Instituto Tecnológico y de Estudios Superiores de Monterrey

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

Casa Monarca – Ayuda humanitaria al migrante ABP

Ortega Castellanos Diego A01754351
Villarreal González Andrés A00833915
Galgani Hernandez Axel Andrea A00835225
Segura Mariano Santiago Humberto A01246578
Juarez Hernandez Gerardo A01732799
Vidal Torres Salvador A01732983

Uso de álgebras modernas para seguridad y criptografía

Profesores: Dr. Luis Miguel Méndez Díaz, Dr. Daniel Otero Fadul

Índice

Abstract

Este proyecto se enfoca en abordar de manera efectiva los desafíos de seguridad en el almacenamiento de datos para la organización socio formadora Casa Monarca, una asociación sin fines de lucro. La iniciativa se centra en desarrollar un método integral de protección de datos, especialmente relevante al tratar información sensible de migrantes en búsqueda de asistencia y apoyo. Se exploran diversas opciones criptográficas, incluyendo el cifrado de extremo a extremo, tokenización y gestión de accesos, así como medidas de seguridad física y en la nube. Además, se presta especial atención a la conformidad con regulaciones de privacidad, la implementación de privacidad por diseño y la mitigación de riesgos de seguridad, con el objetivo de asegurar un almacenamiento de datos robusto y seguro para la organización.

This project focuses on effectively addressing security challenges in data storage for the partner organization Casa Monarca, a non-profit association. The initiative centers on developing a comprehensive data protection method, especially relevant when handling sensitive information from migrants seeking assistance and support. Various cryptographic options are explored, including end-to-end encryption, tokenization, and access management, as well as physical and cloud security measures. Additionally, special attention is given to compliance with privacy regulations, implementation of privacy by design, and mitigation of security risks, with the goal of ensuring robust and secure data storage for the organization.

Palabras clave: Criptografía Asimétrica, AES (Advanced Encryption Standard), Protección de Datos Personales, Casa Monarca, data, organization y protection

1. Introducción

El proyecto se centra en la creación de una aplicación web para la gestión segura de cuestionarios y datos sensibles, utilizando técnicas de cifrado avanzadas. La herramienta está diseñada para organizaciones y entidades que manejan información confidencial, particularmente en contextos humanitarios y de asistencia social, como albergues y centros de ayuda. En este caso específico, la aplicación se desarrolla para Casa Monarca, una institución dedicada a la asistencia de migrantes y personas en situación vulnerable en Monterrey, México.

El nicho del objeto de estudio es la necesidad de proteger datos personales y sensibles recopilados a través de cuestionarios, asegurando que sólo personal autorizado pueda acceder a ellos. Utilizando el algoritmo de cifrado AES (Advanced Encryption Standard), se garantiza que los datos almacenados en la base de datos sean inaccesibles para personas no autorizadas, incluso en caso de una brecha de seguridad.

Además, la aplicación permite la gestión de usuarios con diferentes niveles de jerarquía, asegurando que sólo aquellos con los permisos adecuados puedan acceder a determinadas funcionalidades, como la administración de usuarios y la consulta de información cifrada. Esta estructura jerárquica es esencial para organizaciones que necesitan controlar el acceso a información sensible y mantener la integridad de los datos.

El objetivo final es proporcionar una solución robusta y eficiente que combine la facilidad de uso de una interfaz web con la seguridad necesaria para manejar datos sensibles, cumpliendo con los estándares de protección de datos y confidencialidad requeridos en el contexto actual.

2. Método

En la actualidad, existen numerosos recursos criptográficos disponibles para la protección de datos, algunos de los cuales pueden ser especialmente útiles para organizaciones o gobiernos que manejan información sensible sobre migrantes u otras poblaciones vulnerables.[4] A continuación, se presenta una lista de algunos recursos criptográficos comunes:

- Cifrado de datos
- Cifrado de extremo a extremo (E2EE)
- Hashing
- Protocolos de seguridad
- Infraestructura de clave pública (PKI)
- Librerías de criptografía modernas
- Tokenización
- Autenticación multifactor (MFA)
- Firewalls y filtrado de paquetes
- Protección en la nube

Por accesibilidad, costos y mantenimiento, se decidió utilizar cifrado de extremo a extremo, ya que garantiza que los datos solo sean legibles por el emisor y el receptor, evitando que terceros, incluido el proveedor de servicios, accedan a los datos en texto plano.

2.1. Estándares de cifrado

Se revisaron los estándares existentes para el cifrado y se consideraron tanto el cifrado simétrico como el asimétrico para el proyecto. Sin embargo, se decidió utilizar uno de bloque simétrico.[2] Este es un método de cifrado que utiliza una sola clave para cifrar y descifrar mensajes entre el emisor y el receptor. Los dos comunicantes necesitan conocer esta clave para poder intercambiar mensajes de manera segura. La clave debe mantenerse secreta para asegurar la seguridad del sistema. El principal desafío de este tipo de cifrado es la distribución segura de la clave entre las partes, dado que interceptar la clave durante su intercambio compromete la seguridad de la comunicación. A pesar de la posibilidad de que los ordenadores modernos puedan descifrar claves rápidamente debido a su capacidad

de cálculo, el cifrado simétrico sigue siendo eficaz si se maneja adecuadamente el tamaño de la clave y la seguridad en su intercambio.[5]

2.2. Ejemplos cifrado simétrico

- **AES (Advanced Encryption Standard):** Es el estándar ampliamente utilizado a nivel mundial. AES puede utilizar claves de 128, 192 o 256 bits para el cifrado, siendo extremadamente eficiente tanto en software como en hardware.
- **DES (Data Encryption Standard):** Aunque ya se considera obsoleto debido a su clave relativamente corta de 56 bits, fue uno de los primeros estándares de cifrado simétrico adoptados a nivel mundial.
- **3DES (Triple Data Encryption Standard):** Una versión mejorada de DES que aplica el algoritmo tres veces a cada bloque de datos para aumentar la seguridad. Aunque es más seguro que DES, es más lento y también está siendo reemplazado por AES.
- **Blowfish y Twofish:** Son algoritmos de cifrado simétrico diseñados para ser rápidos y eficientes en una amplia variedad de hardware y software.[3] Blowfish tiene una longitud de clave variable, mientras que Twofish fue uno de los finalistas en el proceso de selección de AES.

2.3. Análisis comparativo de esquemas

Esquema	Seguridad	Eficiencia	Implementación
AES	Alta	Alta	Fácil
RSA	Alta	Media	Compleja
ECC	Alta	Alta	Compleja
SHA-256	Alta	Alta	Fácil
MD5	Alta	Alta	Fácil

Cuadro 1: Comparación de diferentes esquemas criptográficos

Decidimos usar AES porque es extremadamente seguro debido a su estructura y al tamaño de las claves que utiliza. La complejidad matemática de su diseño hace que sea inviable para los atacantes descifrar los datos sin conocer la clave, incluso utilizando computadoras muy potentes.[8] Además, la longitud de la clave determina la dificultad de un ataque de fuerza bruta: mientras más larga sea la clave, más difícil es para los atacantes probar todas las combinaciones posibles.

AES funciona mediante un proceso de cifrado que se repite en varias rondas, dependiendo de la longitud de la clave: 128 bits: 10 rondas, 192 bits: 12 rondas, 256 bits: 14 rondas. Este proceso transforma los datos originales en una forma cifrada que parece aleatoria. Para descifrar los datos, se realiza el proceso inverso utilizando la misma clave.[1]

AES es recomendable por varias razones: ofrece un alto nivel de seguridad que pro-

tege los datos contra ataques sofisticados; es rápido y eficiente, tanto en software como en hardware, lo que lo hace ideal para una amplia gama de aplicaciones; y es un estándar adoptado mundialmente, lo que garantiza su compatibilidad y fiabilidad en diversos sistemas y plataformas.

2.4. Recursos necesarios

En la preparación para abordar el desafío propuesto, es esencial contar con una serie de recursos físicos y software que permitan llevar a cabo las tareas de manera eficiente y efectiva. La combinación adecuada de componentes físicos y herramientas digitales garantizará un entorno propicio para el desarrollo y ejecución de las soluciones planteadas.[9] A continuación, se presenta una lista detallada de los elementos necesarios para enfrentar el reto con éxito:

- Streamlit
- SQL
- AWS
- Python
- GitHub

Se presentan a continuación una variedad de bibliotecas y herramientas utilizadas para la criptografía, así como para acceder a recursos de seguridad. Cada una de estas herramientas ofrece ventajas específicas en términos de funcionalidad, rendimiento y facilidad de uso. Sin embargo, nosotros decidimos usar las siguientes librerías por simplicidad y costo, además de que son fáciles de entender debido a su extensa cantidad de información que existe en internet.

```
import json
from Crypto.Cipher import AES
from Crypto.Util.Padding import pad, unpad
from Crypto.Random import get_random_bytes
import streamlit as st
from streamlit_option_menu import option_menu
from datetime import datetime
import base64
from PIL import Image
import io
import pandas as pd
import plotly.express as px
import mysql.connector
```

De todas estas herramientas, todas son gratuitas, con la excepción de AWS, que costaría aproximadamente 430 pesos por mes con un uso estándar de flujo de usuarios.[6] Es importante destacar que aunque se sugiere AWS, otras opciones como Microsoft Azure y Google Cloud Platform también son viables. Cada proveedor tiene servicios gratuitos para organizaciones sin fines de lucro, y la elección del proveedor queda sujeta a las prefe-

rencias y políticas de la organización que realiza el desafío. La flexibilidad en la elección del proveedor permite adaptarse a diferentes entornos y necesidades específicas.[7] En este proyecto se decidió usar AWS por sus bajos costos en comparación con la competencia, pero Casa Monarca podría buscar a algunos de estos proveedores para financiar el uso de almacenamiento de datos en la nube completamente gratis.

3. Resultados

3.1. Resultados de forma escrita

El primer paso involucra la recolección de datos a través de cuestionarios que detallan información demográfica y de datos personales confidenciales de la persona y la captura de imágenes relevantes para temas de identificación física de las persona, que pueden ser necesarias para el registro y verificación de identidad u otros propósitos. Estos datos incluyen información personal de los migrantes, como nombres, direcciones, y detalles de sus situaciones particulares, así como cualquier otro dato relevante para proporcionar asistencia efectiva. La precisión y exhaustividad en esta etapa son cruciales para el proceso subsiguiente de protección de datos.

Una vez que la información ha sido recopilada, se procede a la transformación de los datos. Esta etapa implica el procesamiento y adecuación de la información para que se ajuste al formato necesario para el cifrado. La transformación de datos es un paso crítico que incluye la estructuración de datos textuales y la conversión de imágenes a formatos binarios que puedan ser cifrados. El objetivo aquí es asegurar que los datos estén en una forma que facilite el cifrado mientras se mantiene su integridad y usabilidad. Por dicho motivo se recomienda almacenar una copia de seguridad de forma física en algún usb que o computador con seguridad que permita a Casa Monarca obtener acceso a esa información bajo cualquier circunstancia. Además, se cuenta con un dashboard en tiempo real que permite a Casa Monarca visualizar la información cuantitativa de los migrantes con seguimiento diario y continuo. Cabe resaltar que esta información no está encriptada con el método AES si no que solo se encuentra resguardada con la seguridad que ofrecen los servicios de AWS.

Posteriormente, los datos cifrados se almacenan en formato JSON, lo cual permite una integración sencilla con otras plataformas y facilita el manejo de grandes volúmenes de información estructurada de forma segura. Este formato es adecuado para el almacenamiento seguro en sistemas en la nube como AWS Redshift, donde la información puede ser gestionada eficientemente, manteniendo su accesibilidad y seguridad. Un tema importante a mencionar es que los datos cruciales se guardan en formato JSON encriptado que sólo se puede acceder cuando se tiene la llave privada, en caso contrario esa información no será descifrada de ningún otra forma dando por perdida esa información.

El siguiente paso en el procedimiento es el cifrado de la información. Utilizando el algoritmo AES (Advanced Encryption Standard), los datos transformados son cifrados

para garantizar que solo aquellos con las credenciales adecuadas puedan acceder a la información en su formato original. El uso de AES permite un alto nivel de seguridad, ya que cifra los datos tanto en tránsito como en reposo. Python se utiliza para desarrollar los scripts que realizan el cifrado y descifrado de datos, mientras que SQL maneja la inserción y recuperación de estos datos cifrados en la base de datos.

Un componente vital del sistema es la gestión de llaves. Para asegurar el acceso controlado a los datos cifrados, se genera una llave privada única necesaria para descifrar la información. Esta llave se descarga y se almacena en un entorno seguro, accesible solo por personal autorizado. La gestión adecuada de esta llave es crucial para mantener la integridad del sistema de cifrado, garantizando que solo individuos con permisos apropiados puedan acceder a los datos cifrados. Por dicho motivo, se recomienda guardar las llaves en una carpeta con contraseña y almacenada en un dispositivo externo como un USB para aislar la información de los computadores que regularmente llegan a ser los dispositivos con mayor concurrencias a ataques.

Cuando un usuario autorizado necesita acceder a la información, el sistema utiliza la llave privada para descifrar los datos. Los datos cifrados, combinados con la llave secreta y la autenticación del usuario, permiten recuperar la información en su formato original. Este proceso asegura que solo usuarios con permisos adecuados puedan acceder a la información sensible. El descifrado se lleva a cabo utilizando Python, que emplea la llave privada y el algoritmo AES para restaurar los datos a su forma original.

Finalmente, los datos descifrados se presentan al usuario en forma de fichas técnicas o reportes, los cuales contienen toda la información necesaria para la toma de decisiones informadas. Estos informes se generan automáticamente y se presentan en un formato claro y comprensible, asegurando que la información sea útil y segura para su uso inmediato. Esta presentación final de los datos facilita su utilización práctica mientras se mantiene la seguridad y privacidad a lo largo de todo el proceso.

Además de las medidas de protección de datos, el sistema implementado en Casa Monarca incluye un robusto mecanismo de control de accesos a través de una opción de inicio de sesión. Este sistema de login asegura que solo el personal autorizado pueda visualizar y manipular la información sensible almacenada. Se ha diseñado con tres niveles de jerarquía de acceso para proporcionar diferentes grados de permisos, adaptándose a las necesidades específicas de los roles dentro de la organización.

El primer nivel de jerarquía proporciona acceso únicamente al cuestionario. Este nivel está destinado a los usuarios que necesitan recopilar y registrar información de los migrantes sin acceso a datos adicionales. Estos usuarios pueden introducir datos en el sistema, garantizando la entrada precisa y segura de información inicial, pero no tienen la capacidad de ver otros datos almacenados o resultados del procesamiento.

El segundo nivel de jerarquía permite acceso tanto al cuestionario como al dashboard. El dashboard ofrece una visión general y analítica de la información recopilada, permitiendo a los usuarios analizar datos de manera agregada sin acceder a detalles individuales sensibles.

Este nivel es adecuado para personal que requiere comprensión y evaluación de tendencias y patrones a partir de los datos recolectados, sin la necesidad de interactuar con datos detallados o manejar información técnica específica.

El tercer y más alto nivel de jerarquía otorga acceso completo, incluyendo el cuestionario, el dashboard, y la ficha técnica detallada, además de capacidades administrativas para el control de usuarios. Los usuarios en este nivel tienen la capacidad de ver información detallada y generar informes técnicos completos. Además, pueden gestionar el acceso de otros usuarios, lo que incluye la capacidad de otorgar o revocar permisos de acceso según las necesidades operativas y de seguridad de la organización. Este nivel es esencial para los administradores y personal de seguridad de la información, que requieren un control completo sobre la gestión y la seguridad de los datos sensibles.

Este sistema de jerarquías garantiza que la información esté disponible de manera controlada y segura, minimizando el riesgo de acceso no autorizado y asegurando que los datos sean utilizados de manera apropiada según las responsabilidades y necesidades de cada usuario. La integración del inicio de sesión y las jerarquías de acceso refuerza el enfoque integral de seguridad de datos de Casa Monarca, proporcionando una solución adaptable y escalable que protege la información mientras facilita su uso efectivo por parte del personal autorizado.

3.2. Mantenimiento

Para garantizar que el sistema de seguridad continúe protegiendo de manera efectiva la información sensible, es crucial seguir un conjunto de recomendaciones que aseguren la integridad y la actualización constante del sistema. Estas recomendaciones son esenciales para enfrentar las crecientes amenazas de seguridad y mantener la conformidad con las mejores prácticas en la protección de datos.

- **Actualizaciones:** Es fundamental mantener todos los componentes del sistema actualizados con los últimos parches de seguridad. Esto incluye el software utilizado para el cifrado (como bibliotecas criptográficas en Python), los sistemas de bases de datos (como AWS Redshift), y las plataformas de implementación (como Heroku). Las actualizaciones regulares corrigen vulnerabilidades conocidas y mejoran la resistencia del sistema contra nuevos tipos de ataques.
- **Auditorías:** Realizar auditorías de seguridad periódicas para evaluar la eficacia de las medidas de protección actuales es crucial. Estas auditorías deben incluir pruebas de penetración para identificar posibles vulnerabilidades y asegurarse de que las prácticas de seguridad cumplen con las normativas vigentes y los estándares de la industria.
- **Capacitación:** Proporcionar capacitación continua al personal sobre las mejores prácticas de seguridad es vital. Esto incluye formación sobre cómo manejar de manera segura la información sensible, identificar intentos de phishing y otras tácticas de ingeniería social, y comprender la importancia de las políticas de contraseñas se-

guras. Mantener al personal informado sobre las amenazas de seguridad emergentes ayuda a crear una cultura de seguridad dentro de la organización.

- **Gestión de contraseñas:** Adoptar la autenticación multifactor (MFA) para acceder al sistema, además de requerir contraseñas fuertes y únicas, mejora significativamente la seguridad. MFA añade una capa adicional de protección al combinar algo que el usuario conoce (una contraseña) con algo que el usuario tiene (un dispositivo móvil para códigos de verificación), reduciendo el riesgo de accesos no autorizados.
- **Gestión de acceso:** Revisar y ajustar periódicamente las jerarquías de acceso basadas en roles para asegurarse de que los permisos de usuario estén alineados con las responsabilidades actuales. Esto incluye eliminar rápidamente el acceso de los empleados que ya no requieren ciertos permisos, y ajustar los niveles de acceso según las necesidades cambiantes de Casa Monarca.
- **Encriptación:** Continuar utilizando cifrado de extremo a extremo para todos los datos sensibles, tanto en tránsito como en reposo. Además, realizar copias de seguridad regulares de los datos cifrados en ubicaciones seguras y comprobar la integridad de estas copias de seguridad regularmente para asegurarse de que se pueden restaurar en caso de un incidente de seguridad.
- **Nuevas tecnologías:** Estar atentos a las nuevas tecnologías y metodologías en seguridad de la información. Adoptar soluciones innovadoras que puedan ofrecer una mejor protección frente a amenazas emergentes, como la inteligencia artificial para la detección de amenazas.

3.3. Plan de respuesta contra incidentes

Para mantener la integridad y seguridad del sistema de gestión de información de Casa Monarca, es esencial contar con un plan de respuesta a incidentes que sea efectivo y adaptable. Este plan abarca desde la preparación inicial hasta la recuperación completa, asegurando que la organización pueda manejar cualquier brecha de seguridad de manera eficiente, proteger la información sensible, y continuar operando con interrupciones mínimas.

La preparación es el primer paso crucial en la gestión de incidentes. Esto implica el desarrollo de políticas y procedimientos claros que definen cómo se manejarán los incidentes de seguridad. Es esencial asignar roles y responsabilidades específicas dentro del equipo de respuesta a incidentes para garantizar una reacción rápida y coordinada. El entrenamiento y la capacitación continua del personal son fundamentales para que todos los miembros de la organización sepan cómo reconocer y reportar posibles incidentes de seguridad. Además, disponer de las herramientas necesarias, como plataformas de comunicación de crisis, asegurar que la organización esté lista para responder de manera efectiva a cualquier amenaza.

La identificación de incidentes es la siguiente fase, centrada en la detección y confirmación de cualquier problema de seguridad. Utilizar metodologias de monitoreo continuo

ayuda a detectar actividades sospechosas, como intentos fallidos de inicio de sesión o tráfico de red inusual. Configurar alertas automáticas que notifiquen al equipo de seguridad en caso de comportamientos anómalos es vital. Una vez que se detecta un posible incidente, es importante evaluar y confirmar su validez para asegurar una respuesta adecuada basada en la gravedad y el impacto potencial del problema.

En la fase de contención, el objetivo es limitar el alcance y el impacto del incidente. Esto puede requerir aislar sistemas afectados, como desconectar dispositivos de la red o bloquear el acceso a ciertas áreas del sistema. Implementar medidas temporales, como cambiar contraseñas o redirigir el tráfico de red, ayuda a mitigar el daño mientras se investiga el incidente. Es crucial evaluar los daños para determinar la extensión del impacto, identificar la información comprometida y entender las vulnerabilidades explotadas.

La erradicación se enfoca en eliminar la causa raíz del incidente y restaurar los sistemas a su estado seguro. Esto incluye corregir las vulnerabilidades que permitieron el incidente, como aplicar parches, eliminar malware y fortalecer configuraciones de seguridad. Verificar los sistemas y datos para asegurar que no queden rastros del ataque es esencial. Además, actualizar contraseñas y regenerar llaves criptográficas garantizan que los atacantes no puedan reutilizar accesos.

La fase de recuperación tiene como objetivo restaurar los sistemas y servicios a su operación normal de manera segura. Esto implica reiniciar servicios y sistemas afectados de manera controlada y asegurar que todas las funciones críticas estén operativas antes de declarar la recuperación completa. Realizar pruebas para confirmar que los sistemas restaurados funcionan correctamente y que no hay más signos de compromiso es vital. Implementar monitoreo adicional ayuda a detectar cualquier signo de recurrencia del incidente y asegura que la recuperación es efectiva.

La notificación es un paso clave para informar a las partes interesadas pertinentes sobre el incidente. Esto incluye la comunicación interna con los equipos relevantes, como TI, administración, y personal afectado, así como la notificación externa a autoridades regulatorias, socios, y otras partes externas afectadas según sea necesario. Proporcionar información clara y precisa a las personas cuyas datos pudieron haber sido comprometidos es fundamental, indicando las medidas tomadas para proteger sus datos y cualquier acción que necesiten tomar.

Finalmente, las lecciones aprendidas son cruciales para mejorar la respuesta futura y prevenir incidentes similares. Conducir una revisión detallada del incidente ayuda a entender qué sucedió, cómo se manejó y qué se puede mejorar. Documentar los hallazgos y recomendaciones permite actualizar políticas, procedimientos y planes de respuesta a incidentes basados en las lecciones aprendidas. Proporcionar capacitación adicional al personal basada en estas lecciones mejora la preparación y respuesta a futuros incidentes.

Mantener una documentación adecuada a lo largo de todo el proceso es esencial. Esto incluye registrar todos los detalles del incidente, las acciones de contención, erradicación, recuperación, y las lecciones aprendidas. Crear informes de incidentes puede ser útil para

análisis futuros, cumplimiento de normativas y evaluación de la efectividad de las medidas de respuesta.

3.4. Resultados de forma tabular

Aspecto evaluado	**Descripción**	**Herramientas**
Cifrado de datos	Implementación de cifrado de extremo a extremo usando AES para proteger datos sensibles en tránsito y en reposo. Python se utilizó para el desarrollo de scripts de cifrado y descifrado, SQL para manejar operaciones de inserción y recuperación de datos cifrados, y Numpy para la manipulación de datos cifrados.	Python, SQL, Numpy
Gestión de accesos	Desarrollo de un sistema de login seguro con autenticación y jerarquía de usuarios. Streamlit se utilizó para crear una interfaz de usuario para la autenticación, y Heroku para el despliegue de la aplicación, asegurando su accesibilidad y escalabilidad. SQL se utilizó para el almacenamiento de la información creando una tabla nueva dentro de nuestra base de datos.	Streamlit, Heroku, SQL
Seguridad física y en la nube	Implementación de seguridad en la nube con AWS Redshift, proporcionando cifrado en tránsito y en reposo. Se recomienda medidas de seguridad física como control de acceso a las instalaciones y vigilancia continua.	AWS Redshift, Heroku
Conformidad con regulaciones	Aseguramiento de conformidad con regulaciones de privacidad como GDPR y la Ley de Protección de Datos Personales en México. Python y Pandas se utilizaron para crear scripts que gestionen la conformidad y generen reportes automáticos.	Python, Pandas
Privacidad por diseño	Integración del principio de privacidad por diseño en todo el sistema, incluyendo la minimización de datos, cifrado por defecto y acceso basado en roles. Python se utilizó para implementar estas características.	Python, Pandas
Mitigación de riesgos de seguridad	Desarrollo de estrategias para la evaluación continua de vulnerabilidades y la implementación de actualizaciones de seguridad. Python se utilizó para scripts automatizados de escaneo de seguridad, y AWS Redshift para la gestión de registros de seguridad.	Python, AWS Redshift, Heroku
Almacenamiento de datos	Diseño de un sistema de almacenamiento robusto utilizando SQL para la gestión de bases de datos y AWS Redshift para almacenamiento en la nube, garantizando alta disponibilidad y seguridad de datos.	SQL, AWS Redshift

3.5. Forma matemática

Explicación del método matemático para la encriptacion y desencriptacion:

1. **Encriptación por Alice**:
   - Alice tiene un mensaje M que quiere enviar a Bob de manera segura.
   - Alice y Bob comparten una clave secreta K.
   - Alice divide M en bloques $M_1, M_2, \ldots, M_n$, donde cada bloque es de 128 bits.
   - Alice encripta cada bloque M_i usando AES y la clave K para obtener los bloques cifrados C_i.

   Matemáticamente:

$$C_i = \text{AES}_K(M_i)$$

donde AES_K representa la función de encriptación AES con la clave K.

El mensaje cifrado completo C es la concatenación de todos los bloques cifrados:

$$C = C_1 \| C_2 \| \ldots \| C_n$$

2. **Transmisión**:
   - Alice envía el mensaje cifrado C a Bob.
3. **Desencriptación por Bob**:
   - Bob recibe el mensaje cifrado C.
   - Bob divide C en bloques $C_1, C_2, \ldots, C_n$.
   - Bob desencripta cada bloque C_i usando AES y la clave K para recuperar los bloques originales M_i.

   Matemáticamente:

$$M_i = \text{AES}_K^{-1}(C_i)$$

donde AES_K^{-1} representa la función de desencriptación AES con la clave K.

El mensaje original M es la concatenación de todos los bloques desencriptados:

$$M = M_1 \| M_2 \| \ldots \| M_n$$

3.6. Resultados Forma Gráfica

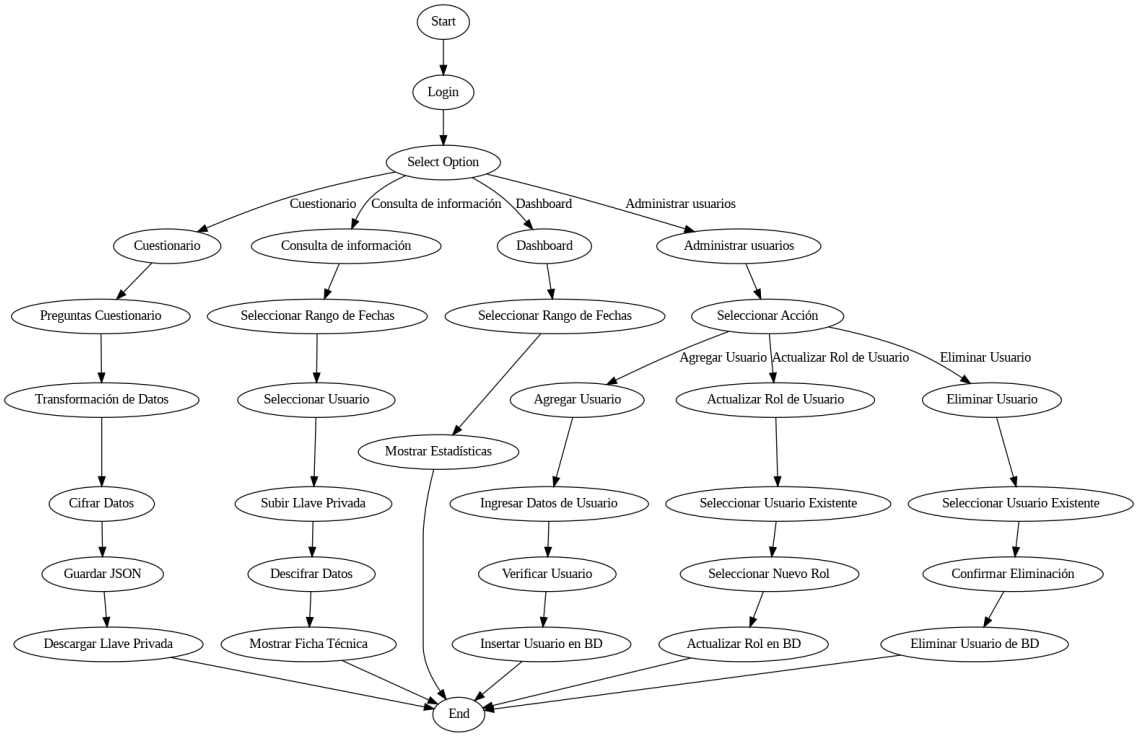

Figura 1: Resultados Forma Gráfica

4. Conclusiones

La creación de la interfaz para acceder a información encriptada ha facilitado el desarrollo de una solución segura y viable para la visualización y manejo de datos confidenciales. Este proyecto ha demostrado que es viable ejecutar un sistema que mantenga la confidencialidad de los datos mediante medios de encriptación sólidos y al mismo tiempo presente los datos de una manera sencilla y accesible a través de una interfaz básica y orientada al usuario.

Algunos de los logros e importancia clave incluyen mayor seguridad, donde se mantiene la información confidencial a salvo del acceso no autorizado a través del uso de cifrado fuerte. Hay valor añadido por la seguridad mejorada a través de la clave secreta empleada para descifrar la información. Además, la usabilidad mejorada es evidente, ya que la interfaz de usuario diseñada permite a los usuarios acceder a información codificada de una manera sencilla, ya que los datos están restringidos por rango de fechas y usuario especificado de tal manera que los datos útiles se puedan acceder fácilmente sin amenazar la seguridad.

También se ha logrado un mayor nivel de eficiencia en la recuperación de datos, ya que el hecho de que los datos sean capaces de ser representados matemáticamente, verbalmente, tabularmente, gráficamente y numéricamente hace que sea fácil y accesible realizar inferencias a partir de los datos para facilitar la toma de decisiones informadas. La interfaz en

Streamlit es, por lo tanto, un punto crítico en lo que respecta a la usabilidad y flexibilidad, ya que está diseñada de tal manera que se requiere poco entrenamiento para hacer uso de ella, por lo que incluso una persona que no esté acostumbrada a usar software puede hacer un uso efectivo de ella.

Finalmente, las ventajas de tener este tipo de interfaz en funcionamiento no solo serían la seguridad y el acceso a la información encriptada, sino también una herramienta que se modificaría y extendería con los requisitos de los socios formadores de una manera tan resistente y flexible.

4.1. Recomendaciones para el socio formador

Se aspira a que, para poder sacar el máximo provecho de este recurso, los profesionales encargados de trabajar a través de la interfaz estén adecuadamente entrenados para usarla productivamente en todos sus niveles. También deberían ocurrir regularmente auditorías de seguridad para identificar y resolver lagunas en el sistema y, por lo tanto, asegurar que la protección de los datos esté actualizada con los nuevos desarrollos que representan una amenaza.

La interfaz de usuario y los sistemas de cifrado respectivos también deben mantenerse actualizados, con el desarrollo de mejoras y nuevas características basadas en la experiencia de los usuarios y los avances tecnológicos. Sería igualmente beneficioso vincular esta interfaz con otras aplicaciones empresariales internas para el mejor control de la información y el flujo de trabajo más eficiente.

Sería importante tener un estricto control de las políticas de manejo de claves secretas que se utilizan para encriptar y desencriptar datos, y esto se aplicaría a la forma en que se establecen, distribuyen, almacenan y destruyen con seguridad las claves. Finalmente, un sistema en línea de monitoreo continuo y generación de informes se haría cargo de monitorear el uso de la interfaz, de modo que sea posible detectar cualquier acceso no autorizado o actividades sospechosas que puedan sugerir que hay una amenaza para la seguridad.

Todas las recomendaciones hechas serían para que el sistema permanezca seguro, eficiente y se adhiera a las normas de la industria.

5. Anexos

5.1. Manual de usuario

Haga clic aquí para abrir el Manual de Funcionamiento

Referencias

[1] E. adSalsa. *Cómo Proteger Una Base De Datos.* (2023, May 24). URL: https://www.adsalsa.com/como-proteger-una-base-de-datos/ (visitado 26-02-2024).

[2] J. Chavez. *CEUPE.* 8 de Octubre de 2019. URL: https://www.ceupe.com/blog/cifrado-simetrico.html (visitado 22-02-2024).

[3] J. Chavez. *CEUPE.* 8 de Octubre de 2019. URL: https://www.ceupe.com/blog/cifrado-asimetrico.html (visitado 22-02-2024).

[4] Ikusi. *¿Cómo proteger tu base de datos?* (2023, August 11). URL: https://www.ikusi.com/mx/blog/como-proteger-tu-base-de-datos/ (visitado 28-02-2024).

[5] Kaspersky. *Kaspersky.* (s. f.). URL: https://latam.kaspersky.com/resource-center/definitions/encryption (visitado 25-02-2024).

[6] Criptografía en Python con PyCrypto. *Criptografía en Python.* (s. f.). URL: https://www.ellaberintodefalken.com/2014/04/criptografia-python-pycrypto.html (visitado 28-02-2024).

[7] Mi Diario Python. *Criptografía en Python - RSA.* (2020, 22 diciembre). URL: https://pythondiario.com/2020/07/criptografia-en-python-rsa.html (visitado 28-02-2024).

[8] B. Schneier. *Cryptography for Beginners.* (2020, February 1). URL: https://esgeeks.com/guia-para-principiantes-de-criptografia/ (visitado 28-02-2024).

[9] TS2 Space. *Criptografía.* (2019, June 17). URL: https://rico-schmidt.name/pymotw-3/cryptographic.html (visitado 27-02-2024).