Plataforma Web de Firmado Digital basada en Infraestructura de Clave Publica para la Transformación hacia la Universidad Digital

Colaboración
Jaziel Isai Anguiano Mariz; Ismael Amezcua Valdovinos; Patricia Elizabeth Figueroa Millán, Tecnológico Nacional de México / Campus Colima

Fecha de recepción: 05 de noviembre 2025
Fecha de aceptación: 05 de noviembre de 2025

RESUMEN: La pandemia de COVID-19 evidenció las brechas digitales en las instituciones de educación superior (IES), haciendo esencial la transformación hacia una Universidad Digital. Este trabajo aborda las ineficiencias de los procesos manuales de emisión y validación de documentos en la Universidad de Colima mediante Firmare, una plataforma web de firma digital basada en Infraestructura de Clave Pública (PKI). Desarrollada con un enfoque iterativo, la solución garantiza autenticidad, integridad y no repudio. Los resultados de su validación funcional demuestran su capacidad para reducir significativamente los tiempos de emisión, mejorar la trazabilidad y promover la sostenibilidad al disminuir el uso de papel, alineándose con los Objetivos de Desarrollo Sostenible (ODS). Si bien la plataforma ha sido validada, su implementación institucional aún no se ha completado, por lo que se proponen estrategias de adopción como un manual interactivo para facilitar su integración.

PALABRAS CLAVE: Certificados académicos, Firma Digital, Infraestructura de clave pública (PKI), Sostenibilidad, Universidad Digital.

ABSTRACT: The COVID-19 pandemic highlighted the digital gaps in higher education institutions (HEIs), making the transition to a Digital University essential. This work addresses the inefficiencies of manual document issuance and validation processes at the University of Colima through Firmare, a web-based digital signature platform based on Public Key Infrastructure (PKI). Developed with an iterative approach, the solution ensures authenticity, integrity, and non-repudiation. The results of its functional validation demonstrate its capacity to significantly reduce issuance times, improve document traceability, and promote sustainability by decreasing paper use, aligning with the Sustainable Development Goals (SDGs). While the platform has been functionally validated, its institutional implementation has not yet been completed; therefore, adoption strategies such as an interactive manual are proposed to facilitate its integration.

KEYWORDS: Academic certificates, Digital Signature, Public Key Infrastructure (PKI), Sustainability, Digital University.

INTRODUCCIÓN

La transformación digital en las instituciones de educación superior es esencial en el contexto de la Industria 4.0. Las universidades digitales deben modernizar sus procesos administrativos para una gestión inteligente y sostenible [1]. La digitalización impacta la gestión administrativa, donde la falta de automatización y la dependencia de métodos tradicionales como el papel generan ineficiencias [2]. En este contexto, la

gestión documental electrónica y la firma digital son fundamentales. La firma digital basada en Infraestructura de Clave Pública (PKI) utiliza criptografía asimétrica para garantizar la autenticidad, integridad y no repudio de los documentos, siendo ideal para validar certificados académicos [3]

La Universidad de Colima enfrenta la necesidad de optimizar la emisión y validación de certificados, procesos que aún dependen de validaciones manuales, generando ineficiencias y errores. Aunque existen plataformas comerciales de firma digital, su adopción presenta desafíos como altos costos y dificultades de interoperabilidad [1].

El objetivo de esta investigación es presentar Firmare, una plataforma web de firmado digital basada en PKI, diseñada para entornos universitarios, con el fin de agilizar la emisión de documentos académicos y contribuir a la sostenibilidad. Sustentada en PKI y estándares internacionales como X.509 [4], garantiza autenticidad, integridad y no repudio, además de validez legal y protección contra fraudes [2]. Firmare contribuye a la reducción del consumo de papel, alineándose con los Objetivos de Desarrollo Sostenible (ODS). Además, mejora la trazabilidad y auditoría de los documentos, ya que cada acción se registra de forma inmutable [5]. Se plantea que su implementación facilitará la digitalización de procesos, reduciendo tiempos y optimizando recursos.

Revisión de la literatura

La adopción de la firma digital en las IES ha sido impulsada por la necesidad de agilizar la gestión documental. Plataformas comerciales como DocuSign y PandaDoc, aunque populares, enfrentan obstáculos como altos costos de suscripción y baja personalización para entornos universitarios [6], [7], [8].

Como respuesta, algunas instituciones han desarrollado plataformas propias. La Universidad Nacional de Barranca (UNAB) redujo los tiempos de emisión de documentos de 10 días a 1-2 días [8]. Sin embargo, estudios en otras universidades identifican tres factores críticos que limitan la implementación de la firma digital: (1) altos costos, (2) dificultades de integración, y (3) resistencia institucional por falta de cultura digital [8], [9], [10]Esto refuerza la necesidad de abordar la transformación digital de manera integral. Por ello, en este artículo se presenta el desarrollo de Firmare, una plataforma web de firmado digital basada en PKI y diseñada para el entorno universitario, que busca subsanar las limitaciones identificadas mediante el uso de tecnologías de código abierto y una arquitectura adaptable.

MATERIAL Y MÉTODOS

El desarrollo de Firmare se llevó a cabo en la Facultad de Telemática de la Universidad de Colima para automatizar la emisión y gestión de certificados académicos. Su objetivo es reemplazar procesos manuales por una solución basada en PKI, conforme al Código de Comercio [11] y la norma X.509 [4]. Su desarrollo siguió un enfoque iterativo e incremental inspirado en la metodología SCRUM, con una estructura de roles de Desarrollador y Asesor académico.

El proceso se estructuró en sprints con entregables verificables y revisión técnica continua. La estructura metodológica incluyó los siguientes roles y ciclos de trabajo:

- **Desarrollador:** diseño, implementación y pruebas de cada módulo.
- Asesor: revisión semanal de avances y retroalimentación en temas como PKI.

El ciclo de trabajo por sprint incluyó:

- **Planificación:** definición de objetivos por iteración.
- **Ejecución:** implementación de funcionalidades.
- **Revisión:** presentación de resultados al asesor.
- **Ajustes:** corrección de errores e incorporación de mejoras."

A continuación, la Tabla 1 detalla la evolución del desarrollo de Firmare, mostrando las funcionalidades clave implementadas y validadas en cada sprint, lo que subraya el enfoque iterativo e incremental seguido.

Tabla 1. Evolución del desarrollo por sprint.

Sprint	Módulo Desarrollado	Actividades Clave
1	Dashboard de Gestión	-Autenticación de usuarios con Google OAuth 2.0.
		- Carga y almacenamiento de PDFs en Supabase.
		- Integración de la tabla pdf_metadata.
2	Vista de Firma Digital	- Validación de certificados .cer y claves .key.
		- Generación de hashes SHA-256.
		- Incrustación de firmas en PDFs con pdf-lib.
3	Visor Público de Certificados	- Renderizado de PDFs con @react-pdf-viewer.
		- Generación de UUIDs y códigos QR.
		- Implementación de enlaces públicos seguros.

Fuente: Elaboración propia.

La arquitectura de Firmare se organiza en tres capas funcionales principales, cada una de las cuales emplea tecnologías de código abierto para garantizar escalabilidad, seguridad e interoperabilidad:
Frontend: Esta capa se encarga de la interfaz de usuario y la visualización de documentos. Se desarrolló utilizando Next.js [12] e incorpora componentes accesibles de Mantine UI [13]. Para la visualización segura de documentos PDF, se emplea la librería react-pdf-viewer.

Backend: Responsable de la autenticación de usuarios, la gestión de datos y el almacenamiento de archivos. Para estas funciones, se utiliza Supabase [14], que provee servicios de autenticación mediante Oauth 2.0, una base de datos PostgreSQL robusta y capacidades de almacenamiento de archivos.

Criptografía: Esta capa es fundamental para la gestión de claves y la firma digital. Implementa Forge.js [15], una librería que permite trabajar con certificados digitales que cumplen con el estándar X.509 [16] y utiliza el algoritmo RSA-2048 para la generación y verificación de firmas digitales.

Por otro lado, el flujo de interacción entre los componentes de ésta durante el proceso de autenticación del usuario y firma digital de un documento PDF se ilustra a continuación.

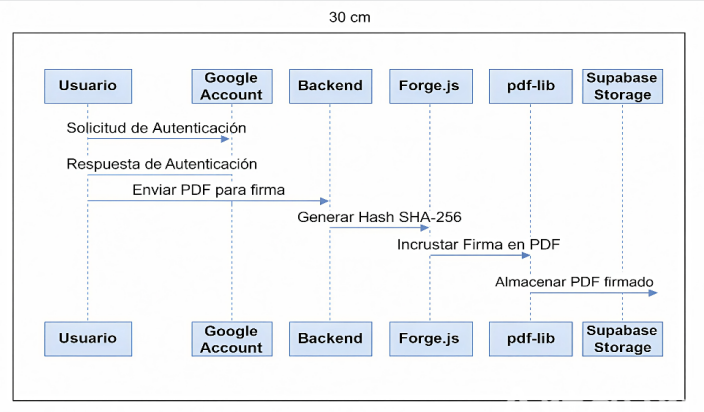

Figura 1. Interacción de componentes en Firmare.
Fuente: Elaboración propia.

Como se presenta en la Figura 1, el proceso se establece como sigue:
Autenticación de usuario: El usuario accede mediante su cuenta de Google. La autenticación se valida vía OAuth 2.0 y permite el acceso al dashboard de la plataforma.

Carga (envío) del documento: El usuario selecciona el archivo PDF a firmar. Se valida el formato, almacena el archivo y registra metadatos como nombre, fecha y estado ("pendiente de firma o firmado").

Generación de hash SHA-256: El backend crea un resumen criptográfico único del documento, el cual es firmado posteriormente con la clave privada del usuario. Este proceso cumple con el estándar X.509 para certificados digitales.

Firma digital del documento: Se firma el hash utilizando RSA-2048. Se incrustan en el PDF elementos de validación como el UUID (Identificador Único Universal) que es una cadena alfanumérica de 36 caracteres [17], la firma en formato Base64, la cadena original, el nombre del firmante, la fecha de firma y un código QR que establece una matriz de puntos o barras bidimensional que sirve para la encriptación de información [18] y el cual se vincula a una URL única para validación pública. Esto se realiza mediante pdf-lib y react-pdf-viewer. Estos metadatos en garantizan documentos únicos, íntegros y verificables. El UUID evita duplicados, el QR permite validación externa mediante URL única, y la firma digital autentica al firmante. La cadena original protege contra alteraciones, mientras los datos de firmante y fecha aportan transparencia.

Almacenamiento del PDF firmado: El documento firmado se guarda en Supabase Storage mediante un bucket privado y se actualiza la base de datos con metadatos finales. El acceso al documento se proporciona mediante un enlace público seguro mediante protocolo TLS.

La plataforma se construyó utilizando Visual Studio Code como entorno de programación y Git para el control de versiones

RESULTADOS

La plataforma Firmare se estructuró en tres vistas interconectadas: Dashboard, vista de firma y visor de certificados firmados, diseñadas para optimizar la gestión documental en la Universidad de Colima.

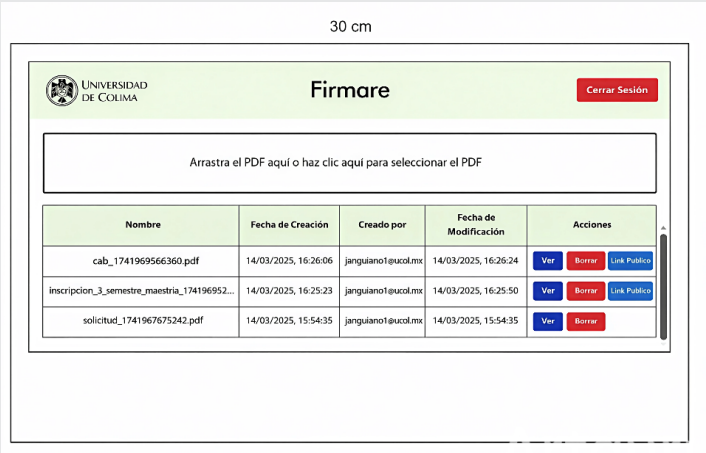

Figura 2 Dashboard.
Fuente: Elaboración propia.

El Dashboard Figura 2, desarrollado con Next.js y Supabase, funciona como el núcleo de gestión de documentos. Los usuarios autenticados mediante

Google OAuth 2.0 cargan, gestionan y dan seguimiento al firmado de certificados académicos en formato PDF, asegurando la trazabilidad documental. La integración con la base de datos PostgreSQL de Supabase permite almacenar metadatos esenciales como el estado de firma y fechas de modificación. Cada acción actualiza automáticamente la interfaz, y el uso de UUIDs únicos evita conflictos de nombres.

En la vista de Firma, se implementó el corazón de la Infraestructura de Clave Pública (PKI). Los usuarios cargan su certificado digital (.cer) y clave privada (.key), validados mediante el estándar X.509 y el algoritmo RSA-2048.

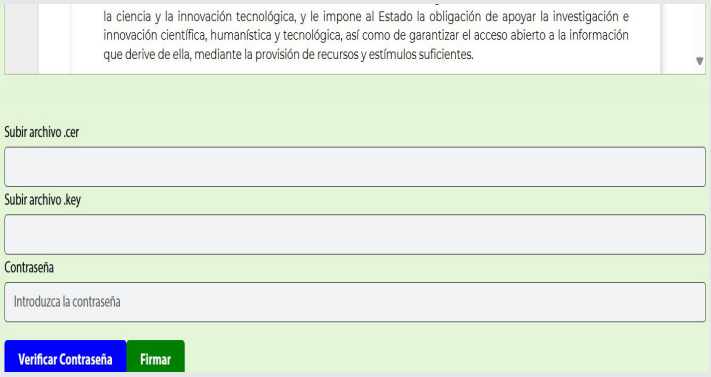

Figura 3 Vista de firma.
Fuente: Elaboración propia.

En la vista de Firma (Figura 3), se implementó el núcleo de la Infraestructura de Clave Pública (PKI). Los usuarios cargan su certificado digital (.cer) y clave privada (.key), que son validados mediante el estándar X.509 y el algoritmo RSA-2048. Tras la verificación de la contraseña, el sistema genera un hash SHA-256 del documento, lo firma digitalmente y lo incrusta en una nueva página del PDF. Esta vista incorpora elementos para la transparencia: un código QR, la fecha de firma y una cadena original que resume los datos del certificado.

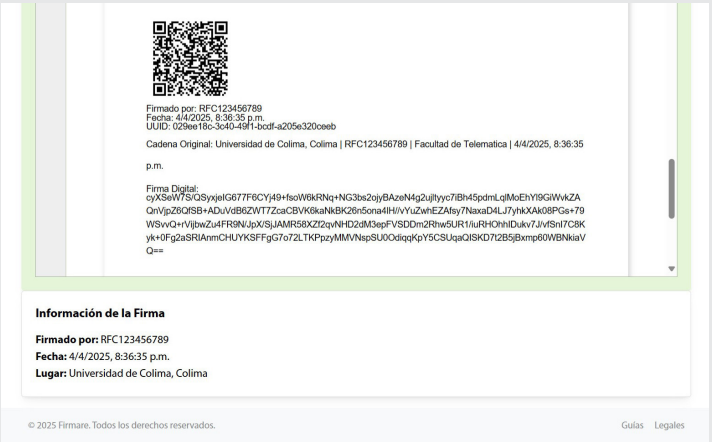

Figura 3 Vista de firma.
Fuente: Elaboración propia.

El visor (Figura 4) permite la verificación externa de documentos. Mediante un enlace público único protegido por un UUID, cualquier persona puede acceder al certificado y validar su autenticidad. La integración de @react-pdf-viewer facilita la visualización del PDF, mientras un panel inferior muestra metadatos esenciales como el nombre del firmante y la firma digital.

La interacción entre los módulos demostró un flujo de trabajo cohesivo, y la arquitectura cumplió con los estándares PKI, estableciendo un modelo escalable. Los resultados confirman la validación funcional y técnica de Firmare, demostrando que sus módulos operan según lo diseñado. Aunque la plataforma está en fase de preparación para su implementación institucional, las pruebas han confirmado su capacidad para realizar las funciones de firmado y validación de manera segura y eficiente.

RESULTADOS

El desarrollo de Firmare demuestra la viabilidad de implementar sistemas de firma digital en entornos universitarios mediante tecnologías de código abierto, ofreciendo una alternativa funcional, personalizable y escalable frente a soluciones comerciales. A continuación, la Tabla 2 presenta una comparación entre Firmare y otras soluciones.

Tabla 1. Evolución del desarrollo por sprint.

Características	DocuSign y PandaDoc	UNAB	Firmare (Propuesta)
Tipo	Comercial	Desarrollo interno	Código abierto + PKI
Costo	Alto (licencias, suscripciones)	Bajo (sin licencias)	Bajo (tecnologías open-source)
Infraestructura	PKI	PKI	PKI
Integración con sistemas existentes	Limitada, adaptación y configuración complejas	Depende de la infraestructura institucional	Alta (Supabase)
Personalización	Moderada (flujos predefinidos)	Alta (adaptable)	Alta (módulos modulares, código abierto)
Dependencia de proveedores	Alta	Moderada (dependencia parcial de RENIEC)	Baja (Supabase bajo demanda)
Estándares	eIDAS, X.509	X.509	X.509
Trazabilidad documental	Sí (registro de auditoría)	Parcial (depende del desarrollo)	Sí (metadatos inmutables, QR, UUID)

Fuente: Elaboración propia.

Como se muestra en la tabla, Firmare incorpora una infraestructura PKI y el uso de SHA-256 con costos operativos bajos. Ofrece una alternativa funcional y escalable frente a soluciones comerciales como DocuSign, PandaDoc, así como la solución de la UNAB. Firmare asegura los documentos mediante certificados X.509 y hashes SHA-256 para garantizar integridad. Los metadatos inmutables (UUID, QR) se incrustan en el PDF, mientras la autenticación delegada a Google (OAuth 2.0) simplifica el acceso. En términos de costos, Firmare representa una solución de bajo costo al eliminar pagos recurrentes por licencias.

Respecto a la infraestructura, todas las soluciones analizadas emplean PKI, pero Firmare además contempla mecanismos como SHA-256, UUID y códigos QR para fortalecer la trazabilidad. En interoperabilidad, Firmare destaca por su capacidad de integración con sistemas existentes al usar tecnologías estándar y abiertas como PostgreSQL y APIs RESTful. Finalmente, la trazabilidad documental y el uso de estándares como X.509 la convierten en una solución tecnológicamente válida.

Es importante señalar que, debido a que Firmare se encuentra en la fase de preparación para su implementación, este estudio se centra en los resultados de su desarrollo y validación funcional. Las métricas cuantitativas sobre su adopción a gran escala se documentarán en futuros estudios.

CONCLUSIONES

La implementación de Firmare evidenció que la Infraestructura de Clave Pública (PKI) es indispensable para cumplir con los estándares legales y técnicos en la gestión documental universitaria. El empleo del algoritmo SHA-256 asegura la integridad del documento, ya que cualquier modificación posterior alterará el hash, lo que detectará la alteración. Su alineación con el estándar X.509 permite que la firma digital tenga validez legal y sea interoperable.

Durante el desarrollo, se superaron desafíos clave como la validación estricta de certificados para evitar suplantaciones y el cifrado de claves privadas para mitigar accesos no autorizados. La adición de metadatos en páginas separadas del PDF preservó el contenido académico original. Este proyecto posiciona a la Universidad de Colima como un referente en la adopción de tecnologías PKI, demostrando que es posible migrar procesos administrativos tradicionales a entornos digitales sin comprometer la seguridad.

Sin embargo, el éxito a largo plazo dependerá de la adopción por parte del personal y la integración con los sistemas académicos existentes. Como trabajo futuro, se está desarrollando un manual interactivo integrado en la plataforma para facilitar la capacitación del personal. Se considera que Firmare contribuye a la transición a una universidad digital más robusta, transparente y alineada con los desafíos tecnológicos del siglo XXI.

AGRADECIMIENTOS

Los autores expresan su agradecimiento a la Universidad de Colima la Facultad de Telemática y al sistema de becas nacionales de SECIHTI por el apoyo brindado en el desarrollo de esta investigación.

BIBLIOGRAFÍA

[1] E. Barrientos y Y. Areniz, «Universidad inteligente: Oportunidades y desafíos desde la Industria 4.0», Rev. Ingenio, vol. 16, n.o 1, pp. 56-60, ene. 2019, doi: 10.22463/2011642X.2343.

[2] D. A. C. Gaibor y C. Gaibor, «TRANSFORMACIÓN DIGITAL EN LA UNIVERSIDAD ACTUAL», 2020.

[3] A. A. B. González, «Firma Electrónica o Digital», 2021.

[4] ITU, «Recomendación X.509: Estructura de certificados y listas de revocación de certificados (CRL) para infraestructuras de clave pública (PKI). Unión Internacional de Telecomunicaciones.» 2019. [En línea]. Disponible en: https://www.itu.int/rec/T-REC-X.509-201910-I/es

[5] M. E. García, «La firma electrónica: Un nuevo paradigma en el derecho.», Universidad Autónoma de Nuevo León, 2005. [En línea]. Disponible en: http://eprints.uanl.mx/20256/1/1020150966.pdf

[6] DocuSign Inc, «DocuSign: Platform for digital signatures.» 2023. [En línea]. Disponible en: https://www.docusign.com

[7]PandaDoc Inc, «PandaDoc: Document automation and digital signature solution.» 2023. [En línea]. Disponible en: https://www.pandadoc.com/es/software-firma-electronica/

[8] R. M. Ampuero, «Aplicación de la plataforma de firma digital en la emisión de los documentos académicos de una Universidad Pública», Alpha Centauri, vol. 5, n.o 3, pp. 24-33, sep. 2024, doi: 10.47422/ac.v5i3.176.

[9] J. D. D. Ortega, J. C. De La Cruz Maldonado, y D. Abrego Almazán, «Aplicación de la firma digital en una institución de educación superior», RECAI Rev. Estud. En Contad. Adm. E Informática, vol. 13, n.o 37, p. 15, may 2024, doi: 10.36677/recai.v13i37.22367.

[10] S. Ramos, «DESARROLLO DE UN PROGRAMA DE FIRMA DIGITAL WEB OPTIMIZADO PARA PROCEDIMIENTOS ADMINISTRATIVOS DE LA

UNIVERSIDAD JOSÉ CARLOS MARIÁTEGUI, MOQUEGUA 2024», 2024.

[11] M. Código de Comercio, «Código de Comercio». Diario Oficial de la Federación, 28 de marzo de 2018. [En línea]. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/CCom.pdf.

[12] Vercel, «Introduction | Next.js». Accedido: 2 de mayo de 2025. [En línea]. Disponible en: https://nextjs.org/docs.

[13] Mantine, «Getting started | Mantine». Accedido: 2 de mayo de 2025. [En línea]. Disponible en: https://mantine.dev/getting-started/

[14] Supabase, «Supabase: The open source Firebase alternative». 2023. [En línea]. Disponible en: https://supabase.io/.

[15] npm, «node-forge», npm. Accedido: 2 de mayo de 2025. [En línea]. Disponible en: https://www.npmjs.com/package/node-forge.

[16] Entrust, «¿Qué es una PKI (Infraestructura de clave pública)? | Entrust». Accedido: 2 de mayo de 2025. [En línea]. Disponible en: https://www.entrust.com/es/resources/learn/what-is-pki.

[17] Cockroachlabs, «What is a UUID, and what is it used for?» Accedido: 2 de mayo de 2025. [En línea]. Disponible en: https://www.cockroachlabs.com/blog/what-is-a-uuid/.

[18] M. Castro, M. Hernández, y E. Aína, «Mosaico no 38. Revista para la promoción y apoyo a la enseñanza del español - libreria.educacion.gob.es». Accedido: 2 de mayo de 2025. [En línea]. Disponible en: https://www.libreria.educacion.gob.es/libro/mosaico-no-38-revista-para-la-promocion-y-apoyo-a-la-ensenanza-del-espanol_184086/.