Estudios y Perspectivas Revista Científica y Académica
ISSN en línea 3005-2599, Julio - Septiembre 2026,
Volumen 6, Número 3.

DOI: https://doi.org/10.61384/r.c.a.v6i3

# DIGISIGN: PLATAFORMA DE FIRMA DIGITAL CON AUDITORÍA ASISTIDA POR IA PARA PROCESOS ADMINISTRATIVOS EN INSTITUCIONES PÚBLICAS DE EDUCACIÓN SUPERIOR

## *DIGISIGN: DIGITAL SIGNATURE PLATFORM WITH AI-ASSISTED AUDITING FOR ADMINISTRATIVE PROCESSES IN PUBLIC HIGHER EDUCATION INSTITUTIONS*

**Ismael Guadalupe Gonzalez Lomelí**
Universidad de Guadalajara - CUCEI, -México

**Fabian Martinez Torres**
Universidad de Guadalajara - CUCEI, -México

**Cristian Isaac Aguilar Guzman**
Universidad de Guadalajara - CUCEI, -México

**Emmanuel Franco López Velarde**
Universidad de Guadalajara - CUCEI, -México

E. COUTURE
Educación y Ciencias Sociales

Estudios y Perspectivas
Revista Científica y Académica

Estudios y Perspectivas
Revista Científica Multidisciplinaria

**DOI:** https://doi.org/10.61384/r.c.a..v6i3.2076

# Digisign: Plataforma de Firma Digital con Auditoría Asistida por ia para Procesos Administrativos en Instituciones Públicas de Educación Superior

| | |
|---|---|
| **Ismael Guadalupe Gonzalez Lomelí** | **Fabian Martinez Torres** |
| gonzaleslomeli2550@gmail.com | fabianmatineztorres@gmail.com |
| https://orcid.org/0009-0000-5357-0531 | https://orcid.org/0009-0009-1444-8192 |
| Universidad de Guadalajara - CUCEI, -México | Universidad de Guadalajara - CUCEI, -México |
| **Cristian Isaac Aguilar Guzman** | **Emmanuel Franco López Velarde** |
| cristianisac2983@gmail.com | emmanuel.flopezvelarde@academicos.udg.mx |
| https://orcid.org/0009-0008-8304-1022 | https://orcid.org/0009-0000-1200-199X |
| Universidad de Guadalajara - CUCEI, -México | Universidad de Guadalajara - CUCEI, -México |

**RESUMEN**

La transformación digital de la educación superior requiere mecanismos seguros para validar documentos administrativos, pues el uso de firmas manuscritas o imágenes sin respaldo criptográfico genera riesgos de autenticidad y demoras operativas. Este estudio presenta DIGISIGN, una plataforma de firma digital basada en certificados X.509 y el estándar PAdES para proteger la integridad, autenticidad y trazabilidad de documentos PDF. La investigación aplicada siguió un enfoque mixto, con alcance descriptivo y evaluativo. El diagnóstico institucional combinó revisión documental, observación directa y entrevistas a dos informantes clave; la evaluación técnica incluyó pruebas funcionales, métricas de rendimiento y un conjunto sintético de 5.000 registros para calibrar el algoritmo Isolation Forest. El modelo alcanzó una exactitud del 97,00 % y un F1-score de 0,6796 para la clase anómala. Su integración con reglas deterministas eliminó los errores de clasificación en una simulación controlada de 1.000 transacciones. Las pruebas de carga mantuvieron una tasa de éxito del 100 % hasta 20 usuarios concurrentes, pero esta disminuyó al 80 % con 50 usuarios. Los resultados respaldan la viabilidad técnica de DIGISIGN en el entorno evaluado, aunque su implementación institucional requiere validación con datos operativos reales y una infraestructura de mayor capacidad

***Palabras clave***: firma digital; PAdES; inteligencia artificial; educación superior; procesos administrativos

# DIGISIGN: Digital Signature Platform with AI-Assisted Auditing for Administrative Processes in Public Higher Education Institutions

**ABSTRACT**

The digital transformation of higher education requires secure mechanisms for validating administrative documents, as handwritten signatures and signature images without cryptographic support create authenticity risks and operational delays. This study presents DIGISIGN, a digital signature platform based on X.509 certificates and the PAdES standard to protect the integrity, authenticity, and traceability of PDF documents. The applied research followed a mixed-methods approach with a descriptive and evaluative scope. The institutional assessment combined document review, direct observation, and interviews with two key informants. The technical evaluation included functional testing, performance metrics, and a synthetic dataset of 5,000 records used to calibrate the Isolation Forest algorithm. The model achieved an accuracy of 97.00% and an F1-score of 0.6796 for the anomaly class. Its integration with deterministic rules eliminated classification errors in a controlled simulation of 1,000 transactions. Load testing maintained a 100% success rate with up to 20 concurrent users, but this rate decreased to 80% with 50 users. The findings support the technical feasibility of DIGISIGN in the evaluated environment, although its institutional implementation requires validation with real operational data and higher-capacity infrastructure

***Keywords*:** digital signature; PAdES; artificial intelligence; higher education; administrative processes

**Recibido: 12- mayo-2026 / Aprobado: 07-septiembre-2026**

## INTRODUCCIÓN

La transformación digital ofrece herramientas para agilizar los procesos administrativos de las instituciones de educación superior (IES) (Adapting, 2018). Pese a estos avances, trámites como la firma de oficios, actas y documentos relacionados con el servicio social todavía dependen de soportes físicos y de la presencia de las autoridades responsables. Esta dinámica prolonga los tiempos de gestión y mantiene costos asociados con el uso de papel, tinta y traslado de documentos.

La digitalización universitaria no se limita a incorporar tecnologías en las aulas. También exige renovar la infraestructura y adaptar los modelos de gestión académica y administrativa (De Giusti, 2023). En esta área persisten sistemas que almacenan imágenes de firmas o registros simples sin mecanismos criptográficos suficientes (Martínez Alcántara, 2025). Una imagen insertada en un archivo PDF no vincula de manera verificable la identidad del firmante con el contenido ni permite detectar por sí misma modificaciones posteriores. Ortega Gámez et al. (2024) advierten que la dependencia de documentos físicos y tareas manuales produce flujos lentos que justifican la sistematización de los procesos institucionales.

En México, la Ley de Firma Electrónica Avanzada establece el marco para reconocer los efectos jurídicos de este mecanismo cuando se cumplen los requisitos aplicables. Entre sus principios se encuentra la equivalencia funcional, según la cual una firma electrónica avanzada puede producir efectos equivalentes a los de una firma autógrafa, sin que esta correspondencia derive únicamente de digitalizar su apariencia (León Izquierdo, 2011). Por ello, una plataforma institucional debe proteger la autenticidad del firmante, la integridad documental y la trazabilidad de las operaciones, además de ajustarse a las disposiciones internas de la organización que la adopte.

La propuesta se apoya, en primer lugar, en la infraestructura de clave pública (PKI) y el estándar X.509 para administrar certificados e identidades criptográficas (Celada & Filandini, 2016). En los documentos PDF, el estándar PAdES permite incorporar firmas electrónicas con información verificable sobre el certificado y el estado del archivo. Sus perfiles orientados a la validación

prolongada requieren datos adicionales, como sellos de tiempo y evidencias de validación, para conservar la capacidad de comprobación después del vencimiento del certificado.

Vintimilla-Rodríguez y Criollo-Bonilla (2024) analizaron en un entorno universitario una infraestructura que combinó funciones hash SHA-256, cifrado RSA de 2.048 bits y certificados gestionados institucionalmente. Sus pruebas también mostraron los riesgos derivados de una administración deficiente de las credenciales: un contenedor PKCS#12 protegido por una contraseña vulnerable fue comprometido después de 1.950.258 intentos realizados durante 21 minutos. Este resultado indica que la solidez de los algoritmos no sustituye las políticas de contraseñas, la custodia de claves, el control de acceso y el sellado de tiempo.

La elección del formato documental también incide en la seguridad y conservación de los archivos. El uso de PAdES en la administración electrónica permite integrar la firma al documento PDF y verificar si el contenido fue alterado después de su aplicación (Martínez Alcántara, 2025). Su adopción puede reducir operaciones manuales, aunque los efectos sobre los costos y los tiempos deben comprobarse en el entorno institucional. La conservación de los documentos exige, además, reglas para su almacenamiento, consulta y disposición durante todo el ciclo de vida. El modelo propuesto por Lozada Ávila (2025) destaca la necesidad de articular repositorios y bases de datos que mantengan accesibles y verificables los archivos electrónicos.

El segundo componente corresponde a la auditoría de los registros de actividad. Los mecanismos criptográficos protegen el documento, pero no identifican necesariamente comportamientos atípicos durante el uso de la plataforma. Los métodos de aprendizaje automático pueden apoyar el análisis de grandes volúmenes de datos y la detección de patrones que se apartan del comportamiento esperado (González-García, 2018). DIGISIGN incorpora para esta función el algoritmo no supervisado Isolation Forest y lo complementa con reglas deterministas asociadas con roles, horarios y condiciones de acceso.

La investigación se desarrolló en áreas académicas y administrativas del Centro Universitario de Ciencias Exactas e Ingenierías de la Universidad de Guadalajara. Aunque existen propuestas sobre

firma electrónica, gestión documental y certificados institucionales, persiste la necesidad de integrar en una misma plataforma la firma PAdES, la gestión de certificados X.509, la verificación mediante códigos QR y la auditoría asistida por inteligencia artificial. El objetivo del estudio fue presentar y evaluar la viabilidad técnica de DIGISIGN para la firma digital y la detección de anomalías en procesos administrativos universitarios. La evaluación comprendió el diagnóstico institucional, pruebas funcionales, calibración del modelo y mediciones de rendimiento en un entorno controlado; por tanto, no buscó demostrar una implementación institucional definitiva ni su eficacia en condiciones reales de producción.

En este contexto, la transformación digital universitaria requiere integrar la eficiencia administrativa con mecanismos verificables de confianza, interoperabilidad y gobernanza tecnológica (Organización para la Cooperación y el Desarrollo Económicos [OCDE], 2023). La autenticación institucional debe sustentarse en procesos de gestión de identidad proporcionales al riesgo de cada operación (Temoshok et al., 2025), mientras que los certificados X.509 permiten vincular identidades y claves públicas dentro de una infraestructura criptográfica normalizada (Cooper et al., 2008). Asimismo, el estándar PAdES establece perfiles para incorporar firmas digitales y evidencias de validación en documentos PDF (European Telecommunications Standards Institute [ETSI], 2016). Esta protección puede complementarse mediante Isolation Forest, algoritmo que identifica observaciones anómalas al aislarlas mediante particiones aleatorias, sin requerir inicialmente clases etiquetadas (Liu et al., 2008). Estos fundamentos respaldan una arquitectura que articule firma digital, control de acceso y auditoría automatizada, cuya eficacia debe comprobarse con datos operativos institucionales.

## METODOLOGÍA

### Enfoque y diseño de la investigación

La investigación siguió un enfoque mixto y una orientación aplicada. El componente cualitativo se utilizó para comprender los problemas asociados con la gestión y seguridad de los documentos internos de la universidad, mientras que el componente cuantitativo comprendió la evaluación

funcional de DIGISIGN, la calibración del modelo de detección de anomalías y las pruebas de rendimiento de la plataforma.

El estudio tuvo alcance descriptivo y evaluativo y se organizó en dos fases. La primera correspondió a un estudio de caso institucional, dirigido al diagnóstico de los procesos de validación y firma documental. La segunda consistió en el desarrollo tecnológico y la evaluación experimental de la plataforma mediante datos y escenarios simulados. Por esta razón, el diseño no se considera exclusivamente no experimental y transversal: el diagnóstico se realizó en un periodo delimitado, pero las pruebas técnicas implicaron modificar parámetros, niveles de concurrencia y configuraciones del modelo.

**Contexto e informantes**

La fase institucional se desarrolló en el Departamento de Innovación Basada en la Información y el Conocimiento del Centro Universitario de Ciencias Exactas e Ingenierías de la Universidad de Guadalajara. Mediante una selección intencional se incluyeron dos informantes con participación en los procesos estudiados: la jefa de un departamento académico y un profesor de tiempo completo adscrito al mismo departamento, especializado en ciberseguridad y transformación digital.

El número de informantes respondió al carácter diagnóstico del estudio de caso y no tuvo como propósito representar estadísticamente al personal universitario. Sus aportaciones se utilizaron para identificar necesidades operativas y definir requerimientos funcionales y de seguridad de la plataforma.

**Técnicas de diagnóstico**

El diagnóstico combinó tres técnicas:

- **Revisión documental:** se examinaron normas universitarias y disposiciones mexicanas relacionadas con la firma electrónica para identificar requisitos técnicos e institucionales aplicables.
- **Observación directa:** se revisaron los flujos de generación, traslado, validación y firma de documentos oficiales en las oficinas del centro universitario.

- **Entrevistas semiestructuradas:** se entrevistó a los dos informantes sobre carga administrativa, seguridad, gestión documental y tiempos de tramitación. Las entrevistas se registraron en audio con autorización de los participantes y luego se transcribieron. Las transcripciones se examinaron para identificar necesidades recurrentes, limitaciones del procedimiento existente y requerimientos para el diseño de DIGISIGN.

La información obtenida mediante las tres técnicas se contrastó para relacionar las necesidades expresadas por los informantes con los procesos observados y las exigencias documentales revisadas.

**Desarrollo de DIGISIGN**

El desarrollo se gestionó mediante iteraciones cortas basadas en Scrum y un repositorio de GitHub para mantener la trazabilidad del código. La plataforma se implementó con una arquitectura contenerizada en Docker. El backend se desarrolló con Django REST Framework y PostgreSQL, mientras que la interfaz de usuario se construyó en React mediante Vite.

La autenticación utilizó tokens JWT firmados y un segundo factor basado en contraseñas de un solo uso generadas por tiempo (TOTP). El control de acceso se organizó en tres roles: el capturador, encargado de la validación inicial y la digitalización; el administrador, responsable de comprobar identidades y autorizar certificados; y el firmante, titular de la clave privada y el certificado empleado para firmar. El sistema también incorporó notificaciones mediante el protocolo SMTP.

La función de firma se implementó con PyMuPDF, Cryptography y pyHanko. PyMuPDF se empleó para gestionar metadatos y controles de aplicación orientados a evitar firmas duplicadas. Cryptography y pyHanko se utilizaron para calcular el hash SHA-256 y aplicar firmas PAdES incrementales con certificados X.509 y sellos de tiempo. Este procedimiento permite verificar la integridad del PDF y detectar modificaciones posteriores, sin atribuir al software por sí solo la validez jurídica de las firmas.

El almacenamiento se distribuyó en volúmenes separados para documentos firmados, claves privadas y certificados. El material correspondiente a la autoridad certificadora se mantuvo aislado de los demás componentes. Esta segmentación buscó reducir la exposición de las credenciales y separar los recursos de acuerdo con su función.

**Modelo de detección de anomalías**

La auditoría asistida por inteligencia artificial se implementó mediante Isolation Forest, un algoritmo de aprendizaje no supervisado. El modelo analizó la hora y el día del evento, el tipo de operación, el rol del usuario y la dirección IP para identificar registros que se apartaran del comportamiento esperado.

La calibración se efectuó con un conjunto sintético de 5.000 registros, compuesto por 4.734 eventos clasificados como normales y 266 como anómalos. Se probaron distintas combinaciones de hiperparámetros y se seleccionó la configuración según el F1-score de la clase anómala, junto con la precisión, la sensibilidad y la exactitud global.

El modelo probabilístico se complementó con reglas deterministas relacionadas con permisos, horarios y condiciones de acceso. El funcionamiento conjunto se evaluó mediante una simulación controlada de 1.000 transacciones concurrentes: 735 eventos legítimos y 265 vectores de ataque sintéticos. La comparación entre las etiquetas asignadas a los eventos y la clasificación producida por el sistema se representó mediante una matriz de confusión.

**Evaluación funcional y de rendimiento**

La evaluación técnica comprendió pruebas funcionales y de carga. Las primeras verificaron la ejecución de las firmas electrónicas, la validación criptográfica de los documentos, los controles contra firmas duplicadas y la legibilidad de los códigos QR incorporados en los archivos PDF.

Las pruebas de carga midieron el tiempo medio de respuesta, la tasa de operaciones completadas y el consumo de CPU y memoria ante escenarios de 1, 5, 10, 20 y 50 usuarios concurrentes. La plataforma se desplegó en una máquina virtual e2-micro de Google Cloud Platform, ubicada en la zona northamerica-south1-c. La instancia disponía de dos vCPU compartidas, 1 GB de memoria RAM, Ubuntu 22.04 LTS sobre arquitectura x86_64 y un disco persistente estándar de 18 GB con permisos de lectura y escritura. Esta configuración representa un entorno de recursos limitados y no una infraestructura institucional de producción.

Los resultados se analizaron mediante estadística descriptiva. Para el modelo se calcularon precisión, sensibilidad, F1-score, exactitud y matriz de confusión. En las pruebas de carga se registraron tiempos medios de respuesta, tasas de éxito y consumo de recursos. No se realizaron pruebas inferenciales.

**Consideraciones éticas**

La investigación no involucró poblaciones vulnerables ni utilizó datos personales sensibles en las pruebas técnicas. Los dos informantes recibieron información sobre el propósito académico del estudio y otorgaron su consentimiento para participar y para registrar las entrevistas. Los documentos empleados durante las pruebas fueron generados y controlados por el equipo de desarrollo, por lo que no se procesaron expedientes institucionales reales.

**Delimitación del alcance**

DIGISIGN se desarrolló y evaluó como un prototipo funcional para firmar y auditar documentos PDF previamente elaborados. La plataforma no automatizó el trámite administrativo completo ni fue validada con datos operativos reales. Su adopción oficial requeriría autorización institucional, adecuación al marco normativo aplicable, gestión formal de certificados y pruebas en una infraestructura de producción. Las funciones futuras relacionadas con la emisión automatizada de constancias, pagos en línea y edición colaborativa no formaron parte de la evaluación presentada.

**RESULTADOS Y DISCUSIÓN**

**Diagnóstico institucional**

El diagnóstico cualitativo realizado en el Centro Universitario de Ciencias Exactas e Ingenierías (CUCEI) integró la revisión documental, la observación de los procesos y las entrevistas semiestructuradas a dos informantes: la jefa del Departamento de Innovación Basada en la Información y el Conocimiento y un profesor de tiempo completo especializado en ciberseguridad y transformación digital. La comparación de estas fuentes permitió identificar problemas operativos y requerimientos para el diseño de DIGISIGN.

La informante del área técnico-administrativa señaló que cerca de 20 flujos documentales dependían de firmas manuscritas. Según su estimación, los reportes de calificaciones de cierre de ciclo

comprendían alrededor de 700 secciones académicas, con documentos de hasta cinco páginas, y requerían la revisión manual de más de 2.000 hojas. El proceso podía concentrar hasta una semana de trabajo y dependía de la presencia física de los responsables. Estas cifras proceden de la entrevista y describen el funcionamiento del departamento estudiado; no corresponden a mediciones obtenidas mediante registros administrativos institucionales.

El diagnóstico también identificó limitaciones en los mecanismos empleados para digitalizar las firmas. De acuerdo con los informantes y la observación realizada, algunos procedimientos consistían en insertar imágenes de firmas en archivos PDF sin vincularlas mediante certificados criptográficos. Este mecanismo no permite comprobar de forma independiente la identidad del firmante ni detectar con certeza modificaciones posteriores, sobre todo cuando el documento circula fuera de los sistemas internos de la universidad.

El segundo informante indicó que la elaboración de oficios, dictámenes e invitaciones podía representar decenas de documentos mensuales y cientos al año por académico. La ubicación de los responsables en distintos espacios físicos prolongaba las autorizaciones desde algunas horas hasta varios días. Desde su experiencia en seguridad informática, identificó como requerimientos la autenticación reforzada, la protección de certificados y claves, la integridad de los archivos y la trazabilidad de las operaciones.

Ambos informantes consideraron que la firma remota mediante credenciales institucionales podría reducir los traslados físicos y situar determinados periodos de autorización entre uno y dos días hábiles. Este valor representa una proyección de los participantes y no un tiempo medido después de implementar DIGISIGN. También destacaron la utilidad de incorporar códigos QR para consultar la validez del documento y manifestaron interés en participar en una prueba institucional controlada. Tal prueba permitiría obtener registros operativos reales para evaluar el desempeño de la plataforma y ajustar el modelo de detección de anomalías al entorno universitario, siempre que se establezcan las autorizaciones y medidas de protección de datos correspondientes.

**Validación de la arquitectura y correspondencia normativa**

Las pruebas funcionales confirmaron la generación de firmas PAdES con certificados X.509 y la posterior verificación de la integridad de los archivos PDF. Durante las pruebas de carga no se observaron alteraciones en los documentos procesados ni inconsistencias en la base de datos PostgreSQL. La separación de documentos, claves, certificados y material de la autoridad certificadora en volúmenes independientes mantuvo la segmentación prevista por la arquitectura.

Los controles implementados en la aplicación rechazaron intentos de agregar firmas duplicadas no autorizadas sobre un mismo documento. Este resultado comprueba el funcionamiento del control en los escenarios ensayados, pero no demuestra que el sistema sea inmune a cualquier forma de alteración o ataque. Del mismo modo, el control de acceso basado en roles restringió las operaciones de acuerdo con los permisos asignados. No puede afirmarse que haya eliminado por completo la suplantación de identidad, pues este riesgo también depende de la protección de credenciales, claves privadas, sesiones y dispositivos de los usuarios.

La arquitectura incorporó mecanismos relacionados con la integridad, autenticidad y trazabilidad previstas en la Ley de Firma Electrónica Avanzada y en el Acuerdo RG-10-2026 de la Universidad de Guadalajara. Esta correspondencia constituye una revisión técnica preliminar, no una certificación de cumplimiento jurídico ni una autorización institucional para utilizar DIGISIGN en producción. La validez de las firmas dependerá de la gestión de certificados, la identificación de los firmantes, la custodia de las claves y las disposiciones aplicables a cada procedimiento.

Frente a los esquemas basados únicamente en imágenes de firmas descritos en el diagnóstico y en antecedentes nacionales (Guzmán Ávalos, 2010), DIGISIGN integra firma criptográfica, verificación mediante códigos QR y auditoría asistida por inteligencia artificial. Esta combinación constituye el aporte técnico de la propuesta. Su capacidad para reducir el uso de papel, mejorar los tiempos administrativos o fortalecer la autonomía tecnológica deberá comprobarse mediante una implementación piloto con documentos y usuarios reales.

**Comportamiento del modelo de inteligencia artificial e integración híbrida**

La auditoría de DIGISIGN incorporó el algoritmo no supervisado Isolation Forest para detectar patrones atípicos en las bitácoras. La calibración se realizó mediante búsqueda en rejilla (*grid search*) sobre 5.000 registros sintéticos. Con el parámetro de contaminación configurado automáticamente, el F1-score de la clase anómala descendió hasta 0,1431. La mejor configuración evaluada utilizó 300 estimadores y una contaminación de 0,05, con un F1-score de 0,6796 para las anomalías y una exactitud global del 96,70 %, redondeada al 97 % en la Tabla 1.

La matriz de resultados del modelo aislado registró 74 falsos positivos, correspondientes a eventos legítimos clasificados como anómalos, y 91 falsos negativos, es decir, anomalías identificadas como normales. Isolation Forest separa observaciones mediante particiones aleatorias y asigna puntuaciones según su grado de aislamiento; por ello, no interpreta directamente las políticas institucionales asociadas con roles, horarios o permisos. Esta limitación justificó la incorporación de una capa determinista basada en reglas de negocio.

La capa contextual verificó la matriz de roles y permisos, aplicó restricciones de acceso entre las 22:00 y las 06:59 horas y bloqueó operaciones en días no laborables. El comportamiento del sistema híbrido se evaluó con 1.000 transacciones simuladas: 735 eventos legítimos y 265 vectores de ataque sintéticos relacionados con suplantación de roles, accesos nocturnos, actividad automatizada y direcciones IP no habituales. La distribución de las clasificaciones se presenta en la Tabla 2.

La complementariedad entre ambos componentes puede observarse en dos situaciones. Ante varios errores consecutivos al introducir un código TOTP durante el horario autorizado y desde la red institucional, Isolation Forest puede considerar atípica la frecuencia del evento. La regla determinista aplica el bloqueo temporal previsto después de cinco intentos fallidos, pero diferencia este incidente de una alerta de mayor criticidad cuando las demás condiciones de acceso son legítimas. Por otra parte, si una credencial comprometida se utiliza durante un horario permitido, las reglas temporales podrían no detectar la amenaza. En ese caso, el modelo puede generar una alerta cuando el patrón de acceso, incluida la dirección IP, se aparta de los registros sintéticos considerados normales.

En la simulación controlada, la arquitectura híbrida clasificó correctamente los 735 eventos legítimos y los 265 ataques generados, sin falsos positivos ni falsos negativos (Tablas 2 y 3). Este resultado equivale a una exactitud del 100 % dentro del conjunto simulado, pero no demuestra el mismo rendimiento en producción. Las reglas se evaluaron sobre escenarios previamente definidos y el modelo utilizó datos sintéticos; por tanto, será necesario validar el comportamiento con registros operativos independientes antes de estimar su capacidad de generalización.

**Telemetría de la infraestructura y métricas de carga**

La plataforma se evaluó en una instancia e2-micro de Google Cloud Platform ubicada en la zona northamerica-south1-c, con dos vCPU compartidas, 1 GB de memoria RAM, Ubuntu 22.04 LTS y un disco persistente de 18 GB. Las pruebas midieron el comportamiento del backend de Django durante solicitudes concurrentes de firma PAdES con certificados X.509.

El tiempo medio de respuesta aumentó de 1,77 segundos con un usuario a 7,23 segundos con cinco, 48,47 segundos con diez y 92,62 segundos con veinte usuarios concurrentes. La progresión no fue estrictamente lineal, sino que mostró una degradación acentuada a partir de diez usuarios. La tasa de operaciones completadas se mantuvo en el 100 % hasta veinte usuarios, sin alteraciones detectadas en los documentos PDF procesados. Con cincuenta solicitudes concurrentes, el tiempo medio superó el límite de espera de 300 segundos y la tasa de éxito disminuyó al 80 %, lo que señala la saturación del entorno evaluado (Tabla 4).

La telemetría de los contenedores mostró que el backend concentró el mayor consumo de recursos. De acuerdo con la Tabla 5, su utilización pasó del 22,22 % de CPU y 128,4 MiB de memoria en reposo a 1.346,34 % de CPU y 183,3 MiB durante el escenario de cincuenta solicitudes. El frontend mantuvo un uso de CPU entre el 1,21 % y el 2,37 %, mientras que PostgreSQL pasó del 0,00 % al 0,90 %. La memoria de estos componentes permaneció dentro de márgenes reducidos.

El registro de 1.346,34 % de CPU no es directamente compatible con una máquina virtual limitada a dos vCPU, cuya medición agregada normalmente no debería superar el 200 % bajo la convención utilizada por docker stats. Antes de publicar este resultado, debe verificarse si la telemetría se obtuvo

en otro host, si el porcentaje fue acumulado entre muestras o si la herramienta aplicó una normalización diferente. Mientras no se documente ese criterio, el valor solo puede presentarse como el dato reportado por la herramienta y no como consumo efectivo de la instancia e2-micro.

Los tiempos de respuesta y la estabilidad relativa de la memoria sugieren que el procesamiento de las firmas ejerce mayor presión sobre la CPU que sobre la RAM. Sin embargo, estas métricas no bastan para atribuir el cuello de botella exclusivamente al cifrado asimétrico ni para descartar problemas en el código, la configuración del servidor o la gestión de procesos. Esta conclusión requeriría perfiles de CPU, tiempos desagregados por operación y mediciones repetidas bajo las mismas condiciones.

Para un despliegue institucional con mayor concurrencia, los resultados respaldan la evaluación de instancias optimizadas para cómputo, como las pertenecientes a la serie e2-highcpu o sus equivalentes. Un mayor número de vCPU permitiría configurar más procesos trabajadores y distribuir las operaciones de firma. Esta alternativa debe compararse con el procesamiento asíncrono mediante colas de tareas, el escalamiento horizontal y la optimización del backend, pues el aumento de recursos no garantiza por sí solo tiempos de respuesta estables.

**Tabla 1.** Desempeño del modelo Isolation Forest sobre el conjunto sintético de evaluación

| **Métrica** | **Clase normal (1)** | **Clase anómala (−1)** | **Promedio ponderado** |
|---|---|---|---|
| Precisión | 0,98 | 0,70 | 0,97 |
| Sensibilidad | 0,98 | 0,66 | 0,97 |
| F1-score | 0,98 | 0,68 | 0,97 |
| Soporte | 4.734 | 266 | 5.000 |
| Exactitud global | — | — | 0,967 |

**Nota**. Resultados obtenidos con 5.000 registros sintéticos después de la optimización de hiperparámetros. La configuración seleccionada utilizó 300 estimadores y un factor de contaminación de 0,05. La exactitud global fue del 96,70 %, equivalente al 97 % al redondear a números enteros. Debe precisarse si estas métricas proceden de un conjunto independiente o del mismo conjunto utilizado para ajustar el modelo. Elaboración propia.

**Tabla 2.** Matriz de confusión del motor híbrido en la simulación controlada

| Clase real | Predicha como normal | Predicha como anómala |
|---|---|---|
| Evento legítimo (73,5 %) | 735 (verdaderos negativos) | 0 (falsos positivos) |
| Ataque sintético (26,5 %) | 0 (falsos negativos) | 265 (verdaderos positivos) |

**Nota**. Se consideró la anomalía como clase positiva. La simulación incluyó 1.000 transacciones: 735 eventos legítimos y 265 vectores de ataque sintéticos. La ausencia de errores corresponde exclusivamente a los escenarios y reglas evaluados; no representa una validación en producción. Elaboración propia.

**Tabla 3.** Cobertura de escenarios por los componentes del motor híbrido

| Escenario evaluado | Reglas deterministas | Modelo de IA | Componente principal |
|---|---|---|---|
| El capturador intenta eliminar una cuenta | Sí | No | Reglas |
| El administrador inicia sesión en un día no laborable | Sí | No | Reglas |
| Un bot opera en horario autorizado | No | Sí | Modelo de IA |
| Se firma desde una dirección IP externa no habitual | No | Sí | Modelo de IA |
| Se registran cinco intentos fallidos de TOTP | Sí | Sí | Reglas |

**Nota**. La tabla muestra la complementariedad observada en los escenarios simulados. Las reglas aplican restricciones previamente definidas, mientras que Isolation Forest identifica patrones atípicos que podrían no infringir una regla estática. La clasificación depende de la configuración y de los datos utilizados, por lo que debe validarse con registros operativos reales. Elaboración propia.

**Tabla 4.** Latencia y tasa de éxito en los escenarios de carga concurrente

| Usuarios concurrentes | Tiempo medio de respuesta (s) | Tasa de éxito (%) |
|---|---|---|
| 1 | 1,77 | 100 |
| 5 | 7,23 | 100 |
| 10 | 48,47 | 100 |
| 20 | 92,62 | 100 |
| 50 | >300,00 | 80 |

**Nota**. Pruebas efectuadas en una máquina virtual con dos vCPU compartidas y 1 GB de RAM. El aumento de la latencia no fue estrictamente lineal. En el escenario de 50 usuarios se superó el límite de espera de 300 segundos y la tasa de operaciones completadas disminuyó al 80 %. Elaboración propia.

**Tabla 5.** Consumo de recursos de los contenedores Docker durante la prueba con 50 usuarios concurrentes

| Contenedor | Métrica | Reposo | Pico registrado |
|---|---|---|---|
| Backend | CPU | 22,22 % | 1.346,34 %ª |
| | Memoria | 128,4 MiB | 183,3 MiB |
| | Memoria respecto del límite | 13,39 % | 19,44 % |
| Frontend | CPU | 1,21 % | 2,37 % |
| | Memoria | 47,06 MiB | 35,42 MiB |
| | Memoria respecto del límite | 4,91 % | 3,70 % |
| Base de datos | CPU | 0,00 % | 0,90 % |
| | Memoria | 59,00 MiB | 62,61 MiB |
| | Memoria respecto del límite | 6,16 % | 6,53 % |

**Nota**. Los valores corresponden a la telemetría reportada durante el escenario de mayor carga. ªEl registro de 1.346,34 % de CPU no es directamente compatible con una máquina virtual limitada a dos vCPU bajo la convención habitual de docker stats. Antes de publicar la tabla debe verificarse la herramienta, el host y el método de normalización utilizados. Si el dato no puede reproducirse, no debe interpretarse como consumo efectivo de la instancia e2-micro. Elaboración propia.

Los resultados respaldan la viabilidad técnica de DIGISIGN, pero su alcance debe circunscribirse al entorno controlado en el que fue evaluado. La implementación mediante Scikit-learn proporciona una base reproducible para el entrenamiento y la comparación de modelos de aprendizaje automático (Pedregosa et al., 2011); aun así, el rendimiento obtenido con registros sintéticos no garantiza un comportamiento equivalente frente al tráfico institucional real, debido a las diferencias que pueden surgir entre los datos experimentales y las condiciones operativas (Sommer & Paxson, 2010). La combinación de Isolation Forest con reglas deterministas reduce errores dentro de la simulación, aunque su aplicación sostenida exigirá supervisar cambios en los datos, configuraciones y dependencias del sistema (Sculley et al., 2015). La utilidad de esta auditoría también dependerá de una gestión que asegure la generación, protección, conservación y revisión de las bitácoras (Kent & Souppaya, 2006).

Por último, el incremento de la latencia bajo concurrencia confirma que el desempeño debe evaluarse considerando los tiempos extremos de respuesta y no solamente los valores promedio (Dean & Barroso, 2013). En conjunto, estos elementos justifican una prueba piloto con datos reales antes de adoptar la plataforma a escala institucional.

**CONCLUSIONES**

El desarrollo y las pruebas realizadas respaldan la viabilidad técnica preliminar de DIGISIGN como plataforma para firmar y verificar documentos PDF en el contexto universitario estudiado. El diagnóstico mostró las limitaciones operativas y de seguridad de los procedimientos basados en firmas manuscritas o imágenes sin respaldo criptográfico. La integración de certificados X.509, firmas PAdES, control de acceso y trazabilidad ofrece mecanismos para comprobar la identidad asociada con la firma y detectar modificaciones posteriores. Su correspondencia jurídica e institucional deberá validarse antes de cualquier implementación oficial.

El modelo Isolation Forest alcanzó una exactitud del 96,70 % y un F1-score de 0,6796 para la clase anómala en el conjunto sintético. Su combinación con reglas deterministas clasificó correctamente los 1.000 eventos de la simulación controlada. Este resultado confirma la complementariedad de ambos componentes en los escenarios evaluados, pero no permite afirmar que el sistema eliminará los falsos positivos y negativos cuando opere con datos reales.

Las pruebas de carga mantuvieron una tasa de éxito del 100 % hasta 20 usuarios concurrentes, aunque la latencia aumentó de forma considerable. Con 50 usuarios, el tiempo de respuesta superó los 300 segundos y la tasa de éxito descendió al 80 %. Los resultados muestran una limitación de capacidad en el backend, pero no permiten atribuirla exclusivamente al cifrado ni descartar factores relacionados con el código o la configuración del servidor. El registro máximo de CPU también deberá verificarse antes de sustentar decisiones de infraestructura.

La validación institucional requiere una prueba piloto con usuarios, documentos y registros operativos reales, además de evaluaciones jurídicas y de seguridad. Como trabajo futuro, se propone comparar el escalamiento vertical con arquitecturas de procesamiento asíncrono mediante colas de tareas,

como Celery o RabbitMQ, y estudiar modelos capaces de analizar secuencias temporales en las bitácoras. Estas ampliaciones deberán evaluarse con conjuntos independientes y métricas que permitan estimar su desempeño fuera de los escenarios sintéticos empleados en esta investigación.

**REFERENCIAS BIBLIOGRÁFICAS**


Adapting. (2018). *Compendio de retos de la era de la transformación digital en LATAM*. https://www.adapting.com/wp-content/uploads/2018/11/22_compendio_retos_era_transf_digital_latam.pdf

Celada, G. J., & Filandini, J. M. (2016). *Ampliación y mejora de servicios en la infraestructura de clave pública para e-ciencia de la UNLP (PKIGrid UNLP)* [Tesis de grado, Universidad Nacional de La Plata]. SEDICI. http://sedici.unlp.edu.ar/handle/10915/59094

Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., & Polk, W. (2008). *Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile* (RFC 5280). RFC Editor. https://doi.org/10.17487/RFC5280

Dean, J., & Barroso, L. A. (2013). The tail at scale. *Communications of the ACM, 56*(2), 74–80. https://doi.org/10.1145/2408776.2408794

De Giusti, A. E. (2023). Transformación digital en educación superior: Posibilidades y desafíos. *Revista Iberoamericana de Tecnología en Educación y Educación en Tecnología, 35*, 9–15. https://doi.org/10.24215/18509959.35.e1

European Telecommunications Standards Institute. (2016). *Electronic signatures and infrastructures (ESI): PAdES digital signatures—Part 1: Building blocks and PAdES baseline signatures* (ETSI EN 319 142-1 V1.1.1). https://www.etsi.org/deliver/etsi_en/319100_319199/31914201/01.01.01_60/en_319142001v010101p.pdf

González-García, C. (2018). En qué consiste el aprendizaje automático (*machine learning*) y qué está aportando a la neurociencia cognitiva. *Ciencia Cognitiva*. https://www.cienciacognitiva.org/?p=1697

Guzmán Ávalos, A. (2010). La firma electrónica en México. *Anuario de la Facultad de Derecho, 28*, 507–533. https://dialnet.unirioja.es/descarga/articulo/3438233.pdf

Kent, K., & Souppaya, M. (2006). *Guide to computer security log management* (NIST Special Publication 800-92). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-92

León Izquierdo, A. (2011). La implementación de la firma electrónica en México. *Economía Informa, 369*, 97–103. https://economia.unam.mx/publicaciones/econinforma/369/08leonizquierdo.pdf

Liu, F. T., Ting, K. M., & Zhou, Z.-H. (2008). Isolation Forest. En *2008 Eighth IEEE International Conference on Data Mining* (pp. 413–422). IEEE. https://doi.org/10.1109/ICDM.2008.17

Lozada Ávila, C. (2025). *Modelo de gestión de documentos electrónicos para instituciones de educación superior* [Trabajo de investigación, Universidad de Medellín]. Repositorio Institucional de la Universidad de Medellín. https://repository.udemedellin.edu.co/items/b8c50c90-21f4-4f9f-9511-7dc442790f65

Martínez Alcántara, M. L. (2025). *Sistema de firma electrónica PAdES aplicada a la administración electrónica* [Trabajo académico, Universidad Politécnica de Cartagena]. Repositorio Digital de la Universidad Politécnica de Cartagena. https://repositorio.upct.es/entities/publication/79cbfad6-5f9b-470e-8c8e-1bc569e789b3

Organización para la Cooperación y el Desarrollo Económicos. (2023). *OECD digital education outlook 2023: Towards an effective digital education ecosystem*. OECD Publishing. https://doi.org/10.1787/c74f03de-en

Ortega Gámez, J. D. D., De la Cruz Maldonado, J. C., & Ábrego Almazán, D. (2024). Aplicación de la firma digital en una institución de educación superior. *RECAI Revista de Estudios en Contaduría, Administración e Informática, 13*(37), 15–28. https://doi.org/10.36677/recai.v13i37.22367

Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., Blondel, M., Prettenhofer, P., Weiss, R., Dubourg, V., VanderPlas, J., Passos, A., Cournapeau, D., Brucher, M., Perrot, M., & Duchesnay, É. (2011). Scikit-learn: Machine learning in Python. *Journal of Machine Learning Research, 12*, 2825–2830. https://www.jmlr.org/papers/v12/pedregosa11a.html

Sculley, D., Holt, G., Golovin, D., Davydov, E., Phillips, T., Ebner, D., Chaudhary, V., Young, M., Crespo, J.-F., & Dennison, D. (2015). Hidden technical debt in machine learning systems. En C. Cortes, N. Lawrence, D. Lee, M. Sugiyama, & R. Garnett (Eds.), *Advances in Neural Information Processing Systems 28* (pp. 2503–2511). Curran Associates. https://proceedings.neurips.cc/paper/2015/hash/86df7dcfd896fcaf2674f757a2463eba-Abstract.html

Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. En *2010 IEEE Symposium on Security and Privacy* (pp. 305–316). IEEE. https://doi.org/10.1109/SP.2010.25

Temoshok, D., Galluzzo, R., LaSalle, C., Lefkovitz, N., Regenscheid, A., Choong, Y.-Y., Proud-Madruga, D., & Gupta, S. (2025). *Digital identity guidelines* (NIST Special Publication 800-63-4). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63-4

Universidad de Guadalajara. (2026). *Acuerdo RG-10-2026 que actualiza las Bases Generales para el Uso de Firma Electrónica en la Universidad de Guadalajara*. Secretaría General. https://secgral.udg.mx/sites/default/files/Acuerdos/Acuerdo%20RG-10-2026%20Que%20actualiza%20las%20Bases%20Generales%20para%20el%20uso%20de%20Firma%20Electro%CC%81nica%20en%20la%20Universidad%20de%20Guadalajara%20%282%29.pdf

Vintimilla-Rodríguez, T. R., & Criollo-Bonilla, R. R. (2024). Esquema de generación de certificados de firma electrónica avanzada en la Universidad Católica de Cuenca: Un estudio técnico basado en modelos de criptografía aplicada. *MQRInvestigar, 8*(3), 1543–1565. https://doi.org/10.56048/MQR20225.8.3.2024.1543-1565