VNiVERSiDAD D SALAMANCA

CAMPUS DE EXCELENCIA INTERNACIONAL

De la celulosa al silicio: La inteligencia artificial como coadyuvante de la fe pública. Un modelo de workflows agénticos para la actuación notarial a distancia en el derecho español y argentino.

Trabajo de Fin de Máster

Inteligencia Artificial y Legaltech

(Primera edición)

Septiembre de 2025

Autor

Walter César Schmidt

Tutora

Dra. Vanessa Jiménez Serranía

Resumen

Esta tesis aborda la adaptación de la fe pública notarial a la era digital. Propone un modelo de "*workflows* agénticos" (asistentes de IA) para realizar actos a distancia con una seguridad funcionalmente superior a la presencial. La IA no sustituye al notario, sino que potencia su juicio con herramientas de "inmediación aumentada" que verifican la identidad, analizan el comportamiento y detectan posibles vicios del consentimiento. El trabajo detalla una arquitectura tecnológica y la función de 12 agentes de IA, analizando su viabilidad técnica y su riguroso encuadre jurídico bajo la normativa de la UE (RGPD, Ley de IA) y Argentina. Ofrece una vía robusta para la evolución de la seguridad jurídica en el entorno digital.

Palabras claves: Plataforma de actuación a distancia, inmediación aumentada, *workflows* agénticos, videoconferencia, notariado

Abstract

This thesis addresses the adaptation of notarial public trust to the digital era. It proposes an "agentic workflow" model (AI assistants) to perform remote acts with security functionally superior to in-person acts. AI does not replace the notary but enhances their judgment with "augmented immediacy" tools that verify identity, analyze behavior, and detect possible defects in consent. The work details a technological architecture and the function of 12 AI agents, analyzing their technical viability and rigorous legal framework under EU (GDPR, AI Act) and Argentine regulations. It offers a robust path for the evolution of legal certainty in the digital environment.

Key words: Remote action platform, augmented immediacy, agentic *workflows*, videoconferencing, notary services.

MAESTRIA UNIVERSIDAD DE SALAMANCA

INTELIGENCIA ARTIFICIAL Y LEGALTECH

De la celulosa al silicio: La inteligencia artificial como coadyuvante de la fe pública. Un modelo de workflows agénticos para la actuación notarial a distancia en el derecho español y argentino.

INDICE

Glosario Introductorio

A continuación, se presenta un glosario de términos y acrónimos clave utilizados a lo largo de esta tesis. El objetivo es proporcionar al lector una comprensión fundamental de los conceptos tecnológicos, jurídicos y de inteligencia artificial que sustentan la investigación sobre la actuación notarial a distancia y la implementación de *workflows* agénticos.

A

- **AML (Anti-Money Laundering)**: Traducido como "Anti-Lavado de Dinero" o "Prevención de Blanqueo de Capitales". Se refiere al conjunto de leyes, regulaciones y procedimientos destinados a prevenir que los delincuentes disfracen fondos obtenidos ilegalmente como ingresos legítimos. En el ámbito notarial, implica la obligación de identificar y reportar actividades sospechosas.
- **Análisis de Grafos**: Es una técnica de análisis de datos que se centra en las relaciones y conexiones entre entidades. En un contexto de IA, permite modelar y analizar redes complejas, como las transacciones financieras para detectar patrones de fraude o lavado de dinero (AML), identificando vínculos ocultos entre las partes.
- **APIs (Application Programming Interfaces)**: Son conjuntos de definiciones y protocolos que permiten que diferentes aplicaciones de software se comuniquen entre sí. Actúan como puentes, facilitando la integración de distintos sistemas, por ejemplo, conectando una plataforma notarial con un sistema de verificación de identidad o una base de datos gubernamental.

C

- **Chip NFC (Near Field Communication)**: Es una tecnología de comunicación inalámbrica de corto alcance que permite el intercambio de datos entre dispositivos cercanos. En el contexto de la identificación, los pasaportes y documentos de identidad electrónicos modernos incorporan un chip NFC que almacena de forma segura los datos biométricos y biográficos del titular, permitiendo su lectura para una verificación rápida y segura.
- **Cloud (Nube)**: Se refiere a la red global de servidores y la infraestructura que los soporta, utilizada para almacenar y gestionar datos, ejecutar aplicaciones y ofrecer servicios a través de internet. Para la función notarial, ofrece escalabilidad y acceso remoto a documentos y sistemas, aunque plantea importantes desafíos en materia de seguridad y jurisdicción de los datos.

- **Clustering (Agrupamiento)**: Es una técnica de aprendizaje automático no supervisado que consiste en agrupar un conjunto de objetos (datos) de tal manera que los objetos en el mismo grupo (o clúster) son más similares entre sí que con los de otros grupos. Puede usarse para segmentar clientes o detectar anomalías en transacciones.
- **CVs (Computer Vision) o "Visión por Computadora":** Es un campo de la inteligencia artificial que entrena a las computadoras para interpretar y comprender el mundo visual. Mediante imágenes y videos, los sistemas de CV pueden identificar personas, verificar documentos de identidad (ID) y analizar expresiones faciales, siendo fundamental para la identificación remota.

D

- **Datasets (Conjuntos de Datos)**: Son colecciones de datos estructurados y etiquetados que se utilizan para entrenar y evaluar modelos de aprendizaje automático (ML). La calidad y representatividad del dataset son cruciales para el rendimiento y la equidad del modelo de IA resultante.

E

- **E2EE (End-to-End Encryption) o "Cifrado de Extremo a Extremo":** Es un método de comunicación segura que impide que terceros accedan a los datos mientras se transfieren de un sistema o dispositivo a otro. En las actuaciones notariales a distancia, garantiza que solo el emisor y el receptor previstos (por ejemplo, el ciudadano y el notario) puedan leer el contenido de la comunicación, protegiendo la confidencialidad.

G

- **GMMs (Gaussian Mixture Models)**: Son modelos probabilísticos que asumen que los datos se generan a partir de una mezcla de un número finito de distribuciones gaussianas con parámetros desconocidos. Se utilizan en clustering y reconocimiento de voz o de hablantes.
- **GRUs (Gated Recurrent Units)**: Son un tipo de red neuronal recurrente (RNN), similar a las LSTMs, utilizadas en el procesamiento de secuencias de datos, como el texto o el habla. Son computacionalmente más eficientes que las LSTMs y se

emplean en tareas de Procesamiento del Lenguaje Natural (PNL) y reconocimiento de voz (STT).

H

- **HSM (Hardware Security Module)**: Es un dispositivo criptográfico físico diseñado para proteger y gestionar claves digitales. Ofrece un nivel de seguridad superior al software, ya que las claves nunca abandonan el dispositivo. Es fundamental para la infraestructura de clave pública (PKI) y la emisión de firmas electrónicas cualificadas (QES), garantizando la integridad y el no repudio.

I

- **ID (Identity Document) o Documento de Identidad:** Se refiere a cualquier documento oficial emitido por una autoridad gubernamental que certifica la identidad de una persona (e.g., pasaporte, DNI). Su verificación es el primer paso en cualquier proceso de KYC.

K

- **Keylogger**: Es un tipo de software o hardware malicioso que registra las pulsaciones de teclas realizadas en un teclado sin el consentimiento del usuario. Representa una amenaza significativa para la seguridad, ya que puede capturar contraseñas, claves privadas y otra información sensible durante una sesión notarial remota.
- **KYC (Know Your Customer) o "Conozca a su Cliente":** Es el proceso mediante el cual una entidad (como un banco o un notario) verifica la identidad de sus clientes para cumplir con las regulaciones AML/CFT (Contra la Financiación del Terrorismo). Implica recopilar y verificar datos biográficos y, a menudo, biométricos.

L

- **Logs (Registros)**: Son archivos que registran eventos, acciones o mensajes que ocurren dentro de un sistema informático. En el contexto de la seguridad y la auditoría, los logs son cruciales para reconstruir una secuencia de eventos, detectar accesos no autorizados y proporcionar evidencia digital (trazabilidad) de las operaciones realizadas.

- **LSTMs (Long Short-Term Memory networks)**: Son un tipo avanzado de red neuronal recurrente (RNN) diseñadas para aprender y recordar patrones en secuencias de datos a largo plazo. Son especialmente potentes en tareas de PNL, como la traducción automática, y en el análisis de series temporales.

M

- **MFA (Multi-Factor Authentication) o "Autenticación de Múltiples Factores":** Es un método de seguridad que requiere que el usuario proporcione dos o más factores de verificación para acceder a un recurso. Estos factores suelen ser algo que el usuario conoce (contraseña), algo que posee (un token o teléfono) y/o algo que es (biometría), aumentando drásticamente la seguridad del acceso.
- **ML (Machine Learning) o "Aprendizaje Automático":** Es una rama de la inteligencia artificial que se centra en el desarrollo de algoritmos que permiten a las computadoras aprender de los datos y mejorar su rendimiento en una tarea sin ser explícitamente programadas para ello.
- **MRZ (Machine Readable Zone) o "Zona de Lectura Mecánica":** Es la sección de un documento de identidad (como un pasaporte) que contiene texto codificado en un formato estandarizado (ICAO 9303) para ser leído automáticamente por un escáner. Contiene información clave del titular y es un primer paso fundamental en la verificación de documentos.

O

- **Outliers (Valores Atípicos)**: Son observaciones en un conjunto de datos que difieren significativamente de las demás. En el análisis de datos, la detección de outliers es fundamental para identificar transacciones fraudulentas, comportamientos anómalos de usuarios o errores en los datos.

P

- **PKI (Public Key Infrastructure) o "Infraestructura de Clave Pública":** Es un sistema de hardware (HSMs), software, políticas y procedimientos necesarios para crear, gestionar, distribuir, usar, almacenar y revocar certificados digitales. Es la base tecnológica que sustenta la firma electrónica, garantizando la autenticidad, integridad y no repudio de los documentos digitales.

- **PNL (Procesamiento del Lenguaje Natural) o NLP por sus siglas en inglés:** Es un campo de la IA que se ocupa de la interacción entre las computadoras y el lenguaje humano. Permite a las máquinas leer, comprender, interpretar y generar texto. Sus aplicaciones incluyen la clasificación de documentos, la extracción de información y la traducción.
- **POS (Part-of-Speech Tagging)**: Es una técnica de PNL que consiste en identificar y etiquetar la categoría gramatical de cada palabra en un texto (verbo, sustantivo, adjetivo, etc.). Es un paso fundamental para análisis sintácticos más complejos y la extracción de significado.
- **Prompt**: En el contexto de los modelos de lenguaje de IA (como los Transformadores), un prompt es la instrucción o pregunta inicial que se le da al modelo para que genere una respuesta. La ingeniería de prompts ("prompt engineering") es la disciplina de diseñar entradas efectivas para obtener los resultados deseados.

Q

- **QES (Qualified Electronic Signature) o "Firma Electrónica Cualificada":** Según el reglamento eIDAS de la Unión Europea, es el tipo de firma electrónica con el mayor nivel de seguridad y que es jurídicamente equivalente a una firma manuscrita. Debe ser creada utilizando un dispositivo cualificado de creación de firmas (QSCD) y basarse en un certificado cualificado.
- **QSCD (Qualified Signature Creation Device) o "Dispositivo Cualificado de Creación de Firma Electrónica":** Es un dispositivo de hardware (como un HSM o una tarjeta inteligente) o software que cumple con los requisitos del reglamento eIDAS para crear una QES, garantizando que la clave de firma privada del firmante está protegida de forma segura.

R

- **RGPD (Reglamento General de Protección de Datos) o GDPR por sus siglas en inglés:** Es una regulación de la Unión Europea sobre protección de datos y privacidad para todos los individuos dentro de la UE y el Espacio Económico Europeo. Establece un marco estricto para el tratamiento de datos personales, con un impacto global.

S

- **SCORE**: En el contexto de ML, un "score" o puntuación es un valor numérico que asigna un modelo para indicar la probabilidad o confianza de una predicción. Por ejemplo, un score de riesgo crediticio o un score de probabilidad de que un documento sea fraudulento.
- **SSI (Self-Sovereign Identity) o "Identidad Auto-Soberana"**: Es un modelo de identidad digital en el que los individuos tienen el control total sobre su información personal. Utiliza tecnologías como blockchain y las credenciales verificables (VCs) para permitir a los usuarios gestionar sus propios datos de identidad sin depender de un proveedor centralizado.
- **Stemming (Lematización)**: Es una técnica de PNL que consiste en reducir las palabras a su raíz o forma base (lema). Por ejemplo, "caminando", "caminó" y "caminante" se reducirían a "caminar". Es útil para normalizar texto y mejorar la eficiencia del análisis.
- **STT (Speech-to-Text) o "Voz a Texto"**: Es una tecnología que convierte el lenguaje hablado en texto escrito. Es fundamental para transcribir declaraciones en videoconferencias notariales, crear registros automáticos y permitir la interacción por voz con sistemas de IA.
- **SVM (Support Vector Machine) o "Máquina de Vectores de Soporte":** Es un algoritmo de aprendizaje automático supervisado utilizado tanto para clasificación como para regresión. Es especialmente eficaz en espacios de alta dimensión y se utiliza para tareas como la clasificación de textos y el reconocimiento de imágenes. *Nota: SVMs es simplemente el plural.*

T

- **TEEs (Trusted Execution Environments) o "Entornos de Ejecución Confiable":** Es un área segura dentro del procesador principal de un dispositivo que garantiza que el código y los datos cargados en su interior estén protegidos con respecto a la confidencialidad e integridad. Proporciona un nivel de seguridad basado en hardware para ejecutar aplicaciones sensibles, como las de firma digital o verificación biométrica.
- **Transformadores (Transformers)**: Es una arquitectura de red neuronal que revolucionó el PNL. Se basa en un mecanismo de "atención" que le permite ponderar la importancia de diferentes palabras en una secuencia de entrada. Modelos como

GPT (Generative Pre-trained Transformer) se basan en esta arquitectura y son la base de los sistemas de IA generativa modernos.

- **Tampering:** Refiere a la manipulación, alteración o interferencia deliberada y no autorizada sobre un objeto, sistema o conjunto de datos. Esta acción compromete la integridad, seguridad o el correcto funcionamiento del elemento afectado, ya sea de forma física o lógica. En el ámbito de la seguridad informática y de la evidencia forense, el *tampering* busca modificar o corromper información de manera maliciosa.

V

- **VC (Verifiable Credentials) o "Credenciales Verificables":** Son un estándar del W3C para expresar credenciales (como un título universitario o un certificado de nacimiento) en un formato digital que es criptográficamente seguro, respetuoso con la privacidad y verificable por máquina. Son un pilar fundamental del modelo de identidad auto-soberana (SSI). *Nota: VCs es el plural.*

W

- **W3C (World Wide Web Consortium)**: Es la principal organización internacional de estándares para la World Wide Web. Desarrolla protocolos y directrices abiertas para asegurar el crecimiento a largo plazo de la Web, incluyendo estándares cruciales para la identidad digital como las VCs.
- ***Workflows* o "Flujos de Trabajo":** Son secuencias de tareas, procesos o pasos que deben ejecutarse para completar una operación. En el ámbito notarial, un workflow describe el proceso completo de un acto, desde la identificación de las partes hasta la firma y archivo del documento.
- ***Workflows* agénticos**: Es un concepto avanzado donde los *workflows* no son simplemente secuencias pasivas, sino que son orquestados y ejecutados por "agentes" de inteligencia artificial. Estos agentes pueden tomar decisiones, interactuar con usuarios y otros sistemas (vía APIs), y adaptar el flujo de trabajo en tiempo real basándose en la información recibida, automatizando procesos complejos como la debida diligencia en un acto notarial.

X

- **XAI (Explainable AI) o "Inteligencia Artificial Explicable"**: Es un campo emergente de la IA que se enfoca en desarrollar sistemas cuyos resultados y decisiones puedan ser comprendidos por los seres humanos. En un contexto jurídico, la XAI es crucial para garantizar la transparencia, la rendición de cuentas y el derecho a una explicación cuando un sistema de IA toma una decisión con consecuencias legales, como la denegación de un crédito o la calificación de una transacción como sospechosa.

Introducción.

El Derecho se encuentra en un punto de inflexión histórico ante la irrupción de la inteligencia artificial (IA), que interpela conceptos milenarios como la identidad, la prueba, la intencionalidad y la voluntad. El impacto de la tecnología ya no es un capítulo periférico del estudio del derecho; es el nuevo contexto en el que todo el ordenamiento jurídico debe ser repensado.

Esta revolución silenciosa, pero inexorable, nos compele a investigar como estas nuevas herramientas cognitivas pueden integrarse en el ecosistema jurídico no solo como herramientas de eficiencia, sino como garantes de principios fundamentales. La pregunta ya no es si la IA transformará la abogacía, la notaría o la judicatura, sino cómo podemos gobernar esa transformación para fortalecer el Estado de derecho, la seguridad jurídica y el acceso a la justicia. Esta tensión es particularmente aguda en el ámbito de la fe pública, cuya función primordial es dotar de certeza y seguridad jurídica a los actos y negocios más trascendentes de la vida civil y comercial.

El problema central que esta tesis aborda es la aparente incompatibilidad entre la necesidad social y económica de realizar actuaciones notariales a distancia y la salvaguarda de los principios estructurales del notariado de tipo latino, como son: la inmediación, la correcta identificación de los otorgantes y la verificación de un consentimiento humano libre, informado y exento de vicios.

Por lo tanto, la pregunta de investigación que ha de guiar a este trabajo es: ¿Es posible diseñar un modelo teórico-práctico, auxiliado por inteligencia artificial, que permita realizar actuaciones notariales protocolares a distancia con un nivel de robustez en la acreditación de la identidad y en la manifestación de la voluntad que sea funcionalmente equivalente, o incluso superior, al de la actuación presencial tradicional, respetando y potenciando los principios fundamentales y la esencia de la función notarial?

Frente a este escenario, se postula la siguiente hipótesis central: La creación de un workflow agéntico —un sistema de agentes de IA diseñado como asistente cognitivo del notario— permite superar las limitaciones actuales de la actuación a distancia, construyendo un ecosistema de confianza digital que eleva la robustez del acto a un estándar superior al tradicional y generando un nuevo paradigma de "inmediación aumentada"[16].

El aporte original de esta tesis no reside en la mera sugerencia de usar IA, sino en el diseño de una arquitectura conceptual y funcional específica. Se propone un modelo donde la IA no se limita a verificar datos, sino que realiza un análisis holístico, en tiempo real, correlacionando datos biométricos (reconocimiento facial, de voz, análisis de micro-expresiones) con la verificación criptográfica de documentos, el análisis contextual del entorno del otorgante y la creación de una traza de auditoría inmutable. Este workflow no sustituye el juicio del notario -que permanece como el centro insustituible del acto-, sino que lo dota de un caudal de información verificada y alertas inteligentes que potencian su capacidad de juicio y decisión.

En esencia, esta tesis propone el paso de una "tecnología de la comunicación" (la videoconferencia) a una "tecnología de reporte analítico" (el workflow agéntico), ofreciendo una solución escalable y segura que podría sentar las bases para la evolución de la fe pública en el siglo XXI.

Capítulo II: Actuación a distancia

El principio de inmediación frente a la comparecencia en línea en una actuación a distancia, tanto en el ámbito judicial como notarial [1]

En otras oportunidades hemos sostenido que el principio de inmediación es “el principio según el cual los jueces los magistrados miembros del tribunal y los secretarios judiciales, respecto de aquellas funciones que le son propias, habrán de estar presentes en la práctica de las pruebas y en cualquier otro acto que deba llevarse a cabo contradictoria y públicamente”.[2] Este principio es aplicable a todas las ramas del derecho. Así se habla del

[1] En este tema, seguimos los lineamientos generales expuestos en Cosola, S. J. y Schmidt, W.C. (2021) *El Derecho y la Tecnología*, Tomo I, Parte General, Thomson Reuters, La Ley, Buenos Aires, p. 76 y en Galletti, P.O., Longhi, M.I.; Manassero Vilar, L.E.; Molina, D.L., Saenz, C.A.; Di Castelnuovo, F; Scattolini, S.F.O. y Schmidt, W. C. (2021) *La actuación notarial en el ámbito virtual: Su aplicación en la Plataforma de Actuación Notarial Virtual de la Provincia de Buenos Aires, Argentina*. Presentado en las Jornadas Notariales Iberoamericanas celebradas en San Juan de Puerto Rico en octubre de 2021 en el marco del Premio a la Investigación jurídica “Profesora Cándida Rosa Urrutia de Basora”. (inédito).

[2] https://dpej.rae.es/lema/principio-de-inmediaci%C3%B3n Último acceso 19/07/2025

principio de inmediación en el derecho procesal[3], penal[4], laboral[5], de familia y por supuesto también en el derecho notarial[6]. Sobre el presente principio se han desarrollado, sostenido y fundamentado teorías sobre las cuales se menciona que para el cumplimiento de este principio es necesaria la presencia del operador jurídico (juez, abogado, notario, profesor de derecho, etcétera) en relación directa con la persona u objeto de la actuación.

El principio de inmediación constituye el núcleo dogmático y el baluarte argumental sobre el que pivotea toda la discusión en torno a la actuación notarial protocolar a distancia por lo que cabe preguntarse: ¿es la inmediación un sinónimo inmutable de contigüidad física, o es una función cuyo objetivo puede ser alcanzado por otros medios tecnológicos? En el debate actual, este trabajo adopta la postura evolucionista que sostiene que la inmediación no es un fin en sí mismo, sino un medio que regula la convivencia social[7] para alcanzar fines superiores: la correcta identificación de la persona, la constatación de su capacidad jurídica y la garantía de un consentimiento humano libre, pleno e informado.

Concordante con esta postura el Tribunal Supremo español ha sostenido que la interpretación de las normas procesales debe ser teleológica[8], mientras que la Corte Suprema de Justicia de la Nación Argentina, en reiterada jurisprudencia ha sostenido que al momento de interpretar una norma, cualquiera sea, debe estarse primordialmente a la

[3] Tayro, E.A. (2016) *La videoconferencia. Un nuevo enfoque del principio de inmediación procesal.* Revista Oficial Del Poder Judicial. Órgano De Investigación De La Corte Suprema De Justicia De La República Del Perú, 8 (10), p. 547-559. https://doi.org/10.35292/ropj.v8i10.251 Amoni Reverón, G. A. (2013) *El uso de la videoconferencia en cumplimiento del principio de inmediación procesal* Revista del Instituto de Ciencias Jurídicas de Puebla. México. Número 31, Enero-Junio 2013 p. 67-85

[4] Corte Suprema de Justicia de la Nación Argentina fallo del 12/12/2006 "Benítez, Aníbal Leonel s/ lesiones graves" Causa Número 1524C. https://repositorio.mpd.gov.ar/documentos/Ben%C3%ADtez,%20An%C3%ADbal%20Leonel.pdf

[5] Vitantonio, N. J.R. Ponencia general de la comisión de procesal laboral. XXVI Congreso Nacional de Derecho Procesal. https://www.aadproc.org.ar/pdfs/ponencias/Procesal_Laboral_Vitantonio.pdf Último acceso 19/07/2025

[6] El artículo 62 del código internacional del notariado aprobado en 2025 expresa: "Comparecencia ante notario. Las partes expresan su consentimiento en presencia física ante el notario…".

[7] Tayro, E. A. (2016) *La videoconferencia. Un nuevo enfoque del principio de inmediación procesal.* Revista Oficial Del Poder Judicial. Órgano De Investigación De La Corte Suprema De Justicia De La República Del Perú.

[8] Sentencia Tribunal Supremo 776/2014 Sala 1 Civil del 28 de abril de 2015 se sostiene: "…Como puede observarse, aunque instrumentalmente la interpretación literal suela ser el punto de partida del proceso interpretativo, no obstante, ello no determina que represente, inexorablemente, el punto final o de llegada del curso interpretativo, sobre todo en aquellos supuestos, como el presente caso, en donde de la propia interpretación literal no se infiera una atribución de sentido unívoca que dé una respuesta clara y precisa a las cuestiones planteadas (STS de 18 de junio de 2012, núm. 294/2012). En estos casos, por así decirlo, el proceso interpretativo debe seguir su curso hasta llegar a la "médula" de la razón o del sentido normativo, sin detenerse en la mera "corteza" de las palabras o términos empleados en la formulación normativa…." https://vlex.es/vid/570062178

finalidad de la misma.[9] La interpretación literal no siempre es un método recomendable, ya que el espíritu de la ley debe determinarse en procura de una aplicación racional, que elimine el riesgo de un formalismo paralizante,[10] pues lo importante no es atarse a rígidas pautas gramaticales sino alcanzar el significado profundo de las normas.[11]

En virtud del impacto tecnológico esta tesis postula comenzar a transitar la transición conceptual desde la "presencia física" hacia la "comparecencia fehaciente". Una comparecencia es fehaciente no por la contigüidad espacial, sino porque el sistema tecnológico coadyuvante del notario le proporciona al ejercicio de su función un conjunto de herramientas verificables para validar, con un grado de certeza jurídicamente exigible, los pilares del acto notarial.

El “Decálogo para las escrituras notariales con comparecencia en línea” [12] de la Unión Internacional del Notariado, dentro de las conclusiones no elude uno de los temas más importantes que impactan en la actuación notarial y sostiene: “La escritura notarial con “comparecencia en línea” lleva a reinterpretar el principio de inmediación en la comparecencia y a cambiar las formas de contacto de las partes con el notario interviniente. Lo importante no es la presencia física ante el notario, sino la comparecencia directa con el notario que es responsable de la autenticación, aunque sea a través de una plataforma tecnológica”. No es una simple declaración, es el reconocimiento institucional al más alto nivel de que la esencia de la función notarial reside en el juicio, el control y la responsabilidad del fedatario, y no en la presencia física de los requirentes.

Un hito en esta transformación es la Ley española 11/2023, del 08 de mayo, que regula la creación de un protocolo electrónico y de forma aún más disruptiva, autoriza la comparecencia por videoconferencia para una serie de actos y negocios jurídicos. Este

---

[9] Corte Suprema de Justicia de la Nación Argentina. Fallos: 305:1262; 322:1090; 330:2192; 344:1810

[10] Corte Suprema de Justicia de la Nación Argentina. Fallos: 326:2095; 329:3666; 330:2093; 344:223

[11] Corte Suprema de Justicia de la Nación Argentina. Fallo: 344:2591

[12] El decálogo original denominado “Decálogo para las escrituras notariales para las escrituras a distancia” fue elaborado por el grupo de trabajo “Nuevas Tecnologías” de la Unión Internacional y aprobado por el Consejo de Dirección el 26 de febrero de 2021. En el grupo de trabajo hay representantes de los siguientes países: Argentina, Austria, Canadá, España, Italia, Rusia, Alemania, Francia, Costa de Marfil. Posteriormente dicho decálogo fue puesto en consideración del Grupo de Trabajo Acto auténtico cuya denominación y texto final fue aprobado en la Asamblea de la Unión Internacional del Notariado del 3 de diciembre de 2021.

otorgamiento remoto debe realizarse a través de la Sede Electrónica Notarial, una plataforma segura y centralizada gestionada por el propio notariado.

Por su parte, la República Argentina no tiene normativa nacional sobre una actuación notarial a distancia. En las jurisdicciones que actualmente se desarrolla esta actividad, el soporte normativo está dado por una interpretación de la normativa vigente y el dictado de una resolución de cada uno de los colegios profesionales que rigen la actividad.

El desafío, y el núcleo propositivo de esta tesis, es definir la arquitectura de esa "plataforma tecnológica". No se trata de un mero software de comunicación, sino de un ecosistema digital robusto, que integre sinérgicamente criptografía de clave pública para la firma, biometría multifactorial para la identificación, sellado de tiempo cualificado para la integridad y agentes de inteligencia artificial capaces de realizar análisis contextuales y de comportamiento en tiempo real. Este enfoque transforma radicalmente la discusión: la tecnología deja de ser una amenaza para el principio de inmediación y se convierte en su más poderoso garante en el siglo XXI, dando lugar a un nuevo paradigma que denominamos "inmediación aumentada": el uso de sistemas tecnológicos para dotar al notario de un caudal de información verificada y de un nivel de percepción multisensorial y analítico que supera las capacidades humanas en un entorno puramente físico.

Capítulo III: Identidad, identificación, identidad digital e identidad soberana

Identificación: Evolución a lo largo de la historia

La función notarial, erigida como un baluarte de la justicia preventiva y la seguridad jurídica, se cimienta sobre un acto primigenio y absolutamente esencial: la correcta y certera identificación de las personas que otorgan un acto o negocio jurídico. Sin una identidad cierta, esa confianza colectiva delegada por el Estado en el notario, carece de sustento material[13]. El instrumento notarial, concebido como prueba preconstituida para prevenir futuros litigios, se desmoronaría en su base si la identidad de sus protagonistas fuera incierta.

Siendo la identificación de los comparecientes uno de los temas medulares en la función notarial y teniendo en cuenta una actuación a distancia, la identificación ha evolucionado desde el conocimiento personal en la antigüedad (escriba egipcio, tabelión romano), pasando por la fe anclada en la comunidad (notario medieval), hasta la identidad

[13] Lucas-Baque, S.J. y Albert-Márquez, J.J, (2019), *Los principios notariales como aporte a la justicia preventiva y a la seguridad jurídica.* Dialnet. https://dialnet.unirioja.es/descarga/articulo/7164381.pdf

administrada por el Estado a través del documento físico (DNI) en la era moderna. Hoy, enfrentamos un nuevo paradigma: la identidad desmaterializada y algorítmica, donde la confianza se deposita en la presunta infalibilidad de la biometría y los sistemas de IA. Este salto a la biometría completa la transferencia de la función del notario al Estado, pero de una manera radicalmente nueva: la confianza ya no se deposita en la integridad de un proceso burocrático que emite un documento físico, sino en la precisión matemática de los algoritmos ".

El mecanismo de estos sistemas, como el Sistema de Identidad Digital (SID) del Registro Nacional de las Personas (RENAPER) en Argentina o servicios comerciales equivalentes, se basa en el uso de algoritmos de inteligencia artificial para comparar una entrada biométrica (una imagen facial capturada en tiempo real ("selfie")) con una base de datos estatal centralizada. Para prevenir fraudes mediante el uso de fotografías o vídeos pregrabados, el proceso incorpora una "prueba de vida" (liveness detection), que puede ser activa (solicitando al usuario realizar gestos específicos) o pasiva (analizando micromovimientos y texturas imperceptibles).

El proceso técnico de verificación biométrica de RENAPER, por ejemplo, funciona comparando la selfie del usuario con la fotografía oficial almacenada en la base de datos del gobierno. Las entradas requeridas son el número de Documento Nacional de Identidad (DNI) y la selfie, pudiendo añadirse opcionalmente el nombre y el género para una mayor precisión. El sistema no devuelve una simple confirmación, sino una evaluación de riesgo probabilística (bajo, medio, alto) o un resultado de coincidencia basado en el grado de correlación de los datos faciales, el nombre y el género.

La identidad se fragmenta en múltiples identidades digitales. La identificación se vuelve contextual (cómo te identificas en un banco vs. en una red social). Conceptos como la autenticación multifactor (MFA) combinan "algo que sabes" (contraseña), "algo que tienes" (teléfono, token) y "algo que eres" (biometría). Emergen ideas como la Identidad Auto-Soberana (Self-Sovereign Identity - SSI), a menudo basada en blockchain, donde el usuario controla sus propios datos de identidad verificados.

La siguiente tabla sintetiza la evolución de las prácticas identificatorias, destacando el desplazamiento de la fuente de confianza y la naturaleza del riesgo en cada etapa.

Tabla 1: Análisis comparativo de métodos de identificación notarial

Era	Método Primario	Base Legal/Doctrinal	Fuente de Confianza	Riesgo Principal
Antiguo Egipto	Conocimiento personal (faz, nombre)	Costumbre, Orden Divino (Heródoto)	Confianza en el Escriba como guardián de la memoria y el orden	Error humano, pérdida del registro
Roma Clásica	Testigos (instrumentales y de conocimiento)	Derecho Romano (Digesto, Código)	Confianza distribuida (Tabelión + Testigos + Sello)	Falso testimonio, corrupción de testigos
Edad Media	Fe de Conocimiento (vecindad)	Siete Partidas, Ars Notariae (Rolandino Passeggeri)	Confianza en el Notario como jurista y cuasi-funcionario (ciencia + autoridad)	Suplantación en comunidades anónimas
Estado Moderno	Documento de Identidad (DNI)	Ley del Notariado (Esp), CCyCN (Arg)	Confianza en la burocracia y el registro del Estado	Falsificación de documentos, robo de identidad
Era Algorítmica	Verificación Biométrica (RENAPER)	Leyes de Firma Digital, Regulación de datos	Confianza en el algoritmo y la seguridad de la base de datos estatal	Sesgo algorítmico, deepfakes, hackeo masivo, error sistémico

Las fragilidades del algoritmo y la sociedad del riesgo

Las innovaciones tecnológicas y sus bondades suelen ser cautivantes para el intelecto, la imaginación y la prospectiva futurista, pero se debe estudiarla para poder aprehender las fortalezas y debilidades que la misma ofrece. No debemos caer en el facilismo de dejar que todo lo haga una IA, ni dejarnos obnubilar por las mieles de las creaciones y decisiones automatizadas.

Si bien es cierto que en la evolución algorítmica se aprecia y se demuestra, en 1910, con la obra de Russel y Whitehead, que todo pensamiento es lógico y todo principio lógico

puede ser representado en una ecuación matemática[14], también es cierto que posteriormente Kurt Gödel, en 1931 con su teoría de la incompletitud, logra demostrar que no es posible reducir todas las matemáticas a un sistema axiomático lógico[15]. Con Russel y Whitehead se demuestra que todo pensamiento podía ser expresado matemáticamente, pero quedaba pendiente saber si ese pensamiento expresado como ecuación matemática podía ser resuelto mecánicamente. Turing[16] en su ensayo explica que el entscheidusproblem es saber si un problema tiene solución, y para esto siguiendo solamente procedimientos mecánicos, lo que logra demostrar es que matemáticamente hay problemas que nunca sabríamos si tienen solución o no. O sea, esto ratificó que los sistemas matemáticos no son completos, a lo que podemos agregar que las matemáticas además tienen un sistema de representación, en la mecánica electrónica y digital, que es limitado por la propia arquitectura informática.[17]

La promesa de infalibilidad que acompaña a la identificación algorítmica esconde nuevas y profundas vulnerabilidades de naturaleza sistémica. En primer lugar, emerge el problema del sesgo algorítmico. Numerosos estudios han demostrado que los sistemas de reconocimiento facial presentan tasas de error significativamente más altas para ciertos grupos demográficos. Este no es un mero fallo técnico, sino una fuente potencial de discriminación y exclusión social sistémica. Un sistema que funciona de manera desigual socava el principio de igualdad de acceso a los servicios notariales y, por extensión, a la seguridad jurídica que estos proveen. En segundo lugar, la proliferación de la tecnología deepfake representa una crisis para la evidencia visual. La capacidad de generar videos y audios sintéticos hiperrealistas puede engañar no solo a la percepción humana, sino también a los sistemas de verificación biométrica, incluidos los que emplean pruebas de vida.

[14] Russel, B. & Withehead, A.N. (1950). *Principia Mathematica.* Cambridge At the University Press**.**

[15] Gödel, K. (2006) *Sobre proposiciones formalmente indecidibles de los Principia mathematica y sistemas afines.* KRK. Oviedo. España

[16] Turing, A. (1937), On computable numbers, with an application to the entscheindungsproblem. John Wiley and Sons. *Proceedings of the London Mathematical Society.* 1937.Vol s2-42.p. 230-265. London Mathematical Society

[17] Ejemplo de esto puede verse en la cantidad de bits que posee una máquina para poder representar las instrucciones. Si bien es cierto que existen diferentes mecanismos de representación para optimizar el uso como el complemento a 1, complemento a 2, en coma fija o en coma flotante, todo ello indica una limitación de la mecánica para representar las matemáticas y en consecuencia una limitante en las resoluciones de la IA. Para ampliar puede verse Stallings, W. (2005) *Organización y arquitectura de computadores.* Pearson. Prentice Hall. Madrid. España

Este nuevo panorama puede ser analizado a través de los marcos teóricos de Ulrich Beck[18] y Thomas Kuhn[19]. La "sociedad del riesgo" de Beck describe cómo la modernidad tardía genera riesgos que son incalculables, invisibles y producto de la propia innovación tecnológica, no de la naturaleza. Los riesgos algorítmicos encajan perfectamente en este modelo: son riesgos "manufacturados". La función notarial, en consecuencia, se desplaza de la prevención de litigios individuales a la gestión de riesgos sistémicos y abstractos, cuya seguridad es probabilística y está constantemente amenazada por factores globales.

Desde la perspectiva de Thomas Kuhn, la transición a la identificación algorítmica puede entenderse como un cambio de paradigma. El paradigma anterior, la “identificación por juicio humano y/o documental”, se enfrenta a la “anomalía” de no poder gestionar la escala y velocidad del mundo digital. El nuevo paradigma, la “identificación por probabilidad algorítmica”, resuelve esta anomalía, pero, como toda revolución científica, introduce un nuevo conjunto de problemas: los riesgos del viejo paradigma (suplantación de identidad individual, falsificación de un documento) son fundamentalmente diferentes y más comprensibles que los del nuevo (sesgo sistémico, fraude con inteligencia artificial, colapso criptográfico cuántico). Al aplicar conjuntamente las teorías de Kuhn y Beck, se obtiene una visión potente: el cambio de paradigma en la identificación nos ha arrojado a la “sociedad del riesgo” de Beck. El notariado ha intercambiado un conjunto de riesgos comprensibles y manejables a nivel individual por un nuevo universo de riesgos abstractos, sistémicos y de consecuencias potencialmente catastróficas. Este progreso ha venido acompañado de la introducción de nuevos y formidables riesgos sistémicos para la seguridad jurídica. La suplantación de identidad, antes un delito artesanal, ahora puede ser industrializado mediante el hackeo masivo de bases de datos. El sesgo, antes un posible fallo individual del notario, ahora puede ser codificado en algoritmos que afectan a millones de personas.

En virtud de ello puede decirse que si bien la tecnología ha transformado radicalmente los medios de identificación, no ha eliminado la necesidad de la función notarial, sino al contrario, la ha hecho más indispensable. Al delegar la tarea mecánica de la identificación a "cajas negras" algorítmicas, la labor insustituible del notario como jurista experto -que controla la legalidad del acto, juzga la capacidad de los otorgantes, interpreta y da forma a su voluntad, y previene litigios- se vuelve aún más crucial. En este escenario, el

[18] Beck, U. (1986) *La sociedad del riesgo. Hacia una nueva modernidad.* Paidós. Barcelona.
[19] Kuhn, T.S. (2004) *Las estructuras de las revoluciones científicas.* 8 reimp. FCE. Buenos Aires.

notario se erige como el último garante humano de la legalidad y la voluntad en un mundo crecientemente automatizado, y es por ello que se ha de sostener en todo este aporte el valor fundamental que juega en este planteo el principio human in command.

Identidad personal y digital. Modalidades de identificación actuales y futuras

Actualmente en una actuación notarial física presencial, el notario identifica a la persona por conocimiento que posee de ella[20] o por exhibición de documento o documentos idóneos que la persona haga, a los efectos de hacer llegar al notario a una razonable convicción que esa persona es quien supuestamente dice que es.[21]

El uso de herramientas tecnológicas como el reconocimiento facial o la identificación dactilar no es habitual en el ejercicio profesional notarial con presencia física, sin embargo y a pesar del bajo nivel de seguridad en la identificación de las personas son insignificantes los casos de sustitución de personas teniendo en cuenta la cantidad de actos notariales que se realizan diariamente.

El advenimiento y la consolidación de la esfera digital han transformado irrevocablemente las interacciones humanas, económicas y sociales. En este nuevo dominio, la identidad, como conjunto de atributos que definen a un individuo de manera única, ha sido gestionada a través de modelos que, si bien funcionales, han revelado profundas deficiencias estructurales en materia de seguridad, privacidad y control. En respuesta a estas carencias, emerge un nuevo paradigma conocido como Identidad Digital Autosoberana (SSI, por sus siglas en inglés, Self-Sovereign Identity). Este modelo representa un cambio fundamental, una re-arquitectura de la confianza digital que sitúa al individuo en el epicentro de su propia identidad, otorgándole la gestión y el control sobre sus datos personales de una manera descentralizada y segura.[22]

La reconfiguración de la identidad en la era digital fue evolucionando y modificándose por diferentes modelos, pasando del paradigma centralizado para evolucionar en el modelo federado y recaer definitivamente en el de identidad autosoberana.

En este nuevo paradigma, el usuario recupera la soberanía sobre sus datos. Utiliza una "cartera digital" (wallet) personal, normalmente en un dispositivo móvil, que actúa como un contenedor seguro para sus credenciales digitales. Estas credenciales son emitidas por

[20] Artículo 306 inc. b) del CCCN
[21] Aicega, M.C. y Canto, P. (2023), Justificación de la identidad, en *Calificación y configuración notarial,* Ignacio Alterini y Francisco J. Alterini (Directores). Thomson Reuters-La Ley, Buenos Aires. Argentina.

[22] https://walt.id/white-paper/self-sovereign-identity-ssi https://www.dock.io/post/self-sovereign-identity

autoridades de confianza (gobiernos, universidades, empleadores) pero se entregan directamente al usuario, quien las almacena y controla de forma exclusiva. El modelo está diseñado para ser inherentemente más privado, seguro, transparente y democrático, devolviendo al individuo el control que había perdido en las etapas anteriores de la evolución de internet.

El marco regulatorio europeo: eIDAS 2.0 y la cartera europea de identidad digital (EUDI Wallet)

Si bien la identidad autosoberana nació como un movimiento tecnológico y filosófico, su transición hacia una realidad tangible y de adopción masiva está siendo catalizada por un marco jurídico sin precedentes: la revisión del Reglamento sobre Identificación Electrónica y Servicios de Confianza (eIDAS) en la Unión Europea. El nuevo Reglamento (UE) 2024/1183, conocido como eIDAS 2.0, no solo reconoce los principios de la SSI, sino que los convierte en un mandato legal, estableciendo el ecosistema de identidad digital más avanzado y ambicioso del mundo.

La disposición más transformadora del reglamento es la obligación para cada Estado miembro de la UE de ofrecer, a más tardar en 2026, al menos una Cartera Europea de Identidad Digital (EUDI Wallet) a sus ciudadanos y empresas. Esta cartera deberá ser gratuita para las personas físicas y su uso será voluntario.

En conclusión, la identidad autosoberana ha cruzado el umbral de la viabilidad técnica para entrar en la fase de preparación para el mercado. Los pilares fundamentales -estándares maduros, tecnología disponible y un marco regulatorio claro (en Europa)- ya están resueltos, lo que resta es perfeccionar la experiencia de usuario y definir las reglas de gobernanza que permitirán que estos ecosistemas descentralizados escalen de forma segura y fiable, sin perjuicio de los obstáculos que siguen existiendo a nivel de desafíos técnicos como la interoperabilidad y escalabilidad, desafíos de usabilidad como una solución a la recuperación de claves y el posible robo o suplantación de identidad, o los desafíos de gobernanza por la imputación de responsabilidad ante algún hecho dañoso.

Argentina y el ID Digital

El ecosistema de identidad digital en Argentina presenta una dualidad interesante que refleja la transición global desde modelos centralizados hacia paradigmas descentralizados. Por un lado, el Estado Nacional ha consolidado una plataforma centralizada de servicios y credenciales digitales. Por otro, un vibrante ecosistema de proyectos privados y del tercer sector está impulsando activamente la adopción de la identidad autosoberana (SSI).

El escenario argentino es un microcosmos de la evolución global de la identidad digital. Coexisten dos visiones:

1. Una visión centralizada, liderada por el Estado ("Mi Argentina"), que ha logrado una masiva digitalización de credenciales y servicios, mejorando la eficiencia y el acceso para millones de ciudadanos, pero manteniendo un paradigma de control gubernamental.
2. Una visión descentralizada, impulsada por la sociedad civil y el sector privado (DIDI, QuarkID, etc.), que busca implementar los principios de la Identidad Autosoberana para empoderar a los individuos, especialmente a los más vulnerables, dándoles control directo sobre sus datos.

Esta dualidad no es necesariamente un conflicto, sino una oportunidad. La madurez y el alcance de la plataforma estatal podrían, en el futuro, converger con la flexibilidad, seguridad y privacidad del modelo SSI, creando un ecosistema de identidad híbrido y robusto que aproveche lo mejor de ambos mundos.

Capítulo IV: De la teoría a la propuesta práctica

Arquitectura conceptual y tecnológica para la identificación de una persona y una manifestación de voluntad robusta

Introducción

En el escenario de actividad protocolar, como ya hemos anticipado en la introducción de esta tesis, es que desarrollamos la propuesta, sabiendo que la arquitectura que se propone es la ideal para una identificación y manifestación de voluntad robusta, pero de ningún modo significa que sea la arquitectura básica para el desarrollo de una plataforma de actuación a distancia.

Se plantea el norte a alcanzar, siendo conscientes que actualmente se desarrolla esta clase de actuación sin la arquitectura propuesta. Sin embargo, en la prospectiva, siempre se debe tener presente que se debe fortalecer, con las herramientas que se cuentan, cualquier actuación a distancia teniendo en miras la seguridad jurídica preventiva y la prevención de litigios.

En virtud de ello, en el presente capítulo, se ha de desarrollar la arquitectura conceptual y tecnológica para una actuación notarial mediante videoconferencia para actos protocolares, dejando de lado la actuación judicial.[23]

La piedra angular de esta tesis reside en validar a distancia la identidad de una persona y que cada acción ejecutada por él en un ambiente digital no sea un mero evento gráfico, sino una manifestación de voluntad jurídicamente válida, demostrable y susceptible de ser adjudicada a la persona que la ha expresado mediante videoconferencia.

La exigencia que las actuaciones en este ambiente (audiencias, transacciones de bienes y servicios) gocen de la fe pública notarial[24] impone un nivel de aseguramiento que supera con creces los mecanismos de identificación habituales en entornos digitales. Necesitamos construir un sistema donde el no repudio sea una propiedad intrínseca y demostrable.

En este escenario, debemos desglosar la arquitectura conceptual y tecnológica que se requiere para llevar adelante el proyecto de un ambiente digital donde se puede llegar a la identificación de una persona y a una manifestación de voluntad robusta que nos permita acercarnos un poco más al principio de no repudio[25].

---

[23] Si bien es cierto que una actuación notarial o judicial mediante videoconferencia poseen características similares, principios generales compartidos y la columna vertebral ha de ser la misma, no podemos dejar de advertir que las diferentes normas y variables que existen por la distinta clase de actuación que tiene cada actividad, nos obliga, por tiempo y principalmente claridad expositiva, a circunscribir el análisis a uno de esos actos. En una plataforma de actuación judicial deberíamos de prever la posibilidad de acceso público a la audiencia que no sería necesario en una actuación notarial, asimismo en una audiencia judicial deberíamos de prever la posibilidad de crear un canal seguro entre cliente y abogado, cosa que no sería imprescindible en un acto notarial. Las distintas variantes, así como las diferentes normativas que deberíamos de citar generarían una confusión al trabajo que intenta abordar la posibilidad de una implementación de actuación a distancia. Durante el desarrollo analítico se deberá evaluar que la versatilidad de la plataforma ha de permitir, con pequeños ajustes, adaptarse a la audiencia judicial independientemente del país en el que se lo quiera adoptar. En estos sistemas se podrían incorporar un workflows agéntico para declaración de testigos compuesto por una IA principal y administradora del ciclo de vida del expediente judicial, se le integran las herramientas de *Statement Reality Analysis, (*analiza la validez y fiabilidad de la declaración en base a determinados parámetros, de *Reality Monitoring* (herramienta que sirva para evaluar la credibilidad del testimonio sobre una lista de ocho ítems) y una IA que analiza los microgestos, lo cual permitiría, además, detectar las micro expresiones enumeradas y desarrolladas por Paul Ekman (1971), como la ira, tristeza, alegría, miedo, sorpresa y desprecio. Puede ampliarse este concepto en Ekman, P. (2017) *El rostro de las emociones.* RBA. Matsumoto, David & Hwang, H.S. & López, Rafael & Pérez Nieto, Miguel. (2013). *Reading facial expressions of emotions: Basic research on emotions recognition improvement.* Ansiedad y Estrés.

[24] Podría aplicarse a la fe pública judicial también

[25] No escapa a nuestro conocimiento las actuaciones judiciales y notariales que actualmente se encuentran en funcionamiento y que las manifestaciones de voluntad son plenamente válidas y adjudicables a cada una de las personas. Sin embargo lo que se pretende con el presente trabajo es acercarnos un poco más a la inobjetabilidad de las acciones que se desarrollen en el ambiente digital y es por ello que se propone esta arquitectura conceptual y tecnológica, que luego será complementada por *workflows* agénticos. La propuesta no significa que las actuaciones en las vigentes plataformas carezcan de validez o se encuentren afectadas por algún vicio, sino que se plantea una idea superadora y mejorada de las actuales tecnologías en uso, robusteciendo aún más las actuaciones vigentes.

Se propone una arquitectura básica fundamentada en cinco etapas que van desde la verificación robusta de identidad como anclaje indiscutible entre la identidad personal del mundo físico y la representación digital, hasta la auditabilidad y posibles mejoras de los sistemas en funcionamiento. Las fases de la arquitectura son::

Fase 1: Verificación robusta de identidad. Anclaje en el mundo físico

Fase 2: Credencial de identidad digital

Fase 3: Entorno seguro de videoconferencia

Fase 4: Registro inmutable, auditable y conservación segura del acto a distancia

Fase 5: Auditorías y mejoras conjuntas.

1. Fase Uno: El anclaje indiscutible en el mundo físico – Verificación robusta de identidad (Enrolamiento)

Antes que un usuario pueda operar en la plataforma notarial, su identidad física debe ser comprobada con un rigor equivalente o superior al exigido para la obtención de documentos de identidad nacionales o la apertura de cuentas bancarias (procesos KYC/AML robustos).

Para ello es ideal:

- La integración con sistemas nacionales de identidad electrónica (eID). Aprovechar infraestructuras existentes como las compatibles con el reglamento eIDAS en Europa que ya proporcionan identidades digitales verificadas y vinculadas a ciudadanos físicos, siempre teniendo en cuenta que nivel de seguridad con el cual se identifique a la persona sea “sustancial” o “alto”.[26]
- Verificación remota de identidad con biometría y, eventualmente, prueba de vida. Utilizar soluciones avanzadas que combinen la verificación de documentos de identidad oficiales con análisis biométricos faciales (u otros) que incluyan detección de vida para prevenir suplantaciones mediante fotos o vídeos. Este proceso debe ser supervisado o certificado por entidades de confianza.[27]

[26] Cosola, S.J. & Schmidt, W.C. (2021) *El Derecho y la tecnología.* Thomson Reuters-La Ley. Buenos Aires. Argentina. Tomo 1.

[27] En el caso de la Argentina, este servicio es brindado por el Registro Nacional de las Personas (RENAPER), que es el organismo estatal argentino encargado de registrar e identificar a las personas que residen en el país. Es responsable de emitir el Documento Nacional de Identidad (DNI) y los pasaportes. Otra aplicación que se puede utilizar para el otorgamiento de una credencial de identidad verificada es “Mi Argentina” que es el perfil digital de los ciudadanos argentinos, una plataforma oficial del gobierno para acceder a trámites, servicios y documentación del Estado de forma digital.

El resultado de este proceso de enrolamiento inicial generaría la emisión de una credencial de identidad digital verificada o un perfil de alta seguridad asociado al usuario en la plataforma de actos a distancia.

Para cada sesión, podría requerirse una re-verificación simplificada si ha pasado mucho tiempo o si la naturaleza del acto lo justifica.

2. Fase Dos: La credencial de identidad digital – Fundamento criptográfico (SSI y PKI)

Esta fase debe asegurar que quien accede a la videoconferencia y participa en el acto es la persona cuya identidad ha sido previamente verificada, y que sus acciones (como consentir o firmar) están vinculadas inequívocamente a ella.

En esta fase debemos tener en cuenta tres elementos a desarrollar:

- Credencial
- Autenticación para el acceso a la videoconferencia
- Vinculación de la credencial a la persona que accede a la videoconferencia

Credencial

La credencial emitida no es un simple identificador, el usuario debe tener el control exclusivo sobre esta credencial y sus claves asociadas. Si bien la Identidad Auto-Soberana (SSI) es un paradigma interesante para la inmediatez y la aceptación legal actual en actos notariales[28], nos enfocaremos en la utilización de certificados digitales y PKI ya establecidos.

Para ello el usuario europeo deberá tener un certificado de firma electrónica cualificada (QES), emitido por prestadores de servicios de confianza cualificados, mientras que el usuario argentino deberá tener un certificado de firma digital emitido por algún certificador licenciado bajo la Ley 25.506.

Autenticación para el acceso a la videoconferencia

Idealmente se debiera requerir una autenticación Multifactor (MFA), que es la combinación de "algo que se sabe" (contraseña), "algo que se tiene" (token de hardware/software, certificado en dispositivo seguro) y/o "algo que se es" (biometría para desbloquear el acceso a la clave privada).

[28] En esto también es plenamente aplicable a los actos judiciales

La clave privada para la firma debe estar, ineludiblemente, bajo el control exclusivo del usuario, en dispositivos criptográficos hardware, o entornos seguros (TEEs).

Vinculación de la credencial a la persona que accede a la videoconferencia

La plataforma debe asegurar que el participante activo en la videoconferencia es el titular de la credencial que se usará para firmar.

Para ello se sugiere la utilización de:

- Credenciales Verificables (Verifiable Credentials - VCs): Formato estándar del W3C para emitir declaraciones (atributos de identidad, autorizaciones, etc.) firmadas digitalmente por un emisor confiable (la entidad que verificó la identidad en la fase uno (1)) y en posesión del usuario. Estas credenciales (ej. "Identidad verificada nivel alto", "poder notarial válido") pueden ser presentadas selectivamente.
- Infraestructura de Clave Pública (PKI): La credencial estará asociada a un par de claves criptográficas (pública y privada). La clave privada, custodiada de forma segura por el usuario, es esencial para autenticarse y firmar acciones. Dentro de las posibles soluciones de alojamiento y custodia segura de clave privada podemos encontrar dispositivos criptográficos hardware o entornos seguros (TEEs).

3. Fase Tres: El entorno seguro de videoconferencia – Garantizando la integridad y validez del acto

El objetivo de esta etapa es generar un entorno de videoconferencia seguro donde se garantice la identidad continua del requirente, la libre expresión de la voluntad, la formalización del acto y el cumplimiento de los principios notariales.

Esta etapa es la más crucial de todas, ya que aquí se ha de desarrollar el acto notarial. En consecuencia, debemos analizar la seguridad del entorno y además desde distintas aristas el acto notarial. Para ello, hemos de separar el análisis de cada uno de los tópicos que deben ser estudiados con la tecnología que se requiere. Las diferentes aristas que se presentan en esta fase para analizar son dos:

- Seguridad de la plataforma de videoconferencia
- Acto notarial:
  - Identificación y verificación durante la sesión
  - Cumplimiento de los principios notariales fundamentales
  - Gestión de documentos y pruebas digitales
  - Manifestación y constancia del consentimiento válido

Seguridad de la plataforma de videoconferencia

La plataforma debería de cumplir con:

- Cifrado de extremo a extremo (E2EE), para todas las comunicaciones de audio, video y datos compartidos.
- Controles de acceso robustos mediante el cual solo los participantes autorizados puedan unirse a la sala de videoconferencia. Opcionalmente, se podría prever la posibilidad de desarrollar salas de espera virtuales.
- Una autenticación continua, mediante mecanismos discretos para re-verificar la presencia del participante autorizado durante sesiones largas o antes de actos críticos.
- Protección contra grabaciones no autorizadas y tampering.[29]

Acto notarial

Identificación y verificación durante la sesión

En el ideal de este escenario el notario debería estar en la videoconferencia junto a los requirentes, y en caso de no conocerlos, solicitar a cada uno de los requirentes, mediante un canal seguro entre la plataforma y los requirentes, que el requirente se tome una fotografía de su rostro, la cual se envía mediante este canal seguro a la plataforma y desde la misma plataforma el notario realiza la consulta con la base de datos nacionales del país a los efectos de validar, mediante biometría, la identidad del requirente. Validada la misma se continúa con la actuación.[30]

Para el caso que en el país que se aplique no sea posible una validación biométrica on line desde la sala de videoconferencia de la plataforma, una opción posible sería que el notario deba poder verificar visualmente al participante contra la imagen de su documento de identidad (previamente cargado y verificado en Fase 1) al inicio y reforzar dicha validación de identidad en cada uno de los momentos claves de la actuación.

Cumplimiento de los principios notariales fundamentales[31]

[29] El *tampering* refiere a la manipulación, alteración o interferencia deliberada y no autorizada sobre un objeto, sistema o conjunto de datos.

[30] Este proceso de validación de la identidad no es teórico, sino que ya se encuentra implementado en la plataforma de actuación a distancia del Colegio de Escribanos de la Provincia de Buenos Aires, República Argentina. Dentro de la sala de videoconferencia y mediante el "asistente de funcionalidad móvil" el requirente se toma la foto, la cual se envía directamente a la plataforma y desde allí el notario consulta con el Registro Nacional de las Personas (RENAPER), el cual valida biométricamente la identidad del requirente a los efectos de continuar con el acto notarial. Se puede consultar su proceso en www.e-notariado.org.ar

[31] Para el caso que quiera desarrollarse una plataforma de actuación judicial se debería contemplar además que la sala de videoconferencia debe cumplir con los principios de:
Publicidad: Se debe prever permitir el acceso público seguro y controlado si el tipo de audiencia lo requiere.

Sin perjuicio del desarrollo, análisis y cumplimiento de cada una de los requerimientos normativos y técnicos que se necesiten, si no se tienen en cuenta este tópico, podríamos quedar expuestos a posibles vicios del acto que lo invalidarían. Es por ello que la plataforma debe cumplir con los siguientes principios:

- Inmediación: La plataforma debe permitir una interacción visual, auditiva clara y directa, sin obstáculos entre requirentes y notario.
- Continuidad: El acto debe desarrollarse en una secuencia continua, minimizando interrupciones técnicas. Si estas ocurren, deben registrarse y gestionarse adecuadamente. Quedando a criterio del notario continuar o, eventualmente, realizar una nueva actuación.
- Jurisdicción: La plataforma debe permitir mediante un canal seguro, la geoposición global del notario a los efectos de ubicarlo en el lugar de su competencia territorial, y, si la normativa lo exige, la geoposición de los requirentes. La geoposición global debería ser tomada del dispositivo móvil que el notario posea registrado en la misma plataforma.[32]

Gestión de documentos y pruebas digitales

La sala de videoconferencia necesariamente debe tener la funcionalidad de compartir, visualizar conjuntamente, y si es necesario, modificar un documento por parte del notario, mientras los demás integrantes visualizan y emiten opinión de conformidad o disconformidad con el texto que se está redactando. Todo ello en tiempo real.[33]

Asimismo se pueden prever la integración con sistemas de gestión documental notarial, que darían mayor eficacia y eficiencia a la tarea desarrollada.

Manifestación y constancia del consentimiento válido

Confidencialidad: Establecer canales seguros para comunicación privada entre el abogado y su cliente durante la audiencia, distintos del enlace principal de la audiencia.

[32] Cuando se habla de la geolocalización del notario, no se está pensando en la geolocalización de la conexión de la PC pues es fácilmente vulnerable sino que el notario se geolocalice mediante el móvil que el notario posea. Esta tecnología tampoco es teórica sino que ya se encuentra implementada a través del "asistente de funcionalidad móvil" en la plataforma de actuación a distancia que posee el Colegio de Escribanos de la Provincia de Buenos Aires.
En aquellos países con organización nacional federal (como lo es el caso de Argentina, Alemania, Brasil o México) suele ocurrir que se exija que el requirente se encuentre dentro de un radio territorial determinado para que el notario sea competente.

[33] Esta funcionalidad ya se encuentra utilizando la plataforma de actuación a distancia (PAND) del Colegio de Escribanos de la Provincia de Buenos Aires.

Este proceso es crucial, neurálgico en la estructura de la actuación e invalidante, pues ante el incumplimiento de esta etapa podríamos incurrir en un vicio del acto notarial. En virtud de ello se debe tener en cuenta:

- Información previa y asesoramiento: El notario debe asegurarse de que las partes comprenden la naturaleza y consecuencias del acto. Este proceso puede darse en forma previa al acto notarial, ya que la plataforma debería de prever usar la sala de videoconferencia no solo para el acto notarial sino además para los actos preparativos de la audiencia notarial donde el notario podría explicar allí mismo la naturaleza y consecuencias del acto.

  En el caso de la audiencia notarial, toda o parte de la actuación, podría ser grabada.[34]
- Prevención de vicios del consentimiento (error, dolo, violencia o intimidación):
  - El notario debe estar atento a señales de coacción, falta de comprensión o capacidad.
  - La plataforma podría incluir la posibilidad de que el notario hable en privado con una de las partes si sospecha alguna irregularidad.
  - Se podría incluir declaraciones juradas de las partes sobre la ausencia de coacción y la comprensión del acto, las que deberían de exigir una acción positiva por parte de los requirentes realizando la manifestación.
- Firma del Acto: El "clic" o la acción de firmar dentro de la plataforma debe desencadenar el inicio de la operación criptográfica que utiliza la firma electrónica cualificada (QES) en la UE, o la firma digital bajo la ley argentina, empleando la clave privada del firmante (que reside en su dispositivo seguro, como un token USB, una tarjeta inteligente, o en el entorno seguro de su ordenador o móvil), vinculando criptográficamente la voluntad expresada por el requirente al documento digital final (acta o escritura). Este acto de firma debe ser el culmen del proceso de consentimiento.

4. Fase Cuatro: Registro inmutable, auditable y conservación segura del acto a distancia

El objetivo de esta fase es la creación de un registro fidedigno, inalterable, trazable y perdurable de todas las transacciones de documentos pertenecientes a una actuación,

[34] La posibilidad de la grabación del acto de la audiencia notarial dependerá de la normativa de cada uno de los países pues las soluciones son diferentes. Desde aquellos que no permiten que se grabe la audiencia notarial pasando por aquellos en los cuales la grabación es optativa (como Argentina) hasta aquellos países que exigen de manera obligatoria que se grabe la audiencia.

asimismo de cada una de las manifestaciones de voluntad, actuaciones, consentimientos y firmas.

Para el cumplimiento de la presente fase debemos tener en cuenta:

1. Qué debe ser guardado
2. Cómo debe ser guardado, y
3. Bajo que tecnología se aconseja guardarla.

En virtud de ello en esta fase se analiza:

- Grabación audiovisual integral y segura
- Instrumento digital firmado
- Sellado de Tiempo Cualificado (Qualified Timestamps)
- Utilización de tecnología de registro distribuido (DLT)
- Conservación de las actuaciones

Grabación audiovisual integral y segura

Dependiendo lo que establezca la normativa nacional la sesión (acto notarial) podrá o deberá ser grabada en formato audiovisual.

En caso de grabación, la misma debe ser almacenada de forma segura, con controles de acceso estrictos y medidas anti-tampering.[35]

Instrumento digital firmado

El documento resultante debe ser firmado digitalmente (firma electrónica cualificada (QES) en la UE, o firma digital en Argentina), por el notario y todas las partes intervinientes requeridas.[36]

Este documento digital es el original y la principal prueba del acto.

Sellado de tiempo cualificado (Qualified Timestamps)

Aplicar sellos de tiempo cualificados tanto a la grabación audiovisual (en el caso que exista) como al instrumento digital firmado. Esto certifica fehacientemente el momento exacto de la realización del acto y de las firmas, robusteciendo el principio de no repudio.

[35] El *tampering* refiere a la manipulación, alteración o interferencia deliberada y no autorizada sobre un objeto, sistema o conjunto de datos.

[36] Para el caso que la normativa nacional de algún país prevea la posibilidad de suscribir un documento notarial protocolar sin firma electrónica cualificada o firma digital, se podrá aceptar que esta manifestación sea dada por lo aceptado normativamente en el país, teniendo en cuenta que las demás seguridades establecidas en la plataforma a nivel de enrolamiento en la fase 1 y la vinculación de la credencial con la persona en la fase 2. Podria darse el caso de un enrolamiento con SSI y de allí que no posea firma electrónica cualificada (UE) o firma digital (Argentina)

Aplicar sellos de tiempo emitidos por prestadores de servicios de confianza cualificados para certificar fehacientemente el momento exacto en que se produjeron las firmas y los eventos claves, añaden otra capa de no repudio temporal.

Utilización de tecnología de registro distribuido (Blockchain)

Dentro de las tecnologías de registro distribuido se propicia el uso de una blockchain permisionada (controlada por un consorcio de confianza, por ejemplo el poder judicial, los colegios notariales e incluso los notarios). Siendo una blockchain de objetivo específico, no se requeriría de criptomoneda ni "gas" para la misma.[37] El método de consenso sería el de prueba de autoridad, y teniendo en cuenta el contenido de la misma, la blockchain debería registrar el hash de cada uno de los documentos emanados de la actuación notarial a los efectos de una posible pericia informática y pedido judicial de lo actuado.

Dentro de los beneficios que trae aparejada un registro de este tipo es que añade una capa superior de inmutabilidad, trazabilidad, transparencia (controlada) y auditabilidad.

La adopción de esta solución plantea ciertos desafíos a nivel de gobernanza, escalabilidad, costos y la necesidad de un marco legal que reconozca plenamente la función probatoria de estos registros blockchain.[38]

Conservación a largo plazo:

[37] Para el caso que la Blockchain sea con más integrantes se deberá prever una destilería. Esta destilería es un Smart contract operado por la misma Blockchain al que se le asigna una cantidad determinada de gas y la posibilidad de distribuirlo entre los nodos selladores de la Blockchain. De esta manera se puede controlar los nodos y se genera un mecanismo de control de los nodos para poder detectar posibles abusos o fallos de programación (como un loop permanente) que haga colapsar la Blockchain.

[38] En este sentido la primera vez que el Tribunal Supremo español acepta a la Blockchain como prueba es en un caso de criptomonedas en la sentencia 326/2019 del 20 de junio. https://www.poderjudicial.es/search/AN/openCDocument/cac2ec927df2ac2484b8072b28c6b92a42e4a9c597691621, mientras que el juzgado de lo mercantil de Barcelona en un procedimiento de medidas cautelares se trató tanto Blockchain como NFT. ECLI:ES:JMB:2022:1900ª. El artículo 299 de la ley de enjuiciamiento civil establece como medios de prueba entre los que enumera taxativamente a "Artículo 299. Medios de prueba… 3. Cuando por cualquier otro medio no expresamente previsto en los apartados anteriores de este artículo pudiera obtenerse certeza sobre hechos relevantes, el tribunal, a instancia de parte, lo admitirá como prueba, adoptando las medidas que en cada caso resulten necesarias."
En tanto en Argentina, mediante resolución 17/2022 de la Secretaria de Innovación pública de la jefatura de gabinete de ministros se creó el Comité Nacional de Blockchain, mientras que en la provincia de Buenos Aires, se ha celebrado un convenio entre el la Suprema Corte de Justicia de la Provincia de Buenos Aires, el Colegio de Escribanos de la Provincia de Buenos Aires y el Registro de la Propiedad Inmueble de la Provincia de Buenos Aires, mediante el cual se crea una red Blockchain permisionada, con nodos en cada uno de estos organismos y allí se registrarán todos los actos judiciales y notariales.

Conforme a las normativas de los archivos de protocolos notariales, se deben tomar las medidas necesarias que aseguren la legibilidad y autenticidad a lo largo del tiempo.[39][40]

5. Fase Cinco: Auditorias y mejoras conjuntas. Un ecosistema dinámico de confianza

La construcción de una plataforma para la actuación notarial a distancia, tal como se ha delineado en las fases precedentes, no constituye un proyecto con un fin estático. Por el contrario, representa la creación de un ecosistema socio-técnico dinámico que debe garantizar su robustez, pertinencia y seguridad jurídica de manera perpetua. La confianza en el sistema no se establece únicamente en su diseño inicial, sino que se refrenda y fortalece mediante un compromiso ineludible con la vigilancia, la evaluación y la adaptación constantes.

Esta quinta fase es la garante de la resiliencia y longevidad del sistema, asegurando que la arquitectura no solo sea sólida en su concepción, sino que también evolucione para enfrentar nuevas amenazas, se adapte a marcos regulatorios cambiantes y aproveche las innovaciones tecnológicas futuras.

Para ello, se propone un modelo de gobernanza y control basado en tres pilares de auditoría interdependientes y un ciclo de mejora proactivo.

[39] Para el caso que se quiera desarrollar una plataforma de actuación judicial, la misma además de lo mencionado debe preveer (además de los mencionados en las notas 64 y 73):

- Un mecanismo que garantice el principio de contradicción y el derecho de defensa.
- Protocolos claros para la presentación y exámen de testigos y peritos a distancia, asegurando su identificación y la espontaneidad de su testimonio, con un control del entorno físico del declarante.
- Gestión de la publicidad de las audiencias, si corresponde, mediante sistemas de transmisión o acceso remoto controlado.

[40] Una posibilidad es que se guarde el texto de la actuación notarial en el bloque de la Blockchain y además el hash del documento firmado, mientras que el documento firmado se guarda afuera de la Blockchain (sería una blockchain de hash y no de documentos, pero sería más eficiente computacionalmente e igual de segura pues al momento de recuperar el documento firmado se debería cotejar el hash del documento con el hash registrado en la Blockchain para asegurar la integridad del mismo).

1. Auditorías periódicas y multidimensionales

El programa de auditoría debe ser integral, abarcando las dimensiones técnica, procesal y ética del sistema. Estas no deben ser vistas como eventos aislados, sino como un proceso continuo y planificado.

- Auditoría de seguridad tecnológica (Ciberseguridad)
  - Pruebas de intrusión (Pentesting) y análisis de vulnerabilidades: Se deberán realizar, con una periodicidad mínima anual y ante cada actualización sustancial del software, pruebas de intrusión exhaustivas por parte de terceras partes independientes y especializadas. El objetivo es identificar y remediar proactivamente vulnerabilidades en todos los componentes de la arquitectura: la plataforma de videoconferencia, los módulos de autenticación, las API de integración con registros nacionales y los sistemas de almacenamiento.
  - Auditoría criptográfica: Un análisis específico debe validar la correcta implementación de los protocolos criptográficos, la robustez de los algoritmos utilizados, la seguridad en la gestión del ciclo de vida de las claves y la integridad de los entornos seguros (TEEs/HSMs) donde residen las claves privadas de los firmantes.
  - Auditoría de la infraestructura DLT/Blockchain: En el caso de la blockchain permisionada propuesta, la auditoría debe verificar la seguridad de los nodos, la correcta implementación del mecanismo de consenso de “Prueba de Autoridad”, la lógica de registro de hashes y los controles de acceso a la DLT.
- Auditoría de cumplimiento normativo y procesal
  - Auditoría jurídico-notarial: Se evaluará la adecuada conservación del instrumento digital.
  - Auditoría de protección de datos personales: Esta es una auditoría crucial. Deberá certificar el cumplimiento de normativas como el GDPR europeo o el cumplimiento de la Ley argentina de datos personales 25.326. Se examinará la aplicación efectiva de los principios de minimización de datos, limitación de la finalidad, y la existencia de mecanismos claros para el ejercicio de los derechos de los interesados.
- Auditoría de los sistemas biométricos y de IA
  - Evaluación de sesgos y equidad: Los algoritmos de reconocimiento facial deben ser auditados regularmente para detectar y mitigar sesgos demográficos (de edad, género, etnia) que pudieran generar inequidades en el acceso al servicio.

- Pruebas de resistencia a ataques de suplantación (Anti-spoofing): Los mecanismos de detección de vida (liveness detection) deben ser puestos a prueba continuamente contra las técnicas más avanzadas de suplantación, incluyendo deepfakes y otros ataques de presentación generados por IA, garantizando así la eficacia del anclaje con el mundo físico.

2. Gobernanza para la mejora continua

La auditoría solo es útil si los resultados que surgen, impulsan la mejora. Se debe establecer un modelo de gobernanza claro para este fin.

- Ciclo de retroalimentación y adaptación
  - Vigilancia tecnológica y regulatoria: Se debe instituir un proceso formal de vigilancia para monitorear la aparición de nuevas amenazas cibernéticas, la evolución de estándares criptográficos y tecnológicos (como eIDAS 2.0 y el monedero europeo de identidad digital), y las modificaciones en la legislación aplicable a nivel nacional e internacional.
  - Canales de feedback estructurados: Deben existir canales formales para que los notarios y los ciudadanos usuarios puedan reportar incidentes, proponer mejoras o expresar inquietudes. Esta retroalimentación directa es una fuente invaluable de información para la mejora continua.
  - Planificación de la evolución arquitectónica: La arquitectura, basada en estándares abiertos, debe tener una hoja de ruta de evolución. El comité de supervisión debe planificar la migración a algoritmos cuántico-resistentes, la adopción de nuevos formatos de credenciales verificables o la mejora de los protocolos de la DLT, asegurando que la plataforma no caiga en la obsolescencia tecnológica o jurídica.

La incorporación de esta quinta fase transforma la arquitectura propuesta, que va de un producto tecnológico robusto a un sistema de confianza resiliente y sostenible. La auditoría sistemática y la mejora continua no son un apéndice, sino el corazón que mantiene vivo y confiable el sistema, garantizando que la fe pública notarial, en su tránsito hacia el dominio digital, no solo conserve su valor, sino que lo acreciente.

Este enfoque dinámico asegura que el sistema pueda defenderse de las amenazas del mañana, alinearse con el marco jurídico del futuro y, en última instancia, fortalecer de manera perdurable el pilar del no repudio en el que descansa toda la estructura.

Garantizando la robustez y minimizando dudas

Este enfoque arquitectónico, basado en la vinculación criptográfica fuerte entre una identidad física rigurosamente verificada y las acciones realizadas por una persona, utilizando tecnologías probadas (PKI, QES, y blockchain para el registro), ofrece actualmente la base más sólida concebible para una plataforma de actuación notarial para actos protocolares a distancia.

- La posesión exclusiva de la clave privada en un dispositivo seguro es el pilar para mitigar el riesgo de suplantación de identidad.
- La vinculación de la plataforma con el organismo nacional que otorga los documentos nacional de identidad y permite la validación biométrica en línea mientras se desarrolla la videoconferencia, es una herramienta poderosa frente a las técnicas de inteligencia artificial, asegura la identidad de los requirentes evitando el riesgo de suplantación de las personas.
- Las firmas electrónicas cualificadas y las firmas digitales vinculan inequívocamente la acción a la identidad verificada, asegurando el principio de no repudio. El registro inmutable en una DLT, en nuestro caso una Blockchain, solidifica la prueba.
- La plataforma se alinea con los principios de eIDAS y otros marcos legales para la identificación y firma electrónica de alta seguridad o firma digital.
- Sería aconsejable prever que el desarrollo de la plataforma se base en estándares abiertos, que permitan la interoperabilidad y la adaptación a futuras evoluciones tecnológicas y regulatorias.

Conclusión y recomendaciones

La arquitectura conceptual y tecnológica aquí esbozada, ofrece una vía robusta y jurídicamente fundada para materializar la realización de actos notariales protocolares a distancia. El camino implicará una inversión significativa y una cuidadosa revisión y adecuación a los marcos regulatorios, pero los beneficios en términos de eficiencia, accesibilidad y modernización de la fe pública son innegables.

La clave reside en una simbiosis entre tecnología de vanguardia (identificación biométrica con liveness detection, validación de identidad en línea con el organismo del Estado encargado de otorgar los documentos de identidad, mientras se desarrolla la videoconferencia de actuación notarial, criptografía avanzada, plataformas de videoconferencia seguras, QES/firma digital, el registro en una DLT, en nuestro caso, blockchain) y un diseño de procesos que respete minuciosamente las garantías legales y los principios fundamentales del derecho.

Este proyecto transformador de la actuación notarial protocolar, utilizando una plataforma a distancia responde a las demandas de una sociedad cada vez más digital. Si a esta arquitectura además le incorporamos un workflow agéntico para reforzar aún más la identidad y una prestación del consentimiento fuerte, no solo logramos tener una actuación notarial robusta sino además reconceptualizaremos el término "seguridad", pasando de una seguridad digital estática a una seguridad digital dinámica.

Capítulo V: Workflows agénticos

Propuesta superadora y coadyuvante de la función pública para una identificación y una manifestación de voluntad robusta en una actuación a distancia

Introducción

La inteligencia artificial generativa ha evolucionado vertiginosamente en estos dos últimos años, pasando de un agente conversacional multipropósito y multitarea que solo podía recibir una solicitud (input) en formato de texto y devolver una salida (output) en el mismo formato, a modelos de agentes multimodales donde puedo ingresar un input ya sea en texto, imágenes, video o audio para devolver un output en cualquiera de los formatos antes mencionados, eliminando las barreras iniciales de formatos de información a procesar y generar[41]. En este escenario, la IA puede procesar un documento visual, interpretarlo y responder en lenguaje natural. Esta evolución es sustancial para poder fundamentar y demostrar la viabilidad de la propuesta de solución que se plantea en el presente capítulo, pudiendo avanzar en la evaluación de las diferentes tecnologías que han de trabajar coordinadamente para poder llegar a vincular indiscutiblemente la identidad y voluntad de la persona a una actuación notarial.

[41] Corvalán, J.G. y Sánchez Caparrós, M., (2025) *Agentes de inteligencia artificial y wokflows agénticos: la nueva frontera de la automatización.* Laboratorio de Inteligencia Artificial de la Facultad de Derecho de la Universidad de Buenos Aires. (IALAB) y Banco de Desarrollo de América Latina y el Caribe (CAF). p.17

Mientras los primeros agentes multitareas y multipropósitos tenían la limitación de recibir y devolver la información en un solo formato, su evolución ha permitido la creación de agentes multimodales. Los actuales agentes basados en IA generativa combinan modelos de lenguaje con otras herramientas que permiten acceder a otros recursos como páginas web, memoria, programación de tareas, acceso a la información creada o analizada por otros agentes de IA, entre otras funciones que posibilitan ejecutar flujos de trabajos completos de forma autónoma y dinámica.[42]

La actuación notarial con presencia física junto al notario se rodea de ciertos formalismos, pero además se realiza en un ambiente controlado, aprehensible y manejado por el oficial público donde la interacción y presencia física de todas las partes permite eliminar el riesgo de eventuales vicios de la voluntad, como son la violencia o intimidación en el mismo ambiente donde se desarrolla la actuación notarial al momento de prestar la conformidad al acto.[43]

Cuando se habla de actuación a distancia una de las primeras objeciones que se plantearon fue la imposibilidad de poder controlar el ambiente donde se encuentra el requirente, así como otros aspectos relativos a la identidad y a la veracidad del acto y de las manifestaciones de las partes. Con el tiempo se fueron encontrando mecanismos y soluciones alternativas que viabilizaron la actuación notarial a distancia, permitiendo su realización.[44]

La propuesta en este capítulo no solamente tiene en miras esas primigenias objeciones que se hicieron y luego fueron sorteadas, sino que profundiza en la posibilidad de robustecer las actuales soluciones con la ayuda que el avance tecnológico y la inteligencia artificial nos permite.

Actualmente la dación de fe se basa en la experiencia que el oficial público tiene, sumado a las diferentes técnicas, herramientas y mecanismos que utiliza a través de preguntas y repreguntas, el notario subjetivamente, se crea un estado de situación personal del requirente y a partir de allí continúa con el acto hasta su autorización.

---

[42] Corvalán, J.G. y Sánchez Caparrós, M., (2025) *Agentes de inteligencia artificial y wokflows agénticos: la nueva frontera de la automatización.* Laboratorio de Inteligencia Artificial de la Facultad de Derecho de la Universidad de Buenos Aires. (IALAB) y Banco de Desarrollo de América Latina y el Caribe (CAF). p.12

[43] Se sostiene que se eliminan esos vicios en el lugar donde se desarrolla la actuación porque la violencia o intimidación a la que pueda estar expuesto el requirente puede ocurrir fuera de la notaría y ella escapa al control que pueda realizar el oficial público.

[44] Las mismas o similares objeciones pueden encontrarse en aquellos primeros detractores de las audiencias judiciales a distancia.
Actualmente existe actuación notarial a distancia en los notariados de la Unión Europea, pero también en Canadá, Brasil y Argentina, todos con modalidades y competencias diferentes, dependiendo el orden jurídico de cada uno de los países.

La propuesta es la de coadyuvar al análisis personal subjetivo, mediante datos objetivos que permitan una evaluación híbrida (subjetiva-objetiva) del oficial público para continuar o no con la actuación ante la posibilidad de alguna duda en la identidad de las personas o un eventual vicio de la voluntad de alguno de los requirentes.

Esta propuesta viene a complementar la actuación notarial, ofreciendo una herramienta coadyuvante y superadora a la propia observación y calificación subjetiva del notario, pero nunca invalidante de la calificación y actuación notarial.

En virtud de ello, y teniendo en cuenta la importancia que significa brindar y garantizar seguridad jurídica en una actuación a distancia, sumado a ello, el avance tecnológico incipiente en la implementación de workflows agénticos se propone su integración de éstos a la arquitectura conceptual desarrollada en el capítulo anterior. Un ecosistema de agentes de inteligencia artificial (IA) especializados puede añadir capas dinámicas de seguridad y verificación al robusto marco criptográfico ya descripto en el capítulo anterior.

Este enfoque "agéntico" no reemplaza la criptografía ni la actuación notarial –que sigue siendo el pilar fundamental del no repudio– sino que la complementa y refuerza, monitoreando patrones, contextos y comportamientos que los sistemas puramente deterministas no pueden evaluar.

Imaginemos un flujo de trabajo (workflow) donde distintos agentes de IA colaboran entre sí con las tecnologías base de cada etapa crítica del proceso. El objetivo es construir un mecanismo de defensa robusto, donde múltiples capas de agentes con análisis inteligente validen continuamente la legitimidad de la interacción y la manifestación de voluntad de la persona.

En este escenario pensamos en la interacción de doce (12) agentes que se encuentran repartidos en las cinco (5) fases que hemos de detallar:

Los doce agentes inteligentes son:

1. Agente 1: Analista de riesgo preliminar (ARP)
2. Agente 2: Verificador documental avanzado (VDA)
3. Agente 3: Analista biométrico y de prueba de vida (ABPV)
4. Agente 4: Consolidador de verificación y decisión (CVD)
5. Agente 5: Analista de contexto de acceso (ACA)
6. Agente 6: Monitor de biometría conductual (MBC - Pasivo y Continuo)
7. Agente 7: Intérprete de lenguaje natural y sentimiento (ILNS)
8. Agente 8: Detector de anomalías transaccionales y comportamentales (DATC)
9. Agente 9: Asistente legal contextual (ALC - Opcional)

10. Agente 10: Orquestador de sesión y riesgo pre-firma (OSRP)
11. Agente 11: Analista forense de patrones (AFP)
12. Agente 12: Asistente de resolución de disputas (ARD)

Las fases en las cuales han de desarrollar la actividad cada uno de los agentes mencionados son:

1. Fase 1: Esta etapa no se encuentra reflejada en el marco conceptual del capítulo anterior por cuanto es una evaluación de riesgo inicial, previo al enrolamiento del requirente.
2. Fase 2: Vinculada a la verificación robusta de identidad y desarrollada en la fase uno de la arquitectura conceptual.
3. Fase 3: Autenticación y acceso al entorno notarial. Desarrollada en la fase dos de la arquitectura conceptual.
4. Fase 4: Dedicada a la actividad que se desarrolla durante la sesión notarial, su registro y la vinculación de la manifestación de voluntad a la persona. Desarrolladas en las fases 3 y 4 de la arquitectura conceptual
5. Fase 5: Coincidentemente con la fase 5 de la arquitectura conceptual, refiere a las auditorias y mejoras que puedan encontrarse luego de una sesión

Workflow agéntico para una identificación fuerte en el entorno notarial de videoconferencia

Fase 1: Pre-Solicitud y evaluación de riesgo inicial

El usuario manifiesta interés en acceder al entorno notarial.

Agente IA 1: Analista de riesgo preliminar (ARP)

En este escenario, comienza a actuar el Agente IA 1, dedicado al análisis del riesgo preliminar. Este agente no posee ninguna tecnología vinculada directamente sino que utiliza metadatos iniciales (IP, huella del dispositivo, geolocalización tentativa, hora).

Su función es la de evaluar el riesgo contextual inicial para saber si la conexión proviene de una ubicación o red sospechosa. Si el dispositivo tiene indicadores de compromiso conocidos o eventualmente hay patrones de intento de acceso anómalos

Una vez recibido los datos básicos de la solicitud, genera un score de riesgo inicial, pudiendo consultar bases de datos externas de IP o dispositivos maliciosos y pasa el score a la siguiente fase.

La implementación de este agente tiene como beneficio de seguridad que puede filtrar tempranamente intentos de acceso claramente fraudulentos o de alto riesgo antes de iniciar el proceso de verificación de identidad que es costoso tecnológicamente.

Fase 2: Verificación de identidad robusta

El usuario inicia el proceso de verificación, subiendo documentos y realizando la captura biométrica de su rostro.

Agente IA 2: Verificador documental avanzado (VDA)

En este escenario el agente de IA dedicado a la verificación documental y biométrica, posee la tecnología necesaria como para la verificación de los documentos y la identidad, mediante OCR y análisis de imágenes, mediante la visión de computadoras (VC) y el procesamiento de lenguaje natural (PNL)

Su función, mediante la tecnología incorporada es la de analizar la autenticidad del documento de identidad: microimpresiones, hologramas (si la captura lo permite), consistencia de datos, detección de patrones de falsificación (comparación con bases de datos de documentos fraudulentos conocidos), validación de MRZ/códigos de barras/chips NFC. En caso que sea posible normativamente[45] cruza datos extraídos con la información externa.

Recibida las imágenes y/o los datos del documento, interactúa con las bases de datos externas. Con ello, pasa el resultado de la verificación y un score de confianza documental al agente consolidador que es el Agente IA 4.

La implementación de este agente tiene como beneficio de seguridad la detección de falsificaciones sofisticadas que podrían eludir verificaciones básicas, dando una mayor certeza sobre la autenticidad del documento presentado y generando un score mayor de seguridad jurídica.

Agente IA 3: Analista biométrico y de prueba de vida (ABPV)

Este agente tiene como tecnología vinculada a la biometría y prueba de vida. De esta manera, el agente procesa la captura biométrica (ej. facial), realiza la comparación 1:1 con la foto del documento validado por el Agente IA 2 (VDA). Si pasa la validación de

[45] Como en el caso de Argentina que es posible acceder a esos servicios a través de convenios específicos, que se encuentran actualmente vigentes y en funcionamiento con algunos notariados provinciales. En la Unión Europea no sería posible pues está vedado la posibilidad que empresas privadas accedan a las base de datos de los Estados. En Japón sería posible aunque el acceso a esas bases está muy restringido ya que no hay un mecanismo generalizado que lo permita, pero no se encuentra prohibido como lo es en China. Para la aplicación en los Estados Unidos de América hay que estar a la normativa de cada Estado por su organización federal.

comparación, ejecuta algoritmos avanzados de prueba de vida, como sería los algoritmos de análisis de textura 3D, parpadeo, movimientos oculares, respuesta a desafíos aleatorios, a los efectos de mitigar ataques de presentación de fotos, vídeos, máscaras y deepfakes.[46] Con todo ello, evalúa la calidad de la muestra biométrica.

Una vez recibido el dato biométrico, pasa el resultado del análisis, el score de la prueba de vida y la calidad de la muestra al agente consolidador, o sea al Agente IA 4.

La implementación de esta IA tiene como beneficio de seguridad que la tecnología empleada posee una resistencia muy alta a intentos de suplantación mediante artefactos o deepfakes durante la captura biométrica.

Agente IA 4: Consolidador de verificación y decisión (CVD)

Este agente no posee ninguna tecnología directa vinculada sino que actúa como orquestador de los datos recibidos por los demás agentes. Su función es la de recibir y evaluar los scores y resultados de los agentes 1 (ARP), 2 (VDA) y 3 (ABPV). En el análisis de los datos recibidos, busca inconsistencias, como por ejemplo un documento válido pero una prueba de vida con score bajo, un riesgo de IP alto pero una biometría validada. Este agente aplica reglas de negocio y modelos de riesgo configurables. Decide si la verificación es exitosa, fallida, o requiere revisión humana. Para esta clase de “decisiones” se ha de utilizar una IA explicable[47], a los efectos de justificar las decisiones de riesgo.

Un vez recibido los datos de los agentes 1, 2, 3, se comunica con el sistema operativo con el cual se está trabajando para pasar a revisión humana en caso que fuera necesario. El resultado final del análisis (éxito/fallo + score de riesgo consolidado) dispara la emisión o no de credenciales.

La implementación de esta IA tiene como beneficio de seguridad una visión holística del riesgo del enrolamiento de una persona, correlacionando distintas señales. Reduce falsos positivos o negativos y proporciona una trazabilidad de la decisión.

Una vez validada la persona el sistema debe:

- Emitir las credenciales verificables (CVs) fundamentales, como por ejemplo: "Identidad Verificada Nivel Alto eIDAS", firmada por la entidad verificadora y asociadas a la CV.

[46] Se podría utilizar FaceTorch que es una biblioteca de Python basada en PyTorch con modelos preentrenados para diversas tareas de análisis facial, incluido el reconocimiento de expresiones, la detección de unidades de acción y la detección de *deepfakes*.

[47] Un ejemplo de ello podria ser a través de árbol de decisión

- Realizar un guardado seguro de la clave privada asociada al CV en el dispositivo/wallet del usuario mediante una gestión segura de claves (QSCD) o equivalente.

Las tecnologías involucradas para la realización de estas acciones son las mencionadas anteriormente como credenciales verificables (CVs), sistema de clave pública (PKI) y gestión segura de claves (QSCD).

Fase 3: Autenticación y acceso al entorno notarial de videoconferencia

El usuario intenta acceder al entorno notarial usando su identidad verificada, presentando su credencial (CV) y firma con su clave privada.

La tecnología vinculada a esta fase está dada por la autenticación mediante las CVs y firma PKI, idealmente desde el mismo gestor de clave segura (QSCD).

Agente IA 5: Analista de contexto de acceso (ACA)

El Agente IA 5 dedicado a analizar el contexto del acceso de los usuarios comienza a monitorear la sesión y el dispositivo por el cual se conecta el usuario.

Su función es evaluar el contexto del intento de acceso, analizando si el dispositivo es uno conocido y está registrado o no. Si la geolocalización o su IP son consistentes con el perfil.

Una vez recibido los datos del intento de login y del dispositivo del usuario, los compara con su perfil histórico y actualiza dinámicamente un score de riesgo de sesión. Pasa el score al Agente IA 10, denominado orquestador de sesión.

La implementación de este agente tiene como beneficio de seguridad la detección de intentos de acceso desde dispositivos comprometidos o en contextos anómalos, incluso si la credencial criptográfica es válida, ya que la misma puede haber sido robada.

Agente IA 6: Monitor de biometría conductual (MBC - Pasivo y Continuo)

Este agente tiene como función analizar los patrones de interacción del usuario.

De esta manera, una vez iniciada la sesión, el agente comienza a monitorear -de forma transparente para el usuario pero con consentimiento previo del mismo- micro-patrones de comportamiento y reconocimiento de emociones, por ejemplo: cómo interactúa con la interfaz, velocidad y ritmo de escritura (en caso que pueda darse este supuesto), patrones de movimiento del cursor, reconocimiento de microexpresiones, detección de

deepfakes,[48] reconocimiento de emociones de voz, etc. Con todos estos datos construye un perfil dinámico.

Una vez recibido el flujo de datos de la interacción, no bloquea activamente pero calcula continuamente una puntuación de desviación respecto al perfil que posee registrado e informa desviaciones significativas al agente orquestador de sesión.

La implementación de este agente tiene como beneficio de seguridad la detección de cambios sutiles que podrían indicar que un tercero ha tomado control de la sesión (session hijacking) después de una autenticación inicial válida, proporcionando una autenticación continua.

Desde una perspectiva tecnológica, una IA emocional multimodal, combinando voz, expresión facial, gestos y texto, presenta una oportunidad para crear sistemas más precisos y conscientes del contexto.[49] Estos avances podrían permitir una comprensión emocional en tiempo real.

En este sentido, MorphCast es una solución sin servidor, basada en navegador, que analiza más de 130 expresiones faciales en tiempo real, priorizando la privacidad al procesar datos localmente, e integrando las emociones centrales de Paul Ekman[50] y el modelo circunflejo de Russell para un análisis matizado. [51]

Fase 4: Durante la sesión notarial (Interacción y transacción aumentada por IA)

Los participantes interactúan, discuten, presentan documentos y expresan consentimiento.

Agente IA 7: Intérprete de lenguaje natural y sentimiento (ILNS)

El agente tiene como función procesar la transcripción del diálogo y analizar la misma mediante la tecnología de procesamiento de lenguaje natural (PLN) y modelo de emociones basadas en texto.

[48]En este sentido se puede pensar en FaceTorch que es una biblioteca de Python basada en PyTorch con modelos preentrenados para diversas tareas de análisis facial, incluido el reconocimiento de expresiones, la detección de unidades de acción y la detección de *deepfakes*. También en Deep-Emotion que es una implementación de PyTorch que utiliza una red convolucional atencional y redes de transformadores espaciales para el reconocimiento de expresiones faciales. Otra herramienta es OpenSMILE que es un kit de herramientas bien establecido para extraer características de audio, ampliamente utilizado en el reconocimiento de emociones de voz, permitiendo a los desarrolladores trabajar directamente con datos acústicos y construir sistemas afectivos en tiempo real. Citados por Vivek Chavan, Arsen Cenaj, Shuyuan Shen, Ariane Bar et all, *Feeling Machines: Ethics, Culture, and the Rise of Emotional AI. https://arxiv.org/pdf/2506.12437*

[49] Reglamento de Inteligencia Artificial (RIA) de la UE 2024/1689

[50] Ekman, P. (2017) *El rostro de las emociones.* RBA. Matsumoto, David & Hwang, H.S. & López, Rafael & Pérez Nieto, Miguel. (2013). *Reading facial expressions of emotions: Basic research on emotions recognition improvement.* Ansiedad y Estrés.

[51] Vivek Chavan, Arsen Cenaj, Shuyuan Shen, Ariane Bar et all, (2025) *Feeling Machines: Ethics, Culture, and the Rise of Emotional AI. https://arxiv.org/pdf/2506.12437*

Estos modelos infieren emociones a partir de una entrada de texto, lo que permite la clasificación de emociones o el etiquetado de sentimientos.[52]

De esta manera, en el análisis del diálogo transcripto identifica:

- Afirmaciones claves de consentimiento y/o acuerdo.
- Posibles ambigüedades, contradicciones o signos de confusión en las declaraciones.
- Indicadores lingüísticos de posible estrés, coacción o falta de entendimiento, como por ejemplo. vacilaciones excesivas, respuestas evasivas, cambios de tema.

Una vez recibida la transcripción del audio genera las alertas sobre los puntos problemáticos.

Puede interactuar con el agente asistente legal (IA 9) para verificar si el lenguaje usado corresponde a las cláusulas discutidas e informa al agente orquestador de sesión (IA 10)

La implementación de este agente trae como beneficio de seguridad que ayuda a evaluar la calidad del consentimiento del acto (más allá del "sí" formal), pudiendo detectar posibles vicios de la voluntad o falta de capacidad natural que podrían invalidar con posterioridad el acto.[53] Este agente puede servir como apoyo a la labor del notario ya sea para ratificar indicadores válidos o incluso para informar sobre ciertos indicadores que adviertan al notario sobre una posible incomprensión del acto o duda en la suscripción del mismo. De esta manera el notario podrá volver a explicar el mismo o incluso pedir ratificación del consentimiento ya brindado.

Agente IA 8: Detector de anomalías transaccionales y comportamentales (DATC)

El agente tiene como función monitorear los eventos de la sala de videoconferencia, analizar los patrones del mismo y advertir al agente orquestador de la sesión (IA10).

En su actividad, monitorea la secuencia de acciones dentro de la sesión, evaluando si se siguen los pasos esperados de un procedimiento notarial, si existen interacciones inusuales con la interfaz o el entorno, si el usuario intenta realizar acciones no permitidas, si existen discrepancias entre lo discutido (y captado por ILNS) y las acciones realizadas.

[52] Como por ejemplo los modelos DistilRoBERTa, BERT, RoBERTa, o Feel-it o Beto, citados por Vivek Chavan, Arsen Cenaj, Shuyuan Shen, Ariane Bar et all, (2025) *Feeling Machines: Ethics, Culture, and the Rise of Emotional AI. https://arxiv.org/pdf/2506.12437*

[53] En el análisis profundo de este agente nos explayamos sobre la limitación que tiene la tecnología en este sentido pues es muy difícil crear un modelo que distinga fiablemente entre estrés normal por la formalidad del acto y estrés por coacción, o entre reflexión y confusión. En virtud de ello es que solo serán indicadores que puedan alertar al notario pero que no deben de ser invalidantes para la continuación del acto.

Además analiza el comportamiento de la persona (controlado por MBC) para poder evaluar si se desvía drásticamente de los parámetros históricos que tiene.

Una vez que recibe logs de eventos de la sala de videoconferencia, datos de red, scores de MBC y alertas de ILNS, busca patrones anómalos o combinaciones sospechosas e informa al agente orquestador de sesión (IA 10).

La implementación de este agente trae como beneficio de seguridad, la detección de fraudes en curso, la manipulación del proceso, o acciones que no se corresponden con la voluntad expresada o el procedimiento estándar.

Agente IA 9: Asistente legal contextual (ALC)

Este agente tiene como función analizar las cláusulas de documentos presentados en la sala de videoconferencia y proporcionar explicaciones en lenguaje claro, identificar potenciales riesgos o implicaciones, o verificar la consistencia con la legislación aplicable, teniendo en cuenta la base de conocimiento con la cual se haya entrenado. Para ello es necesario que cuente con tecnología de procesamiento de lenguaje natural (PLN), recuperación de información y además con una base legal que le permita el análisis contextual.

El agente, ya sea a petición del usuario o del notario, puede analizar cláusulas de documentos presentados previamente o en el mismo momento en la sala de videoconferencia y proporcionar explicaciones en lenguaje claro, identificando potenciales riesgos, verificando adecuación o inconsistencias con la legislación aplicable.

Una vez que el agente recibe el texto, proporciona un análisis del mismo con una explicación incluso en leguaje claro o lenguaje entendible para un usuario lego. Podría incluso, interactuar con agente IA 7 (ILNS) para asegurar que la explicación fue comprendida.

Si bien la existencia o no de este agente no invalida la solución a la creación de este entorno de actuación a distancia, la implementación del mismo tiene como beneficio una mejora en la comprensión y el consentimiento informado de las partes, reduciendo riesgos de nulidad por vicios en la voluntad.

Este agente puede servir como apoyo a la labor del notario a los efectos de lograr la máxima comprensión del acto por parte de los usuarios.

Acción Crítica: Firma del acto notarial

El sistema solicita la firma electrónica cualificada (QES)[54] al o los usuarios. Para ello se vale de las tecnologías de infraestructura de clave pública (PKI), firma electrónica cualificada (QES) y de un dispositivo con gestión segura de clave (QSCD).

[54] En Argentina a esta tecnología se la reconoce como firma digital

Agente IA 10: Orquestador de Sesión y Riesgo Pre-Firma (OSRP)

El Agente IA 10 es el cerebro orquestador de agentes que genera un modelado compuesto del riesgo de la sesión que se está llevando a cabo en la sala de videoconferencia del entorno notarial.

Su función es la de actuar como el "cerebro" de la seguridad durante la sesión. Recibe continuamente los scores y alertas de los agentes 5 (ACA), 6 (MBC), 7 (ILNS) y 8 (DATC). Justo antes de habilitar la firma electrónica cualificada (QES), calcula un score de confianza de la sesión global. Si el score está por debajo de un umbral crítico (o si hay alertas graves activas), puede:

- Alertar al notario con un resumen de los riesgos detectados, para lo cual se requiere la implementación de una IA explicable.
- Requerir pasos adicionales de verificación (por ejemplo: re-autenticación biométrica activa).
- En casos extremos y configurables, bloquear temporalmente la posibilidad de firmar hasta tanto el notario evalúe la situación.

Una vez recibido los datos de los agentes 5 (ACA), 6 (MBC), 7 (ILNS) y 8 (DATC), se comunica con la interfaz del notario y con el módulo de firma de la plataforma a los efectos de habilitar el módulo de firma o esperar una acción por parte del notario. La evaluación de este agente debe quedar registrada.

La implementación de este agente trae como beneficio de seguridad un punto de control holístico antes del acto de la firma, permitiendo, a través del análisis de los scores, prevenir firmas bajo coacción, error, confusión, o en sesiones comprometidas que no fueron detectadas por las capas individuales.

Acción del Sistema (Post-Firma):

Una vez firmado el documento, se obtiene un sello de tiempo cualificado y se registra en registro de tecnología distribuida (DLT), pudiendo ser una Blockchain[55] u otra similar.

En el registro de tecnología distribuida se registra el hash del documento firmado, la o las firmas electrónicas cualificadas (QES), el timestamp, las referencias a las CVs de

[55] Debemos distinguir “Blockchain” (con mayúscula) de “blockchain” (con minúscula). Con la primera nos referimos a la tecnología empleada para la creación de las bases de datos, mientras que con la segunda nos referimos a las bases de datos ya creadas y que, en algunos casos, se suelen denominar con el mismo nombre de la tecnología que las sustenta. Para ampliar en el tema, Cosola, S.J. & Schmidt, W.C. (2021) *El Derecho y la tecnología.* Thomson Reuters-La Ley. Buenos Aires. Argentina. Tomo 2 p.2

participantes, y un hash o resumen verificable del estado final de riesgo determinado por el IA 10 (OSRP) y las alertas relevantes de otros agentes.

Fase 5: Post-Sesión, Auditoría y Mejora Continua

Agente IA 11: Analista Forense de Patrones (AFP)

Finalizado el acto de suscripción del documento y la actuación notarial, comienza a actuar el agente IA 11 (AFP), analizando logs agregados y anonimizados de múltiples sesiones (incluyendo datos de todos los agentes IA) para detectar patrones de fraude emergentes, posibles anillos de colusión (por ejemplo: usuarios con patrones de riesgo similares interactuando repetidamente), o vulnerabilidades sistémicas.

Finalizado el análisis del mismo puede que el agente identifique mejoras para los modelos de los otros agentes.

Este agente sería un machine learning (con análisis de clustering y detección de outliers), con análisis de grafos.

Una vez que el agente accede a los logs históricos, genera informes para los equipos de ciberseguridad y desarrollo, pudiendo proponer actualizaciones a los modelos de otros agentes.

La implementación de este agente trae como beneficio de seguridad la detección proactiva de amenazas sofisticadas o a gran escala, mejorando de forma continua de la eficacia de los agentes IA.

Agente IA 12: Asistente de Resolución de Disputas (ARD)

En caso de un conflicto sobre un acto notarial realizado, el agente puede procesar la consulta en lenguaje natural, recuperar toda la evidencia relevante del registro inmutable (firmas, timestamps, logs de interacción, CVs presentadas, alertas de IA registradas), y presentarla de forma estructurada y comprensible para los humanos (jueces, árbitros), resaltando los puntos clave y la secuencia de eventos según el registro.

Para ello es necesario que este agente cuente con tecnologías vinculadas al procesamiento de lenguaje natural (PLN), tecnologías de recuperación de información y de visualización de datos.

Una vez que el agente accede a los registros específicos, previa autorización o solicitud judicial o arbitral, genera un resumen y presenta el informe. El agente no toma decisiones ni califica, sino que objetivamente presenta la evidencia.

La implementación de este agente tiene como beneficio que puede facilitar y acelerar la resolución de disputas al organizar y presentar la compleja evidencia digital de manera eficaz.

Workflows: Un análisis profundo de dos agentes

Análisis profundo del Agente IA 6 monitor de biometría conductual (MBC) y del Agente IA 7 intérprete de lenguaje natural y sentimiento (ILNS)

Teniendo en cuenta que los agentes de IA 6 (MBC) y 7 (ILNS) son de los más innovadores y delicados en la estructura del workflows, así como la importancia que los mismos revisten en la consideración de la vinculación del accionar de una persona con la realización y concreción de un acto notarial válido, nos parece importante realizar un análisis profundo de cada uno, evaluando la viabilidad técnica y la elección de proveedores, fundamentando cada una de las opciones y explorando su factibilidad en el contexto actual.

Para realizar el análisis de los agentes hemos de discriminarlos en diferentes aristas, a los efectos de permitir abarcar en su totalidad tanto la función de los mismos como su posible puesta en ejecución. De esta manera abordaremos el análisis de cada uno de ellos, a partir de los siguientes puntos:

A. Función técnica
B. Tecnologías subyacentes
C. Potenciales proveedores y tecnologías específicas
D. Viabilidad y justificación técnica

Análisis del Agente IA 6: Monitor de Biometría Conductual (MBC).

A. Función técnica

El monitor de biometría conductual (MBC) opera como un vigilante silencioso y continuo post-autenticación inicial. Su misión es verificar pasivamente la identidad del usuario a lo largo de la sesión en la sala de videoconferencia, basándose en la premisa de que cada individuo interactúa con los sistemas digitales de una manera única y característica, similar a una firma conductual. No requiere acciones explícitas del usuario, sino que monitorea patrones inherentes a su interacción.

El objetivo principal es detectar anomalías que sugieran que la persona que controla los dispositivos ya no es el usuario legítimamente autenticado, como por ejemplo detectar si la sesión ha sido secuestrada por un tercero o el dispositivo fue pasado o capturado por otra persona.

Asimismo mediante agentes de inteligencia artificial emocionalmente receptiva, a través del reconocimiento de emociones, pueden servir como mecanismo de detección temprana de dependencia emocional que permitan una comprensión en tiempo real.[56]

En el monitoreo de comportamientos que se realiza durante la sesión, se pueden evaluar distintos aspectos:

- Interacción con interfaces: Patrones de uso de mandos o controladores, mediante la presión de botones, movimiento de mouse, velocidad y precisión al señalar o seleccionar objetos.
- Seguimiento ocular: Patrones de fijación visual, exploración de la escena, tiempo de permanencia en áreas de interés, correlación mirada con acción posterior.
- Reconocimiento de expresiones, micro expresiones y análisis facial
- Patrones de escritura en el caso que se use teclado físico o virtual: Ritmo, velocidad, latencia entre pulsaciones, uso de teclas específicas.
- Voz en el caso que se utilice para interacción o comandos: Podríamos incluir análisis básico de ritmo o patrones de habla, aunque el análisis profundo estará dado por el Agente IA 7 (ILNS).

B. Tecnologías subyacentes

El monitor de biometría conductual se basa en una combinación de captura de datos de sensores, preprocesamiento y modelos de Machine Learning (ML):

La captura de datos se realiza mediante el acceso a APIs de bajo nivel de la cámara web con seguimiento ocular[57] y controladores para obtener datos de:

- Movimiento de cabeza y manos.
- Posicionamiento absoluto y relativo de la persona mediante su seguimiento.
- Estado de botones, mouse y/o touchpads de los controladores.
- Datos del seguimiento ocular, mediante coordenadas de la mirada y diámetro pupilar.
- Logs de interacción con la interfaz de la sala de videoconferencia.

[56] Vivek Chavan, Arsen Cenaj, Shuyuan Shen, Ariane Bar et all, (2025) *Feeling Machines: Ethics, Culture, and the Rise of Emotional AI. https://arxiv.org/pdf/2506.12437*

[57] Barba Alonso, R. (2021) *Diseño e implementación de un sistema de captura de datos de entrenamiento para la realización de eye-tracking sin hardware específico. https://uvadoc.uva.es/handle/10324/50018*

El preprocesamiento de datos se basa inicialmente en una limpieza de datos, normalización de los mismos, extracción de características relevantes a partir de los datos crudos[58].

Los modelos de machine learning sobre los cuales ha de trabajar el agente de IA tienen tres aristas que se detallan a continuación:

- Aprendizaje de perfil: Durante el período inicial el sistema aprende el patrón de comportamiento "normal" del usuario legítimo, el cual se va a adaptando continuamente. Se usan técnicas como:
  - Modelos de series temporales (LSTMs, GRUs, Transformadores)[59] para capturar dependencias temporales en los movimientos e interacciones.
  - Modelos estadísticos (GMMs)[60] para modelar distribuciones de características conductuales.
- Detección de Anomalías: Una vez establecido el perfil del usuario, el sistema compara continuamente el comportamiento actual con el perfil aprendido, mediante las siguientes técnicas:
  - One-Class SVM[61].
  - Autocodificador, que es un tipo de red neuronal que aprenden a reconstruir la entrada normal y luego a reconstruirlos a partir de esa representación, pero suelen fallar en reconstruir datos anómalos.
  - Isolation Forests, que es un algoritmo para la detección de anomalías en datos mediante árboles binarios
  - Cálculo de distancia o divergencia respecto al perfil base, mediante la distancia de Mahalanobis y la divergencia de Kullback-Leibler.[62]

[58] Por ejemplo calcular velocidad media de giro de cabeza, frecuencia de parpadeo, tiempo de reacción a estímulos, métricas de fluidez del movimiento

[59] Los LSTM (memoria a corto y largo plazo) y los GRU (unidad recurrente cerrada) son dos tipos de capas de redes neuronales recurrentes (RRN) diseñadas para manejar datos secuenciales. Los transformadores surgen a partir del trabajo de Ashish Vaswani, Llion Jones, Noam Shazeer, Aidan N. Gomez, Niki Parmar, Jakob Uszkoreit, Łukasz Kaiser e Illia Polosukhin denominado “Attention is all you need”. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://proceedings.neurips.cc/paper_files/paper/2017/file/3f5ee243547dee91fbd053c1c4a845aa-Paper.pdf

[60] Un GMM o modelo de mezcla Gaussiana es un método de aprendizaje automático que se utiliza para determinar la probabilidad de que cada punto de datos pertenezca a un grupo determinado.

[61] One-Class SVM, o Máquinas de Vector Soporte de una Clase, es una técnica de aprendizaje automático no supervisado utilizada para la detección de anomalías en conjuntos de datos.

[62] De Medeiros Martins, Allan; Dantas de Melo Jorge; Duarte Doria Neto, Adrião *Comparison between Mahalanobis distance and Kullback-Leibler divergence in clustering análisis.*

- Puntuación de Riesgo: El sistema genera un score continuo que indica la probabilidad que el comportamiento actual sea anómalo o no corresponda al usuario legítimo.

C. Potenciales proveedores y tecnologías específicas

Si bien el tema que estamos tratando se encuentra en permanente evolución, los proveedores suelen ser empresas que se dediquen a ciberseguridad adaptando las tecnologías existentes o ser los propios fabricantes de plataformas o hardware.

- Empresas de Ciberseguridad como puede ser BioCatch, BehavioSec, o IBM (Security Verify).
- Plataformas de Inteligencia Artificial y Machine Learning en la nube como podrían ser: MorphCast, Visage Technologies, Affectiva, Viso Suite, Face Rader,[63] Google Cloud AI Platform / Vertex AI, AWS SageMaker / Kinesis / Lookout for Metrics, Microsoft Azure Machine Learning / Cognitive Services (Detector de anomalías).

Herramientas y metodologías de reconocimiento de emociones

En la actualidad existe una variedad de kits de herramientas y metodologías para extraer información afectiva de diversas modalidades como imágenes, voz y señales fisiológicas. Estas herramientas son fundamentales para construir sistemas emocionalmente receptivos, existiendo distintas bibliotecas de las que nos podemos aprovechar.

A la ya citada biblioteca de FaceTorch, podemos agregar que existen las siguientes: Emotic, Deep-Emotion y OpenFace.[64]

Probablemente la solución al monitoreo de biometría conductual sea una combinación de APIs con la plataforma de actuación a distancia, a los efectos de recolectar y procesar los datos con un motor de inteligencia artificial[65] que realice el análisis de anomalías.

D. Viabilidad y Justificación Técnica

La viabilidad de esta solución es alta ya que la biometría conductual es una tecnología madura en dominios 2D, tanto en web como en móvil.

La autenticación inicial (incluso con QES) solamente asegura el ingreso a la plataforma pero las sesiones en la sala de videoconferencias pueden ser largas, y el riesgo de

https://scholar.google.com.ar/scholar?q=Mahalanobis+distance,+KullbackLeibler+divergence&hl=es&as_sdt=0&as_vis=1&oi=scholart

[63] Los últimos tres citados por Vivek Chavan, Arsen Cenaj, Shuyuan Shen, Ariane Bar et all, (2025) *Feeling Machines: Ethics, Culture, and the Rise of Emotional AI. https://arxiv.org/pdf/2506.12437*

[64] Los últimos tres citados por Vivek Chavan, Arsen Cenaj, Shuyuan Shen, Ariane Bar et all, (2025) *Feeling Machines: Ethics, Culture, and the Rise of Emotional AI. https://arxiv.org/pdf/2506.12437*

[65] Este motor de IA puede ser de un tercero especializado, o del proveedor de la plataforma o incluso construido a medida en una nube de IA.

compromiso durante la sesión[66] es real. El monitoreo de biometría conductual ofrece una capa de seguridad continua y pasiva.

El monitor de biometría conductual no reemplaza la criptografía ni la actuación profesional sino que es una herramienta complementaria que colabora con la actuación del notario, añadiendo una señal de alerta contextual basada en el comportamiento real del usuario, difícil de replicar exactamente por un impostor. Al ser pasivo, no interrumpe la experiencia del usuario a menos que se detecte una anomalía grave.

Sin embargo, la implementación de este tipo de agente no está exenta de algunos desafíos que debemos de atender y no perder de vista para una implementación exitosa. De esta manera debemos prestar atención a la estabilidad del perfil, a la adaptabilidad, la privacidad y aceptación y a la resistencia a los ataques

Análisis profundo del agente IA 7: ILNS (Componente de análisis lingüístico)

En el análisis del agente de IA 7 (INLS) nos centraremos en cómo la inteligencia artificial, a través del procesamiento del lenguaje natural (PLN), puede identificar en el diálogo, ya sea hablado o escrito, indicadores lingüísticos asociados a posible estrés, coacción o falta de entendimiento.

Este análisis es fundamental, ya que toca el núcleo de la función notarial: asegurar que el consentimiento sea libre, informado y que las partes comprendan la naturaleza y consecuencias del acto jurídico que celebran. La IA aquí no busca reemplazar el juicio del notario, sino ofrecerle una herramienta de apoyo basada en evidencia lingüística objetiva.

A. Función Técnica Detallada (Análisis Lingüístico y sentimiento)

El ILNS, procesa el contenido textual del diálogo[67] para identificar patrones y marcadores específicos que la psicolingüística, la pragmática y la lingüística forense han asociado con ciertos estados mentales o situaciones comunicativas relevantes para la validez del consentimiento.[68]

El objetivo de esta función es detectar y señalar al notario patrones lingüísticos que podrían sugerir:

[66] Las distintas maneras de comprometer una sesión puede ser mediante un keylogger en la PC o por ingeniería social

[67] Obtenido mediante la técnica de *Speech-to-text*

[68] Cabe aclarar que la psicolingüística, la pragmática y la lingüística forense no ha podido demostrar en forma concluyente que se puedan identificar fehacientemente diálogos con ciertos estados mentales, sin embargo, una apreciación de estos indicadores pueden ayudar y colaborar para requerir del notario una reconfirmación del consentimiento

- Estrés o ansiedad elevados que podrían interferir con la comprensión o la libre expresión de la voluntad. Los indicadores que pueden dar la alerta serían la falta de fluidez en el habla, como por ejemplo "ehh", "mmm", o pausas injustificadas, auto-correcciones frecuentes, fragmentación de frases, repeticiones de palabras o ideas, uso de lenguaje evasivo o minimizador, cambios abruptos en la velocidad del habla[69], frases inusualmente cortas o simplificadas.

  Sin embargo, cabe mencionar que la principal dificultad en este tipo de detecciones reside en interpretar correctamente estos marcadores. El mismo patrón lingüístico puede tener significados diferentes según el contexto, el hablante y la cultura. Los modelos de IA aún luchan con este nivel profundo de comprensión pragmática y psicológica. Es muy difícil crear un modelo que distinga fiablemente entre estrés normal por la formalidad del acto y estrés por coacción, o entre reflexión y confusión. De ahí que solo sean indicadores que puedan alertar al oficial público, pero que no han de ser invalidantes para la continuación del acto.
- Posible coacción o presión externa, cuando la voluntad expresada podría no ser genuina. Los indicadores que pueden dar la alerta sería un lenguaje excesivamente dubitativo o cualificado, como por ejemplo "quizás", "supongo", "tal vez", "no estoy seguro pero...", respuestas renuentes o indirectas a preguntas directas, deferencia excesiva hacia la otra parte presente, afirmaciones contradictorias a lo largo de la conversación, cambios súbitos de opinión sin justificación clara, uso de frases que sugieren influencia externa, falta de espontaneidad, respuestas telegráficas o monosilábicas inusuales.
- Falta de entendimiento o confusión sobre los términos, naturaleza o consecuencias del acto. Los indicadores que pueden dar la alerta es la formulación frecuente de las mismas preguntas o solicitud de repetición de información ya dada, uso incorrecto o inconsistente de terminología técnica o legal clave, preguntas que revelan una incomprensión fundamental del acto, vaguedad excesiva en las respuestas, acuerdo demasiado rápido o pasivo sin demostración de comprensión, descripciones del acto que no coinciden con su naturaleza jurídica.

El dato de entrada sería un texto transcripto de la conversación. Es necesario que este texto tenga la identificación del hablante con diarización[70].

El dato de salida del agente no sería una "detección" definitiva de estrés, coacción o confusión, sino una identificación y resaltado de los marcadores lingüísticos específicos

[69] Para esto se requiere análisis del *Speech-to-text* con *timestamps*.
[70] La diarización es separar y etiquetar quien dice lo que dice.

encontrados. Potencialmente, un índice o "score" de alerta basado en la frecuencia y co-ocurrencia de estos marcadores y la fundamentación sobre la cual se ha generado la alerta cumpliendo con el principio de explicabilidad le daría al notario la explicación de por qué se generó la alerta y que marcadores específicos se detectaron, permitiendo al notario evaluar su relevancia en el contexto.

B. **Tecnologías subyacentes (PLN)**

Se requiere una cadena de procesamiento PLN sofisticada:

1. Convertir palabras habladas a texto (Speech-to-Text (STT)) de alta precisión: La calidad de la transcripción es la base fundamental. Debe manejar acentos, ruido ambiental y, crucialmente, realizar diarización.
2. Preprocesamiento de texto mediante la tokenización, normalización textual (minúsculas, puntuación), lematización/stemming.
3. Análisis de la falta de fluidez en el habla mediante los algoritmos específicos para detectar y cuantificar muletillas del habla, pausas, repeticiones, auto-correcciones en la transcripción.
4. Análisis sintáctico y de complejidad:
   - POS (Part-of-Speech Tagging) que refiere al proceso de asignar etiquetas gramaticales a cada palabra en una oración, indicando su función gramatical (como sustantivo, verbo, adjetivo, etc.).

     El análisis sintáctico (Parsing) es un paso más allá, que implica construir una estructura jerárquica de una oración para mostrar cómo las palabras se relacionan entre sí. Estas técnicas de análisis de dependencias sirven para entender la estructura gramatical.

   - Métricas de legibilidad y complejidad de Flesch y Gunning Fog, que sirven para evaluar la complejidad del lenguaje usado por el participante, ya sea que fuese inusualmente simple o inusualmente complejo. Mientras que índice Flesh mide la facilidad de lectura, el índice Gunning Fog estima el nivel educativo necesario para comprender el texto.

   - Longitud media de las frases en el momento que tiene que hablar.

5. Análisis Semántico y Pragmático:
   - Reconocimiento de entidades nombradas (REN), que permite identificar menciones a términos legales, personas, cantidades. Así como verificar su uso correcto.

- Análisis de sentimiento, que permitiría detectar polaridad (positiva/negativa/neutra) y quizás intensidad. Útil para detectar lenguaje excesivamente negativo o incongruente.
- Los modelos Wav2Vec2 y Whisper (como por ejemplo, SpeechBrain/emotion-recognition-wav2vec2-IEMOCAP) extraen emociones directamente de las señales de voz y son vitales en determinadas aplicaciones como los asistentes de voz.
- El modelo de datos de urdu de Audeering y Talha amplía la cobertura lingüística y demográfica.[71]
- Extracción de palabras claves permite identificar los temas centrales de la conversación y la contribución de cada parte.
- Detección de incertidumbre permite identificar palabras o construcciones que expresan duda, certeza, obligación, posibilidad (ej. "creo", "debo", "podría").
- El análisis de actos de habla permite clasificar cada turno de habla (pregunta, afirmación, acuerdo, desacuerdo, petición de aclaración). Permite además detectar patrones (ej. ausencia total de preguntas por parte de un participante).

6. Modelos de Clasificación Específicos (Machine Learning):
   - Entrenamiento Supervisado: Idealmente, se entrenarían modelos (ej. Transformers como DistilRoBERTa, BERT y RoBERTa o sus derivados, SVMs, Random Forests) sobre datasets de diálogos (simulados o reales anonimizados y con consentimiento) anotados por expertos (lingüistas, psicólogos, juristas) para identificar segmentos que indiquen confusión, estrés o posible coerción. Estos modelos aprenderían a ponderar la combinación de múltiples indicadores lingüísticos.
   - Los modelos Feel-it y Beto brindan soporte para italiano y español.[72]
   - Aprendizaje no supervisado/detección de anomalías: Podrían usarse para detectar patrones lingüísticos que se desvían significativamente de una "norma" conversacional o del propio estilo habitual del usuario (si hubiera interacciones previas).

C. **Potenciales Proveedores y Tecnologías Específicas**

[71] Vivek Chavan, Arsen Cenaj, Shuyuan Shen, Ariane Bar et all, (2025) *Feeling Machines: Ethics, Culture, and the Rise of Emotional AI. https://arxiv.org/pdf/2506.12437*
[72] Vivek Chavan, Arsen Cenaj, Shuyuan Shen, Ariane Bar et all, (2025) *Feeling Machines: Ethics, Culture, and the Rise of Emotional AI. https://arxiv.org/pdf/2506.12437*

El mercado ofrece herramientas para las distintas capas de PLN, pero una solución integral para este caso de uso específico probablemente requiera de una integración y personalización.

- Proveedores de Speech-to-Text (con diarización): Google Cloud Speech-to-Text, AWS Transcribe, Microsoft Azure Speech Services, Deepgram, AssemblyAI,
- Proveedores de plataformas PLN generales (Cloud): Google Cloud Natural Language API / Vertex AI, AWS Comprehend / SageMaker, Microsoft Azure Cognitive Service for Language / Azure ML
- Modelos de lenguaje y plataformas abiertas: OpenAI API (GPT-5, etc.) Cohere, Hugging Face,
- Empresas de IA Conversacional / Análisis de Interacciones: Gong, Chorus.ai - ahora parte de ZoomInfo.
- Empresas de Legal Tech con PLN: Litera, Luminance, Relativity.

Conclusión parcial:

No existe como producto un intérprete de lenguaje natural y sentimiento (ILNS) específico para una actuación notarial lista para usar.

La solución requerirá integrar una tecnología de conversión de palabras a texto (Speech-to-text (STT)) de alta calidad con servicios PLN, probablemente de un proveedor cloud generalista o usando modelos de Hugging Face, que deberán ser configurados, y configurado especialmente, además de entrenarlo a medida, para detectar los marcadores lingüísticos específicos relevantes para el contexto notarial, con umbrales de alerta cuidadosamente calibrados.

D. **Viabilidad, Justificación Técnica y Fundamentación Doctrinal/Web**

- Viabilidad Técnica:
  - La viabilidad de la detección de marcadores es alta. Las técnicas PLN actuales son muy capaces de identificar y cuantificar los indicadores lingüísticos mencionados (disfluencias, complejidad, sentimiento, palabras clave, etc.).
  - La viabilidad de la interpretación contextual se ubica entre moderada a baja.
    En este sentido, tal como lo hemos dicho, la principal dificultad reside en interpretar correctamente estos marcadores ya que es muy difícil crear un modelo que distinga fiablemente entre estrés normal por la formalidad del acto y estrés por coacción, o entre reflexión y confusión, siendo imperioso y necesario la calibración y validación del modelo para minimizar falsos positivos y negativos.
- Justificación Técnica:

- Apoyo al notario: Ofrece una "segunda opinión" objetiva basada en datos lingüísticos, ayudando al notario a enfocar su atención en momentos o aspectos de la interacción que podrían requerir mayor indagación.
- Consistencia: Puede ayudar a aplicar criterios de evaluación más consistentes entre distintos notarios o sesiones.
- Registro de Evidencia: Las alertas generadas (con su justificación) pueden formar parte del registro auditable de la sesión, documentando las preocupaciones observadas (aunque no sean concluyentes).

El Reglamento de inteligencia artificial (RIA) de la Unión Europea y el Principio de "Human in Command" (HIC)

El RIA es la primera legislación integral sobre IA en el mundo. Su objetivo es establecer un marco legal para el desarrollo y uso de la IA en la UE, garantizando al mismo tiempo la protección de los derechos fundamentales y la seguridad de las personas. El RIA se basa en un enfoque basado en el riesgo, clasificando los sistemas de IA en diferentes categorías según su nivel de riesgo. Los sistemas de IA considerados de alto riesgo, como los utilizados en la atención sanitaria, en el transporte, la justicia decisoria e incluso en el entorno que proyectamos para la actuación notarial a distancia, están sujetos a requisitos más estrictos.

El principio de HIC es un elemento central del RIA y un pilar fundamental para garantizar que la IA se utilice de manera ética y responsable. El RIA establece que los sistemas de IA de alto riesgo deben diseñarse y utilizarse de manera que se garantice el control humano. Sin embargo, la implementación del principio de HIC enfrenta varios desafíos, incluyendo la definición de "control humano" y la necesidad de medidas técnicas y organizativas para garantizar su aplicación efectiva. ¿Qué nivel de control es necesario para garantizar que los humanos sigan siendo los últimos responsables de las acciones de la IA? ¿Cómo se puede garantizar que los humanos comprendan y supervisen las decisiones de la IA? ¿Qué medidas técnicas y organizativas son necesarias para garantizar que los humanos tengan el control sobre los sistemas de IA? ¿Cómo se puede capacitar a los humanos para que comprendan y utilicen los sistemas de IA de manera efectiva?

El HIC es medular y fundamental en una actuación como la que se plantea y es por ello, que las respuestas a todas estas preguntas que aquí mencionamos han sido

respondidas durante el desarrollo del workflows agéntico, con la interacción del agente de IA 4, que es el consolidador de verificación y decisión y luego con el agente de AI 10 que es el orquestador de sesión y riesgo pre-firma.

A pesar de estos desafíos, el principio de HIC es fundamental para garantizar que los humanos sigan siendo los últimos responsables de las acciones de la IA.

Conclusiones y Recomendaciones

El uso de PNL para analizar indicadores lingüísticos de estrés, coacción o confusión (ILNS lingüístico) es técnicamente factible para la detección de marcadores, pero su interpretación fiable como prueba de un estado interno específico es altamente compleja y muy limitada en el estado actual de la IA y la lingüística.

Se recomienda:

1. Implementar como herramienta de apoyo, no decisoria: El ILNS debe funcionar como un sistema que alerta al notario sobre patrones lingüísticos atípicos o preocupantes, proveyendo la evidencia lingüística detectada. La interpretación final y la decisión sobre cómo proceder (hacer más preguntas o detener el acto) debe ser exclusivamente del notario humano.
2. Priorizar transparencia y explicabilidad (XAI): El notario debe entender por qué se generó una alerta (qué marcadores se detectaron). El usuario debe ser informado que se realiza análisis lingüístico con fines de asegurar la validez del acto y obtener la aprobación con el consentimiento informado.
3. Enfoque cauteloso y gradual: Empezar por detectar marcadores más objetivos y menos interpretativos (ej. frecuencia de preguntas de aclaración, uso incorrecto de términos clave, alta tasa de disfluencias) antes de intentar inferir estados complejos como "coacción" basados en combinaciones sutiles.
4. Rigurosa calibración y validación: Probar exhaustivamente el sistema con notarios y datos relevantes, mediante una IA específica, calibrada con el idioma, los modismos locales, culturales, las normas sociales y la expresión emocional ya que esta puede variar dependiendo de las regiones y países, ya sea en tonos, gestos, metáforas y contexto. Una IA no supervisada o mal calibrada corre el riesgo de entregar resultados erróneos. Se la debe validar exhaustivamente para ajustar umbrales y minimizar falsas alarmas o fallos de detección.

5. Emplear técnicas de aprendizaje por refuerzo a partir de retroalimentación humana y adaptación de bajo rango (LoRA) utilizando incluso dialectos regionales y conjunto de datos locales.
6. Gestión prioritaria de la privacidad: Dada la sensibilidad del diálogo notarial, aplicar las máximas garantías de seguridad, cifrado y cumplimiento normativo para la transmisión y procesamiento de transcripciones.
7. Formación notarial: Los notarios necesitarán formación para interpretar correctamente las alertas del sistema y no caer en una confianza excesiva o un rechazo injustificado. La educación del usuario es esencial.

En resumen, el ILNS lingüístico puede ser un complemento valioso si se diseña e implementa con extrema cautela, priorizando su rol de asistencia informada al juicio profesional insustituible del notario y respetando rigurosamente la privacidad y los derechos de los participantes.

Conclusión a la implementación de workflows agénticos

La integración de un workflow agéntico basado en IA sobre la sólida arquitectura criptográfica propuesta representa la vanguardia en la búsqueda de una vinculación indiscutible y segura entre las personas físicas y su expresión de voluntad para actos de alta consecuencia legal. Transforma la seguridad de un estado estático (validación criptográfica puntual) a uno dinámico y contextual, capaz de detectar amenazas más sutiles y adaptativas.

Sin embargo, su implementación exige un rigor técnico, ético y legal aún mayor, poniendo especial énfasis en la transparencia, la privacidad, la explicabilidad, la equidad y la supervisión humana cualificada. Es un camino complejo, pero potencialmente puede ofrecer la confianza necesaria para que los actos notariales protocolares prosperen en una actuación a distancia.

Capítulo VI: Normativa a tener en cuenta para la propuesta práctica

Introducción

Luego del desarrollo predominantemente técnico y funcional de la propuesta, es necesario analizar la normativa que debe tenerse en cuenta para la implementación así como el cumplimiento de los principios jurídicos más importantes desde una visión normativa tanto europea como argentina, centrándonos en el aspecto más novedoso como el workflow agéntico, analizaremos y evaluaremos los principios de explicabilidad, gestión del consentimiento, la necesidad del control humano en las decisiones finales, el marco regulatorio de

la inteligencia artificial, la manera de mitigar los riesgos en un ambiente digital y, por último, la necesaria robustez que se requiere tecnológicamente para resistir posibles ataques.

Consideraciones adicionales para la implementación agéntica

El desarrollo técnico explicativo del workflows no puede carecer de un análisis jurídico de ciertas condiciones que mínimamente deben de mencionarse, sin perjuicio del desarrollo efectuado en el resto de los capítulos.

Es por ello que, cualquier desarrollo de implementación, ya sea de agentes artificiales únicos o de workflows agénticos, deben de considerar ineludiblemente el cumplimiento de los siguientes principios:

1. Explicabilidad de las decisiones de los agentes de IA

Las decisiones de los agentes de IA, y en particular del orquestador de sesión y riesgo prefirma (OSRP), deben ser interpretables y auditables ("cajas blancas"). Esta exigencia es un pilar fundamental para la aceptación jurídica y la protección de los derechos de los individuos. Un sistema de "caja negra", cuyas decisiones no puedan ser comprendidas o justificadas, resulta incompatible con los marcos normativos de la UE y las tendencias regulatorias en Argentina, teniendo en cuenta la composición de un régimen causalista donde se exige una fundamentación en cada una de las decisiones que se adopten.

En este escenario debemos atender dentro del marco normativo de la Unión Europea al Reglamento general de protección de datos que establece un marco robusto para la protección de datos personales que incluye derechos específicos relacionados con las decisiones automatizadas. Debe prestarse especial atención a los artículos 13(2)(f), 14(2)(g), 15(1)(h) y 22 apartados 1 y 4. La "información significativa" es la piedra angular del derecho a la explicación en el contexto de la IA.

El artículo 22 del RGPD otorga al interesado el derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles. El OSRP, al generar una evaluación de riesgo que puede ser determinante para la formalización de un acto notarial, podría encuadrarse en el artículo 22 si sus decisiones son puramente automatizadas y tienen un impacto significativo. La jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE) ha venido a reforzar esta línea interpretativa en la sentencia del caso Schufa Holding (C-634/21), como también en el asunto Dun & Bradstreet Austria (C-203/22), vinculado a la transparencia algorítmica.

En el ámbito de la ley de inteligencia artificial de la UE, es altamente probable que varios agentes del workflow, en particular el OSRP, ABPV (Analista Biométrico y de Prueba de Vida), MBC (Monitor de Biometría Conductual) y DATC (Detector de Anomalías Transaccionales y Comportamentales), sean clasificados como "sistemas de IA de alto riesgo" según el Anexo III de la Ley.

Para el OSRP, esto significa que su arquitectura debe permitir la trazabilidad de las decisiones y la comprensión de los factores que condujeron a una determinada evaluación de riesgo, debiendo esta información estar disponible para auditorías y para la supervisión del notario, siendo la calidad de los datos un prerrequisito para la explicabilidad: si los datos de entrada son opacos, sesgados o de mala calidad, la lógica del sistema será inherentemente difícil de explicar y justificar, y las decisiones resultantes carecerán de fiabilidad.

Dentro de la legislación argentina, la ley de protección de datos personales (Ley 25.326) no contiene una referencia explícita al "derecho a la explicación" de decisiones algorítmicas comparable a la del RGPD, aunque consagra el derecho del titular de los datos a solicitar y obtener información sobre sus datos personales incluidos en bancos de datos, las finalidades del tratamiento y la identidad de los responsables.

Implicaciones para el workflow y el agente orquestador sesión y riesgo pre firma (OSRP)
Para el workflow agéntico propuesto, y específicamente para el OSRP, los requisitos de explicabilidad y auditabilidad implican un diseño de caja blanca, así como la documentación técnica completa y actualizada sobre la arquitectura del OSRP, las interfaces de explicación, un registro de auditoría (logging), a lo que debe sumarse la capacitación del notario para comprender las capacidades y limitaciones del OSRP.

La explicabilidad es, además, una condición sine qua non para una auditabilidad efectiva y para la correcta atribución de responsabilidad, especialmente en un contexto donde el notario debe mantener el control final del proceso.

2. Gestión del consentimiento y privacidad con especial énfasis en el monitor de biometría conductual (MBC) y el intérprete de lenguaje natural (ILNS)

La monitorización conductual (MBC) y el análisis de diálogo y sentimiento (ILNS) requieren consentimiento explícito, informado y granular. Se deben aplicar técnicas de minimización y anonimización donde sea posible el cumplimiento estricto de GDPR y leyes locales.

La implementación de agentes como el monitor de biometría conductual (MBC) y el intérprete de lenguaje natural y sentimiento (ILNS) impone obligaciones estrictas en cuanto a la gestión del consentimiento y la protección de la privacidad, dado que procesan datos personales potencialmente sensibles y de manera continua o intrusiva.

En este escenario debemos atender dentro del marco normativo de la Unión Europea al Reglamento general de protección de datos que en su artículo 7 establece las condiciones para la validez del consentimiento, el cual debe ser libre, específico, informado e inequívoco, manifestado mediante una declaración o una clara acción afirmativa.

La definición del artículo 4.14 del RGPD abarca claramente los datos recopilados por el MBC. Por su parte, el ILNS, al analizar el lenguaje y el sentimiento, podría inferir datos sensibles, como el estado de salud (ej. estrés, ansiedad), opiniones políticas o filosóficas, lo que activaría las protecciones del artículo 9.

La principal excepción a esta prohibición, relevante para el MBC y el ILNS, es el consentimiento explícito del interesado para uno o más fines especificados (artículo 9(2)(a) RGPD). Este consentimiento explícito debe ser aún más robusto que el consentimiento general, requiriendo una manifestación de voluntad clara y directa. Adicionalmente, debemos saber que los principios generales del tratamiento de datos del artículo 5 del RGPD son plenamente aplicables.

En el ámbito de las directrices del comité europeo de protección de datos (CEPD), se detallan los elementos de un consentimiento válido, enfatizando la necesidad de que sea específico y granular. Esto significa que el consentimiento para la monitorización continua por el MBC debe ser distinto del consentimiento para el análisis de diálogo por el ILNS, y si el ILNS tuviera múltiples sub-finalidades (ej. detección de fraude y mejora del servicio), cada una podría requerir un consentimiento granular.

Las directrices sobre el tratamiento de datos biométricos (como la directriz 05/2022) se aplican al MBC, exigiendo un alto estándar de protección y una justificación legal robusta, siendo el consentimiento explícito la más probable.

Aunque no existan directrices específicas del CEPD exclusivamente para el "análisis de sentimiento" como el realizado por el ILNS, los principios generales del RGPD y las directrices son aplicables.

Dentro de la legislación argentina de conformidad con el artículo 5 de la ley 25.326 el requisito de consentimiento con altos estándares (libre, expreso, informado y documentado) es directamente aplicable a la recolección y procesamiento de datos por parte del MBC y el ILNS.

Es crucial destacar que, a diferencia del RGPD, el consentimiento del titular, por sí solo, no siempre es suficiente para levantar la prohibición del tratamiento de datos sensibles en Argentina; debe concurrir alguna de las circunstancias excepcionales previstas en el artículo 7 de la ley como razones de interés general autorizadas por ley, o cuando los datos se traten con fines estadísticos o científicos y los titulares no puedan ser identificados.

Los datos biométricos, como los que procesaría el MBC, son considerados datos personales. Si la biometría conductual analizada por el MBC o las inferencias del ILNS (ej. un estado de ánimo alterado que pudiera sugerir un problema de salud) caen dentro de esta categoría de datos sensibles, su tratamiento se enfrentaría a las restricciones del artículo 7. Esto representa una diferencia significativa con el RGPD, donde el consentimiento explícito es una base más general para el tratamiento de datos sensibles.

Requisitos de consentimiento explícito, informado y granular para el monitor de biometría conductual (MBC) y el intérprete de lenguaje natural y sentimiento (ILNS)

Para que el tratamiento de datos por parte del MBC y el ILNS sea lícito en ambas jurisdicciones, el consentimiento obtenido debe ser explícito, informado, debe obtenerse de forma separada para cada finalidad de tratamiento que sea distinta y no esté intrínsecamente ligada a la principal.

Técnicas de minimización y anonimización: Obligaciones y mejoras prácticas

La aplicación de los principios de minimización de datos y el uso de técnicas de anonimización o seudonimización son cruciales para cumplir con la normativa y mitigar los riesgos de privacidad.

En este sentido, para la minimización de datos debemos atender, en la UE al artículo 5(1)(c) del RGPD, mientras que en Argentina al artículo 4 de la Ley 25.326.

Aplicación a MBC e ILNS: Para el MBC, en lugar de registrar y transmitir continuamente todos los datos brutos de comportamiento, se podrían diseñar sistemas que procesen estos datos localmente en el dispositivo del usuario (on-device processing) y solo transmitan una señal agregada o un score de confianza, o únicamente alerten en caso de anomalía significativa. Para el ILNS, en lugar de grabar y almacenar indefinidamente todas las

conversaciones, se podría optar por un análisis en tiempo real que extraiga únicamente los indicadores de sentimiento o las palabras clave relevantes para la finalidad (ej. detección de coacción o inconsistencias), descartando el resto del contenido de la conversación una vez analizado, o aplicando técnicas de resumen que eliminen datos personales no esenciales.

Para la anonimización y seudoanonimización debemos atender, en la UE, al artículo 4.5), y los considerandos 26 y 28 del RGPD, mientras que en Argentina, debemos estar a lo establecido en el artículo 7 de la Ley 25.326

Aplicación a MBC e ILNS: Los datos de biometría conductual o los resultados del análisis de sentimiento podrían ser agregados y anonimizados para análisis de patrones generales sin vincularlos a individuos específicos. La seudoanonimización puede ser una medida de seguridad útil durante las fases activas del procesamiento para reducir los riesgos de una exposición directa de la identidad.

Privacidad desde el diseño y por defecto

Tanto el RGPD (artículo 25) como el proyecto de reforma de la Ley 25.326 en Argentina (artículo 38) consagran los principios de protección de datos desde el diseño y por defecto. La granularidad del consentimiento es un aspecto crítico. Dada la diversidad de datos procesados (patrones de tecleo, voz, emociones inferidas) y las distintas finalidades (autenticación, detección de fraude, análisis de coherencia), obtener un consentimiento único y "empaquetado" para todo el workflow o incluso para todas las funciones del MBC y el ILNS sería, con alta probabilidad, considerado inválido en ambas jurisdicciones por no ser suficientemente específico ni permitir una elección libre e informada sobre cada tratamiento particular.

La minimización de datos emerge no solo como una obligación legal, sino como una estrategia fundamental de mitigación de riesgos y aunque la anonimización es una técnica promovida para reducir los riesgos, su efectividad real es un desafío técnico y legal.

3. Principio human in command (Notario)

Tal como lo hemos explicado en el capítulo anterior, los agentes IA son herramientas de apoyo. La decisión final y la responsabilidad legal sobre la validez del acto y la

identidad/capacidad de las partes debe recaer en el notario humano, quien interpreta las alertas de la IA en el contexto global.

El principio de "human in command" o supervisión humana es esencial en el contexto de la utilización de sistemas de IA en funciones críticas como la notarial. Asegura que, a pesar del apoyo tecnológico, la decisión final y la responsabilidad inherente a la fe pública recaigan en un profesional humano cualificado.

En este escenario, dentro de la UE, debemos atender al artículo 14 de la ley de IA de la UE establece requisitos explícitos de supervisión humana para los sistemas de IA clasificados como de alto riesgo. Estos sistemas deben ser diseñados y desarrollados de tal manera que las personas físicas a las que se asigna la supervisión humana puedan ejercerla eficazmente. Estas personas deben poseer la competencia, la formación y la autoridad necesarias para dicha supervisión. Crucialmente, deben ser capaces de comprender plenamente las capacidades y limitaciones del sistema de IA de alto riesgo y ser capaces de supervisar adecuadamente su funcionamiento, con el fin de detectar y abordar anomalías, disfunciones y resultados inesperados. Además, deben poder decidir no utilizar el sistema de IA de alto riesgo en una situación particular, continuar su funcionamiento con modificaciones o interrumpirlo por completo. También deben poder anular una decisión tomada por el sistema o modificar sus resultados. Dado que varios agentes del workflow (especialmente OSRP, ABPV, CVD, DATC) probablemente se clasificarán como de alto riesgo, este artículo es directamente aplicable. El notario, en este contexto, sería la persona designada para ejercer esta supervisión, y su capacidad y autoridad para intervenir y anular o modificar las decisiones o recomendaciones de los agentes de IA son fundamentales.

El artículo 22(3) del RGPD, establece que las decisiones individuales automatizadas (incluida la elaboración de perfiles) que producen efectos jurídicos o afectan significativamente al interesado, incluso cuando dichas decisiones están permitidas (por ser necesarias para un contrato o basarse en el consentimiento explícito), el responsable del tratamiento debe implementar salvaguardas adecuadas. Estas salvaguardas deben incluir, como mínimo, "el derecho a obtener intervención humana por parte del responsable, a expresar su propio punto de vista y a impugnar la decisión". En el workflow propuesto, el notario actuaría como el humano que interviene, revisa la evaluación proporcionada por los agentes de IA y toma la decisión final, garantizando así este derecho del interesado.

En Argentina no hay normativa expresa sin embargo la fe pública no puede ser delegada a un sistema tecnológico, por más avanzado que este sea. La tecnología, incluida

la IA, debe ser considerada una herramienta al servicio del notario, pero nunca un sustituto de su juicio, discernimiento y responsabilidad.

Los agentes de IA como herramientas de apoyo: Alcance y limitaciones

Los doce agentes que componen el workflow están diseñados para automatizar diversas tareas, tales como la verificación de información (VDA), el análisis de riesgo (ARP, OSRP), la detección de patrones (DATC, AFP), la asistencia en la comprensión del lenguaje (ILNS) o la asistencia legal (ALC) y en la resolución de disputas (ARD). El valor agregado de estos agentes reside en su capacidad para procesar grandes volúmenes de información de manera rápida, identificar anomalías o patrones que podrían pasar desapercibidos para un humano, y ofrecer insights que pueden mejorar la eficiencia y, potencialmente, la seguridad y calidad de la función notarial.

Sin embargo, estos sistemas de IA presentan limitaciones inherentes. Carecen de la capacidad de juicio jurídico y ético complejo que es privativo del ser humano y esencial en la función notarial. No pueden realizar una ponderación de valores, interpretar normas en contextos ambiguos, ni comprender las sutilezas de las relaciones humanas y las intenciones de las partes de la misma manera que un profesional del derecho experimentado. Sus resultados y recomendaciones están intrínsecamente ligados a la calidad y representatividad de los datos con los que fueron entrenados y a la corrección de sus algoritmos, lo que los hace susceptibles a errores y sesgos.

Interpretación de alertas de IA y decisión final

El notario debe ser capaz de comprender y valorar críticamente la información y las "alertas" generadas por los agentes de IA, y no aceptarlas de manera acrítica o automática. Su experiencia profesional, su conocimiento del derecho y su prudencia son esenciales para contextualizar esta información y tomar la decisión final sobre la autorización o no del acto. La decisión sobre la validez del acto, la efectiva identificación de las partes, la apreciación de su capacidad para el acto y la constatación de su voluntad libre y consciente recae, en última instancia y de manera exclusiva, en el notario humano.

La implementación del workflow agéntico no redefine la esencia de la función notarial, sino que la dota de nuevas herramientas. El notario, en este escenario, se convierte

en un "orquestador humano" que no solo supervisa pasivamente, sino que dirige, interpreta y valida activamente las contribuciones de los doce agentes. Esta función expandida exige no solo la capacidad técnica para comprender los outputs de la IA, sino también la autoridad legal y fáctica para anular o modificar sus recomendaciones, incluso las provenientes de sistemas sofisticados como el OSRP. Esta autoridad es un corolario de su responsabilidad final.

Para que este modelo funcione, es crucial que tanto los términos contractuales con los proveedores de IA como las eventuales regulaciones específicas definan claramente a estos sistemas como "herramientas de apoyo", evitando cualquier ambigüedad que pueda llevar a una dilución de la responsabilidad notarial.

Finalmente, la efectividad del principio "human in command" depende intrínsecamente de la capacitación continua del notario, quien debe adquirir las competencias necesarias para comprender las capacidades, limitaciones y riesgos inherentes a los agentes de IA que utiliza, tal como lo prevé el artículo 14 de la Ley de IA de la UE y lo demandan las buenas prácticas profesionales.

4. Marco regulatorio de IA

Asegurar el cumplimiento con regulaciones específicas sobre IA (como el RIA) en cuanto a clasificación de riesgo, transparencia, robustez y supervisión humana.

La implementación del workflow agéntico debe asegurar el cumplimiento con las regulaciones específicas sobre IA, particularmente en lo referente a la clasificación de riesgo de cada uno de los doce agentes, y las consecuentes obligaciones en materia de transparencia, robustez y supervisión humana.

De esta manera, teniendo en cuenta el enfoque basado en el riesgo, que establece el es altamente probable que varios agentes del workflow sean clasificados como de alto riesgo donde en el artículo 6 y el Anexo III de la Ley de IA se enumeran los casos de uso considerados de alto riesgo. La clasificación precisa de cada agente como "alto riesgo" requerirá una autoevaluación detallada por parte del proveedor del sistema, considerando su finalidad prevista, el contexto de uso dentro del workflow notarial y el impacto potencial en los derechos fundamentales. La interdependencia de los agentes es un factor crucial: un fallo o un output incorrecto de un agente que alimenta a otro puede propagar y amplificar los riesgos, lo que podría llevar a clasificar como de alto riesgo a agentes que aisladamente no lo serían.

5. Mitigación de sesgos

Auditar y entrenar los modelos de IA para evitar sesgos (demográficos, culturales, etc.) que podrían llevar a discriminación en la verificación o evaluación de riesgos.

La auditoría y el entrenamiento de los modelos de IA para evitar sesgos (demográficos, culturales, etc.) que podrían llevar a discriminación en la verificación o evaluación de riesgos son imperativos éticos y legales.

Dentro del escenario de la UE, debemos estar al artículo 10 (Gobernanza y calidad de los datos) del RIA que es central en este aspecto. El artículo 13 obliga a que la documentación técnica de los sistemas de alto riesgo incluya información sobre cómo el sistema fue diseñado y validado para evitar resultados discriminatorios, mientras que el artículo 14 también contribuye a la mitigación de sesgos, ya que la intervención humana puede detectar y corregir decisiones sesgadas que el sistema pueda perpetuar.

El RGPD no aborda los sesgos algorítmicos con la misma especificidad que la Ley de IA, varios de sus principios son fundamentales para prevenirlos, como los establecidos en los artículos 5, 22 y 9. Mientras que la Carta de derechos fundamentales de la UE en el artículo 21 prohíbe toda discriminación, sea cual sea el medio por el que se produzca, incluyendo los sistemas algorítmicos.

Dentro de Argentina podríamos decir que la columna normativa estaría dada por el artículo 16 de la Constitución Nacional que establece el principio de igualdad ante la ley, el artículo 4 y 7 de la ley 25.326 establece el tratamiento de datos personales y datos sensibles. Por último la ley antidiscriminatoria (Ley 23.592) que sanciona los actos u omisiones discriminatorios determinados por diferentes motivos. Si una decisión tomada o influenciada por un agente de IA resulta ser discriminatoria en los términos de esta ley, podría dar lugar a acciones legales y a la nulidad del acto discriminatorio.

Estrategias de auditoría, entrenamiento y supervisión de modelos para prevenir la discriminación

Para cumplir con las exigencias normativas y éticas, es imprescindible implementar un conjunto de estrategias robustas como:

- La auditoria de algoritmos donde se deben realizar auditorías tanto ex ante (antes del despliegue de los agentes) como ex post (periódicamente durante su ciclo de vida).

- La calidad y representatividad de los datos de entrenamiento, donde esfundamental asegurar que los conjuntos de datos utilizados para entrenar a los 12 agentes, y especialmente a aquellos que realizan perfiles o toman decisiones (ARP, ABPV, CVD, ACA, MBC, ILNS, DATC, OSRP, AFP), reflejen adecuadamente la diversidad de la población de usuarios a la que se aplicarán. La falta de representatividad es una fuente principal de sesgo.
- La supervisión y monitoreo continuo de métricas de equidad relevantes para el contexto específico de cada agente (ej. paridad demográfica, igualdad de oportunidades, igualdad predictiva). Estas métricas deben ser evaluadas para diferentes subgrupos demográficos. La transparencia y explicabilidad que permitan la capacidad de explicar cómo un modelo de IA llega a una determinada decisión o predicción.
- La auditoría y las estrategias de mitigación deben considerar el workflow como un sistema integrado.

6. Robustez contra ataques adversarios

Los modelos de IA pueden ser atacados (ej. intentos de engañar a la prueba de vida, manipular la biometría conductual). Se requieren defensas específicas contra estos ataques.

La robustez de los modelos de IA frente a ataques adversariales, es decir, intentos deliberados de engañar o manipular su funcionamiento (por ejemplo, para superar una prueba de vida o alterar la biometría conductual), es un requisito crítico para la seguridad y fiabilidad del workflow agéntico.

En este escenario, dentro de la UE, debemos estar al artículo 15 de la Ley de IA que establece explícitamente que los sistemas de IA de alto riesgo deben diseñarse y desarrollarse de manera que alcancen un nivel adecuado de precisión, robustez y ciberseguridad, y deben funcionar de manera coherente en esas tres dimensiones a lo largo de todo su ciclo de vida.

En el RGPD no se menciona explícitamente los "ataques adversariales" contra sistemas de IA, pero en su artículo 32 (Seguridad del tratamiento) impone a los responsables y encargados del tratamiento la obligación de aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo. La Directiva NIS 2 (Directiva (UE) 2022/2555 establece obligaciones de ciberseguridad para una amplia gama de entidades consideradas esenciales o importantes en sectores críticos.

Por último debe atenderse también a los informes y guías de ENISA (Agencia de la Unión Europea para la ciberseguridad).

En Argentina debemos estar al artículo 9 de la ley de datos personales (25.326) que establece que el responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales. También podríamos encontrar en el Código Civil y Comercial de la Nación en el artículo 1710 que habla del deber de prevención del daño y adicionalmente, en el ámbito contractual, la doctrina y jurisprudencia argentinas reconocen una obligación tácita de seguridad, derivada del principio de buena fe (artículo 961 del CCyC), que impone a los proveedores de bienes y servicios (incluidos los tecnológicos)

Defensas técnicas y organizativas contra ataques

La protección contra ataques adversariales requiere una combinación de defensas técnicas específicas y medidas organizativas robustas, como pueden dentro de las técnicas de defensa específicas, el entrenamiento adversarial, la detección de entradas adversariales, la validación robusta de entradas, las técnicas de regularización y ensembles de modelos, la criptografía y medidas de seguridad perimetral.

Dentro de las medidas organizativas pueden realizarse evaluaciones de riesgo de seguridad específicas para la IA, equipos rojos y pruebas de penetración, monitoreo del comportamiento del modelo, planes de respuestas a incidentes de seguridad de IA.

Para los estándares es recomendable estar a los dispuesto en la NIST AI risk management framework (AI RMF), los informes y guías de ENISA, los estándares ISO/IEC como la ISO/IEC 27000. La protección contra ataques adversariales es un campo técnico en constante evolución, ya que los atacantes desarrollan continuamente nuevas formas de engañar a los sistemas de IA. Esto implica que la robustez no puede ser una característica estática del sistema, sino que requiere un compromiso continuo con la investigación, la actualización de defensas y la adaptación a nuevas amenazas. La exigencia de robustez del artículo 15 de la Ley de IA de la UE establece un estándar legal claro que va más allá de la ciberseguridad tradicional y obliga a considerar estas amenazas específicas de la IA.

Conclusión

La implementación exitosa requerirá no solo una profunda experticia técnica en cada área, sino también de un cuidadoso cumplimiento del marco jurídico aplicable, con especial atención a la seguridad y la usabilidad. Es una arquitectura compleja, aunque ello no significa

que no sea posible realizar esta clase de actuación si no se alcanza el desarrollo técnico y tecnológico planteado, sino que lo que en el presente trabajo se plantea es la vía más robusta y defendible, tanto técnica como jurídicamente, para alcanzar el objetivo propuesto.

La implementación del workflow agéntico de doce (12) agentes de inteligencia artificial en el ámbito notarial, tanto en la Unión Europea como en Argentina, presenta también un panorama jurídico complejo y en plena evolución. El análisis de las seis áreas clave —explicabilidad, gestión del consentimiento y privacidad, principio de "human in command", marco regulatorio de IA, mitigación de sesgos y robustez contra ataques adversarios— revela la necesidad de un enfoque meticuloso y proactivo para garantizar el cumplimiento normativo y la protección de los derechos fundamentales.

1. **Explicabilidad y auditabilidad:** Existe una clara convergencia regulatoria hacia la exigencia de sistemas de IA "caja blanca", especialmente para aquellos que, como el OSRP, toman decisiones con impacto significativo. Tanto el RGPD y la Ley de IA en la UE, como la Ley 25.326 (interpretada evolutivamente) y los proyectos de ley en Argentina, demandan que la lógica subyacente de las decisiones automatizadas sea comprensible y que los sistemas sean auditables. Esto no implica necesariamente la divulgación completa de algoritmos propietarios, sino la capacidad de explicar los factores determinantes de una decisión de manera significativa para el interesado y para el supervisor humano (el notario). La explicabilidad es una condición indispensable para la auditabilidad efectiva y para la correcta atribución de responsabilidad.

2. **Gestión del consentimiento y privacidad:** El tratamiento de datos por agentes como el MBC (Monitor de Biometría Conductual) y el ILNS (Intérprete de Lenguaje Natural y Sentimiento) requiere un consentimiento explícito, informado, específico y granular en ambas jurisdicciones. La naturaleza de los datos procesados (biometría conductual, contenido de diálogos, inferencias de sentimientos) los sitúa frecuentemente en la categoría de datos sensibles (Art. 9 RGPD; Art. 7 Ley 25.326). En Argentina, la regulación de datos sensibles es particularmente estricta, y el consentimiento por sí solo podría no ser suficiente si no concurre una excepción legal específica. La minimización de datos y la privacidad desde el diseño son principios cruciales para estos agentes.

3. **Principio "Human in Command":** A partir del razonamiento efectuado en el capítulo III donde se desarrolla la fragilidad del algoritmo el notario debe retener en todo momento la

decisión final y la responsabilidad legal sobre la validez del acto y la identidad y capacidad de las partes. Los doce agentes de IA deben operar como herramientas de apoyo, proporcionando información y análisis, pero sin sustituir el juicio profesional y la fe pública indelegable del notario. La Ley de IA de la UE (Art. 14) y los proyectos argentinos refuerzan este principio mediante la exigencia de supervisión humana efectiva, con capacidad de intervención y anulación de las decisiones de la IA. Esto implica la necesidad de una adecuada formación del notario y una clara delimitación contractual del rol de los sistemas de IA.

4**. Marco regulatorio de IA:** La Ley de IA de la UE establece un marco basado en riesgos. Es altamente probable que varios agentes del workflow (ABPV, OSRP, DATC, MBC, entre otros) sean clasificados como de "alto riesgo", lo que desencadena un conjunto exhaustivo de obligaciones (gestión de riesgos, calidad de datos, documentación, transparencia, supervisión, robustez, evaluación de conformidad, registro). Aunque Argentina carece de una ley de IA vigente, los proyectos legislativos actuales siguen una línea similar, anticipando un futuro marco regulatorio convergente. La interdependencia de los agentes en el workflow exige una evaluación de riesgo integral del sistema.

5. **Mitigación de sesgos**: Prevenir la discriminación algorítmica es un imperativo legal y ético. La Ley de IA de la UE (Art. 10) y los principios del RGPD, así como la Constitución argentina (Art. 16) y los proyectos de ley de IA, exigen medidas para asegurar la calidad y representatividad de los datos de entrenamiento y para detectar, prevenir y mitigar sesgos. Esto implica auditorías algorítmicas periódicas (ex ante y ex post), monitoreo continuo, y un enfoque socio-técnico que considere el contexto de aplicación y la diversidad de los usuarios.

6. **Robustez contra ataques adversarios:** La Ley de IA de la UE (Art. 15) exige explícitamente que los sistemas de alto riesgo sean robustos contra manipulaciones malintencionadas. La Ley 25.326 argentina (Art. 9) y los principios generales del Código Civil y Comercial también imponen un deber de seguridad. Agentes como el ABPV (prueba de vida) y el MBC (biometría conductual) son particularmente vulnerables y requieren defensas técnicas y organizativas específicas, alineadas con estándares como el NIST AI RMF y las guías de ENISA.

En definitiva, la implementación de este avanzado workflow agéntico es factible, pero requiere un compromiso riguroso con los principios de transparencia, protección de

datos, supervisión humana, equidad y seguridad. Se recomienda un análisis detallado y continuo de cada agente y del sistema en su conjunto, la adopción de medidas de privacidad y seguridad desde el diseño y por defecto, una documentación exhaustiva, y la capacitación constante de los notarios que interactuarán con estos sistemas. La anticipación a la evolución normativa, especialmente en Argentina, y la adhesión a los más altos estándares internacionales serán clave para el éxito y la legitimidad de esta innovación tecnológica en el sensible ámbito de la fe pública.

Walter César Schmidt

BIBLIOGRAFÍA

Aicega, M.C. y Canto, P. (2023), Justificación de la identidad, en *Calificación y configuración notarial,* Ignacio Alterini y Francisco J. Alterini (Directores). Thomson Reuters-La Ley, Buenos Aires. Argentina.

Amoni Reverón, G. A. (2013) *El uso de la videoconferencia en cumplimiento del principio de inmediación procesal* Revista del Instituto de Ciencias Jurídicas de Puebla. México. Número 31, Enero-Junio 2013

Aparicio Vaquero, J. P. (2024). Sentencia del Tribunal de Justicia de la Unión Europea, de 7 de diciembre de 2023, asunto c-634/21, OQ vs. Land Hessen, con intervención de SCHUFA Holding AG.

Barba Alonso, R. (2021) *Diseño e implementación de un sistema de captura de datos de entrenamiento para la realización de eye-tracking sin hardware específico. https://uva-doc.uva.es/handle/10324/50018*

Beck, U. (1986) *La sociedad del riesgo. Hacia una nueva modernidad.* Paidós. Barcelona.

Corvalán, J.G. & Sánchez Caparrós, M., (2025) *Agentes de inteligencia artificial y wokflows agénticos: la nueva frontera de la automatización.* Laboratorio de Inteligencia Artificial de la Facultad de Derecho de la Universidad de Buenos Aires. (IALAB) y Banco de Desarrollo de América Latina y el Caribe (CAF).

Cosola, S. J. & Schmidt, W.C. (2021) *El Derecho y la Tecnología*. La Ley – Thomson Reuters, Buenos Aires. Argentina. Tomos 1 y 2.

De Medeiros Martins, Allan; Dantas de Melo Jorge; Duarte Doria Neto, Adrião *Comparison between Mahalanobis distance and Kullback-Leibler divergence in clustering análisis.*

Decálogo de Actuación notarial a Distancia de la Universidad Notarial Argentina.

Decálogo para las escrituras notariales a distancia de la Unión Internacional del Notariado.

Ekman, P. (2017) *El rostro de las emociones.* RBA.

Galletti, P.O., Longhi, M.I.; Manassero Vilar, L.E.; Molina, D.L., Saenz, C.A.; Di Castelnuovo, F; Scattolini, S.F.O. y Schmidt, W. C. (2021) *La actuación notarial en el ámbito virtual: Su aplicación en la Plataforma de Actuación Notarial Virtual de la Provincia de Buenos Aires, Argentina.*

Gödel, K. (2006) *Sobre proposiciones formalmente indecidibles de los Principia mathematica y sistemas afines.* KRK. Oviedo. España

Kahneman, D. (2022) *Pensar rápido, pensar despacio*. Debate, Buenos Aires. Argentina

Kuhn, T.S. (2004) *Las estructuras de las revoluciones científicas.* 8 reimp. FCE. Buenos Aires.

Lucas-Baque, S.J. y Albert-Márquez, J.J, (2019), *Los principios notariales como aporte a la justicia preventiva y a la seguridad jurídica.* Dialnet. https://dialnet.unirioja.es/descarga/articulo/7164381.pdf

Matsumoto, David & Hwang, H.S. & López, Rafael & Pérez Nieto, Miguel. (2013). *Reading facial expressions of emotions: Basic research on emotions recognition improvement.* Ansiedad y Estrés.

Reglamento de Inteligencia Artificial (RIA) de la UE 2024/1689

Russel, B. & Withehead, A.N. (1950). *Principia Mathematica.* Cambridge At the University Press**.**

Stallings, W. (2005) *Organización y arquitectura de computadores.* Pearson. Prentice Hall. Madrid. España

Tayro, E.A. (2016) *La videoconferencia. Un nuevo enfoque del principio de inmediación procesal.* Revista Oficial Del Poder Judicial. Órgano De Investigación De La Corte Suprema De Justicia De La República Del Perú, 8 (10), p. 547-559. https://doi.org/10.35292/ropj.v8i10.251

Thaler, R.H. & Sunstein, C.R. (2008) *Nudge: Improving Decisions About Health, Wealth and Happiness.* Yale University Press - New Haven & London. USA

Turing, A. (1937), On computable numbers, with an application to the entscheindungsproblem. John Wiley and Sons. *Proceedings of the London Mathematical Society.* 1937.Vol s2-42.p. 230-265. London Mathematical Society

Vaswani, Ashish, Llion Jones, Noam Shazeer, Aidan N. Gomez, Niki Parmar, Jakob Uszkoreit, Łukasz Kaiser e Illia Polosukhin “Attention is all you need”. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://proceedings.neurips.cc/paper_files/paper/2017/file/3f5ee243547dee91fbd053c1c4a845aa-Paper.pdf

Vitantonio, N. J.R. Ponencia general de la comisión de procesal laboral. XXVI Congreso Nacional de Derecho Procesal. https://www.aadproc.org.ar/pdfs/ponencias/Procesal_Laboral_Vitantonio.pdf

Vivek Chavan, Arsen Cenaj, Shuyuan Shen, Ariane Bar et all, (2025) *Feeling Machines: Ethics, Culture, and the Rise of Emotional AI. https://arxiv.org/pdf/2506.12437*

Sitios Web

http://www.universidadnotarial.edu.ar/una/wp-content/uploads/2021/05/N0321_DECALOGO_ACTUACION_A_DISTANCIA2.pdf

https://bok.idpro.org/article/51/galley/181/download/

https://curia.europa.eu/juris/document/document.jsf?text=&docid=290022&pageIndex=0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=2084344

https://dialnet.unirioja.es/descarga/articulo/7164381.pdf

https://dle.rae.es/remoto

https://doi.org/10.1093/idpl/ipaa020

https://doi.org/10.35292/ropj.v8i10.251

https://curia.europa.eu/juris/document/document.jsf;jsessionid=3016FDB30AD913F664DBD0B121A39D9A?text=&docid=280426&pageIndex=0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=5105051

https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/EBSI+Verifiable+Credentials

https://repositorio.mpd.gov.ar/documentos/Ben%C3%ADtez,%20An%C3%ADbal%20Leonel.pdf

https://www.elconfidencial.com/tecnologia/2019-09-17/fotos-signo-victoria-selfies-robo-huella-dactilar_2237023/

https://proceedings.neurips.cc/paper_files/paper/2017/file/3f5ee243547dee91fbd053c1c4a845aa-Paper.pdf

https://revistas.usal.es/cuatro/index.php/ais/article/view/32052.

https://scholar.google.com.ar/scholar?q=Mahalanobis+distance,+KullbackLeibler+divergence&hl=es&as_sdt=0&as_vis=1&oi=scholart

https://uinl.org/es/publication/decalogo-de-la-uinl-para-las-escrituras-notariales-con-comparecencia-en-linea/

https://walt.id/white-paper/self-sovereign-identity-ssi https://www.dock.io/post/self-sovereign-identity

https://www.aadproc.org.ar/pdfs/ponencias/Procesal_Laboral_Vitantonio.pdf

https://www.aepd.es/documento/premio-angela-ruiz-robles-2024-gataca-labs-slu.pdf

https://www.elconfidencial.com/tecnologia/2019-09-17/fotos-signo-victoria-selfies-robo-huella-dactilar_2237023/

https://www.european-digital-identity-regulation.com/

https://www.icd.go.cr/portalicd/images/docs/uif/doc_interes/acerca_uif/IDENTIDADDIGITAL.pdf

https://www.researchgate.net/publication/303166545_Comparison_between_mahalanobis_distance_and_Kullback-Leibler_divergence_in_clustering_analysis

https://www.w3.org/TR/did-1.1/

www.cfna.org.ar

www.uinl.org

Fallos

Corte Suprema de Justicia de la Nación Argentina fallo del 12/12/2006 “Benítez, Aníbal Leonel s/ lesiones graves” Causa Número 1524C. https://repositorio.mpd.gov.ar/documentos/Ben%C3%ADtez,%20An%C3%ADbal%20Leonel.pdf

Corte Suprema de Justicia de la Nación Argentina. Fallo: 344:2591

Corte Suprema de Justicia de la Nación Argentina. Fallos: 305:1262; 322:1090; 330:2192; 344:1810

Corte Suprema de Justicia de la Nación Argentina. Fallos: 326:2095; 329:3666; 330:2093; 344:223

Juzgado de lo mercantil de Barcelona ECLI:ES:JMB:2022:1900ª.

Sentencia Tribunal Supremo español acepta a la Blockchain como prueba es en un caso de criptomonedas en la sentencia 326/2019 del 20 de junio. https://www.poderjudicial.es/search/AN/openCDocument/cac2ec927df2ac2484b8072b28c6b92a42e4a9c597691621,

Sentencia Tribunal Supremo 776/2014 Sala 1 Civil del 28 de abril de 2015. https://vlex.es/vid/570062178