

Las Tecnologías de la Información y Comunicación en los Medios de Prueba Digitales: Análisis en el Derecho Procesal Civil en Paraguay

The Information and Communication Technologies in Digital Evidence:
Analysis in Civil Procedural Law in Paraguay

Amado Juan Pablo Ramírez Alfonso ¹

RESUMEN

El objetivo del trabajo es analizar la influencia de las Tecnologías de la Información y la Comunicación (TIC) y la Inteligencia Artificial (IA) en la validez, preservación y valoración de las pruebas digitales en los procesos judiciales civiles, así como sus implicancias en la seguridad jurídica en Paraguay. La metodología aplicada enfoque cualitativo con revisión documental y diseño no experimental. El método o la técnica e instrumentos aplicados, fueron análisis de legislación relevante y revisión de sobre TIC, IA y derecho procesal civil. La muestra u objeto de estudio fueron las Tecnologías de la Información y la Comunicación (TIC) y la Inteligencia Artificial (IA) en el contexto del derecho procesal civil en Paraguay. Los resultados son que las TIC han ayudado a la transparencia, eficiencia y accesibilidad en los procesos judiciales, pero presentan desafíos como ciberataques y manipulación de datos. A pesar de avances legislativos, persisten lagunas en protocolos específicos y formación tecnológica de operadores judiciales. Como recomendaciones se presentan: Desarrollar protocolos claros para la preservación, autenticidad y manejo forense de pruebas digitales. Implementar programas de capacitación tecnológica continua para operadores judiciales. Fortalecer las medidas de ciberseguridad para proteger los archivos electrónicos judiciales.

Palabras clave: Tecnologías de la Información y la Comunicación (TIC), Inteligencia Artificial (IA), Pruebas digitales, Seguridad jurídica.

¹ RAMÍREZ ALFONSO, Amado Juan Pablo. Doctor en Derecho Público con énfasis en Gobernabilidad y Doctor en Defensa, Desarrollo y Seguridad Estratégica Nacional (IAEE). Magíster en Planificación y Conducción Estratégica Nacional, Política y Estrategia Aeroespacial, Ciencias Militares y Operaciones Militares. Licenciado en Ciencias Militares y Abogado. Docente y tutor de tesis en programas de maestría y doctorado.

ABSTRACT

The objective of this paper is to analyze the influence of Information and Communication Technologies (ICT) and Artificial Intelligence (AI) on the validity, preservation, and assessment of digital evidence in civil judicial processes, as well as their implications for legal security in Paraguay. The applied methodology includes a qualitative approach with a documentary review and non-experimental design. The methods, techniques, and instruments applied were the analysis of relevant legislation and the review of ICT, AI, and civil procedural law. The sample or object of study was Information and Communication Technologies (ICT) and Artificial Intelligence (AI) in the context of civil procedural law in Paraguay. The results indicate that ICT has improved transparency, efficiency, and accessibility in judicial processes but present challenges such as cyber-attacks and data manipulation. Despite legislative advances, gaps persist in specific protocols and the technological training of judicial operators. Recommendations include developing clear protocols for the preservation, authenticity, and forensic handling of digital evidence, implementing continuous technological training programs for judicial operators, and strengthening cybersecurity measures to protect electronic judicial files.

Keywords: Information and Communication Technologies (ICT), Artificial Intelligence (AI), Digital evidence, Legal security.

Introducción

El propósito de este trabajo es analizar cómo influyen las Tecnologías de la Información y la Comunicación (TIC) y la Inteligencia Artificial (IA) en la validez, preservación y valoración de los medios pruebas en los procesos judiciales civiles y cuáles son las implicancias en la seguridad jurídica en Paraguay.

Sus aspectos legales y técnicos pueden perturbar el normal discurrir de la valoración de la prueba, dado que el manejo inadecuado puede comprometer tanto la justicia como la seguridad jurídica.

La metodología utilizada en el presente ensayo se adecua al enfoque cualitativo con revisión documental y diseño no experimental, teniendo como unidad de análisis: las TIC y la IA.

Su estructura permite analizar la influencia de las TIC y la IA en los procesos judiciales civiles, identificar desafíos legales y técnicos y formular propuestas concretas para garantizar la seguridad jurídica y la integración eficaz de estas tecnologías.

En este sentido, se busca analizar de manera descriptiva aspectos de la influencia de la tecnología, en cuanto a su uso con relación a los medios de pruebas, la validación y preservación de dichos medios y cotejar la metodología que permita su integración eficaz en los procesos judiciales, para que la prueba digital sea aceptada y valorada como evidencia sólida.

El aumento de la dependencia de medios digitales tanto en las actividades cotidianas como en los procesos judiciales exige un cuidado conveniente para no comprometer la seguridad jurídica, el uso de las tecnologías de la información y comunicación (Tics), por un lado, facilita la labor en muchos órdenes y permite el acceso a las informaciones disponibles de manera inmediata.

Por otro lado, puede someter a riesgos por amenazas del ciberespacio sobre los archivos electrónicos judiciales, a estos dos hechos se suma, la aparición de la Inteligencia Artificial (IA) que permite la generación de elementos apócrifos que podrían ser usados como medios de pruebas de difícil detección en cuanto su falsedad.

Esta situación nos presenta la siguiente interrogante: ¿Cómo influyen las Tecnologías de la Información y la Comunicación (TIC) y la Inteligencia Artificial (IA) en la validez, preservación y valoración de los medios pruebas en los procesos judiciales civiles y cuáles son las implicancias en la seguridad jurídica en Paraguay?

De esta pregunta principal se desprenden las siguientes preguntas subsidiarias que guían este ensayo:

- ¿Qué desafíos legales y técnicos presenta el uso de medios de pruebas digitales en el contexto del derecho procesal civil?
- ¿De qué manera las herramientas basadas en Inteligencia Artificial pueden comprometer la autenticidad y confiabilidad de los medios de prueba en procesos judiciales?
- ¿Qué medidas o metodología pueden implementarse para garantizar la integración eficaz y segura de las pruebas digitales en el sistema judicial paraguayo?

En base a las preguntas de investigación nos trazamos la siguiente hipótesis que aborda este ensayo: Una adecuada regulación de las TICs y la IA es esencial para garantizar que las pruebas digitales sean aceptadas y valoradas como evidencia solida en el Derecho Procesal Civil Paraguayo.

Desarrollo

El Derecho Procesal Civil y los medios de Pruebas Digitales

En el Paraguay, la justicia y en especial, el derecho procesal civil, ámbito de esta investigación, ha avanzado en la incorporación de tecnologías para modernizar la gestión judicial, como también la incursión en el ámbito probatorio.

Sin embargo, este progreso enfrenta retos en aspectos normativos, técnicos y de implementación práctica, que de no ser sorteados pueden perjudicar la garantía de la seguridad jurídica.

El marco legal en Paraguay ha evolucionado para integrar los medios de prueba digitales. La Ley N.º 4017/2010, derogada y reemplazada por la Ley N.º 6822/2021, establece las bases para regular los servicios de confianza y documentos electrónicos en los procesos judiciales.

La Ley N.º 6822 reconoce la firma electrónica cualificada como equivalente a la firma manuscrita, garantizando la autenticidad y validez de documentos electrónicos.

Por la Acordada N.º 1108/2016: Se establece el protocolo por la cual la Corte Suprema de Justicia define lineamientos para la tramitación electrónica de documentos, abordando la autenticidad, integridad y conservación de las pruebas digitales.

Aunque estas normativas representan avances significativos, su implementación todavía enfrenta desafíos relacionados con la uniformidad de procedimientos, la capacitación de los operadores jurídicos y la infraestructura tecnológica.

La prueba electrónica o en soporte electrónico se lo define como, aquella información contenida en un dispositivo electrónico a través del cual se adquiere el conocimiento de un hecho controvertido, bien mediante el convencimiento psicológico, bien al fijar este hecho como cierto atendiendo a una norma legal (Sanchís Crespo, 2012).

Naturaleza de los medios de prueba digitales

Los medios de prueba digitales se definen como toda información generada, almacenada o transmitida electrónicamente que puede ser utilizada como evidencia en procesos judiciales. Ejemplos incluyen correos electrónicos, mensajes instantáneos, registros de bases de datos, documentos electrónicos, capturas de pantalla, audios y videos. Estos deben cumplir con criterios de autenticidad, integridad y licitud para ser admitidos como prueba.

Los documentos electrónicos se clasifican según:

- Autenticidad: Que pueda verificarse la identidad del autor o emisor.
- Integridad: Que el contenido no haya sido alterado desde su creación.
- Licitud: Que su obtención respete derechos y libertades fundamentales.

Autenticidad y Validez de los Medios de Prueba Digitales: El documento electrónico puede tener distintos grados de satisfacción a los requisitos autoría (autenticidad), integridad (genuinidad) y estabilidad, lo que debe ser evaluado “ex ante”, si se pretende establecer una estrategia probatoria (Camps, 2021).

Según Torres Traba citado por Camps (2021), el soporte electrónico como forma documental requiere el abordaje de dos cuestiones: una referida a la autenticidad del documento electrónico a partir de las formas de imputación de autoría, la otra, en orden a la característica de inmutabilidad y permanencia del soporte.

Los documentos electrónicos han de observar unas garantías específicas: La autenticidad (constatación de la realidad del sujeto al sujeto que se le atribuye); Integridad o exactitud (que el soporte que se presenta no ha sido alterado y el documento concuerda con su original);

La licitud (obtención con respeto a los derechos y libertades fundamentales) y finalmente la certeza (concordancia del contenido del documento con la realidad) (Lluch, 2011).

Distinciones entre documentos digitales, electrónicos y virtuales

Según Villalba Bernié (2023), en su obra, la prueba en el proceso civil, podemos sintetizar que el concepto y uso generalizado, de los términos documento digital, electrónico y virtual suelen usarse como sinónimos, hay autores que establecen distinciones entre ellos.

Todos estos tipos de documentos comparten un origen común en el concepto de documento, rigiéndose por normas legales relacionadas con su autenticidad, capacidad probatoria, y procedimientos de exhibición o impugnación.

Diferencias clave:

- **Documento digital:** Siempre es un tipo de documento electrónico, pero lo distingue su base en tecnología digital (binaria) frente a la analógica.
- **Documento electrónico:** Puede ser tanto digital como analógico.
- **Documento virtual:** Es un concepto más amplio que engloba a los anteriores. Se refiere a documentos que pueden representar hechos reales en formatos escritos, sonoros o audiovisuales mediante simulaciones o transmisiones digitales. Ejemplo: la "nube virtual".
- **Importancia en el derecho probatorio:** Más allá de las definiciones técnicas, lo relevante es su impacto en el derecho probatorio, específicamente en aspectos como autenticidad y valor como evidencia.

Tecnologías de la Información y Comunicación (TIC) en el Ámbito Judicial

De acuerdo con (Cordella & Continio., 2020) obra corporativa del Banco Interamericano de Desarrollo, las Tecnologías de la Información y la Comunicación (TIC) han transformado los procedimientos judiciales en el ámbito del derecho procesal civil mediante la introducción de herramientas digitales que optimizan la administración de justicia.

Entre los impactos más destacados se encuentran:

Presentación y manejo de pruebas: Las TIC han permitido el desarrollo de sistemas de gestión procesal y expedientes electrónicos que digitalizan la presentación y administración

de pruebas. Esto mejora la transparencia y la seguridad jurídica al garantizar un manejo uniforme y accesible de la documentación judicial.

Automatización y eficiencia: Los sistemas digitales estandarizan los procedimientos, reducen el tiempo y costo asociados a las etapas procesales, y aumentan la eficiencia en la tramitación de casos. Esto incluye la racionalización de tareas administrativas y la automatización parcial de decisiones rutinarias.

Acceso y transparencia: La digitalización ha ampliado el acceso a la justicia mediante herramientas como plataformas de interoperabilidad y portales de expediente electrónico, que facilitan la interacción entre usuarios externos (ciudadanos, abogados) y el sistema judicial.

Impacto en la emisión de sentencias: Las TIC estructuran las acciones de los operadores judiciales mediante sistemas diseñados para asegurar la conformidad jurídica y la uniformidad en la aplicación de las normas, lo que fortalece la legitimidad y predictibilidad de las sentencias.

Estas transformaciones responden a la necesidad de aumentar la eficiencia, reducir costos, y mejorar la legitimidad y accesibilidad del sistema judicial en América Latina y el Caribe.

Vulnerabilidades del Ciberespacio en Sistemas Judiciales Digitales

El uso de Tecnologías de la Información y la Comunicación (TIC) en el ámbito judicial trae consigo varias vulnerabilidades que amenazan la seguridad y la funcionalidad de los sistemas digitales. Entre las amenazas principales se encuentran:

Ataques cibernéticos: Los sistemas judiciales digitales son blancos de ataques cibernéticos como ransomware, que pueden bloquear el acceso a expedientes electrónicos críticos o secuestrar datos sensibles. Esto puede paralizar procesos judiciales y generar pérdidas económicas significativas (Cordella & Continio, 2020).

Hackeos y accesos no autorizados: Los hackers pueden explotar vulnerabilidades en plataformas de justicia electrónica para acceder a información confidencial, manipular registros judiciales o alterar pruebas digitales. Esto socava la confianza pública en los sistemas de justicia (Cordella & Continio, 2020).

Alteraciones en la integridad de los datos: La manipulación intencionada o accidental de documentos electrónicos puede comprometer la validez de las decisiones judiciales. Estas alteraciones dificultan la garantía de autenticidad y la capacidad probatoria de los documentos digitales (NIST, 2013).

Riesgos de interoperabilidad e infraestructura: Las plataformas digitales que conectan múltiples instituciones (como tribunales, fiscalías y policía) pueden ser vulnerables a fallos en la interoperabilidad. Estos problemas crean brechas de seguridad que los ciberdelinquentes pueden explotar para interrumpir los flujos de información o desviar datos sensibles (Cordella & Continio, 2020).

Phishing y ataques dirigidos a operadores judiciales: Los funcionarios del sistema judicial son objetivos frecuentes de ataques de ingeniería social, como el phishing, que buscan obtener credenciales de acceso a sistemas críticos.

Estrategias de mitigación

Para enfrentar estas vulnerabilidades, es crucial implementar soluciones como el cifrado avanzado de datos, auditorías regulares de seguridad, programas de capacitación en ciberseguridad para los operadores judiciales, y el uso de tecnologías de inteligencia artificial para la detección temprana de amenazas.

Seguridad Jurídica y Regulación de las TIC e IA

Principio de Seguridad Jurídica: La seguridad jurídica garantiza certeza, previsibilidad y confianza en las decisiones judiciales y la administración de justicia (Cordella & Continio, 2020).

En el contexto de los medios de prueba digitales, este principio es fundamental para:

- **Certeza normativa:** Establece reglas claras sobre cómo deben manejarse las pruebas digitales, desde su recolección hasta su valoración en procesos judiciales.
- **Protección de derechos fundamentales:** Resguarda la integridad de las pruebas y asegura el debido proceso.
- **Confianza pública:** Refuerza la legitimidad del sistema judicial al prevenir arbitrariedades y errores en la valoración de pruebas digitales.

En Paraguay, la incorporación de tecnologías como las TIC e IA plantea la necesidad de preservar estos principios mediante protocolos claros y accesibles que aseguren la autenticidad, integridad y licitud de las pruebas digitales, tal como lo exige la Ley N.º 6822/2021.

Vacíos normativos en Paraguay

A pesar de los avances legislativos, como la Ley N.º 6822, subsisten lagunas legales que dificultan la implementación efectiva de las TIC e IA:

- **Falta de protocolos específicos:** No existen lineamientos claros sobre la preservación, autenticidad y manejo forense de pruebas digitales en procesos civiles.
- **Capacitación insuficiente:** Muchos operadores judiciales carecen de formación en tecnología, lo que compromete la correcta interpretación y uso de las pruebas digitales.
- **Riesgos de ciberseguridad:** La normativa actual no contempla mecanismos robustos para proteger las pruebas digitales contra manipulaciones o ataques cibernéticos.
- **Integración de IA:** No se han desarrollado regulaciones específicas sobre el uso de IA en la generación, validación y valoración de pruebas electrónicas, lo que podría abrir brechas para la introducción de pruebas apócrifas (Cordella & Continio, 2020)

Propuestas regulatorias - Referencias internacionales

España: La Ley de Enjuiciamiento Civil establece estándares para la certificación y autenticación de documentos electrónicos, reforzando la equivalencia funcional entre pruebas digitales y tradicionales (España, 2020).

Argentina: La Ley 25.506 y su reglamentación sobre firmas digitales aseguran la validez y autenticidad de documentos electrónicos mediante certificados de firma digital calificados (Ley 25506, 2001).

Estándares internacionales: Organismos como la (UNODC, 2021) proponen guías para la integración de tecnologías en sistemas judiciales, con énfasis en la interoperabilidad y la protección de datos.

Aplicabilidad en Paraguay

Desarrollo de protocolos específicos: Elaborar guías técnicas para la cadena de custodia, autenticidad y manejo de pruebas digitales.

Capacitación tecnológica: Implementar programas de formación en TIC e IA para operadores judiciales, asegurando un entendimiento práctico de las herramientas disponibles.

Seguridad cibernética: Incorporar medidas específicas para proteger los archivos electrónicos judiciales contra manipulación y ataques.

Regulación de IA: Establecer un marco normativo que garantice la transparencia en el uso de IA, incluyendo la validación de su autenticidad y confiabilidad como herramienta probatoria (Cordella & Continio, 2020).

Paraguay enfrenta el desafío de modernizar su sistema judicial mediante la incorporación de Tecnologías de la Información Comunicaciones e Inteligencia Artificial, sin comprometer la seguridad jurídica y tecnológica.

La adopción de medidas regulatorias basadas en experiencias internacionales, junto con el fortalecimiento de las capacidades tecnológicas locales, es esencial para garantizar que las pruebas digitales sean válidas, confiables y adecuadamente valoradas.

Esto permitirá un sistema judicial más eficiente y alineado con los principios de justicia y legalidad en la era digital.

Metodologías para la Integración de Pruebas Digitales

Validación de medios de prueba digitales: La validación de las pruebas digitales implica garantizar su autenticidad, integridad y admisibilidad en procesos judiciales. Las siguientes técnicas y herramientas son esenciales para este propósito:

Firma digital y sellos de tiempo: Aseguran la identidad del emisor y la inmutabilidad del contenido desde su creación. Herramientas como las PKI (Infraestructura de Clave Pública) se utilizan ampliamente (Cordella & Continio, 2020).

Algoritmos de hash: Generan un identificador único de un archivo digital, permitiendo detectar alteraciones.

Cadena de custodia electrónica: Registra cada interacción con la prueba digital, documentando quién accede y qué cambios realiza, asegurando su trazabilidad.

Software forense: Herramientas como EnCase y Forensic Toolkit (FTK), son paquetes de software forense digital que se pueden utilizar para recopilar, preservar y analizar evidencia electrónica.

En el contexto paraguayo, la Ley N.º 6822/2021 establece bases para la autenticación de documentos electrónicos, pero requiere protocolos adicionales para integrarlos completamente en el proceso judicial.

Capacitación de operadores jurídicos

La formación de jueces, abogados y peritos es crucial para garantizar que las TIC e IA sean aplicadas correctamente en el ámbito judicial.

Objetivos de la capacitación: Proporcionar conocimiento técnico sobre pruebas digitales, su validez y manejo forense. Enseñar el uso de herramientas tecnológicas específicas para evaluar autenticidad e integridad de las pruebas. Introducir conceptos básicos sobre IA y sus implicancias en la generación y evaluación de evidencias.

Ejemplos de programas internacionales:

En España, el Consejo General del Poder Judicial ofrece cursos de formación en ciberseguridad y pruebas digitales para operadores judiciales.

En Estados Unidos, el Instituto Nacional de Justicia implementa capacitaciones especializadas para fiscales y jueces sobre evidencia digital y cibercrimen (Cordella & Continio, 2020).

En Paraguay, sería beneficioso desarrollar un programa integral de formación continua para que los actores del sistema judicial estén preparados para evaluar adecuadamente la evidencia digital.

Protocolos y buenas prácticas

Los modelos internacionales ofrecen ejemplos valiosos para la preservación y validación de pruebas digitales, que pueden adaptarse al contexto paraguayo: Modelo internacional de

preservación de pruebas digitales ISO/IEC 27037: Estándar que establece directrices para la identificación, recolección, adquisición y preservación de evidencia digital.

La evidencia digital puede provenir de dispositivos móviles, redes sociales, navegadores, correos electrónicos y sistemas de respaldo en la nube. Estas tecnologías no solo registran interacciones humanas, sino que también ofrecen datos geospaciales detallados, como las ubicaciones de un dispositivo móvil o el historial de navegación de un usuario. Estas características amplían significativamente las posibilidades de recolección de pruebas en investigaciones forenses (Ciberseguridad, 2024)

Según la Organización Internacional de Normalización (ISO), "ISO/IEC 17020:2012 es una norma internacional que especifica los requisitos relativos a la competencia de los organismos que realizan actividades de inspección y a la imparcialidad y coherencia de sus actividades de inspección."

La norma esboza los criterios que deben cumplir los organismos de inspección para garantizar que pueden prestar servicios de inspección fiables y coherentes.

Abarca aspectos del funcionamiento de los organismos de inspección, como la estructura organizativa, la competencia del personal, la imparcialidad, la confidencialidad y los procedimientos que utilizan para realizar y registrar los resultados de las inspecciones.

El principal objetivo de la norma ISO 17020 es garantizar que los organismos de inspección cuenten con los conocimientos técnicos y los sistemas de gestión de la calidad necesarios para llevar a cabo las inspecciones con eficacia, precisión e integridad.

Guías del Consejo de Europa: Proponen principios para asegurar que las pruebas digitales respeten los derechos humanos y estándares de protección de datos.

Protocolo de Tallin: Diseñado para conflictos cibernéticos, establece parámetros de responsabilidad y manejo de evidencias digitales en litigios internacionales (Cordella & Continio., 2020).

Adaptación al contexto paraguayo: Creación de un marco normativo específico: Incorporar estándares como la ISO/IEC 27037 en las normativas locales, complementando la Ley N.º 6822.

Digitalización del sistema judicial

Implementar plataformas de interoperabilidad y gestión de documentos electrónicos que cumplan con estándares internacionales.

Supervisión independiente: Establecer unidades especializadas en manejo forense digital, con personal capacitado y recursos tecnológicos adecuados (Cordella & Continio., 2020).

Conclusión

La presente investigación, examinó la situación de los medios de prueba en la era digital, abordando su impacto y relevancia, tuvo por finalidad explicar las influencias de las Tecnologías de la Información y Comunicación, en los medios de prueba y aplicación en el contexto procesal civil.

El objetivo fue analizar cómo influyen las Tecnologías de la Información y la Comunicación (TIC) y la Inteligencia Artificial (IA) en la validez, preservación y valoración de los medios pruebas en los procesos judiciales civiles y cuáles son las implicancias en la seguridad jurídica en Paraguay.

Se han planteados las preguntas, que fueron desarrolladas en el transcurso del ensayo, todas ellas relacionadas al objetivo general citado.

Así tenemos, la Influencia de las TIC y la IA en los medios de prueba y la seguridad jurídica. Las Tecnologías de la Información y Comunicación (TIC) y la Inteligencia Artificial (IA) han revolucionado el derecho procesal civil en Paraguay, permitiendo la digitalización y optimización de procesos judiciales.

Estas herramientas han mejorado la accesibilidad, eficiencia y transparencia, pero también han introducido riesgos que afectan la validez, preservación y valoración de los medios de prueba digitales. La falta de regulación específica y protocolos uniformes puede comprometer la seguridad jurídica, afectando la legitimidad y predictibilidad de las decisiones judiciales.

En referencia a los Desafíos legales y técnicos en el uso de medios de prueba digitales. Entre los principales desafíos se encuentran:

- **Brechas normativas:** Aunque la Ley N.º 6822/2021 regula los servicios de confianza y la firma digital, no aborda aspectos críticos como la interoperabilidad y la cadena de custodia digital.
- **Vulnerabilidades técnicas:** Los sistemas digitales son susceptibles a ciberataques, manipulación de datos y fallos en la infraestructura tecnológica.
- **Capacitación insuficiente:** La falta de formación tecnológica de jueces y abogados limita su capacidad para manejar y valorar pruebas digitales adecuadamente.

Con respecto al, Impacto de la IA en la autenticidad y confiabilidad de los medios de prueba:

- La IA facilita la generación de pruebas digitales, pero también presenta riesgos como la creación de contenidos falsificados y la manipulación de datos.
- La falta de metodologías específicas para evaluar la autenticidad de estas pruebas compromete su confiabilidad.
- La integración de herramientas de IA requiere protocolos rigurosos y regulaciones claras para prevenir abusos y garantizar su aceptación en los procesos judiciales.

Así también tenemos, las Medidas y metodologías para integrar pruebas digitales de manera segura. Para garantizar la integración eficaz de las pruebas digitales en el sistema judicial paraguayo, se recomiendan las siguientes medidas:

- **Establecer protocolos técnicos:** Incorporar estándares internacionales para garantizar la identificación, recolección y preservación de pruebas digitales.
- **Desarrollar marcos normativos específicos:** Complementar la legislación existente con regulaciones enfocadas en la cadena de custodia digital y el uso de IA en procesos judiciales.
- **Capacitar a operadores judiciales:** Implementar programas de formación continua en TIC e IA para jueces, abogados y peritos.
- **Fortalecer la infraestructura tecnológica:** Garantizar sistemas seguros, interoperables y resistentes a ciberamenazas para proteger los archivos electrónicos judiciales.

Con respecto a la hipótesis planteada al inicio del ensayo, se afirma que es válida, ya que una adecuada regulación de las TIC e IA es imprescindible para garantizar que las pruebas

digitales sean aceptadas y valoradas como evidencia sólida en el derecho procesal civil paraguayo.

El uso de las TIC y la IA en el derecho procesal civil paraguayo ofrece beneficios significativos, pero también plantea desafíos que deben abordarse para garantizar la seguridad jurídica.

La implementación de regulaciones claras, protocolos uniformes y una infraestructura tecnológica robusta permitirá que las pruebas digitales sean integradas de manera confiable y aceptada como evidencia sólida en los procesos judiciales.

Esto no solo fortalecerá la justicia, sino que también promoverá la confianza pública en el sistema judicial.

Referencias

- Bielli, G. E. (2019). La Prueba Electrónica - teoría y práctica. *La Ley*, 375-381. C.A.B.A.
- C.S.J., C. S. (2016). Acordada que aprueba el protocolo de tramitación electrónica de la Corte Suprema de Justicia. Asunción, Paraguay.
- Cámara de Valencia. (2024). *Tecnología para los negocios*. <https://ticnegocios.camaravalencia.com/servicios/tendencias/blockchain-que-es-y-que-ventajas-tiene/>
- Camps, C. E. (2021). *Derecho procesal electrónico práctico*. Ciudad Autónoma de Buenos Aires.
- Ciberseguridad, I. (2024). ISO/IEC 27037 *Directrices para la identificación, recopilación, adquisición y preservación de evidencia digital*. https://ciberseguridad.com/normativa/espana/iso-iec-27037-evidencia-digital/#Norma_ISOIEC_27037
- Cordella, A., & Continio, F. (2020). *Tecnologías digitales para mejorar los sistemas de justicia: Un conjunto de herramientas para la acción*. Banco Interamericano de Desarrollo. https://1drv.ms/b/s!AvDCyRnTH4mqg7kZG_UmIyxptWB0Rg?e=PsJefu
- España, L. (2020). Ley reguladora de determinados aspectos de los servicios electrónicos de confianza. <https://www.boe.es/eli/es/l/2020/11/11/6>
- Gonzales Ávila, N. P. (2018). *Las capturas de pantalla como medio de prueba en el proceso civil*. Bolivia.

- InfoLeg, I. L. (2002). Decreto 2628 de Reglamentación de la Ley N° 25.506. Argentina.
<https://servicios.infoleg.gob.ar/infolegInternet/anexos/80000-84999/80733/norma.htm>
- Kamada, L. E. (25 de abril de 2024). La capacitación judicial en tiempos de TIC's (o el choque de dos mundos). Sistema Argentino de Información Jurídica.
<http://www.saij.gob.ar/DACF240039#>
- Ley 25506. (2001). Honorable Congreso de la Nación Argentina.
<https://www.argentina.gob.ar/normativa/nacional/70749/actualizacion>
- Ley N.º 4017, V. J. (2010). Biblioteca y Archivo del Congreso Nacional, Paraguay. de
<https://www.bacn.gov.py/leyes-paraguayas/3550/ley-n-4017-de-validez-juridica-de-la-firma-electronica-la-firma-digital-los-mensajes-de-datos-y-el-expediente-electronico>
- Ley N° 6822. (2021). de los Servicios de Confianza para las Transacciones Electrónicas, del Documento Electrónico y los Documentos Transmisibles Electrónicos.
<https://www.bacn.gov.py/leyes-paraguayas/10318/ley-n-6822-de-los-servicios-de-confianza-para-las-transacciones-electronicas-del-documento-electronico-y-los-documentos-transmisibles-electronicos>
- Lluch, X. A. P. (2011). *La prueba electrónica*. Bosch Editores, Barcelona.
- NIST, S. P. (2013). Security and Privacy Controls for.
- Resoagli, J. M. (2023). Desafíos legales de la era digital en el Marco Legal Argentino. Corrientes.
- Sanchís Crespo, C. (2012). Las Tecnologías de la Información y de la Comunicación en la Administración de Justicia. Análisis sistemático de la Ley 18/2011 en el electrónico. Navarra: editorial Thomson Reuters Aranzadi.
- UNODC. (2021). Convención de la Organización de las Naciones Unidas sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos.
https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_S.pdf
- Villalba Bernié, P. D. (2023). La prueba en el proceso civil. Ciudad Autónoma de Buenos Aires, Argentina.