargar el instalador del On-premises Data Gateway desde el portal de Power Apps o directamente desde el sitio de Microsoft.
- **Instalación:** Ejecutar el instalador en el servidor o la computadora que actúa como servidor local. Seguir las instrucciones del asistente de instalación para completar la instalación.

Configuración del Gateway:

- **Inicio de Sesión:** Una vez instalado, iniciar sesión con las credenciales de la cuenta de Microsoft utilizada para Power Apps.
- **Registro del Gateway:** Registrar el gateway proporcionando un nombre y una clave de recuperación. Esta clave es crucial para restaurar o migrar el gateway a otro servidor si es necesario.
- **Redundancia y Escalabilidad:** Configurar clusters de gateway para asegurar alta disponibilidad y balanceo de carga si se espera un alto volumen de datos o transacciones.

Conexión a la Base de Datos SQL:

- **Configuración de la Fuente de Datos:** En el portal de Power Apps, navegar a la sección de "Gatewaysz agregar una nueva fuente de datos. Seleccionar SQL Server como tipo de fuente de datos.
- **Detalles de Conexión:** Proporcionar los detalles de conexión, incluyendo el nombre del servidor, base de datos, y las credenciales necesarias para acceder a la base de datos gestionada por SQL Workbench.
- **Prueba de Conexión:** Probar la conexión para asegurarse de que el gateway puede comunicarse correctamente con la base de datos SQL local.

Uso en Power Apps:

- **Configuración en Power Apps:** En la aplicación de Power Apps, agregar una nueva conexión y seleccionar la fuente de datos configurada a través del gateway.
- **Acceso y Manipulación de Datos:** Utilizar esta conexión para acceder, manipular y mostrar los datos desde la base de datos SQL en la aplicación de Power Apps, asegurando que los datos se transfieren de manera segura y eficiente.

Seguridad y Protocolos Criptográficos

TLS/SSL:

- **Transporte Seguro:** El On-premises Data Gateway utiliza protocolos de seguridad estándar de la industria como TLS (Transport Layer Security) y SSL (Secure Sockets Layer) para cifrar la comunicación entre la base de datos local y los servicios en la nube de Power Apps.
- **Cifrado de Datos:** TLS/SSL asegura que los datos en tránsito estén cifrados, protegiendo la información sensible contra interceptaciones y ataques man-in-the-middle.

Autenticación y Autorización:

- **Autenticación Fuerte:** El gateway soporta autenticación robusta utilizando credenciales de Active Directory, tokens de acceso y otros métodos de autenticación seguros.
- **Control de Acceso:** Proporciona control granular sobre quién puede acceder y gestionar las conexiones a través del gateway, asegurando que solo usuarios autorizados puedan interactuar con los datos.

Gestión de Certificados:

- **Certificados SSL:** La configuración y gestión de certificados SSL es soportada para validar la identidad de los servidores y cifrar las conexiones de red.

- **Rotación de Certificados:** Implementa mecanismos para la rotación y renovación de certificados, asegurando que las conexiones siempre sean seguras.

Auditoría y Registro:

- **Registros de Auditoría:** Mantiene registros detallados de las conexiones y actividades realizadas a través del gateway, permitiendo auditorías de seguridad y cumplimiento.
- **Monitoreo Continuo:** Facilita el monitoreo continuo de las conexiones y el tráfico de datos para detectar y responder a posibles amenazas de seguridad.

Ventajas del Gateway

Seguridad:

- Proporciona una conexión segura entre Power Apps y la base de datos local, cumpliendo con las políticas de seguridad y regulaciones de datos.

Confiabilidad y Disponibilidad:

- Permite configurar clusters de gateway para asegurar alta disponibilidad y redundancia, minimizando el riesgo de interrupciones en el servicio.

Flexibilidad:

- Facilita la integración de datos locales en aplicaciones en la nube sin necesidad de replicar o migrar los datos, manteniendo la integridad y la seguridad de los datos locales.

4.2.3. Estadísticas

Herramientas Utilizadas

Para el desarrollo del informe y la creación de las estadísticas presentadas, se utilizó Power BI, una herramienta de visualización y análisis de datos desarrollada por Microsoft. Además, se empleó una base de Excel como fuente de datos para almacenar y organizar la información relevante. La actualización automática de los datos se realizó mediante la configuración de

de datos local, permitiendo que las visualizaciones en Power BI se actualicen en tiempo real cada vez que se realizan nuevos registros en el archivo.

Procedimiento

1. **Preparación de los Datos**: Los datos fueron organizados y almacenados en un archivo Excel. Este archivo contiene registros detallados de personas atendidas, incluyendo información demográfica, académica y de sus experiencias de viaje.

2. **Conexión de Datos**: Se estableció una conexión entre Power BI y la base en Excel que se espera posteriormente convertir en una base de MySQL. Esto permite que los datos se actualicen automáticamente en Power BI cada vez que se actualiza el archivo.

3. **Creación de Visualizaciones**:

   - **Gráfico de Barras Agrupadas (Educación y Alfabetización)**: Este gráfico muestra la distribución del nivel educativo de las personas atendidas, desglosado por su capacidad de leer y escribir.
   - **Gráfico de Líneas**: El gráfico de líneas ilustra la tendencia en la cantidad de personas atendidas a lo largo del tiempo, permitiendo identificar periodos de mayor afluencia.
   - **Gráfico de Columnas Agrupadas**: Las columnas agrupadas muestran la distribución del número de personas atendidas que tienen hijos, proporcionando una perspectiva sobre la carga familiar de los migrantes.
   - **Gráfico de Anillos**: En este se representa el estado civil de las personas atendidas, proporcionando una visión sobre su situación familiar.
   - **Mapa**: El mapa generado muestra la distribución geográfica del país de origen de las personas atendidas, destacando los principales países de procedencia.
   - **Tarjetas Informativas**:
     - **Tarjeta 1**: Indica el número de personas que han intentado ingresar a Estados Unidos.

- **Tarjeta 2**: Expone el número de personas que le han pagado a alguien para poder viajar.
- **Tarjeta 3**: Proporciona el número de personas que han sufrido abusos a sus derechos humanos durante su viaje.

4. **Diseño**: Se personalizó la interfaz del informe con un fondo temático y elementos gráficos adecuados, como el logo de la organización socio-formadora y colores corporativos, para facilitar la interpretación de los datos y mejorar la presentación.

5. Resultados

A continuación se muestran los procedimientos y los resultados que generan nuestro método de encriptación:

Primero, se muestra la interfaz generada por nuestro código en donde se selecciona una carpeta desde el directorio.

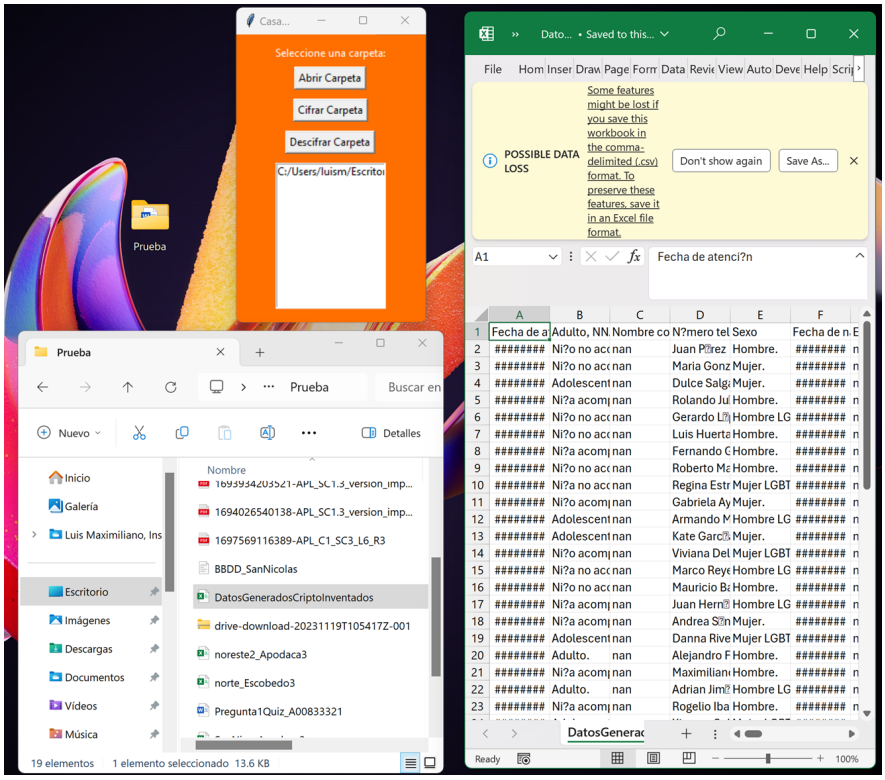

Figura 6: Interfaz, Carpeta seleccionada y Datos a encriptar

Posteriormente al pulsar el botón de 'Cifrar Carpeta', y escribir una contraseña, los archivos dentro quedan encriptados.

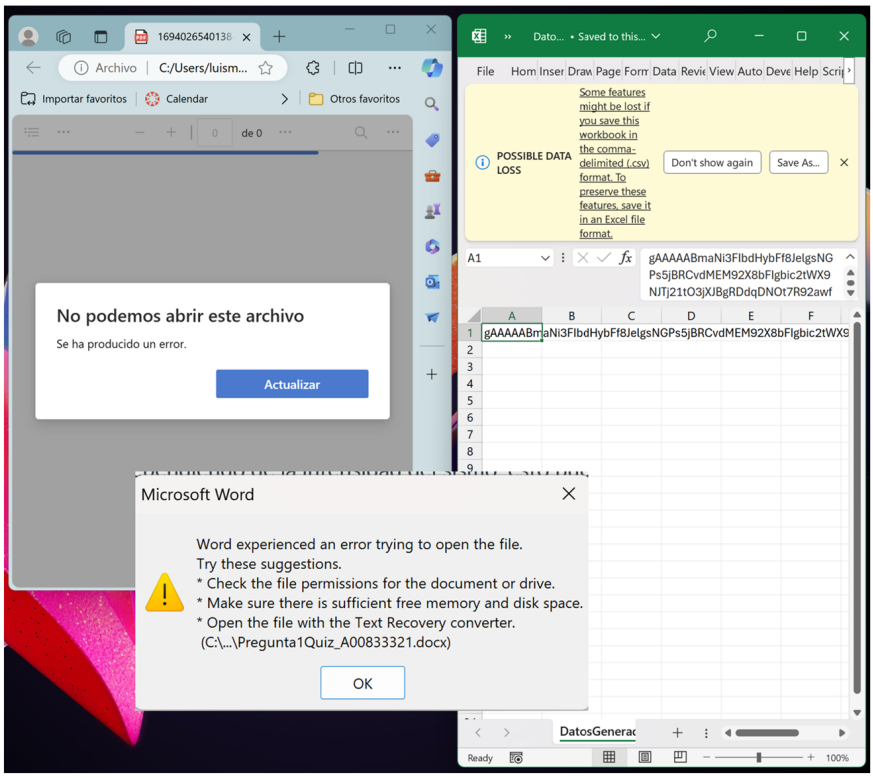

Figura 7: Archivos CSV, WORD y PDF encriptados

Para desencriptarlos, se pulsa el botón de 'Descrifrar Carpeta' y se escribe la contraseña previa.

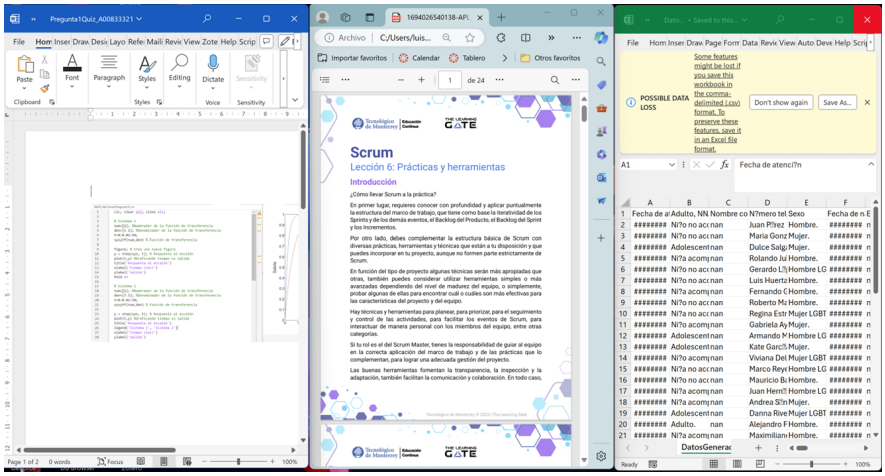

Figura 8: Archivos CSV, WORD y PDF desencriptados

se muestra la generación de clave desde la aplicación local.

Figura 9: Generación de clave por hash.

Por último, se muestra la interfaz generada en PowerApps para la recolección de datos a manera de formulario y estadíticas de los migrantes en Power Bi.

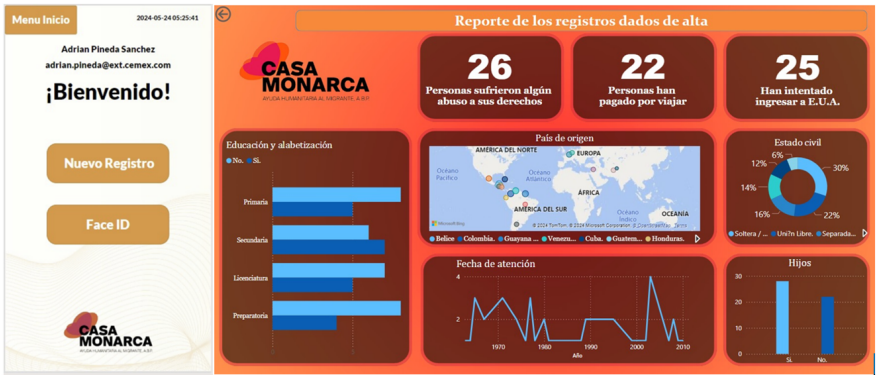

Figura 10: Estadísticas generadas a partir de los datos recolectados

6. Conclusiones

A lo largo de este proyecto, hemos trabajado múltiples aspectos de la criptografía y la seguridad de la información. 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.

Acceder a recursos de la Biblioteca Digital fue fundamental para investigar trabajos previos y encontrar referencias útiles. Encontramos bibliotecas de funciones y recursos informáti-

cos de referencia, como la biblioteca **cryptography** en Python, que nos fue de utilidad para el cifrado y descifrado de datos.

La elección de un esquema de clave simétrica, el cifrado Fernet, nos ayudó para que los datos cifrados no fueran manipulados, manteniendo su integridad. Además, implementamos prácticas para proteger la información sensible en memoria, como el manejo seguro de claves y la limpieza de memoria inmediatamente después de su uso.

Para el almacenamiento seguro de datos, los archivos cifrados se guardaron directamente, sobrescribiendo los datos originales. Esto minimizó el riesgo de exposición de datos sensibles.

Aunque nuestra solución principal utiliza criptografía simétrica, también consideramos la administración segura de claves. Generamos, almacenamos y distribuimos las claves de manera segura, utilizando almacenes de claves seguros y canales seguros para el intercambio de claves.

Toda la documentación, incluidos el código fuente, las licencias utilizadas, y los vectores de prueba, se almacenó en GitHub. Esto no solo facilita la revisión y el mantenimiento del proyecto, sino que también asegura la transparencia y la accesibilidad para futuras referencias y auditorías.

La integración de Power Apps para recolectar información de los migrantes y la creación de un dashboard en Power BI para mostrar estadísticas importantes del negocio agregaron un valor significativo al proyecto. El uso del protocolo TSS y la encriptación SHA256 en SQL con clave asimétrica proporcionaron capas adicionales de seguridad para los datos recolectados.

Todo el proceso se llevó a cabo con un fuerte enfoque en la ética y el beneficio de los migrantes. Nuestra solución no solo protege la información sensible de los migrantes, sino que también ofrece una herramienta económica y práctica para Casa Monarca. Al proporcionar una solución que pueden usar localmente y de forma gratuita, hemos ayudado a reducir costos y aumentar la eficiencia operativa de la organización.

Para futuras mejoras y desarrollo continuo, recomendamos:

- Continuar investigando y actualizando los métodos de cifrado para asegurar que sigan siendo robustos frente a nuevas amenazas.
- Implementar pruebas automatizadas para validar continuamente la seguridad y la efi-

ciencia 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.

Nuestro proyecto no solo cumplió con los requisitos técnicos establecidos en la materia, sino que también abordó de manera exitosa las preocupaciones éticas y prácticas de Casa Monarca, buscando que se quedaran satisfechos con los resultados implementando herramientas adicionales que les fueran de utilidad. 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. A futuro, la mejora continua y la colaboración seguirán siendo claves para mantener y mejorar la seguridad y eficiencia de esta solución.

Referencias

[1] INAI, (2024). Normativa y legislación en PDP Leyes en México para la protección de datos personales. Link del artículo

[2] Casa Monarca, (2024). Casa Monarca: Ayuda Humanitaria al Migrante, A.B.P. Link de la página principal

[3] Rea Enríquez, D. X. (2017). Sistema de voto electrónico con protocolos de curvas elípticas aplicado en elecciones populares [Tesis de pregrado, Universidad Técnica del Norte]. Link del artículo

[4] Ortega Chulde, C. A. (2023). Implementación de mecanismo de seguridad para redes de sensores inalámbricos basado en criptografía de curva elíptica [Tesis de pregrado, Universidad Técnica del Norte].

Link del artículo

[5] UV, *Algoritmos de clave pública*. UV. Link del artículo. Accessed: date.

[6] The Legion of the Bouncy Castle, (2024). Bouncy Castle. Link de la página principal

[7] IBM, (2024). Extensión de criptografía Java (JCE). Link del artículo

[8] Crypto++, (2024). Crypto++ Library 8.9. Link de la página principal

[9] OpenSSL, (2024). OpenSSL Cryptography and SSL/TLS Toolkit. Link de la página principal

[10] Python, (2024). PyCryptodome 3.20.0. Link de la página principal

[11] Python, (2024). Cryptography 42.0.5. Link de la página principal

[12] Trusted Computing Group, (2024). TPM Software Stack (TSS). Link del artículo

[13] Intel, (2024). Intel Software Guard Extensions SDK for Linux OS. Link de la página principal

[14] Intel, (2024). Using the Intel Software Guard Extensions (Intel SGX). Link del artículo

[15] Juan Cano Pradas, *Algunas variantes del algoritmo cuántico de Shor*. Facultad de Matemáticas e Informática Universidad de Barcelona. Link del artículo. Accessed: date.

[16] UNAM. Criptografía. Link del artículo

[17] Anda, P. de. (2018). Instalación de Ubuntu Server en VirtualBox • Factor Evolución. Retrieved from Link de la página principal

[18] Andrea Tironi. (2023, January 26). Qué es y cómo funciona VeraCrypt: la herramienta para encriptar archivos. InnovaciónDigital360. Retrieved from Link de la página principal

[19] Dyllick-Brenzinger, R. (2022). Las 9 mejores bases de datos gratuitas en línea. Retrieved from Link de la página principal

[20] Personio. (2023). Bases de datos en la nube: ¿qué son y para qué sirven? Retrieved from Link de la página principal

[21] Crear tu cuenta gratuita de Azure hoy mismo: Microsoft Azure. (s.f.). Retrieved from Link de la página principal

[22] Anish De. Cryptography with Python using Fernet. Link del artículo

[23] Steven Sigil. Fernet Cryptography. Link del artículo

[24] ThreadSpeed. How do I display an image in PyQt5/PySide2. Link del artículo

[25] Python Software Foundation. hashlib — Secure hashes and message digests. Link del artículo

[26] arthiriyer. (2024, March). What is an on-premises data gateway? - Power Apps. Microsoft.com. Retrieved from Link del artículo

[27] tapanm-MSFT. (2023, March 16). ¿Qué es Power Apps? - Power Apps. Microsoft.com. Retrieved from Link del artículo

[28] Adriano R. (2022, December 27). MySQL, comprender el software de gestión de datos relacionales. Formación En Ciencia de Datos — DataScientest.com. Retrieved from Link del artículo