Instituto Tecnológico y de Estudios Superiores de Monterrey

Grupo 603 - Uso de álgebras modernas para seguridad y criptografía

Semestre Febrero - Junio 2025

Reporte Técnico: Flujo Automatizado
Technical Report: Automated Flow

Alumnos

Rodrigo Leal Torres	A00836930
Máximo Caballero Vargas	A01571607
Pablo Pérez Sandoval	A01710355
Valeria Cárdenas Rodríguez	A01721814
Juan Pablo Guzmán Segura	A01039810

Docentes

Luis Miguel Méndez Díaz
Raúl Gómez Muñoz
Daniel Otero Fadul

11 de junio de 2025, Monterrey, N.L.

Documentación adicional:
https://drive.google.com/drive/folders/1Hsu_K-kP4i8h91VcZmvdIDaeczMuuJIF?usp=sharing

Índice

Resumen

Español

Este proyecto propone el diseño e implementación de un sistema de firma digital sencillo, seguro y eficiente para Casa Monarca, organización que brinda apoyo a personas migrantes y refugiadas. Actualmente, los documentos oficiales que emite la organización pasan por un proceso informal de validación, exponiendo la información a riesgos de manipulación, pérdida de integridad y falta de autenticidad en la aprobación. Por consiguiente, se propone establecer un flujo formal de revisión y firma digital, donde cada persona involucrada pueda aprobar o rechazar documentos de manera controlada, así como firmarlos cuando sea necesario para garantizar su validez. Además, se contempla el almacenamiento de los documentos firmados en una base de datos protegida. Esta iniciativa contribuirá a fortalecer la seguridad de documentos, proteger los derechos de las personas migrantes y mejorar la confianza en la gestión administrativa de Casa Monarca, alineándose con el ODS 9.

English

This project proposes the design and implementation of a simple, secure and efficient digital signature system for Casa Monarca, an organization that provides support to migrants and refugees. Currently, the official documents issued by the organization go through an informal validation process, exposing the information to risks of manipulation, loss of integrity and lack of authenticity in the approval. Therefore, the proposal consists of establishing a formal review and digital signature flow, where each person involved can approve or reject documents in a controlled manner, as well as sign them when necessary to ensure their validity. In addition, the signed documents will be stored in a protected database. This initiative will help strengthen document security, protect the rights of migrants, and improve trust in the administrative management of Casa Monarca, in line with SDG 9.

Introducción

En Casa Monarca, un documento es más que un archivo o un papel; es una prueba de identidad y pertenencia. Para las personas migrantes, cuya vida y futuro dependen muchas veces de un solo documento, la falsificación o manipulación de estos puede tener consecuencias devastadoras. En un entorno cada vez más digital, la protección de estos datos no puede confiarse únicamente a la buena voluntad, sino a sistemas inteligentes que garanticen la autenticidad e integridad documental.

Casa Monarca, organización que apoya a personas migrantes y refugiadas en situación de vulnerabilidad, enfrenta retos en la gestión de información sensible que, sin las medidas de seguridad adecuadas, es susceptible a fraudes o pérdida de confianza institucional.

Este proyecto propone la implementación de un sistema de firma digital que refuerce los derechos de las personas migrantes, prevenga fraudes y fortalezca la confianza en la organización. Para ello, se desarrollará una tecnología basada en firma digital y automatización, empleando algoritmos que aseguren la autenticidad, integridad y no repudio de los documentos.

El sistema se integrará con plataformas existentes de Casa Monarca, como Microsoft 365 y OneDrive, mediante un flujo automatizado de aprobación y seguimiento que optimizará la gestión de documentos oficiales. Además, será accesible a usuarios con conocimientos básicos, asegurando su adopción.

Este proyecto no solo generará un impacto inmediato, sino que también se alinea con el Objetivo de Desarrollo Sostenible 9, promoviendo el uso de la tecnología para proteger a poblaciones vulnerables y construir un entorno más inclusivo y seguro.

Marco Referencial

Marco Teórico

"La privacidad es necesaria para una sociedad abierta en la era electrónica" (**Hughes1993**). La criptografía surge como respuesta a la necesidad de proteger los datos y garantizar su privacidad. Esta disciplina se fundamenta en cuatro pilares esenciales: confidencialidad, integridad, autenticación y no repudio. La confidencialidad asegura que solo las personas autorizadas puedan acceder a la información. La integridad garantiza que la información permanezca sin alteraciones durante su almacenamiento o transmisión. Por su parte, la autenticación verifica la identidad de quienes acceden a los datos y la veracidad de la información que proporcionan. Finalmente, el no repudio impide que una persona niegue haber realizado una acción determinada, como enviar un mensaje o firmar un documento digital. Estos cuatro principios son la base sobre la cual se desarrollan los algoritmos criptográficos, los cuales permiten cifrar información confidencial para mantenerla segura. Dichos algoritmos emplean técnicas matemáticas que transforman los datos de manera que solo quienes posean las claves correspondientes puedan revertir el proceso y acceder a la información original. Entre estos algoritmos se incluyen los algoritmos de cifrado, los algoritmos hash unidireccionales, los algoritmos de distribución de claves y los algoritmos de generación de números aleatorios. La propuesta de este trabajo se enfoca particularmente en los algoritmos de cifrado, es decir, aquellos que convierten la información en un texto ininteligible que únicamente puede ser revertido por usuarios autorizados. Estos algoritmos pueden clasificarse en dos tipos: simétricos, donde se emplea una sola clave secreta compar-

tida entre el emisor y el receptor para cifrar y descifrar la información; y asimétricos, donde se utiliza un par de claves, una pública y una privada, exclusiva de cada usuario. Si bien el cifrado asimétrico es más lento que el simétrico, este ofrece un nivel superior de seguridad. Una de las aplicaciones más eficaces de la criptografía asimétrica en la actualidad son las firmas digitales. Estas funcionan de manera similar a una firma manuscrita, pero en un entorno digital, y se utilizan como método de verificación de identidad en diversos procesos de transacción. La utilidad de las firmas digitales es tan amplia que se emplean en sectores clave de la sociedad. Por ejemplo, en el ámbito empresarial, permiten agilizar procesos legales al reducir tiempos y costos; en el sector gubernamental, facilitan la emisión de certificaciones digitales para verificar identidades; y en las instituciones financieras, refuerzan la seguridad de las transacciones electrónicas. En nuestro caso específico, el uso de firmas digitales permitirá asegurar la autenticidad y acelerar los procesos legales de los documentos correspondientes a las personas migrantes. Esto no solo contribuirá a proteger su identidad y derechos, sino también a fortalecer la confianza en las instituciones que trabajan con esta población vulnerable.

Marco Contextual

La migración es un fenómeno global que cada año afecta a millones de familias. Tan solo en México, más de seis millones de personas se encuentran en situación migratoria. El número de personas que se ven obligadas a recurrir a la migración va en aumento debido a factores como los conflictos armados, crisis económicas, desastres naturales o persecución política, lo que hace indispensable abordar las problemáticas que acompañan este proceso (**AWS**).

Uno de los principales desafíos que enfrentan los migrantes al llegar a un nuevo país es la regularización de sus documentos, los cuales son fundamentales para obtener una residencia definitiva, acceder a empleos formales, recibir ayuda social o, incluso, recibir atención médica primaria. Sin la documentación adecuada, los migrantes quedan en una situación de vulnerabilidad que limita sus oportunidades y los expone a la explotación laboral, discriminación y dificultades para integrarse en la sociedad. Además, la regularización de documentos suele ser un proceso complejo, burocrático y propenso a diversos riesgos, lo que puede derivar en problemas legales, pérdida de derechos y en algunos casos, la deportación.

Estado del Arte

El uso de las tecnologías mencionadas anteriormente ha adquirido gran relevancia en los últimos años. La protección de documentos digitales en contextos donde se requiere resguardar información personal es fundamental, especialmente en el caso de personas migrantes. La necesidad de proteger su identidad e integridad aumenta a medida que estas personas enfrentan procesos complejos de registro y legalización, en los que su documentación es esencial para el acceso a derechos y servicios básicos. Este desafío no es nuevo en la sociedad, pero ha adquirido un contexto global debido al incremento de los flujos migratorios y la creciente preocupación por la seguridad de los datos personales. En respuesta, se han adoptado metodologías tecnológicas como las firmas digitales y la tecnología blockchain, cuyo propósito es garantizar la autenticidad, integridad y confidencialidad de la información sensible. Por ejemplo, las firmas digitales son un mecanismo basado en criptografía asimétrica, que permite verificar la autenticidad de documentos electrónicos y garantizar que no han sido alterados. Algunos de los algoritmos más utilizados para la implementación de firmas digitales son RSA (Rivest-Shamir-Adleman), DSA (Digital Signature Algorithm) y ECDSA (Elliptic Curve Digital Signature Algorithm). Cada uno tiene diferentes variantes y niveles de seguridad que permiten validar la información con base en las necesidades específicas del sistema. Por otro lado, la tecnología blockchain ha sido implementada como una solución innovadora para el registro descentralizado y seguro de información. Uno de los primeros ejemplos destacados es ID2020, una iniciativa que promueve el uso de identidades digitales seguras, éticas y privadas para facilitar el acceso de las personas a servicios sociales, políticos y económicos. Esta organización, en colaboración con Microsoft y Accenture, desarrolló soluciones de identidad digital dirigidas a personas sin documentación oficial, como refugiados y desplazados. Gracias a estas tecnologías, ID2020 ha logrado ofrecer servicios de registro e incluso programas de salud a comunidades vulnerables en distintas partes del mundo. Otro caso relevante es el proyecto Worldcoin, el cual combina el uso de firmas digitales y blockchain para la verificación de identidad mediante la biometría del iris. Esta iniciativa busca asegurar el resguardo y control de la información personal de los usuarios, garantizando al mismo tiempo la autenticidad de los documentos vinculados a dicha identidad digital. A pesar de los avances, la implementación de estas tecnologías enfrenta importantes desafíos. Se requiere de una infraestructura robusta y la colaboración de gobiernos, organizaciones no gubernamentales e instituciones privadas para asegurar el correcto funcionamiento de los sistemas y garantizar el acceso equitativo a estas soluciones tecnológicas. La expansión de iniciativas de este tipo representa un esfuerzo coordinado que permita proteger los datos personales y los derechos de las personas en situación de vulnerabilidad, como lo son las personas migrantes.

Metodología

Para llevar a cabo una solución óptima, funcional y fácil de manipular se combinaron distintas técnicas de automatización de procesos, integración de sistemas y aplicación de tecnologías avanzadas de firma digital, buscando garantizar

la autenticidad, integridad, trazabilidad y no repudio de los documentos, así como la experiencia con los usuarios involucrados en el flujo de firmas.

El diseño del proyecto comenzó con la identificación de riesgos críticos en la ausencia de controles formales de firma digital, desencadenando impactos directos en los derechos y oportunidades de las personas migrantes y refugiadas. Por ello, se diseñó un flujo automatizado que permitiera la recolección de datos, la generaación y firma de los documentos, se registro en una base de datos y su distribución a las distintas partes involucradas, eliminando las tareas manuales y priorizando la huella ambiental al disminuir la distribución de papel.

Flujo con Power Automate

La base fundamental de nuestro proyecto consiste en un flujo desarrollado con la plataforma Power Automate, la cual fue escogida debido a que esta herramienta se encontraba habilitada en el ecosistema Microsoft con el que cuenta Casa Monarca. A partir de esta decisión, el proceso se estructuró en tres flujos distintos:

Primer flujo

Recolección de datos al solicitante: Se diseñó un formulario en Microsoft Forms que recibe la información del solicitante, incluyendo su nombre, correo electrónico, tipo de trámite solicitado, entre otros datos, lo que permitió alimentar directamente el primer flujo de la automatización.

Creación del archivo: A partir de contestar el Forms, el flujo agarra diferentes parámetros de la base de datos de las respuestas del formulario, para crear un archivo nuevo con las mismas especificaciones y formatos ingresados por el solicitante, a partir de la creación, se envía de manera automática a una de las carpetas pertenecientes al one drive de la empresa.

Detección automática: Power Automate supervisa en tiempo real la carpeta de documentos pendientes, al detectar el ingreso de un nuevo archivo, inicia el proceso automatizado del segundo flujo.

Segundo flujo

El segundo flujo comprende mayormente la parte de correos electrónicos, gestionando el registro y diseño de la fase de aprobación.

Obtención de metadatos y preparación del documento: Se recuperan los metadatos esenciales del documento, asegurando que el archivo es identificado de forma única a lo largo del proceso. Además, se genera un vínculo seguro de acceso al documento, así como se inicializan variables que facilitan la traazabilidad del documento, todo esto con el objetivo de que los responsables puedan acceder a cualquier tipo de información en el momento deseado.

Solicitud de aprobación: Hasta esta parte el flujo ya solicita automáticamente la aprobación formal del documento mediante la acción Ïniciar y esperar una aprobación". Este es el momento en donde entra en el proceso el segundo individuo (coordinador), quien tiene la posibilidad de validar que el contenido del documento cumple con los requisitos institucionales antes de su firma oficial.

Ejecución del flujo según la decisión de aprobación: Dependiendo de la respuesta del coordinador, el flujo sigue dos caminos (ver Figura 1):

Aprobación: A partir de que se realiza una respuesta positiva, el flujo introduce un breve retraso para garantizar que el archivo no esté siendo modificado al momento de continuar con el proceso. Posteriormente, el documento es movido a la carpeta de documentos aprobados en OneDrive y se actualizan sus metadatos, incorporando un vínculo de acceso seguro para que se pueda enviar al director para su firma. En paralelo, el flujo consulta la base de datos en Microsoft Excel, y agrega un estatus del documento el cual indica que el documento fue enviado pero aún no ha sido firmado.

Rechazo: Si el documento no es aceptado, simplemente es dirigido a la carpeta de documentos rechazados de OneDrive, notificando al solicitante que el documento no fue aprobado por el coordinador y que realice los cambios pertinentes para que pueda ser aprobado.

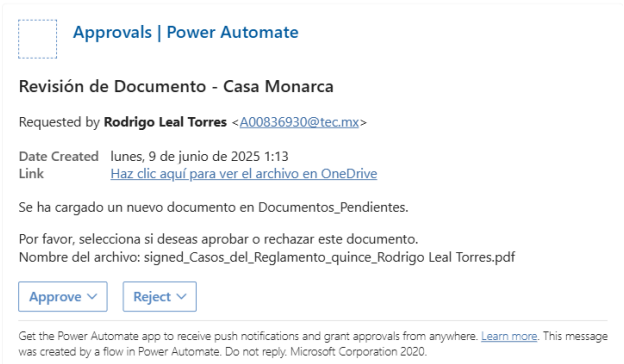


Figura 1: Aprobación o rechazo por coordinador

Cierre del flujo: La segunda parte del proceso termina cuando le llega el correo al director para que este lo pueda firmar con ayuda de un ejecutable, el cual será explicado a continuación.

Firma digital

El paso más crítico del proceso es la firma digital del documento. Para ello, se buscó desarrollar una aplicación personalizada en Python, empaquetada como ejecutable (.exe) mediante PyInstaller, para permitir su ejecución autónoma en los equipos de la orgnaización sin requerir ninguna herramienta de programación adicional.

La lógica que se estableció en este proceso de firma se implementó con la librería PyHanko, la cual permite aplicar firmas digitales avanzadas utilizando una infraestructura de clave pública. Además, el proceso se complementa con el uso de la librería Cryptography, la cual se encarga de la generación y manejo seguro de claves y certificados.

Por otra parte, se utilizó el algoritmo RSA como base para el proceso de firma y cifrado, garantizando seguridad y confianza en los documentos. Además, se implmentó un esquema de doble encriptación de las claves privadas: en primer lugar, las claves se cifran utilizando el algoritmo Fernet con una clave maestra; esta clave a su vez se encuentra protegida y cifrada, asegurnado que las claves de los usuarios no estén expuestas en ningún momento en texto plano dentro del sistema, de la misma forma, también se cuenta con la protección de un usuario y contraseña, por lo que si algún agente maligno llega a robar alguna de las dos iniciativas (clave maestra o contraseña), siempre habrá un segundo factor que dificulta cualquier intento de acceso no autorizado, logrando una gran barrera en el ejecutable elaborado.

Una vez explicadas las fortalezas de nuestro ejecutable, es importante mencionar lo que sucede para verificar que el documento cumpla con la operación.

1. El director sube el documento PDF junto con el tipo de trámite así como una pequeña descripción del escrito.

2. El sistema verifica que el documento no contenga firmas previas que puedan ser sobrescritas incorrectamente. Si ya está manipulado, marca un error que impide que el documento sea nuevamente firmado.

3. Aplica la firma digital utilizando un certificado institucional emitido para Casa Monarca.

4. Incorpora al documento diversos metadatos: nombre del firmante, fecha y hora de la firma, propósito de la firma y hash criptográfico.

5. Verifica la integridad del documento tras la firma, garantizando que no se haya manipulado de ninguna forma el archivo.

Una vez firmado, el documento es automáticamente tranferido a la carpeta de Documentos firmadaso que se encuentra en el OneDrive de la empresa, permitiendo correr el último flujo que termina el ciclo de al firma de documentos.

Tercer flujo

Como se mencionó anteriormente, el tercer flujo automatizado se activa en cuanto el documento firmado es enviado a la carpeta de "Documentos firmados.[en] OneDrive. Este flujo bsuca registrar oficialmente el documento firmado en la base de datos y garantizar su correcta distribución a las partes involucradas.

Obtención de metadatos: Cuando el archivo está en la carpeta, Power Automate se encargar de obtner nuevamente los metadatos relevantos para generar un vínculo seguro que permita compartir, consultar y descargar el documento.

Actualización del estado del documento: El flujo realiza una consulta en la base de datos, localizando la fila correspondiente al documento en cuestión. En esta parte, se actualiza el estatus del documento, cambiando de "documento no firmado.[a] "documento firmado", indicando que el proceos se realizó correctamente y que el documento ya pasó por el director.

Envíos de correos: Como última acción, el flujo envía un correo electrónico tanto al coordinador de Casa Monarca como al solicitante original. Este correo contiene el documento firmado en formato PDF, así como un resumen de la operación realizada.

Una vez finalizado el envío de los correos, se completa el ciclo de la firma digital, asegurando que cada documento quede registrado, distribuido y trazado dentro del sistema de la organización.

Resultados

Para validar el correcto funcionamiento del sistema de firma digital, se realizaron pruebas completas en las que se recorrieron los tres flujos de principio a fin. A continuación, se describe un ejemplo del proceso.

El proceso se incia con la recolección de datos del solicitante a través de un formulario de Microsft Forms (ver Figura 2), donde se recopila la información que alimentará al primer flujo de Power Automate.

Figura 2: Formulario de recolección de datos del solicitante.

A partir de las respuestas obtenidas, el primer flujo genera un documento en formato PDF con la información personalizada del solicitante. Este documento se almacena en una carpeta específica en OneDrive denominada "Documentos pendientes"(ver Figura 3), activando así el segundo flujo.

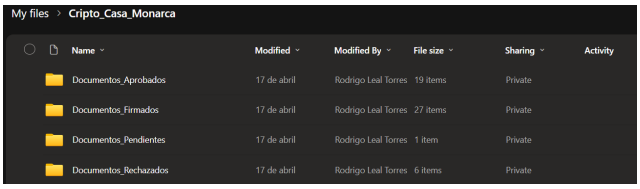


Figura 3: Ambiente de OneDrive con las carpetas pertinentes

El segundo flujo detecta el nuevo archivo, obtiene sus metadatos y envía el proceso de aprobación formal mediante correos. Para poder seguir con el flujo, en el ejemplo a mostrar se va a mostrar el documento como aprobado para que sea enviado correctamente a la carpeta de "Documentos Aprobados"(ver Figura 3) y siga el proceso ideal.

En la etapa de firma digital, se comprobó que el director recibiera el documento aprobado mediante un correo electrónico, logrando visualizarlo y descargarlo (ver Figura 5a). A partir de este correo, es cuando se abre la apliación o ejecutable, donde el director debe de ingresar su usuario y contraseña para acceder a la firma de documentos (ver Figura 4a). Una vez autenticado, el director selecciona el documento previamente descargado y lo carga en la aplicación (ver Figura 4b). Si el documento cumple con los requisitos, el ejecutable procede a aplicar la firma digital utilizando el certificado institucional de Casa Monarca, además de incorporar los metadatos correspondientes.

(a) Interfaz para ingresar a la aplicación

(b) Interfaz para subir el documento

Figura 4: Interfaz para el usuario

Cuando el documento es subido y enviado con las respectivas especificaciones, el documento es firmado y enviado a la carpeta de Documentos firmados en OneDrive (ver Figura 3).

A partir de esto, aparece el resultado principal, el cual es la firma del documento (ver Figura 5b). Esta firma no solo valida oficialmente el contenido del archivo, sino que también garantiza su autenticidad, integridad y no repudio mediante el uso del certificado digital institucional. Este resultado constituye el cierre seguro del proceso de firma digital, permitiendo que el documento sea distribuido y que el último flujo pueda correr.

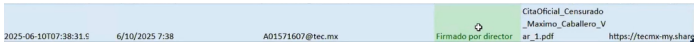
(a) Documento Sin Firmar

(b) Documento Firmado

Figura 5: Interfaz para el usuario

Finalmente, en el tercer flujo, se validó que los documentos firmados eran correctamente detectados por Power Automate y que sus metadatos fueran actualizados en la base de datos del Excel. Como se puede ver en la imagen mostrada a continuación, el estatus de los cambió de "Pendiente firma director.ª "Firmado por director", permitiendo una trazabilidad efectiva. Además, se verificó que los correos electrónicos finales fueran enviados satisfactoriamente tanto al coordinador como al solicitante, incluyendo el documento firmado.

(a) Estatus no firmado



(b) Estatus firmado

A partir de este ejemplo se puede determinar la existencia de un sistema funcional que permite la automatización completa del ciclo de vida de los documentos en Casa Monarca. Las pruebas realizadas confirmaron que cada etapa del flujo opere de forma confiable, reduciendo significativamente los tiempos de gestión y aumentando la seguridad del documento.

Conclusiones

A partir de la metodología y los resultados obtenidos a lo largo de este proyecto, podemos concluir que logramos transformar un proceso que anteriormente era manual y vulnerable, en un flujo seguro y trazable, y todo esto gracias a la integración de las distintas herramientas usadas, las cuales también cuenta Casa Monarca.

Uno de los principales logros que consiguió el equipo fue la garantía de seguridad en el tratamiento de documentos, gracias a la apliación de firmas digitales basadas en un esquema de doble encriptación que protege las llaves privadas, asegurando la integridad y autenticidad de los documentos al disminuir riesgos como la falsificación o manipulación.

De la misma forma, el proceso permitió establecer un control de aprobaciones, garantizando que únicamente los documentos validados sean firmados. Además, la integración de una base de datos actualizada en tiempo real proporciona un rastro digital completo, otorgando la trazabilidad del proceso entero.

Por otra parte, la automatización del flujo ha resaltado de forma importante en el ahorro de tiempo, reduciendo las tareas manuales y minimizando el uso de papel, aspecto el cual contribuye a la sostenibilidad ambiental.

Por último, es importante resaltar que nuestra iniciativa es compatible con todas las plataformas existentes en la organización, lo que facilita la transferencia de la solución, sin necesidad de capacitación técnica avanzada. Además, la forma en como organizamos los flujos y la información es lo suficientemente eficiente como para escalar la solución tanto en número de usuarios como en la incorporación de nuevas funcionalidades o flujos.

El sistema propuesto ofrece una buena base, pero también abre la puerta a futuras mejoras que puedan complementar nuestro trabajo. Por una parte, se toma la iniciativa de extender las herramientas mediante la integración con servicios de Azure, fortificando más el intercambio de llaves y la seguridad en general. Además, se busca implementar la automatización de recordatorios, permitiendo enviar notificaciones automáticas para dar seguimiento a aprobaciones pendientes. Por útlimo, se debe continuar con el desarrollo del chatbot de asistencia, que actualmente se encuentra en versión básica, con el objetivo de facilitar la búsqueda de documentos en las bases de datos.

Recomendaciones socio formador

Con base en el proyecto desarrollado y los resultados obtenidos durante la automatización de este proceso, se puede identificar ciertas recomendaciones que podrían contribuir a optimizar aún más el flujo de gestión de documentos en Casa Monarca.

Primero que nada, se recomienda continuar fortaleciendo la seguridad de las claves y certificados utilizados en el sisema. Aunque actualmente pueden contar con un esquema de doble encriptación y autenticación en el ejecutable, sería ideal explorar la integración con servicios de gestión de claves en la nube, como Azure Key Vault.

Por otra parte, se debe buscar obtener una mejor gestión de la base de datos al realizar una revisión periódica de la estrucutra de la hoja de Excel utilizada como repositorio, con el objetivo de garantizar escalabilidad y eficiencia conforme aumente el volumen de documentos firmados. Herramientas como SharePoint Lists o un sistema de gestión de bases de datos relacional (SQL) podría ser clave para lograr este objetivo.

Además, también se sugiere mantener un proceso de capacitación entre directores o personas involucradas en el uso de los flujos y la aplicación de la firma. Aunque el sistema fue diseñado para ser accesible y fácil de utilizar, la rotación de personal podría generar una brecha de conocimiento de la herramienta y su potencial podría bajar. De igual forma, sería eficiente contar con guías o scripts bien explicados que permitan un buen entendimiento del proceso.

Otro aspecto fundamental es considerar el ahorro de tiempo logrado con esta automatización, ya que no solo representa una mejora en términos operativos, sino que libera recursos y capacidades para que Casa Monarca pueda enfocarse aún más en su misión principal: servir y apoyar a las personas migrantes y refugiadas. Por ello, es sumamente importante invertir en tecnologías e iniciativas que permitan garantizar una reducción de tiempos al momento de hacer papeleos y firmas manuales, y aumentar el impacto social.

Finalmente, el sistema desarrollado puede ser considerado una herramienta valiosa para Casa Monarca, aportando seguridad y trazabilidad. Sin embargo, así como existe esta iniciativa, también hay muchos equipos con distintas ideas que arrojaron aportaciones valiosas. Por ello, también recomendamos juntar a los mejores poryectos para consolidarlos y generar un sistema aún más completo e importante para las tareas del día a día de Casa Monarca.

Referencias

[1] Amazon Web Services. *¿Qué es la criptografía? - Explicación sobre la criptografía*. Retrieved from https://aws.amazon.com/es/what-is/cryptography/#:~:text=La%20criptograf%C3%ADa%20es%20una%20pr%C3%A1ctica,algoritmos%20codificados%2C%20hashes%20y%20firmas

[2] Proofpoint. *¿Qué es la firma digital?*. Retrieved from https://www.proofpoint.com/es/threat-reference/digital-signature

[3] IBM. (2024, October 7). *Conceptos de criptografía*. Retrieved from https://www.ibm.com/docs/es/i/7.5?topic=cryptography-concepts

[4] Hughes, E. (1993). *A cypherpunk's manifesto*. Retrieved from https://medium.com/@rootsec/un-manifiesto-cypherpunk-por-eric-hughes-3aa4660af977

[5] ID2020. (2020). *ID2020 — GHPC — Digital Identity Alliance*. Retrieved from https://www.id2020.org/

[6] El HuffPost. (2024, October 24). *Regresa la empresa que te daba dinero por tu iris: ahora quiere tu pasaporte*. Retrieved from https://www.huffingtonpost.es/tecnologia/regresa-empresa-te-daba-dinero-iris-quiere-pasaporte.html