Firma Digital

Ricardo Kaleb Flores Alfonso
A01198716
José de Jesús Ramírez Mendieta
A00835680
Ana Karen Márquez
A01028413
Génesis Pereyra Camacho
A01734276
Natalia Olvera Ortiz
A01285367

Tecnológico de Monterrey

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

Luis Miguel Méndez Díaz Daniel Otero Fadul Raúl Gómez Muñoz

17 de marzo de 2025

---

1. Abstract

The present work aims to improve the security of the documents emited by an organization which helps inmigrants in Mexico. By developing a digital signature system that identifies each document as unique and can't be manipulated without knowledge from all the responsibles. Given that the forgery of those documents can compromise the opportunities and security of the inmigrants, while reducing the trust between the organization and inmigrants. This system has been developed considering the resource limits that this type of organization have, also the compatibility with Azure components was taken into account.

2. Resumen

Este trabajo busca mejorar la seguridad de los documentos emitidos por una organización que brinda apoyo a migrantes en Mexico. A traves del desarrollo de un sistema de firma digital que identifique cada documento como unico y no pueda ser manipulado sin el conocimiento de los responsables. Esta necesidad surge debido a que la falsificación de dichos documentos pueden comprometer las oportunidades y seguridad de los migrantes asi como reducir la confianza de estos mismos hacia la organización. Para la herramienta desarrollada fue importante tomar en cuenta el limite de recursos que suelen tener las organizaciones, asi como la compatibilidad con los componentes de Azure.

3. Introducción

En los ultimos años, la seguridad de la información se ha convertido en un pilar fundamental para el mundo como lo conocemos. Desde mensajes encriptados por el internet, hasta transferencias de dinero de manera segura e instantanea desde el telefono. Esto ha generado un desarrollo especializado en la ciberseguridad que permite autenticar de manera rapida a los usuarios. La criptografia se vuelve esencial para garantizar dicha seguridad en los sistemas, la cual proporciona confidencialidad e integridad en los intercambios de información. Estos dos puntos se vuelve relevantes en el contexto de la migración, donde las organizaciones emiten documentos clave, como certificados de identidad, tramites internos y cartas de reconocimiento, que deben de ser protegidos contra falsificaciones y fraudes. Debido a esto se desarolla un mecanismo de firma digital que garatice la autenticidad de los documentos, apoya a los inmigrantes pues les permite asegurar la validez de dichos

4. Marco Referencial

4.1. Marco Teórico. A lo largo de la vida, el humano ha tenido necesidad de ocultar mensajes y guardar secretos. Sin embargo, en los últimos años esta necesidad se ha visto urgente especialmente en el ambito tecnólogico debido a la gran digitalización que estamos teniendo. "la criptografía tiene como objetivo permitir que dos personas puedan intercambiarse información de forma confidencial y segura mediante un canal inseguro"(Hernández Encinas 2016). Entonces, a través de métodos como la transposición, la sustitución o el cifrado, se logra transformar el texto original en un texto oculto. Actualmente, la criptografía se utiliza para más que solo ocultar mensajes, podemos ver sus aplicaciones en cifrados de datos y en firmas electrónicas (Hernández Encinas 2016). Uno de los sistemas utilizados es el esquema híbrido, el cual a través de criptosistemas asimértricos y simétricos, envía mensajes cifrados entre dos usuarios con una clave cifrada pública. Además, existen las funciones de resumen (hash). Estas funciones criptográficas permiten comprobar la integridad de los datos, más allá de cifrar un mensaje. Además, las funciones de resumen convierten los mensajes a un valor con una longitud fija, conocido como resumen (Hernández Encinas 2016). Las llaves digitales se crearon con el propósito de evitar suplantación de identidad. Por lo tanto, estas llaves garantizan la integridad y la autoría de un mensaje cifrado utilizando un criptosistema asimértrico. El proceso de generar una llave digital requiere del documento a firmar, una función resumen, la clave privada del firmante y una clave pública. Primero, se calcula el resumen del mensaje, se cifra con la clave privada del firmante y posteriormente puede ser verificada por otro usuario. Un documento puede ser firmado por más de un usuario y las firmas digitales se generan cuando el documento sufre una modificación. Para verificar la firma digital, se necesita conocer el mensaje, la firma y la clave pública del firmante. Si la firma es válida, entonces se comprueba que el mensaje es íntegro y auténtico. Dentro de las llaves digitales más comúnes se realizan a través de algoritmos RSA. Otros métodos para la generación de llaves son ECDSA (Elliptic Curve Digital Signature Algorithm) y el SHA-256 (Cryptography 2025). El algotirmo RSA (Rivest-Shamir-Adleman) utiliza una clave pública para cifrar mensajes y crear firmas digitales. Este algotirmo se basa en la dificultad de factorizar grandes números primos. Como parte de su proceso, RSA genera una clave pública para cifrar mensajes y verificar firmas, además de una clave privada para descifrar mensajes y crear firmas. Un mensaje firmado puede ser verificado por cualquier persona que tenga la clave pública. Por otro lado, existe el algoritmo SHA-256 que a partir de datos produce un hash de 256 bits (32 bytes). Por último, existe el ECDSA, una variante del DSA que utiliza criptografía de curvas elípticas. Este algoritmo es parecido al RSA, sin embargo, utiliza claves mucho más cortas, haciendolo eficiente en rendimiento y uso de recursos (Hernández Encinas 2016). Los protocolos criptográficos son reglas y procedimientos para desarrollar operaciones criptográficas, asegurando la comunicación en una red, autenticación, confidencialidad, integridad y no repudio. Estos son algunos de los principales protocolos criptográficos: • X.509: es un estándar de la Unión Internacional de Telecomunicaciones (UIT-T) que define el formato de los certificados de clave pública. Cada certificado tiene una clave pública y es emitido por una autoridad de certificación (CA). Estos certificados son fundamentales para la infraestructura de clave pública (PKI), la cual busca brindar una navegación segura por internet y firmas digitales para autenticación. • PKCS7: define la sintaxis para los mensajes criptográficos, especifica el formato de datos que puede incluir firmas digitales y contenido cifrado. Este estándar es principalmente utilizado en correos electrónicos. Además, es empleado en la distribución de certificados y listas de revocación de certificados (CRLs) dentro de la PKI. • eIDAS: El Reglamento eIDAS (Electronic Identification, Authentication, and Trust Services) es una normativa de la Unión Europea que regula la identificación electrónica para transacciones electrónicas.

Además, establece requisitos para la validación de firmas electrónicas avanzadas. • FIPS 140-2: La norma Federal Information Processing Standard (FIPS) 140-2 es una regulación del gobierno de los Estados Unidos que establece los requisitos de seguridad para módulos criptográficos. Principalmente, asegura los módulos criptográficos en dispositivos de hardware de seguridad y programas de software. (**cryptography**)

Actualmente, en México existen leyes que protegen a los usuarios en su navegación por internet, así como el tratamiento de dato personales. Estas son algunas de las leyes y regulaciones en México relacionadas a la ciberseguridad: Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), Código Penal Federal (enfocado en delitos cibernéticos), la Estrategia Nacional de Ciberseguridad (uniendo fuerzas de gobierno, sector privado y la sociedad civil para mejorar la resiliencia ante ciberataques) y la Iniciativa de Ley Federal de Ciberseguridad (Fuentes, S. 2023). Por otro lado, las firmas digitales están reguladas por diversas leyes y normativas que garantizan su validez y seguridad. La Ley de Firma Electrónica Avanzada establece los criterios para una firma digital válida, al asegurar la autenticidad, integridad y no repudio de los documentos firmados digitalmente. Asimismo, el Código de Comercio y el Código Civil reconocen que las firmas digitales son equivalentes a firmas manuscritas (Arellano, E. 2023). Por otro lado, La Ley Federal de Protección de Datos Personales en Posesión de los Particulares establece los principios en el tratamiento de datos personales. Desde una perspectiva ética, las firmas digitales deben garantizar la privacidad y la protección de los datos personales de los usuarios (Hacienda 2022).

En el contexto de Python, existen varias librerías que apoyan la creación de algortimos criptográficos para la protección de datos. Una de estas librerías es cryptography, la cual es útil para la tanto para encriptaciones de alto nivel como interfaces de un nivel más bajo. Esta librería permite la cifrados simétricos, resúmen de mensajes y funciones de derivación de claves. Cryptography se divide en 2 niveles: fácil y primitivos criptográficos. El primer nivel es muy fácil de manejar y no requieren una configuración extensa. En cambio, el segundo nivel suele contener criptográficos peligrosos y que requieren de un mayor conocimiento de criptografía para la toma de decisiones (Cryptography 2025). Por otro lado, también existe la librería PyCryptodome, la cual es eficaz en en algoritmos y funciones criptográficas. Dentro de esta librería podemos encontrar operaciones como encriptación, decriptación, hashing y la verificación de firmas. Para nuestro proyecto, esta librería es de gran útilidad ya que brinda firmas digitales y las verifica a través de algoritmos RSA y DSA (Geeks for geeks 2024). De este modo, se cuida la autentidad e integridad de los mensajes, o en nuestro caso, de los documentos.

4.2. Marco Contextual. El panorama mundial de la migración es complejo, con los crecientes conflictos geopolíticos y las recientes acciones tomadas por el gobierno de los Estados Unidos de América. El flujo migratorio en México se ha convertido en un tema social que requiere soluciones en materia de seguridad, protección de derechos y acceso a recursos básicos. La OIM de la ONU (ONU Migración Americas 2024) comenta que se vuelve obligatorio para las organizaciones contar con una aplicación sistemática de medidas de seguridad que garanticen la integridad, seguridad, autodeterminación y protejan los datos de las personas migrantes. Cada año más de medio millon de migrantes cruzan por México (**oim-mexico-2023**), los cuales dependen de organizaciones, para continuar su trayecto. Durante el registro, procesos internos y salida de los migrantes de dichas organizaciones, se toman tanto datos generales, como sus datos personales, los cuales incluyen información sensible para los inmigrantes. Es por esto que se vuelven relevantes las recomendaciones de la ONU respecto a la protección de los datos.

Casa Monarca, un refugio ubicado en el municipio de Santa Catarina, Nuevo León, es una de las muchas organizaciones que enfrentan esta problemática. Sin un sistema de firma electrónica eficiente, los procesos pueden volverse burocráticos y susceptibles a pérdidas o manipulaciones indebidas, lo que representa un riesgo para la protección de los datos de los beneficiarios. Uno de los riesgos presentes es la suplantación de identidad, en 2024 segun KPMG un 45 porciento de organizaciones enfrento un intento de fraude, donde 44 porciento de ellos estan relacionados en el robo de identidad (**orozco-2024**). Estos delitos no solo afectan a las organizaciones financieramente, sino que dañan su reputación. Lo que puede poner en riesgo la credibilidad de organizaciones que recaen en apoyos economicos internacionales como de donaciones locales.

A través de esta iniciativa, se busca demostrar el enfoque humano de la ciberseguridad, beneficiando a un grupo en condición de vulnerabilidad y promoviendo el uso responsable y seguro de la tecnología en favor de la protección de datos.

4.2.1. Estado del Arte. **4.2.1.1. Sistemas de Firma Digital en Contextos Migratorios**

El tema de la migración se ha vuelto un área importante para la digitalización de procesos, lo que permite mejorar la gestión de documentación y la seguridad de la información. El uso de tecnologías digitales en los procesos migratorios ha sido analizado por diferentes organizaciones internacionales. La Red en Defensa de los Derechos Digitales (R3D) resalta que la digitalización en estos contextos ofrece oportunidades, pero también plantea desafíos de seguridad y privacidad para los migrantes y sus defensores (Sánchez Sánchez y col. 2023). Así mismo, Access Now enfatiza la necesidad de implementar medidas de protección de datos para resguardar la información de los migrantes en América Latina (AccessNow 2023). El Gobierno de Perú ha avanzado en la digitalización de sus servicios consulares para mejorar la atención a sus ciudadanos en el extranjero. Una de las iniciativas destacadas es la implementación del Documento Nacional de Identidad Electrónico (DNIe) en el exterior. Este documento incorpora altos estándares de seguridad y permite a los peruanos residentes fuera del país acceder a servicios consulares de manera eficiente. Los planes piloto se han llevado a acabo en ciudades como Buenos Aires, Miami y Roma. Además, se ha proporcionado firma digital a todos los cónsules para facilitar la realización de servicios y actividades digitales, como la apostilla electrónica y el envío de actas electorales (Relaciones Exteriores de Perú 2022). Paraguay ha adoptado medidas importantes para modernizar su gestión migratoria. En 2015, implementó el Sistema Interconectado de Registro e Identificación de Personas y el Sistema de Información y Análisis de Datos sobre la Migración (PIRS/MIDAS), diseñados para la Organización Internacional para las Migraciones (OIM). Este sistema biométrico de control migratorio y fronterizo ha sido implementado en varios puestos de control del país desde 2016, mejorando la capacidad de registro y control de movimientos migratorios (Santi 2020).

4.2.1.2. Tecnologías Utilizadas en Firmas Digitales

De acuerdo con Kurosawa, la criptografía de curva elíptica (ECC) es una técnica criptográfica que utiliza las propiedades de las curvas elípticas para crear sistemas de cifrado más eficientes y seguros (Kurosawa 1973). Una implementación notable de ECC es EdDSA (Edwards-curve Digital Signature Algorithm), que ofrece firmas digitales de alta seguridad y rendimiento. Ed25519 es una variante popular de EdDSA que utiliza la curva Curve25519 y el hash SHA-512, proporcionando una resistencia comparable a cifrados simétricos de 128 bits. Además, EdDSA está diseñado para ser resistente a ataques de canal lateral, ya que no utiliza operaciones que dependan de datos secretos, lo que mejora su seguridad en implementaciones prácticas. Herramientas Utilizadas en la Práctica (NaCl/libsodium, OpenSSL): • NaCl/libsodium: El usuario jedisct1 muestra un repositorio de GitHub sobre NaCl (Networking and Cryptography Library), el cual es una biblioteca de criptografía diseñada para facilitar la implementación de operaciones criptográficas seguras. Libsodium es bifurcación de NaCl que mejora su protabilidad y usabilidad, proporcionando una amplia gama de funciones criptográficas, incluyendo soporte para ECC y Ed25519 (Jedisct1 s.f.). • OpenSSL: Es una biblioteca de software robusta y de uso general que implementa los protocolos SSL y TLS, así como una variedad de funciones criptográficas. OpenSSL ha incorporado soporte para algoritmos de curva elíptica, incluyendo Ed25519, a partir de su versión 1.1.1, permitiendo a los desarrolladores implementar firmas digitales seguras en sus aplicaciones (Project s.f.).

4.2.1.3. Seguridad en Sistemas de Firma Digital y Ataques de Canal Lateral

Uno de los mayores riesgos en la implementación de sistemas de firma digital son los ataques de canal lateral (SCA). Estos ataques aprovechan información secundaria, como el consumo de energía o el tiempo de ejecución de un algoritmo, para extraer claves privadas o información sensible. De acuerdo con González M. et al (2024) Instituto de Tecnologías Físicas y de la Información (ITEFI) del CSIC ha estudiado cómo los ataques de canal lateral afectan la seguridad del algoritmo AES, proporcionando contramedidas efectivas (González de la Torre y col. 2024). Así también, un estudio de la Universidad Politécnica de Madrid hecho por Buurstra Parmo G. (2023) examina la vulnerabilidad de las curvas elípticas frente ataques de tiempo y plantea soluciones para mitigar estos riesgos (Buurstra Parmo 2023). Otra investigación hecha por Legón M. et al (2016), analiza los ataques de canal lateral en implementaciones criptográficas y resalta diferentes contramedidas, como el enmascaramiento de datos y la introducción de ruido aleatorio en cálculos (Legón y col. 2016).

4.2.1.5. Estudios de Caso en la Implementación de la Firma Digital

Implementación de la Firma Electrónica en el sector bancario de Venezuela.

En Venezuela, la banca electrónica ha integrado la firma digital como una herramienta esencial para garantizar la autenticidad, confidencialidad e integridad de las transacciones electrónicas. A través de sistemas de certificación electrónica los bancos han permitido a los usuarios realizar operaciones seguras, fortaleciendo la confianza en el ciberespacio (Rincón Cárdenas 2004). La adopción de la firma digital en la banca ha traído

consigo importantes beneficios. En primer lugar, la autenticidad de las transacciones está garantizada, lo que reduce considerablemente el riesgo de fraudes financieros. Así también, la confidencialidad de la información se ve reforzada mediante el uso de sistemas de encriptación que protegen los datos sensibles de los clientes. Además, la integridad de la información es asegurada, evitando modificaciones o alteraciones durante la transmisión de datos. A pesar de estos avances, la implementación de la firma digital en el sector bancario venezolano enfrenta grandes desafíos. La necesidad de mantener una infraestructura tecnológica robusta y en constante actualización es uno de los principales retos. Igualmente, se refiere una capacitación continua tanto para el personal bancario como para los usuarios, con el fin de garantizar el uso adecuado y seguro de estas herramientas digitales.

Gobierno Electrónico en México: Implementación de la Firma Electrónica.

México ha avanzado en la digitalización de su administración pública, incorporando la firma electrónica en diversos servicios gubernamentales. Este mecanismo ha permitido mejorar la eficiencia y la transparencia en la gestión pública, facilitando a los ciudadanos la realización de trámites en línea y reduciendo los tiempos y costos al uso de documentos físicos (Gil-García, Mariscal Avilés y Ramírez Hernández 2010). Entre los principales beneficios de la firma digital en el gobierno electrónico destacan la agilización de los procesos administrativos, la reducción de la burocracia y una mayor transparencia en las operaciones gubernamentales. Además, la accesibilidad a los servicios públicos se ha incrementado considerablemente, ya que los ciudadanos pueden realizar sus trámites desde cualquier lugar y en cualquier momento. Sin embargo, aún existen desafíos que limitan su adopción. La brecha digital sigue siendo una barrera importante, ya que no todas las regiones del país cuentan con el acceso a tecnología necesario para utilizar estos servicios. Además, la infraestructura tecnológica debe seguir mejorándose para garantizar la disponibilidad y seguridad de los sistemas de firma digital en la administración pública.

5. Metodologia

El plan de trabajo a seguir fue...

6. Resultados

La solucion desarrollada permitio.

7. Conclusiones

Debido a esto podemos concluir...

8. Recomendaciones

Nosotros recomendamos...

9. References

Referencias

AccessNow (2023). *Protección de datos personales en el contexto migratorio latinoamericano*. AccessNow.org. URL: https://www.accessnow.org/wp-content/uploads/2023/12/PROTECCION-DE-DATOS-PERSONALES-EN-EL-CONTEXTO-MIGRATORIO-LATINOAMERICANO-ACCESS-NOW.pdf.

Arellano, E. (2023). *Contratos con firma digital en México: ¿qué marco legal los valida?* URL: https://www.legaldigital.mx/blog/post/contratos-con-firma-digital-en-mexico-que-marco-legal-los-valida.

Buurstra Parmo, G. (2023). «Ataques de Tiempo a Rutinas Criptográficas sobre Curvas Elípticas». Universidad Politécnica de Madrid. URL: https://oa.upm.es/75495/1/TFG_GABRIELA_BUURSTRA_PARMO.pdf.

Cryptography (2025). *Welcome to pyca/cryptography*. URL: https://cryptography.io/en/latest/.

Fuentes, S. (2023). *Ley de Ciberseguridad en México: Conoce la nueva Ley?* URL: https://www.deltaprotect.com/blog/ley-de-ciberseguridad-mexico.

Geeks for geeks (2024). *What is pycryptodome in Python?* URL: https://www.geeksforgeeks.org/what-is-pycryptodome-in-python/.

Gil-García, J. R., J. Mariscal Avilés y F. Ramírez Hernández (2010). «Gobierno electrónico en México: Antecedentes, objetivos, logros y retos». En: *Buen Gobierno* 8. URL: https://www.redalyc.org/pdf/5696/569660516004.pdf.

González de la Torre, M. Á. y col. (2024). «Ataques por canal lateral contra AES mediante correlación de consumo de potencia». En: *Universidad de Sevilla*. URL: https://idus.us.es/server/api/core/bitstreams/d51cb792-d77a-46a1-ba96-ba39c3b77ffe/content.

Hacienda, Secretaría de (2022). «Principios y deberes en materia de protección de datos personales.» En: *Banco del Bienestar*. URL: https://www.gob.mx/cms/uploads/attachment/file/763381/Principios_y_deberes_en_materia_de_Proteccion_de_Datos_Personales.pdf.

Hernández Encinas, L. (2016). *La criptografía: (1 ed.)* Los libros de la Catarata.

Jedisct1 (s.f.). *ChangeLog [Archivo de registro de cambios]*. GitHub. Recuperado de https://github.com/jedisct1/libsodium/blob/a162c09b69075c467dfa985cd605a80955512c48/ChangeLog.

Kurosawa, K. (1973). *Advances in Cryptology – ASIACRYPT 2007*. Springer.

Legón, C. M. y col. (2016). «Side Channel attacks: a real threat to cryptographic algorithms implementations. Ataques de canal colateral: Una amenaza real a las implementaciones de algoritmos criptográficos». En: Recuperado de https://www.researchgate.net/publication/330102388_Side_Channel_attacks_a_real_threat_to_cryptographic_algorithms_implementations_Ataques_de_canal_colateral_Una_amenaza_real_a_las_implementaciones_de_algoritmos_criptograficos.

ONU Migración Americas (2024). *7 recomendaciones para la protección de datos personales*. URL: https://lac.iom.int/es/blogs/7-recomendaciones-para-la-proteccion-de-datos-personales-de-personas-migrantes-en-albergues.

Project, OpenSSL (s.f.). *EVP_SIGNATURE-ED25519 [Documentación técnica]*. OpenSSL. Recuperado de https://docs.openssl.org/master/man7/EVP_SIGNATURE-ED25519/.

Relaciones Exteriores de Perú, Ministerio de (2022). *Informe País sobre la implementación del Pacto Mundial para la Migración Segura, Ordenada y Regular en América Latina y el Caribe*. Migrationnetwork.un.org. URL: https://migrationnetwork.un.org/system/files/docs/Peru%20-%20GCM%20review%202022%20(Spanish).pdf.

Rincón Cárdenas, E. (2004). «Últimos retos para el derecho privado: las nuevas tecnologías de la información». En: *Revista Estudios Socio-Jurídicos* 6.2, pp. 430-500. URL: https://www.redalyc.org/pdf/733/73360215.pdf.

Sánchez Sánchez, C. y col. (2023). *Uso de las tecnologías digitales en los contextos migratorios: necesidades, oportunidades y riesgos para el ejercicio de los derechos humanos de las personas migrantes, defensoras y periodistas*. R3d.mx. URL: https://r3d.mx/wp-content/uploads/Informe-_-Uso-de-las-tecnologias-digitales-en-los-contextos-migratorios-_-Necesidades-oportunidades-y-riesgos-para-el-ejercicio-de-los-derechos-humanos-de-las-personas-migrantes-defensoras-y-periodistas-R3D.pdf.

Santi, S. (2020). «La nueva política migratoria de Paraguay: derechos humanos y seguridad como pilares para el tratamiento político de la inmigración». En: *Estudios de Derecho* 77.169. DOI: 10.17533/udea.esde.v77n169a09.