

Instituto Tecnológico y de Estudios Superiores de Monterrey

Casa Monarca Ayuda Humanitaria al Migrante A.B.P.

Uso de álgebras modernas para seguridad y criptografía (Gpo 603)

Reto. *Firmas solidarias: Tecnología criptográfica para los derechos humanos.*

Challenge. *Solidary signatures: Cryptography technology for human rights.*

Profesores:

Luis Miguel Méndez Díaz

Raúl Gómez Muñoz

Integrantes:

Andrea Renata Garfías Núñez A01369860

Luis Roberto Garza Sánchez A00836982

Carol Jatziry Rendon Guerrero A01425341

Rolando Ruiz Martínez A00835733

Maritza Barrios Macías A00836821

11 de junio de 2025

Índice

1. Resumen	1
2. Introducción	2
3. Marco referencial	3
4. Metodología	6
5. Resultados	9
6. Conclusiones	14
7. Recomendaciones	15
8. Anexos	19
Github	19
Flujos en Power Apps	19

1. Resumen

El presente trabajo se centra en el desarrollo e implementación de una interfaz segura y confiable para la gestión de firmas digitales, utilizando herramientas como Power Apps, Power Automate y funciones de Azure. A través del uso de la biblioteca *Cryptography* de Python y el protocolo criptográfico RSA, los documentos son codificados y firmados digitalmente, garantizando su integridad y autenticidad. El objetivo principal de este sistema es agilizar los procesos administrativos de la organización, permitiéndole concentrarse en su labor humanitaria con personas migrantes. Como resultado, se logró un sistema funcional que permite el procesamiento y la verificación eficiente de documentos firmados digitalmente por múltiples usuarios. Para futuras mejoras, se recomienda la implementación de mecanismos de autenticación multifactor (MFA) y cierres automáticos de sesión tras periodos de inactividad, con el fin de reforzar la seguridad y minimizar la exposición a riesgos de acceso no autorizado.

This work focuses on the development and implementation of a secure and reliable interface for managing digital signatures, using tools such as Power Apps, Power Automate, and Azure functions. Through the use of the *Cryptography* Python library and the RSA cryptographic protocol, documents are securely encoded and digitally signed, ensuring their integrity and authenticity. The main objective of this system is to streamline the organization's administrative processes, allowing it to focus more effectively on its humanitarian work with migrants. As a result, a functional system was achieved that enables the efficient processing and verification of digitally signed documents by multiple users. For future improvements, it is recommended to implement multi-factor authentication (MFA) and automatic session timeouts after periods of inactivity, in order to strengthen security and minimize exposure to unauthorized access risks.

2. Introducción

En la era digital, la seguridad de la información representa un desafío crucial, especialmente en el manejo de documentos electrónicos con validez legal. La firma digital garantiza la autenticidad e integridad de estos archivos, previniendo fraudes, falsificaciones y modificaciones no autorizadas. Su implementación es esencial en sectores donde la certificación de identidad y la validez documental son fundamentales.

Ante este panorama, resulta fundamental desarrollar un sistema confiable de firma digital adaptado a las necesidades de la organización social Casa Monarca, dedicada al apoyo de personas migrantes. Este tipo de instituciones enfrenta procesos administrativos que, con frecuencia, son tardados e ineficientes, lo que limita el tiempo disponible para brindar atención directa. Además, la ausencia de mecanismos seguros de validación documental puede poner en riesgo los derechos de las personas migrantes, ocasionar problemas legales y aumentar su vulnerabilidad ante fraudes.

Como solución, este trabajo propone el desarrollo de una interfaz en Power Apps que permita la firma digital de múltiples documentos desde un mismo entorno, de forma rápida y sencilla. Esta propuesta requiere un enfoque técnico sólido que combine principios de criptografía avanzada y conceptos de matemática abstracta. Asimismo, la optimización de recursos y la velocidad de procesamiento son clave para garantizar un sistema funcional y seguro.

Más allá de su impacto tecnológico, esta iniciativa representa una aportación significativa a la protección de los derechos humanos y al fortalecimiento de la confianza en los entornos digitales, al mejorar la seguridad documental en contextos de alta vulnerabilidad.

3. Marco referencial

Las firmas electrónicas se han vuelto esenciales en el entorno digital actual, ya que permiten validar la identidad de los firmantes y asegurar la integridad de documentos electrónicos (Tosca y Vidal, 2023). Existen dos tipos principales: la firma electrónica, que asocia datos del firmante como dirección IP, correo o número de móvil sin certificar completamente su identidad (Adobe Latinoamérica, 2022), y la firma digital, que emplea criptografía y certificados digitales emitidos por entidades certificadoras para garantizar autenticidad e integridad (Adobe Latinoamérica, 2022).

En Latinoamérica, ambas modalidades poseen validez jurídica, aunque la firma digital ofrece un nivel de autenticación más robusto desde el momento de la firma (Adobe Latinoamérica, 2022). México ha adoptado los principios de la Ley Modelo de Firmas Electrónicas de la CNUDMI en estados como Guanajuato, Sonora, Chiapas, Jalisco e Hidalgo, desarrollando leyes específicas que regulan el uso de la firma electrónica avanzada y establecen el rol de los prestadores de servicios de certificación (CNUDMI, s.f.). Asimismo, la Ley Modelo de Comercio Electrónico de la CNUDMI facilita la adopción de tecnologías mediante principios y procedimientos regulados (CNUDMI, s.f.).

Para garantizar estándares de uso, el gobierno mexicano promulgó la NOM-151-SCFI-2016, que define las condiciones para la conservación de mensajes de datos en documentos electrónicos y los requisitos de digitalización de documentos físicos en procesos empresariales (DocuSign, 2025). En cuanto a proveedores de soluciones, DocuSign es reconocida legalmente en México para certificar que “un documento electrónico fue remitido y aceptado por todos los intervinientes” (DocuSign, 2022), mientras que Viafirma, fundada en Sevilla en 2000, ofrece autenticación basada en certificados digitales y firma biométrica, con más de 5 000 puntos de atención en Colombia y acreditación como prestador cualificado de servicios electrónicos de confianza en Europa desde 2019 (Poveda, 2025).

Funcionamiento de las firmas digitales

Una de las distintas formas de crear una firma digital para verificar la integridad de un documento consiste en utilizar el algoritmo propuesto en la Figura 1. De manera general, este procedimiento se basa en obtener el hash del documento a firmar, encriptar el resultado con una llave criptográfica privada del firmante y transmitir el documento original con este resultado (la firma obtenida) por separado. La verificación se basa entonces en calcular nuevamente el hash del documento recibido y descryptar la firma digital con la llave pública del firmante; si ambos hashes coinciden, entonces es posible asegurar que fue el firmante el que emitió el documento y que, además, este no ha sido alterado en un paso intermedio de la comunicación al receptor.

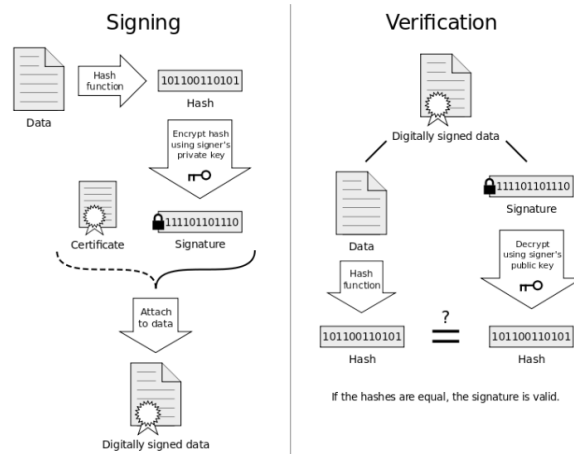


Figura 1: Proceso de firma y verificación de un documento con firma digital

La generación del par de llaves pública-privada es llevada a cabo usualmente mediante el algoritmo RSA basado en el problema de la factorización de enteros, el cual es computacionalmente costoso cuando los primos son lo suficientemente grandes (Cao y Fu, 2008). Alternativa y más recientemente se ha propuesto la utilización de algoritmos basados en curvas elípticas, los cuales proporcionan la misma seguridad de encriptación con una menor longitud de llaves y una mayor velocidad computacional de obtención (Koblitz et al., 2000).

De esta forma, el estado del arte de las firmas digitales mediante versiones ajustadas del algoritmo RSA y de curvas elípticas demuestra que es posible utilizarlas a gran escala en sistemas como estructuras blockchain para mantener un historial íntegro de transacciones entre usuarios con un costo computacionalmente bajo (Fang et al., 2020).

Algoritmos de encriptación

El algoritmo RSA, denominado así por sus creadores Rivest, Shamir y Adleman (1977), es un algoritmo criptográfico de tipo asimétrico. Esto significa que emplea un par de claves: una clave pública y una clave privada. La clave pública, accesible para cualquier usuario, se utiliza para cifrar la información, mientras que la clave privada, conocida únicamente por el receptor autorizado, se emplea para descifrar el mensaje.

El funcionamiento del algoritmo se puede dividir en tres etapas principales:

- **Generación de claves:** consiste en la creación del par de claves (pública y privada) mediante la selección de números primos grandes y la aplicación de funciones matemáticas específicas.
- **Cifrado:** el remitente (emisor) cifra el mensaje utilizando la clave pública del destinatario.
- **Descifrado:** el destinatario emplea su clave privada para recuperar el mensaje original a partir del texto cifrado. (GeeksforGeeks, 2017)

Actualmente, diversos sistemas implementan el algoritmo RSA, tales como OpenSSL, cryptlib, wolfCrypt y otras bibliotecas criptográficas. Asimismo, RSA se emplea ampliamente en navegadores web, sistemas de correo electrónico, redes privadas virtuales (VPN) y otros canales de comunicación segura. (Veritas, s.f.)

Funciones hash criptográficas

El algoritmo SHA-256 (Secure Hash Algorithm 256 bits) pertenece a la familia de funciones hash criptográficas SHA-2, desarrolladas por la Agencia de Seguridad Nacional (NSA)

de los Estados Unidos y publicadas por el Instituto Nacional de Estándares y Tecnología (NIST) en 2001. Su propósito es transformar cualquier mensaje de entrada, independientemente de su longitud, en una cadena única y fija de 256 bits (32 bytes), conocida como hash o resumen criptográfico.

El funcionamiento de SHA-256 consiste, a grandes rasgos, en convertir el mensaje original a su representación binaria, dividirlo en bloques y someter estos bloques a una serie de operaciones lógicas. Cada bloque contiene 64 palabras de 32 bits, y a través de múltiples rondas, se aplican funciones como XOR (OR exclusivo), rotaciones, sumas modulares, mezclas y combinaciones con valores constantes predeterminados. Estas operaciones se diseñan de forma que cada pequeña modificación en la entrada provoque un cambio drástico en la salida, una propiedad conocida como efecto avalancha.

Durante este proceso, el resultado de cada bloque se combina con el siguiente, repitiendo el mecanismo hasta procesar todo el mensaje. El resultado final es una cadena hexadecimal aparentemente aleatoria pero fija: es decir, la misma entrada siempre producirá el mismo hash, aunque no es posible revertir el proceso para obtener el mensaje original a partir del hash, lo que garantiza su irreversibilidad (Alvy, 2022).

Si bien podría parecer aleatorio, cualquier cambio genera una secuencia diferente. Debido a ello, SHA-256 es ampliamente utilizado en aplicaciones que requieren integridad de la información, como la firma digital, la verificación de contraseñas y la tecnología blockchain.

4. Metodología

Para el desarrollo de la solución, se utilizaron herramientas de Microsoft como Azure, Power Automate y Power Apps. Con ello, se diseñó un flujo en Power Automate que invoca funciones alojadas en Azure, el cual se integró con Power Apps para permitir su visualización y ejecución desde una interfaz accesible para el usuario.

El primer paso fue identificar las necesidades específicas en las que se trabajaría. Con ello, se optó por el desarrollo de una interfaz amigable que permitiera subir y firmar documentos de manera rápida, sencilla y segura.

Para el desarrollo de la arquitectura del sistema, se emplearon las siguientes herramientas de Microsoft 365: 1) Power Apps como interfaz gráfica para el ingreso de datos por parte del personal, 2) Power Automate para la automatización del flujo de trabajo, 3) SharePoint como repositorio de almacenamiento de documentos y metadatos y 4) conectores HTTP para el consumo de servicios de firma digital o APIs de terceros.

Para la construcción del flujo se utilizó Power Automate, en donde se implementaron cinco flujos principales (Consulte Anexos - Figuras 14-18). Cabe destacar que Power Automate funciona simplemente como un vínculo, ya que Azure es quien realmente tiene las funciones disponibles. El primero, LaunchUser, se encarga de registrar a cada usuario. Para ello, genera un ID de usuario único a partir de su cadena usando SHA256. Posteriormente, revisa si el usuario ya existe en la tabla, en caso de que no, genera un par de claves RSA (privada y pública) para ese usuario. Finalmente, guarda al usuario y sus claves en Azure Table. A continuación, la figura 2 muestra el flujo esperado tras la creación de un nuevo usuario.

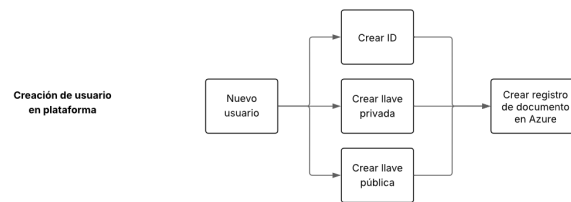


Figura 2: Flujo de LaunchUser

El segundo, Upload & Sign, permite subir un documento y registrar a los usuarios que deben firmar. Para lograrlo, primero convierte el Base64 en bytes (decode) y genera un hash SHA256 del PDF. Luego, revisa si el documento ya fue cargado anteriormente. Además,

recupera información de usuarios (claves, ID, etc.). Después, firma el PDF con la clave privada del creador de la solicitud. Finalmente, guarda la solicitud de firma en la tabla files. El tercero, SendNotification, se encarga de notificar a los usuarios requeridos mediante un correo, informándoles que tienen un documento nuevo pendiente por firmar (Figura 3).

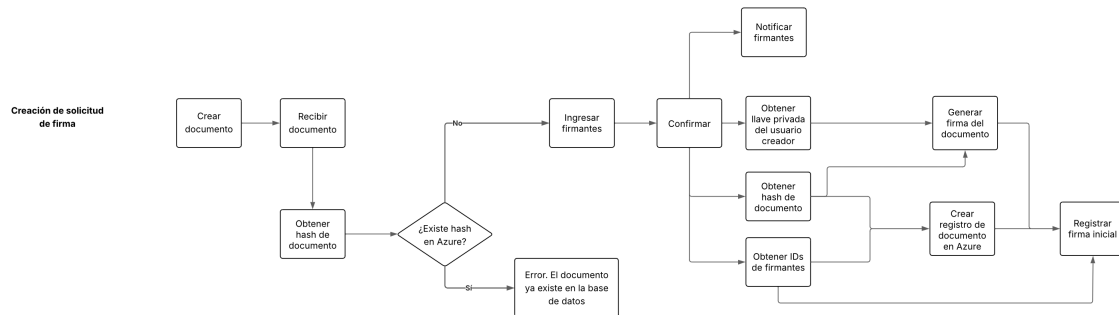


Figura 3: Flujo de Upload & Sign

El cuarto, SignDocument, firma un documento que ya fue previamente cargado. Para ello, recupera el registro de un documento (firmantes, firmas) y posteriormente actualiza las firmas del documento (Figura 8).

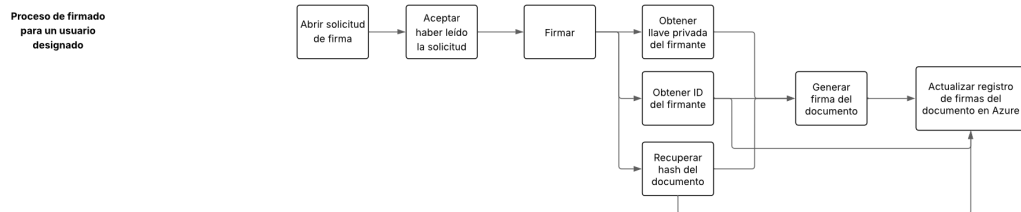


Figura 4: Flujo de SignDocument

Finalmente, el quinto, VerifyDocument, verifica si un documento ya fue totalmente firmado y si todas sus firmas son válidas. (Figura 5).

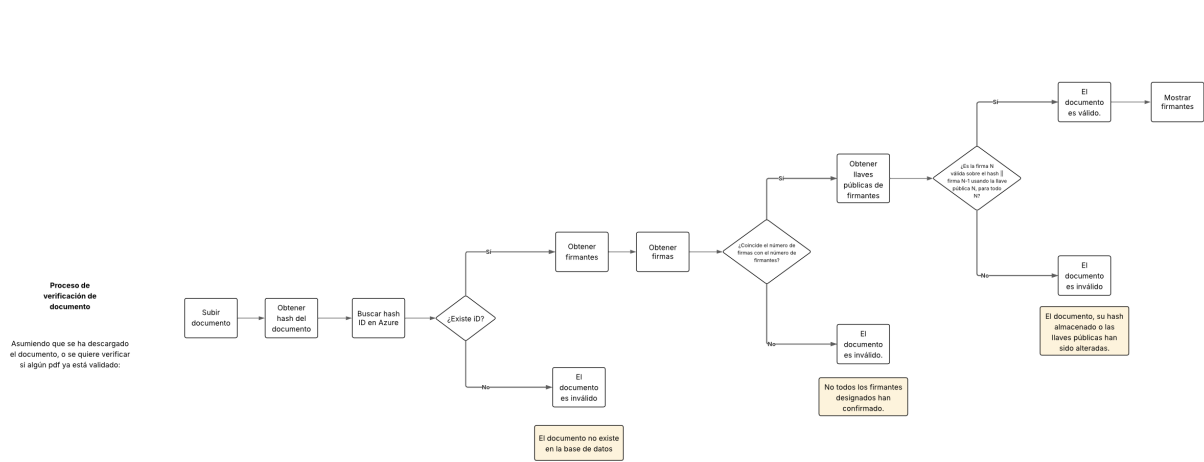


Figura 5: Flujo de VerifyDocument

Finalmente, se llevó a cabo una etapa de pruebas para validar el correcto funcionamiento del flujo automatizado, asegurando que cada acción se ejecutara en el momento adecuado. Entre estas acciones, se verificó específicamente el proceso de generación del hash mediante el algoritmo SHA-256, garantizando que cada documento produjera un valor único e irrepetible. Asimismo, se realizaron pruebas de integridad y validación de firma digital utilizando el algoritmo RSA, con el fin de confirmar que los documentos no hubieran sido modificados tras su firma.

5. Resultados

Como resultado de este proyecto, se obtuvo una interfaz integrada en Power Apps, intuitiva, fácil de manejar y automática. A continuación, se muestra el mensaje de bienvenida que se despliega al entrar a la plataforma (Figura 6).

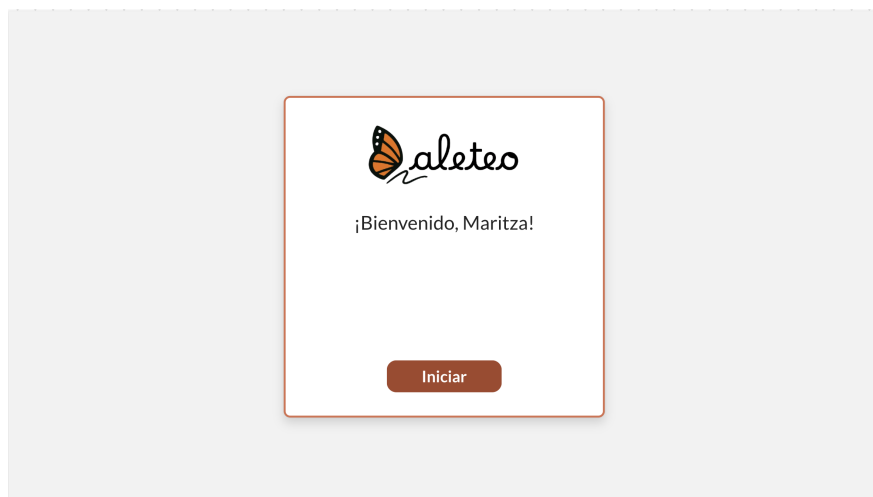


Figura 6: Mensaje de bienvenida

La figura 7 muestra la pantalla de inicio, en donde aparecen dos filtros que permiten buscar documentos por nombre y por departamento. Además, se despliegan todos los documentos para los cuales es requerida la firma del usuario, con su respectivo nombre, departamento y autor (es decir, la persona que solicita las firmas).

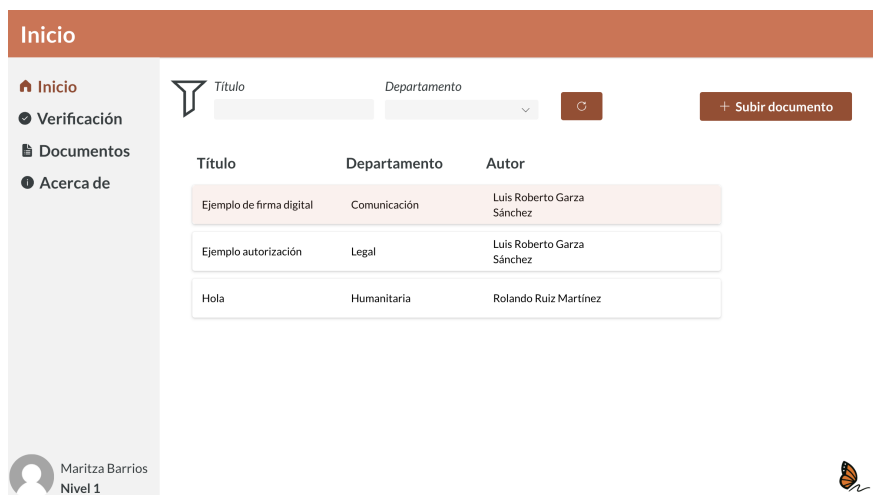


Figura 7: Página de inicio

Al dar click en cualquiera de estos documentos, aparece una nueva pestaña en donde se obtiene una vista previa del documento a firmar, así como una cláusula de aceptación que

es necesaria de oprimir para firmar el documento (Figura 8).

Firmar documento

Vista previa

27/03/21, 15:48 A.M. Correo: Daniel Ivan Laveriega - Outlook

Outlook

RE: Ejemplo Cotización Papelería Abril 2024_Folders / Legajo

Desde: Daniel Ivan Laveriega <comunicacion_sistemas@casamontana.org.mx>
Fecha: Jue 25/03/2023 15:44
Para: Daniel Ivan Laveriega <comunicacion_sistemas@casamontana.org.mx>

De: Natalia Lleras <natalia@casamontana.org.mx>
Enviado: miércoles, 15 de mayo de 2023 a las 20:40
Para: Comisaría <comisaria@casamontana.org.mx>
Cc: Lili Zúñiga <direccion@casamontana.org.mx>; Ivan Laveriega <administracion@casamontana.org.mx>
Asunto: RE: Cotización Papelería Abril 2024_Folders / Legajo

Buen día, estimado:
Autorizado
Comparto comprobante
(se adjunta pdf con el comprobante)
Saludos

☐ Declaro que he leído y comprendido el contenido del presente documento, y manifiesto mi conformidad con los términos establecidos.

Firmar

Volver

Figura 8: Firma de documento

Sumado a ello, aparece la opción de subir documento, que permite subir un nuevo documento y poner sus especificaciones, lo cual incluye su nombre, el departamento, adjuntar el archivo correspondiente y seleccionar a los firmantes requeridos (Figura 9).

Nuevo documento

Volver

* Nombre del documento

* Departamento

* Archivo

There is nothing attached.
 Attach file

Selecciona uno o varios firmantes

	Rolando Ruiz Martinez	A00835733@tec.mx	IT
	Luis Roberto Garza Sánchez	A00836982@tec.mx	IT
	Carol Jatziry Rendon Guerrero	A01425341@tec.mx	IT
	Andrea Renata Garfias Nuñez	A01369860@tec.mx	IT

Firmante(s) seleccionado(s)

Subir

Figura 9: Upload de documento

Tras este proceso, llega un correo de notificación a los usuarios que necesitan introducir su firma. La figura 13 muestra un ejemplo de la estructura del correo.

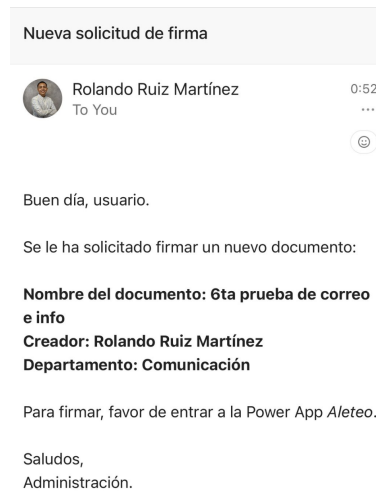


Figura 10: Correo de notificación al usuario

Otra pestaña disponible en la plataforma es *Documentos*, la cual permite ver el progreso de firmas, indicando cuántos usuarios han firmado. Cabe mencionar que esta sección es un privilegio exclusivo de usuarios *Nivel 1*, es decir, de administradores. Esto con el objetivo de que puedan conocer en tiempo real el estatus de cada documento y que tengan conocimiento de todos los movimientos que están siendo realizados en tiempo real.

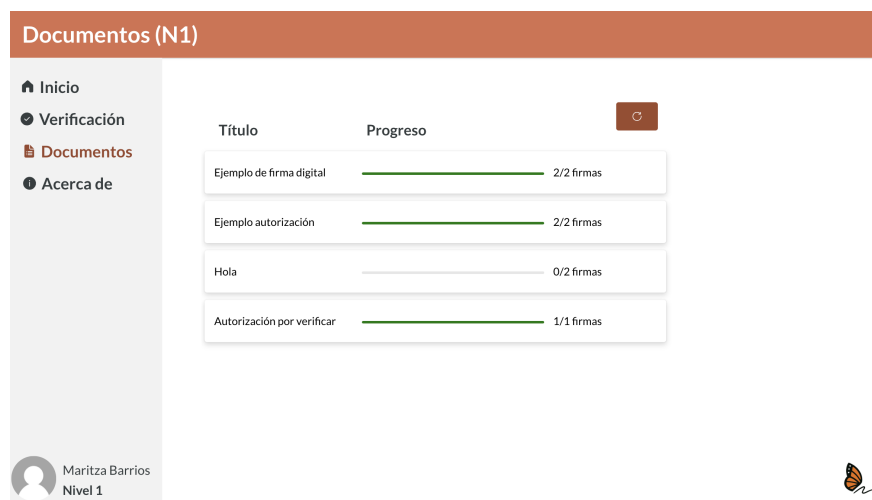


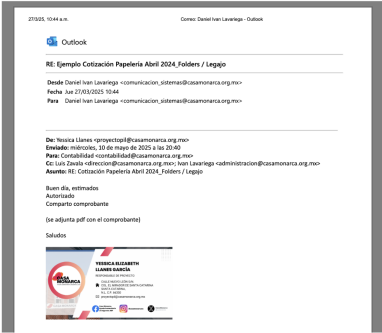
Figura 11: Progreso de documentos

Adicionalmente, si se presiona en cada uno de estos progresos, es posible conocer la fecha

y hora en la que se subió el documento, los firmantes, y si estos ya firmaron el documento. Todo esto adicional a las características generales del documento, lo cual incluye su nombre, departamento y autor, así como su visualización previa. Finalmente, se encuentra habilitado un botón para descargar el documento. En la siguiente figura se muestra una visualización de lo previamente descrito.

Información del documento

Vista previa



← Volver

Nombre del documento:
Ejemplo autorización

Departamento:
Legal

Creado por:
Luis Roberto Garza Sánchez

Fecha y hora de creación:
6/10/2025 2:24 AM

Firmante(s)	Firmado
Rolando Ruiz Martinez	6/10/2025 4:02 PM
Maritza Barrios Macias	6/10/2025 8:32 PM

Descargar

Figura 12: Estatus de documento

Por último, se encuentra la pestaña de *Verificación*, en la que es posible subir cualquier documento para verificar si este ya fue firmado por todos los usuarios solicitados y si estas firmas son válidas. En caso de que todo sea congruente, el documento aparece como *Verificado*, de lo contrario, aparece como *No verificado*, ya sea porque el documento no se encuentra en la base de Azure (nunca ha sido subido anteriormente para su firmado o ha sido alterado), porque no ha sido firmado por todos los usuarios requeridos o bien, porque las firmas han sido modificadas o no son íntegras.

13

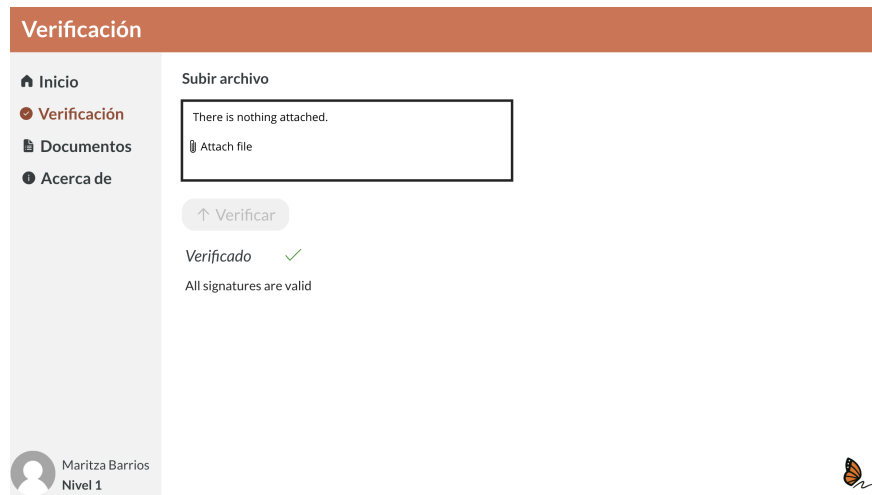


Figura 13: Verificación de documento

6. Conclusiones

Este reto permitió eficientizar procesos administrativos que suelen ser largos y tardados, lo cual es de gran valor para una organización social como Casa Monarca, donde su principal objetivo es ofrecer un trato más humanitario a los migrantes, quienes se enfrentan a situaciones adversas durante su proceso y adaptación. Por ello, es de vital importancia el recordar hacia quién va dirigido el proyecto y con qué objetivo se realiza cada parte del proyecto.

Como características principales de la plataforma, se destaca que sea multifirma, es decir, permite firmar múltiples documentos desde un mismo lugar, de forma rápida y eficiente. Además, para los administradores (*Nivel 1*) incluye un indicador de progreso, que permite visualizar el progreso y la evolución de los documentos pendientes de firma. Sumado a ello, permite subir documentos con gran facilidad y compartirlos a usuarios sin la necesidad de registrarlos manualmente. Otro beneficio de la plataforma es la facilidad para notificar a los usuarios requeridos para firmar mediante un correo base adaptado a las características propias del documento y al solicitante. Finalmente, otro feature relevante se relaciona con el proceso de verificación, ya que la interfaz permite verificar el estado del documento, no

solo comprobando si ya existe, sino también si este cuenta con las firmas requeridas y si son válidas.

El impacto social de esta propuesta se centra en el desarrollo de una plataforma más inclusiva, la cual permita que personas con distintas capacidades accedan y gestionen sus documentos sin barreras, gracias a una interfaz intuitiva y accesible. Esto promueve la equidad digital y garantiza que nadie quede excluido de trámites importantes. Aunado a ello, favorece la transparencia y trazabilidad, ya que permite seguimiento en tiempo real y contar con registros digitales, los cuales fortalecen la confianza en estos procesos. Todo esto asegura que cada acción quede documentada y sea verificable, tanto para los usuarios como para las organizaciones. Así mismo, mejora la eficiencia en organizaciones sociales, ya que reduce la carga administrativa, permitiendo que más tiempo y recursos se enfoquen en la atención directa a las personas migrantes, mejorando así el impacto y alcance de la labor social. Finalmente, contribuye al proceso de digitalización segura al protege la información personal y legal mediante mecanismos digitales confiables y con acceso controlado, evitando pérdidas o mal uso de documentos sensibles.

Se concluye reconociendo la escalabilidad del proyecto, y como este puede ser aplicado a otros procesos, ampliado sin un costo adicional significativo al ser desarrollado con herramientas a las cuales ya se tiene acceso, y ser implementado rápidamente en otras sedes.

7. Recomendaciones

Para reforzar la seguridad y garantizar la confiabilidad del sistema de gestión y verificación documental desarrollado para Casa Monarca, se proponen algunas recomendaciones para la ampliación y mejora del proyecto.

Actualmente, se recomienda limitar el uso del sistema a documentos internos, con el objetivo de evaluar y validar tanto su funcionalidad como su nivel de seguridad en un entorno

controlado. Una vez que se implementen las mejoras propuestas en esta sección, será posible ampliar el uso del sistema para incluir documentos legales y datos sensibles, garantizando así un nivel de protección adecuado para la información crítica de la organización.

En primer lugar, se sugiere la implementación de autenticación multifactor (MFA), ya que la autenticación únicamente mediante usuario y contraseña puede no ser suficiente para prevenir accesos no autorizados, especialmente en casos de robo de credenciales o dispositivos comprometidos. La autenticación multifactor permitiría agregar una capa adicional de verificación de identidad, utilizando códigos temporales (OTP) enviados al celular del usuario, aplicaciones de autenticación como Google Authenticator o Microsoft Authenticator, o preguntas de seguridad dinámicas en sesiones prolongadas. También se podría considerar la integración con servicios como Azure Active Directory para aprovechar sus mecanismos avanzados de verificación y control de acceso.

Además, se recomienda implementar cierres de sesión automáticos tras cierto periodo de inactividad. Una sesión abierta y sin supervisión representa un riesgo considerable, ya que alguien externo podría tener acceso a documentos sensibles de la organización si el usuario no ha cerrado su sesión manualmente. Este cierre automático podría configurarse para activarse después de 10 o 15 minutos de inactividad, con una advertencia previa para permitir al usuario prolongar su sesión si aún está activo.

Otra recomendación importante es habilitar notificaciones o alertas en caso de comportamientos sospechosos, como intentos de acceso desde ubicaciones inusuales, dispositivos desconocidos o múltiples intentos fallidos de inicio de sesión en un corto periodo. Este tipo de mecanismos permite detectar a tiempo posibles intrusiones y tomar medidas preventivas.

También se propone fomentar una cultura de seguridad digital dentro de la organización. Esto implica capacitar periódicamente al personal sobre buenas prácticas, tales como el uso de contraseñas seguras, la importancia de cerrar sesión al dejar el equipo sin supervisión, y cómo identificar posibles intentos de suplantación de identidad a través de correos o enlaces

maliciosos. La concientización es una herramienta clave para reducir los riesgos de seguridad humana, que suelen ser el eslabón más débil en cualquier sistema.

Finalmente, en etapas más avanzadas del proyecto, podría evaluarse la posibilidad de incorporar mecanismos de autenticación mediante biometría o el uso de tokens físicos (como llaves de seguridad USB tipo YubiKey), especialmente para usuarios con permisos privilegiados o acceso a información altamente confidencial.

Estas recomendaciones buscan no solo fortalecer la protección de los documentos que maneja la organización, sino también incrementar la confianza de los usuarios al utilizar la plataforma, ofreciendo garantías de que su información se encuentra adecuadamente resguardada frente a posibles amenazas.

Referencias

- Adobe Latinoamérica. (2022). Diferencias entre firma digital y firma electrónica. <https://blog.adobe.com/es/publish/2022/05/26/existe-alguna-diferencia-entre-firma-digital-y-firma-electronica>
- Alvy. (2022). El algoritmo SHA-256 explicado y visualizado paso a paso, bit a bit.
- Cao, Y., & Fu, C. (2008). An Efficient Implementation of RSA Digital Signature Algorithm. 2, 100-103. <https://doi.org/10.1109/ICICTA.2008.398>
- CNUDMI. (s.f.). Ley Modelo de la CNUDMI sobre Comercio Electrónico (1996) con su nuevo artículo 5 bis aprobado en 1998 [s.f.].
- DocuSign. (2022). La validez jurídica de la firma electrónica en México.
- DocuSign. (2025). NOM 151: qué es y cómo se relaciona con las firmas electrónicas.
- Fang, W., Chen, W., Zhang, W., Pei, J., Gao, W., & Wang, G. (2020). Digital signature scheme for information non-repudiation in blockchain: a state of the art review. <https://doi.org/10.1186/s13638-020-01665-w>
- GeeksforGeeks. (2017). Algoritmo RSA en criptografía [22 de abril].
- Koblitz, N., Menezes, A., & Vanstone, S. (2000). The State of Elliptic Curve Cryptography. Designs, Codes and Cryptography, 19, 173-193.
- Poveda, J. (2025). 500 millones de firmas digitales en 20 países y 4 millones de facturación [20 de febrero]. El Economista. <https://link.gale.com/apps/doc/A828240970/IFME?u=itesmgic&sid=ebsco&xid=3b5085eb>.
- Tosca, C., & Vidal, J. (2023). Impacto de la firma electrónica (E.FIRMA) dentro de la sociedad. UTAP, 2(1). <https://revistap.ejeutap.edu.co/index.php/utap/article/view/68>.
- Veritas. (s.f.). ¿Qué es el cifrado RSA y cómo se compara con otros métodos de cifrado?

8. Anexos

Github

<https://github.com/maritzabmm/RetoCripto>

Flujos en Power Apps

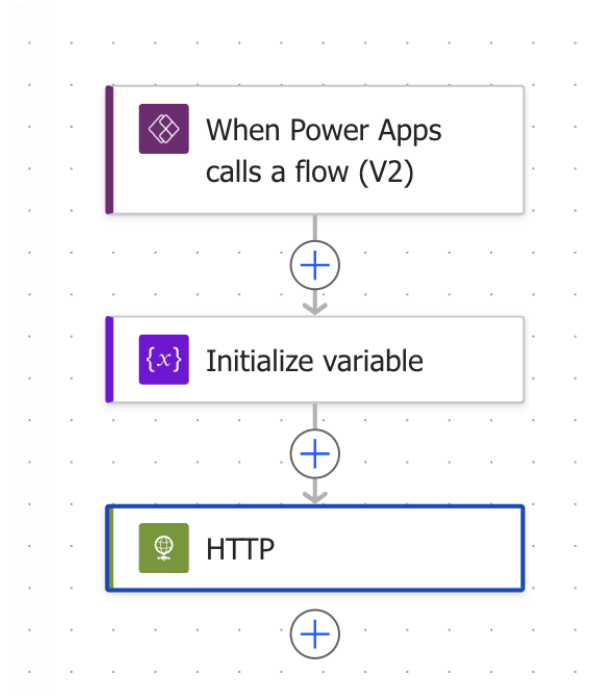


Figura 14: Flujo de LaunchUser

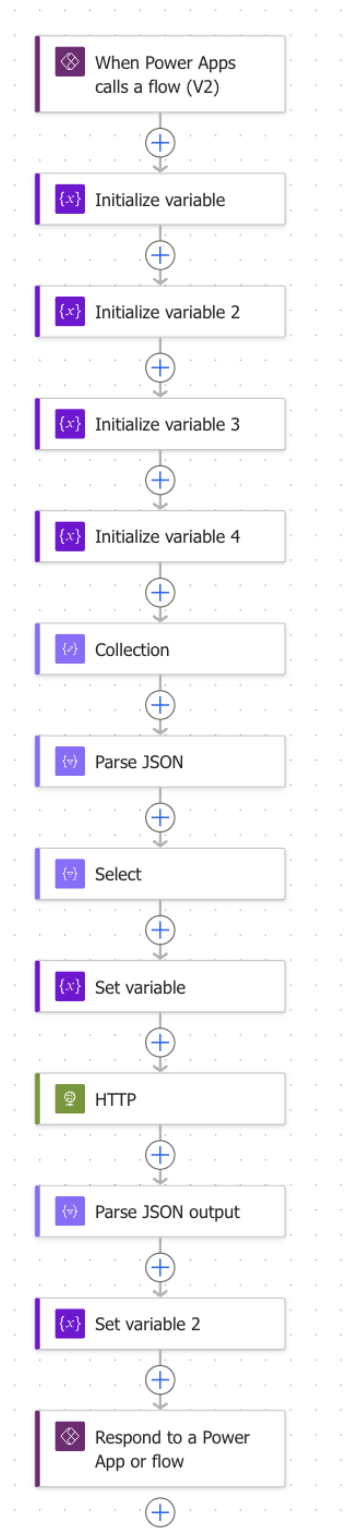


Figura 15: Flujo de Upload & Sign

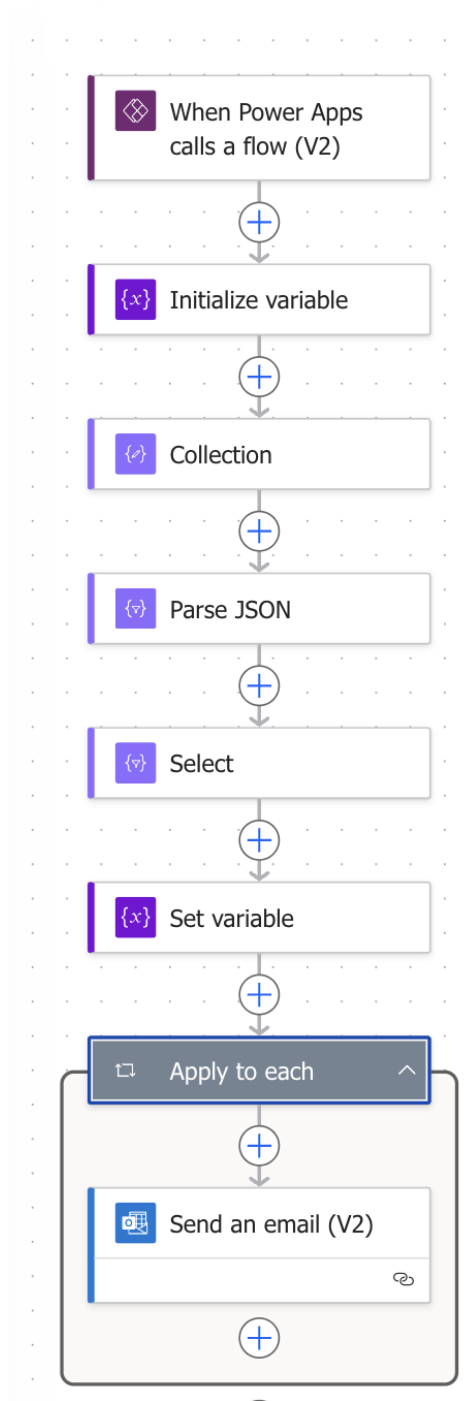


Figura 16: Flujo de SendNotification

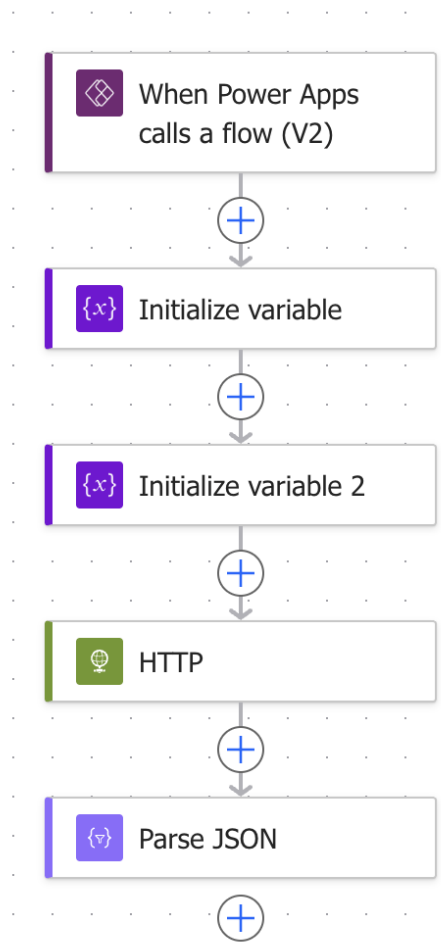


Figura 17: Flujo de SignDocument

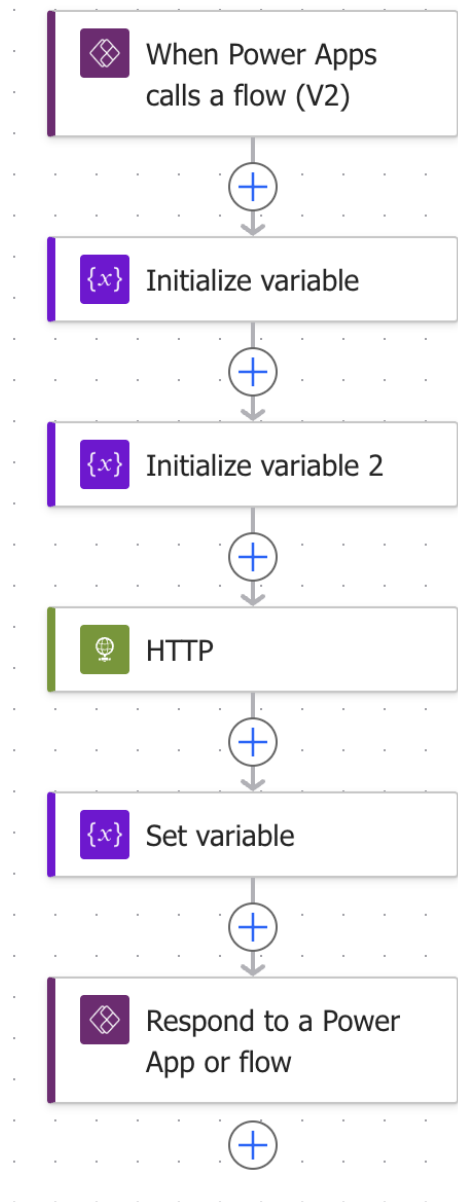


Figura 18: Flujo de VerifyDocument