

Aplicaciones de la inteligencia artificial en la resolución de conflictos en la industria aseguradora: del análisis de datos a la prueba del siniestro

Paula Bing Müller Cauduro¹

Vitor Boaventura Xavier²

Guido Carello³

María Ángel Solórzano Galeano⁴

Juan Francisco Zarta Ortiz⁵

David Augusto Tejeiro Carrillo⁶

¹ Abogada colegiada en el Colegio de Abogados de Brasil, sección Rio Grande do Sul con el número 93.218. Socia de la firma Müller & Moreira Advocacia. Especialista en Derecho de Seguros por la Universidad de Salamanca (España); Licenciada en Derecho con honores por la PUC/RS (Pontificia Universidad Católica de Rio Grande do Sul); presidenta del Grupo de Jóvenes de AIDA Brasil 2024/2026 y 2026/2028; Secretaria de la Comisión Especial de Seguros y Planes Complementarios de Pensiones del Colegio de Abogados de Brasil, sección Rio Grande do Sul.

² Abogado del área de Seguros, Reaseguros y Previsión Privada de Veirano Advogados. Licenciado en Derecho por la Universidad de Brasilia (Universidade de Brasília – UnB). Máster en Regulación (MSc in Regulation) por la London School of Economics and Political Science (Reino Unido). Doctorando en Derecho en la NOVA School of Law – Facultad de Derecho de la Universidad Nueva de Lisboa, bajo la dirección de la Profesora Doctora Margarida Lima Rego. Miembro de AIDA Brasil. Secretario del Grupo de Trabajo sobre Supervisión Estatal de Seguros de AIDA Internacional. Académico de la Academia Nacional de Seguros y Previsiones de Brasil (ANSP). Miembro de la Comisión Especial de Derecho de Seguros y Reaseguros de la Orden de los Abogados de Brasil – Sección de São Paulo (OAB/SP) y del Instituto Brasileño de Derecho del Seguro (IBDS).

³ Abogado egresado de la Facultad de Derecho de la Universidad Nacional de Rosario (Argentina). Posgrado en Derecho del Consumidor y Diplomatura en Derecho del Seguro por la Universidad Católica Argentina. Asociado del Estudio Carello Corbella & Asociados, dedicado principalmente a litigios vinculados a seguros, daños y perjuicios, responsabilidad civil y derecho del consumo, representando a distintas compañías aseguradoras. CEO y cofundador de Juri IA, LegalTech orientada al sector asegurador y jurídico. Miembro titular de AIDA Argentina, integrante de la comisión directiva del Instituto de Derecho del Seguro del Colegio de Abogados de Rosario, miembro de la Cámara Insurtech Argentina, socio activo de la Bolsa de Comercio de Rosario. Autor de diversas publicaciones sobre derecho de seguros, inteligencia artificial, y nuevas tecnologías aplicadas al sector asegurador.

⁴ Estudiante de Derecho de la Universidad Javeriana (Colombia). Actualmente se desempeña como Judicante en el área de indemnizaciones de MAPFRE y es Coordinadora del Semillero de Estudios en Derecho de Daños (SEDD) de la Universidad Javeriana.

⁵ Estudiante de Derecho de la Universidad Javeriana (Colombia). Actualmente se desempeña como asociado y Director del programa de Inteligencia Artificial en la firma Zarta Neira Abogados.

⁶ Abogado graduado con Mención Meritoria de la Universidad del Rosario (Colombia) y Especialista en Contratación Estatal de la misma universidad. Especialista en Derecho de Seguros, Especialista en Derecho Financiero y del Mercado de Valores y Magister en Derecho Administrativo de la Universidad Javeriana (Colombia). Magister en Argumentación Jurídica de la Universidad de Alicante (España). Abogado socio de la firma Tejeiro Abogados, especializada en asuntos de derecho administrativo, de seguros y responsabilidad civil. Profesor de pregrado y posgrado de la Universidad Javeriana, Universidad del Rosario, Universidad Nacional, entre otras. Es miembro del Instituto Colombiano de Derecho Procesal y del Colegio de Abogados Rosaristas y se desempeña como Representante Joven de la Asociación Colombiana de Derecho de Seguros y Relator del Colegio de Abogados Administrativistas.

Tabla de contenido

Resumen.....	3
Introducción	4
1. La regulación y el uso de la inteligencia artificial en la resolución de conflictos en América Latina	6
1.1. Mapeo de tendencias e identidades en la aplicación de la IA para la resolución de disputas en América Latina.	6
1.1.1. Brasil: panorama de la regulación y el uso de herramientas de inteligencia artificial en la resolución de disputas.....	6
1.1.2. Argentina: Panorama general de la regulación y el uso de herramientas de inteligencia artificial en la resolución de controversias.....	8
1.1.3. Colombia: Panorama general de la regulación y el uso de herramientas de inteligencia artificial en la resolución de controversias.....	9
1.2. Estado actual del uso de la inteligencia artificial en el marco de la resolución de conflictos en América Latina.....	10
2. La inteligencia artificial en la gestión del siniestro: valor operativo, riesgos agénticos y gobernanza responsable	11
2.1. Planteamiento general: Usos de la inteligencia artificial en la industria aseguradora.....	11
2.2. Fraude, litigiosidad y riesgo judicial.....	12
2.3. Prueba digital y estándar reforzado de trazabilidad.....	14
2.4. Inteligencia artificial agéntica en seguros.....	15
2.5. Gobernanza, datos y responsabilidad	19
2.6. La IA representa una gran oportunidad para el seguro, pero solo genera valor si se incorpora con controles, transparencia y supervisión humana.	20
3. La aplicación de la inteligencia artificial en prueba del siniestro: el caso del dictamen pericial en los seguros cibernéticos.....	21
3.1. El marco comparado de la prueba pericial en Latinoamérica y España	22
3.1.1. Los problemas que introduce la inteligencia artificial.....	23
3.1.2. El estado de la jurisprudencia comparada y los ejes del problema	25
a) La reserva humana de la valoración	25
b) La fiabilidad y el método verificable	26
c) La contradicción y la idoneidad de quien examina la prueba	26
d) La explicabilidad y el acceso al algoritmo	27
e) El deber de verificación frente a las alucinaciones	27
3.1.3. La aplicación al campo de los riesgos cibernéticos.....	28

3.1.3.1.	El contexto: la transformación digital y el riesgo cibernético	28
3.1.3.2.	Las coberturas en los seguros de riesgos cibernéticos	30
3.1.3.3.	Las dificultades probatorias del siniestro cibernético	30
3.1.3.4.	Las soluciones que aporta la inteligencia artificial como prueba técnica.....	31
3.1.3.5.	El procesamiento masivo de evidencia digital.....	31
3.1.3.6.	La correlación automática de eventos para reconstruir el siniestro	32
3.1.3.7.	La detección de anomalías como mecanismo de identificación del siniestro.....	32
3.1.3.8.	La priorización de la evidencia relevante	32
3.1.4.	El reencuentro con el estándar: las cuatro capacidades a la luz de los cinco ejes	33
3.1.5.	Reflexiones en torno a la aplicación de la inteligencia artificial en la demostración del siniestro en seguros cibernéticos – Análisis del dictamen pericial elaborado por inteligencia artificial como herramienta demostrativa frente al asegurador.....	33
4.	Conclusiones	35
	Bibliografía	37
	Providencias y normas citadas.....	38
	Anexo I	40

Resumen

El presente artículo evalúa el alcance de la inteligencia artificial en la resolución de conflictos en la industria aseguradora latinoamericana desde una perspectiva comparativa y multidimensional. Con ese propósito, el análisis se desarrolla en tres planos. En primer lugar, se examina el estado actual de la regulación y el uso de la inteligencia artificial en la administración de justicia en América Latina, con especial referencia a las experiencias de Brasil, Colombia y Argentina, identificando los elementos comunes y las tendencias divergentes en la incorporación de estas herramientas a los sistemas judiciales de la región. En segundo lugar, se analizan los usos concretos de la inteligencia artificial al interior de la industria aseguradora, con énfasis en la detección de fraude, la gestión del riesgo judicial, la prueba digital y los riesgos específicos que introduce la inteligencia artificial agéntica, todo ello dentro de un marco de gobernanza responsable. En tercer lugar, se aborda el uso de la inteligencia artificial en la demostración del siniestro, tomando como ejemplo el dictamen pericial asistido por inteligencia artificial como medio de prueba técnica en los seguros de riesgos cibernéticos. A partir de un análisis comparado del régimen de la prueba pericial en diez ordenamientos iberoamericanos y de la jurisprudencia comparada relevante, el artículo sistematiza un estándar emergente de cinco ejes que disciplina la admisibilidad y valoración de ese tipo de dictamen, y concluye que los principios de trazabilidad, explicabilidad, supervisión humana y responsabilidad que rigen la gobernanza interna de la inteligencia artificial en las aseguradoras son, en esencia, los mismos que el ordenamiento procesal exige para que sus resultados tengan valor probatorio en el proceso judicial.

Palabras clave: inteligencia artificial, resolución de conflictos, industria aseguradora, prueba pericial, seguros cibernéticos, inteligencia artificial agéntica, trazabilidad, gobernanza algorítmica, derecho comparado, siniestro.

Resumo

O presente artigo avalia o alcance da inteligência artificial na resolução de processos judiciais envolvendo seguros a partir de uma perspectiva comparativa e multidimensional, com foco na América Latina. Para esse fim, a análise se desenvolve em três planos. Em primeiro lugar, examina-se o estado atual da regulação e do uso da inteligência artificial na administração da justiça na América Latina, com especial referência às experiências do Brasil, da Colômbia e da Argentina, identificando os elementos comuns e as tendências divergentes na incorporação dessas ferramentas aos sistemas judiciais da região. Em segundo lugar, analisam-se os usos concretos da inteligência artificial no interior da indústria seguradora, com ênfase na detecção de fraudes, na gestão do risco judicial, na prova digital e nos riscos específicos introduzidos pela inteligência artificial agéntica no âmbito de um marco de governança responsável. Em terceiro lugar, aborda-se o uso da inteligência artificial na regulação do sinistro, tomando como exemplo o laudo pericial assistido por inteligência artificial como meio de prova técnica nos seguros de riscos cibernéticos. A partir de uma análise comparada do regime da prova pericial em dez ordenamentos ibero-americanos e da jurisprudência comparada relevante, o artigo sistematiza um padrão emergente de cinco eixos que disciplina a admissibilidade e a valoração desse tipo de laudo, e conclui que os princípios de rastreabilidade, supervisão humana e responsabilidade regem a governança interna da inteligência artificial nas seguradoras são, em essência, os mesmos que o ordenamento processual exige para que seus resultados tenham valor probatório no processo judicial.

Palavras-chave: inteligência artificial, resolução de conflitos judiciais, indústria seguradora, prova pericial, seguros cibernéticos, inteligência artificial agéntica, rastreabilidade, governança algorítmica, direito comparado, sinistro.

Introducción

En su poema «Pasión», la poeta brasileña Adélia Prado plasma la experiencia de enamorarse cada día y sus sentimientos cuando, ocasionalmente, en sus propias palabras, «Dios le arrebató su poesía» (1978 - El corazón acelerado). En esos días, según Adélia, cuando mira una piedra, solo ve una piedra. En una época en que el mundo parece enamorarse cada día de una nueva herramienta de inteligencia artificial, resulta especialmente necesario analizar esta tecnología con una mirada no poética, buscando verla en su totalidad tal como es, no con una mirada apasionada, lo cual no significa perder de vista su potencial.

El objetivo de este artículo es investigar, desde una perspectiva comparativa, la disciplina del uso de la inteligencia artificial (IA) en los sistemas jurídicos de los países latinoamericanos y, específicamente, la aplicación de herramientas de IA por parte del sector asegurador para la resolución de controversias.

A pesar de la amplitud del campo y las diferencias entre las culturas jurídicas y las prácticas sectoriales de los países analizados, la investigación busca elementos de convergencia e identificar

tendencias, tanto en la regulación de su uso como en su aplicación sectorial por parte del mercado asegurador en la resolución de controversias en las diversas realidades de América Latina.

La metodología comienza con la descripción y el análisis de las realidades locales en la regulación del uso de la IA por parte de los respectivos sistemas jurídicos y su aplicación por el sector asegurador en la muestra de países analizados, compuesta principalmente por Brasil, Colombia y Argentina.

Entre los aspectos compartidos destaca el aumento de los litigios en el poder judicial latinoamericano, con causas históricas y estructurales conocidas, que impone fuertes costos a nuestras sociedades y economías, siendo el sector asegurador particularmente afectado por esta circunstancia. En este contexto, el surgimiento y desarrollo de la inteligencia artificial surge como una posibilidad para resolver disputas, ya sea en el nivel más amplio de las sociedades o particularmente en disputas relacionadas con el sector asegurador.

Así las cosas, para cada uno de los países analizados, se presentarán datos brutos sobre los litigios y su impacto en el sector asegurador, así como los marcos legales que regulan el uso de la IA en cada una de las jurisdicciones. A continuación, para cada uno de los países, se presentará un panorama del estado del arte en la aplicación de herramientas de inteligencia artificial para la resolución de disputas en el sector asegurador, asumiendo que este uso puede darse de diferentes maneras, como en la identificación y prevención del fraude, en la regulación de siniestros y en disputas legales. Tras este viaje por Brasil, Colombia y Argentina, que comenzará en el siguiente párrafo, se analizarán los elementos compartidos y las tendencias en la aplicación de la IA en la resolución de conflictos en el sector asegurador latinoamericano.

El recorrido por los sistemas jurídicos de la región constituye, sin embargo, sólo el punto de partida. Una vez establecido ese panorama regulatorio, el artículo se adentra en el funcionamiento concreto de la industria aseguradora frente a la inteligencia artificial. Allí se examina cómo estas herramientas pueden transformar documentos dispersos en información estructurada y consultable, con aplicaciones directas en la detección de fraude, la gestión del riesgo judicial y la valoración de la prueba digital. Se analiza también el surgimiento de la inteligencia artificial agéntica —sistemas capaces no solo de analizar información sino de actuar dentro de procesos— y los riesgos específicos que su autonomía introduce en una actividad tan regulada y sensible como el seguro. Este segundo bloque concluye con un conjunto de principios de gobernanza responsable, orientados a garantizar que la eficiencia operativa que ofrece la tecnología no se obtenga a costa de la transparencia, la trazabilidad y la protección de los derechos de los asegurados.

Esos principios de gobernanza conducen naturalmente al tercer y último bloque del artículo, que aborda el uso de la inteligencia artificial en la acreditación del siniestro como problema central. Para ello, se realiza un análisis comparado del régimen del medio de prueba más relevante es asuntos relativos al seguro, cual es la prueba pericial, debido a su utilidad en asuntos de índole técnico o científico. Así pues, se analiza dicha prueba en diez ordenamientos iberoamericanos y se sistematiza, a partir de la jurisprudencia comparada, un estándar emergente de cinco ejes que disciplina el uso de la IA como herramienta auxiliar del perito. Ese marco general se desarrolla a través del campo de los seguros de riesgos cibernéticos, elegido por su particular aptitud para ilustrar el problema: en ese ramo, la acreditación del siniestro depende por entero de evidencia técnica y digital, lo que convierte a la inteligencia artificial en un instrumento de uso ya corriente

en la práctica forense y, al mismo tiempo, en el banco de pruebas más exigente para los estándares jurídicos que deben gobernar su empleo.

1. La regulación y el uso de la inteligencia artificial en la resolución de conflictos en América Latina

1.1. Mapeo de tendencias e identidades en la aplicación de la IA para la resolución de disputas en América Latina.

1.1.1. Brasil: panorama de la regulación y el uso de herramientas de inteligencia artificial en la resolución de disputas

El mercado asegurador brasileño es el líder indiscutible en volumen de primas directas emitidas en América Latina.⁷

En el sector asegurador brasileño en su conjunto —excluyendo los seguros de salud complementarios— los ingresos totalizaron R\$ 415.100 millones en 2025⁸. Como reflejo directo de este importante mercado de contratos de pólizas de seguros, se ha producido un aumento sustancial de los litigios relacionados con los productos de seguros.

Según datos del Consejo Nacional de Justicia⁹, Brasil presenta un panorama preocupante en materia de litigios. En abril de 2026, el país registró un retraso de más de 76.000.000 de demandas en curso, con 13.394.041 nuevos casos presentados tan solo en los primeros cuatro meses de ese año.

Analizando el Panel de Estadísticas del Poder Judicial centrado en los principales litigantes (datos del 30 de abril de 2026), se observa que el sector de "actividades financieras, seguros y servicios conexos" representa un volumen significativo de demandas, con un total de 7.685.082 procedimientos judiciales activos durante ese período¹⁰.

⁷ SWISS RE INSTITUTE. **Latin America market report 2024**: Growth to decelerate as global risks rise. Zurich: Swiss Re Institute, nov. 2024. Disponible en: <https://www.swissre.com/institute/research/topics-and-risk-dialogues/economy-and-insurance-outlook/latin-america-market-report-2024.html> Acceso en: 10 jun. 2026.

⁸ CONFEDERAÇÃO NACIONAL DAS SEGURADORAS (CNseg). **Conjuntura CNseg**: editorial e análise de mercado. Rio de Janeiro: CNseg, ano 9, n. 130, fev. 2026. Disponible en: https://production-cms-upload.s3.sa-east-1.amazonaws.com/Conjuntura_131_PDF_1_b363b581cd.pdf

⁹ El Consejo Nacional de Justicia (CNJ) fue creado por la Enmienda Constitucional N° 45 de 2004 y establecido el 14 de junio de 2005, de conformidad con el artículo 103-B de la Constitución Federal. Es un órgano del Poder Judicial con sede en Brasilia (DF) y que opera en todo el territorio nacional.

Entre sus responsabilidades, actúa en pro de la eficiencia de los servicios judiciales: llevar a cabo, promover y difundir las mejores prácticas orientadas a modernizar y agilizar los servicios de los órganos judiciales. Con base en el informe estadístico sobre la actividad procesal y otros indicadores relevantes para la actividad jurisdiccional en todo el país, formular y ejecutar políticas, programas y proyectos judiciales dirigidos a la eficiencia de la justicia brasileña. Fuente:

<https://www.cnj.jus.br/sobre-o-cnj/quem-somos/>

¹⁰ <https://justica-em-numeros.cnj.jus.br/painel-estatisticas/>

En este sentido, la mejora de la inteligencia artificial en los procesos judiciales ha brindado al poder judicial el beneficio de gestionar el cúmulo de casos de seguros, agrupar acciones repetitivas y predecir resultados en función de la materia, lo cual se ha utilizado a gran escala en América Latina.

En Brasil, la incorporación de herramientas de inteligencia artificial al sistema de justicia ha dejado de ser una perspectiva futura para convertirse en una realidad institucional consolidada. En los últimos años, los tribunales superiores y el Consejo Nacional de Justicia (CNJ) han desarrollado e implementado soluciones tecnológicas destinadas a gestionar el elevado volumen de casos, buscando aumentar la eficiencia administrativa, estandarizar la jurisprudencia y optimizar el uso de los recursos públicos.

Entre las iniciativas más relevantes, destaca el “Sistema Victor”, desarrollado por el Tribunal Supremo Federal (STF) de Brasil. Diseñado para ayudar a identificar apelaciones relacionadas con cuestiones de repercusión general ya reconocidas por el Tribunal, la herramienta emplea técnicas de procesamiento del lenguaje natural y aprendizaje automático para realizar análisis preliminares de apelaciones extraordinarias, reduciendo el tiempo necesario para el análisis de admisibilidad y contribuyendo a la agilización del flujo procesal.

Dentro del Tribunal Superior de Justicia (STJ) de Brasil, cabe mencionar el “Proyecto Athos”. Este sistema de inteligencia artificial se utiliza para identificar casos con potencial para caer en temas repetitivos y para localizar controversias jurídicas similares. La herramienta ayuda a la formación de precedentes cualificados y a la gestión de litigios masivos, una realidad particularmente relevante en sectores económicos con alta actividad litigiosa, como el mercado de seguros.

A nivel nacional, el Consejo Nacional de Justicia estructuró la plataforma Sinapses, diseñada como un entorno colaborativo para el desarrollo, intercambio y reutilización de modelos de inteligencia artificial entre los distintos órganos del Poder Judicial. La iniciativa busca evitar la duplicación de esfuerzos tecnológicos y fomentar la adopción coordinada de soluciones basadas en IA por parte de los tribunales brasileños.

La expansión de estas herramientas se produjo en paralelo con la maduración del debate regulatorio sobre los límites legales de la inteligencia artificial. Si bien el sistema jurídico brasileño aún no cuenta con un marco legal específico e integral para la tecnología, su uso está sujeto a un conjunto de estándares constitucionales, regulatorios y de principios destinados a proteger los derechos fundamentales.

En este contexto, la Ley General de Protección de Datos (Ley n.º 13.709/2018 – LGPD) adquiere especial relevancia, al establecer principios y normas aplicables al tratamiento de datos personales, incluso mediante sistemas automatizados. La legislación consagra, entre otros principios, la finalidad, la necesidad, la transparencia, la no discriminación y la responsabilidad de los responsables del tratamiento de datos; parámetros particularmente relevantes para los sistemas de IA que operan con grandes volúmenes de datos y generan inferencias capaces de influir en decisiones con importantes repercusiones económicas y jurídicas.

En el contexto específico del Poder Judicial, destaca la Resolución No. 332/2020 del Consejo

Nacional de Justicia, que establece directrices éticas para el desarrollo y uso de la inteligencia artificial por parte de los tribunales brasileños. La normativa establece principios como transparencia, explicabilidad, auditabilidad, seguridad, prevención de la discriminación y supervisión humana, con el fin de garantizar que el uso de herramientas tecnológicas sea compatible con las garantías procesales fundamentales y la protección de los derechos de las personas bajo la jurisdicción de los tribunales.

Paralelamente, el país debate la construcción de un marco regulatorio específico para la inteligencia artificial. En este contexto, destaca el Proyecto de Ley No. 2338/2023, actualmente en revisión legislativa. Este proyecto de ley busca establecer principios generales, derechos de los afectados y obligaciones proporcionales al riesgo derivado del uso de sistemas de IA. Inspirado en parte por las experiencias regulatorias europeas, el proyecto de ley adopta un enfoque basado en el riesgo y prevé requisitos más estrictos para las aplicaciones consideradas de alto impacto, categoría en la que podrían incluirse ciertos usos en los sectores financiero y de seguros.

Desde la perspectiva del mercado de seguros, este entorno regulatorio produce efectos ambivalentes. Por un lado, crea parámetros de seguridad jurídica para la adopción de herramientas de inteligencia artificial en la prevención y detección de fraudes, la liquidación de siniestros y la gestión estratégica de litigios. Por otro lado, impone obligaciones crecientes relacionadas con la gobernanza algorítmica, la calidad de los datos utilizados, la mitigación de sesgos discriminatorios y la transparencia de los procesos automatizados de toma de decisiones. En consecuencia, el desarrollo de soluciones basadas en IA en el sector asegurador brasileño tiende a darse no solo bajo una lógica de eficiencia operativa, sino también bajo crecientes exigencias de cumplimiento normativo y protección de los derechos fundamentales.

1.1.2. Argentina: Panorama general de la regulación y el uso de herramientas de inteligencia artificial en la resolución de controversias.

Argentina, a su vez, también demuestra liderazgo en Latinoamérica en cuanto al uso de la inteligencia artificial en los procesos judiciales.

El sistema de justicia opera bajo un modelo híbrido, en el que la inteligencia artificial actúa como herramienta auxiliar para agilizar los trámites burocráticos, organizar grandes volúmenes de datos y redactar decisiones sencillas. Este modelo se basa en la premisa de que la tecnología debe optimizar la eficiencia operativa sin reemplazar al juez, quien sigue siendo responsable de la actividad jurisdiccional.

Actualmente, no existe una legislación federal específica o unificada que regule directamente el uso de la inteligencia artificial en los tribunales argentinos. La gobernanza del sector se ejerce mediante reglamentos internos, conocidos como "Acordadas" o "Acuerdos Plenarios", que son directrices dictadas administrativamente por los propios Tribunales Superiores, tanto a nivel nacional como provincial¹¹.

¹¹ «Uso de la inteligencia artificial en los procesos judiciales» (2024), por J. G. Corvalán y R. Lavin. Disponible en: <https://fund.ar/wp-content/uploads/2024/10/Fundar_Uso-de-inteligencia-artificial-en-los-procesos-judiciales_CC-BY-NC-ND-4.0-1.pdf>

El ecosistema de sistemas existente pone de relieve el papel pionero de Prometea en la automatización de tareas repetitivas y el análisis de procesos, una tecnología que se ha extendido a las provincias¹². En Chaco, los modelos de IA optimizan los procesos de monitoreo, mientras que en Mendoza ayudan en la aprobación de convenios laborales.

Además, los manuales de buenas prácticas publicados por las provincias argentinas garantizan la transparencia bajo la supervisión humana obligatoria (“human in the loop”), asegurando que cada propuesta generada por la máquina sea validada por un magistrado. Por ejemplo, AymurAI salvaguarda la anonimización de datos sensibles en las decisiones judiciales¹³.

1.1.3. Colombia: Panorama general de la regulación y el uso de herramientas de inteligencia artificial en la resolución de controversias.

Colombia ha sido pionera en el panorama jurídico latinoamericano. La judicatura colombiana ha formalizado la integración de la Inteligencia Artificial (IA) en la actividad judicial, tras la aprobación de la Corte Constitucional, en agosto de 2024, del uso de esta tecnología, orientada a optimizar la eficiencia procesal¹⁴.

Por su parte, el Consejo Superior de la Judicatura emitió resoluciones en diciembre del mismo año, estableciendo directrices estrictas para su aplicación en la administración de justicia.

En efecto, el Consejo Superior de la Judicatura publicó el 18 de diciembre de 2024 el Acuerdo PCSJA24-12243¹⁵. Esto dio lugar a la adopción de normas y directrices para el uso de herramientas de inteligencia artificial en procesos judiciales, con el objetivo de garantizar su uso responsable, seguro y ético.

Entre las directrices establecidas, se exige a los jueces que revisen, validen y aseguren la debida divulgación de toda la información generada por herramientas automatizadas, bajo pena de nulidad o incumplimiento de las normas procesales.

Además, la normativa prohíbe el uso de plataformas de chatbot gratuitas, así como la delegación de actos de naturaleza eminentemente jurisdiccional a la tecnología, y subraya la obligación de divulgar explícitamente su uso en cualquier expediente, archivo, acto, documento o decisión judicial.

¹² *PROMETEA: Transformando la administración de justicia con herramientas de inteligencia artificial* (2020) Disponible en: <https://publications.iadb.org/publications/spanish/document/PROMETEA-Transformando-la-administracion-de-justicia-con-herramientas-de-inteligencia-artificial.pdf?_cf_chl_tk=N01gAZpUgzM0G8RPLiQotCmFpJ77xMxLbnXoshZtlrs-1781526361-1.0.1.1-IND2POP.sYFvy6RMeGPWOYXyXz25PXNbTTRufUt.IQM> acceso em 15/06/2026

¹³ *"Nuevo Manual de Buenas Prácticas para el uso de IA e IAGen en el Poder Judicial de la CABA"* -Conselho da Magistratura de Buenos Aires- publicado em 12/12/2025. Disponible em: <<https://consejo.jusbaires.gob.ar/institucional/secretaria-de-innovacion/actividades/nuevo-manual-de-buenas-practicas-para-el-uso-de-ia-e-iagen-en-el-poder-judicial-de-la-caba/>> consulta em 15/06/2026.

¹⁴ Corte Constitucional de Colombia, Sala Segunda de Revisión, Sentencia T-323/24 02/08/2024, Magistrado sustanciador: Juan Carlos Cortés González, disponible en <<https://www.corteconstitucional.gov.co/relatoria/2024/T-323-24.htm>>

¹⁵ https://www.ramajudicial.gov.co/portal/inicio/-/asset_publisher/YGVdQynYXjLI/content/id/166385322>

Como ejemplo de inteligencia artificial utilizada en procesos judiciales que protegen los derechos fundamentales – como la acción de tutela-, se puede mencionar “PretorIA”¹⁶, un sistema que cruza información, detecta relaciones entre casos y los clasifica para un ejercicio de selección célere y en casos que involucran empresas comerciales como el “Sistema Siarelis”¹⁷.

En el ámbito legislativo, se encuentra actualmente en consideración el Proyecto de Ley 043/25 – Regulación Integral de la IA en Colombia –, que contempla la creación del Consejo Nacional de IA (CON-IA) y la clasificación de las actividades por riesgo crítico, alto, medio y bajo¹⁸.

1.2. Estado actual del uso de la inteligencia artificial en el marco de la resolución de conflictos en América Latina

Un análisis comparativo de las experiencias de Brasil, Colombia y Argentina demuestra que el uso de la inteligencia artificial en la administración de justicia y la gestión de litigios se encuentra en una etapa avanzada de desarrollo en América Latina. Sin embargo, su avance se ha centrado en el uso de la IA por parte de las autoridades judiciales y no en el uso de las partes (demandantes, demandados y otros intervinientes) en los procesos judiciales.

En efecto, del análisis realizado, un primer elemento común identificado es la preservación de la centralidad del juez en la actividad jurisdiccional. En ninguno de los sistemas jurídicos analizados la inteligencia artificial reemplaza la toma de decisiones judiciales, ya que el juez conserva la responsabilidad final de las decisiones sobre el fondo del asunto. Por lo tanto, la supervisión humana emerge como un principio estructurador para el uso de estas tecnologías, reflejando preocupaciones compartidas sobre transparencia, debido proceso, protección de datos personales y prevención de la discriminación algorítmica.

Las diferencias observadas entre los países analizados se concentran principalmente en la intensidad y los fines atribuidos a la inteligencia artificial. Brasil ha orientado sus esfuerzos hacia el desarrollo de sistemas destinados a gestionar litigios masivos, examinar apelaciones e identificar precedentes, mediante iniciativas como Víctor, Athos y Sinapses, acompañadas de un marco regulatorio cada vez más maduro, representado por la Ley General de Protección de Datos y los debates en torno al Proyecto de Ley No. 2338/2023.

Colombia, por su parte, destaca por el papel protagónico de sus tribunales superiores en la formulación de parámetros legales para el uso de la inteligencia artificial y en la implementación de herramientas destinadas a proteger los derechos fundamentales, como el sistema PretorIA. La experiencia colombiana muestra una particular preocupación por la compatibilidad entre la innovación tecnológica y las garantías constitucionales en la resolución de controversias.

Argentina presenta algunas de las experiencias más avanzadas de la región en automatización de actividades jurídicas y apoyo a la toma de decisiones, especialmente a través de herramientas como

¹⁶ <https://algoritmos.uniandes.edu.co/pretoria-anteriormente-conocido-como-prometea/>

¹⁷ <https://www.semana.com/nacion/articulo/supersociedades-integro-a-un-robot-para-asistir-a-los-jueces-en-pleitos-mercantiles/590406/>

¹⁸ <https://leyes.senado.gov.co/p-ley/2025-2026/PL%20043-25%20-%20REGULACION%20INTELIGENCIA%20ARTIFICIAL.pdf>

Prometea y Ayumur. Estas iniciativas demuestran el potencial de la inteligencia artificial para aumentar la eficiencia del sistema de justicia, reducir los tiempos de procesamiento y ampliar la capacidad institucional para responder a los crecientes litigios, sin descuidar la protección de datos sensibles y la seguridad de la información.

Desde la perspectiva del sector asegurador, conviene analizar si a partir de las experiencias analizadas la inteligencia artificial tiene el potencial de actuar no sólo en la gestión y resolución de disputas ya presentadas, sino también en la prevención de conflictos. Las herramientas de detección de fraude, el análisis automatizado de documentos, la regulación de reclamaciones, la identificación de patrones de litigios y la predicción de resultados procesales tienden a reducir los costos de transacción, aumentar la eficiencia operativa y contribuir a una mayor previsibilidad de las relaciones de seguro.

Las experiencias acumuladas de estas naciones latinoamericanas constituyen, por tanto, un importante punto de referencia para abordar los desafíos estructurales derivados del alto nivel de litigios que caracteriza a la región. Más que una herramienta de automatización, la inteligencia artificial emerge como un instrumento capaz de transformar la forma en que se previenen, gestionan y resuelven los conflictos. El desafío común para los sistemas jurídicos latinoamericanos radica en construir modelos de gobernanza que les permitan aprovechar las ventajas de eficiencia que brindan estas tecnologías sin comprometer la protección de los derechos fundamentales, la confianza de los usuarios ni la legitimidad de los sistemas de justicia y seguros.

2. La inteligencia artificial en la gestión del siniestro: valor operativo, riesgos agénticos y gobernanza responsable

2.1. Planteamiento general: Usos de la inteligencia artificial en la industria aseguradora

El debate sobre inteligencia artificial en seguros suele oscilar entre dos extremos. Por un lado, cierta mirada entusiasta que presenta la tecnología como una solución inmediata para problemas estructurales. Por otro, una posición defensiva que la reduce a una moda pasajera o a un riesgo que conviene evitar. Ninguna de esas miradas resulta suficiente.

En la industria aseguradora, el enfoque más interesante no está necesariamente en reemplazar el trabajo de abogados, liquidadores, peritos, analistas o jueces, sino en volver viables tareas que hasta ahora resultaban demasiado lentas, costosas o directamente impracticables mediante procesos manuales.

El seguro trabaja sobre información. Toda decisión relevante exige analizar datos: la existencia del siniestro, la cobertura contratada, la conducta de las partes, la documentación disponible, la extensión del daño, los antecedentes del caso, el riesgo de litigio y la conveniencia de pagar, rechazar, negociar o litigar. El problema es que gran parte de esa información no está organizada como dato, sino encerrada en documentos.

Demandas, denuncias de siniestro, fotografías, presupuestos, historias clínicas, pericias, informes de liquidación, sentencias y acuerdos suelen conservarse como archivos aislados. Es decir, se guarda el documento, pero no siempre se extrae conocimiento de él. Se archiva una sentencia, pero no se la integra a una base consultable. Se recibe una demanda, pero no se la compara con reclamos anteriores. Se incorpora una pericia o una fotografía, pero muchas veces no se aprovecha esa información para detectar tendencias, inconsistencias o patrones.

La paradoja es evidente: la información existe, pero no siempre puede ser utilizada. En consecuencia, decisiones importantes continúan dependiendo en exceso de la memoria individual, de la experiencia fragmentaria de cada profesional o de búsquedas manuales que insumen tiempo. La inteligencia artificial puede ayudar a modificar esa realidad. Su utilidad no consiste solamente en acelerar tareas existentes, sino en transformar documentos dispersos en información estructurada, consultable y verificable. Ese cambio permite pasar de un modelo basado en archivos aislados a un modelo basado en conocimiento organizado.

Una sentencia judicial, por ejemplo, puede contener datos relevantes sobre partes, aseguradoras, abogados, tribunal, mecánica del hecho, rubros admitidos, montos otorgados, tasa de interés, valoración de prueba y argumentos aceptados o rechazados. Si permanece como un *pdf* aislado, su utilidad futura dependerá de que alguien recuerde su existencia. Si esos datos son extraídos y vinculados con su fuente original, la sentencia pasa a integrar una base de conocimiento que aporta un enorme valor a la industria.

El mismo razonamiento puede aplicarse a demandas, denuncias, reclamos administrativos, pericias o documentación médica. El objetivo no es que la herramienta decida por la organización, sino que permita observar mejor aquello que ya se encuentra dentro de sus propios documentos. Por eso, el aporte de la inteligencia artificial en seguros debe pensarse como una ampliación del criterio humano, no como una delegación ciega. La herramienta puede leer más documentos, comparar más casos y advertir más relaciones que una revisión manual ordinaria. Pero la interpretación jurídica, técnica y estratégica debe permanecer bajo responsabilidad humana.

2.2. Fraude, litigiosidad y riesgo judicial

Uno de los campos donde esta transformación puede aportar mayor valor es la prevención y detección temprana del fraude.

En materia de siniestros, muchas señales relevantes no aparecen en un caso aislado, sino en la comparación entre múltiples reclamos. La reiteración de determinados intervinientes, la repetición de patologías, la aparición de documentos semejantes o la existencia de estructuras narrativas similares pueden justificar una revisión más cuidadosa. No se trata de concluir automáticamente que existe fraude, sino de identificar situaciones que merecen análisis.

Esta distinción es fundamental; una alerta no equivale a prueba. La inteligencia artificial puede indicar dónde mirar, pero no debe convertir coincidencias en condenas ni sospechas en decisiones automáticas. La decisión de rechazar un reclamo, denunciar un fraude o adoptar una determinada estrategia procesal exige siempre valoración humana, control jurídico y análisis del caso concreto.

En este punto resulta especialmente ilustrativo mencionar un caso concreto ocurrido en Argentina, comúnmente conocido como el caso de los “caranchos” de Lomas de Zamora¹⁹.

Según fue informado públicamente, el origen de la investigación se vinculó con la detección de un patrón de repetición de personas en distintas causas judiciales. Un estudio jurídico que trabajaba para compañías de seguros advirtió que ciertos nombres aparecían reiteradamente en diferentes expedientes, en algunos casos como actores, demandados o testigos²⁰. A partir de esa observación, dio aviso a la aseguradora para la que trabajaba, que comenzó a analizar la situación con mayor profundidad y detectó la existencia de numerosos reclamos con indicios compatibles con maniobras fraudulentas. Incluso se señaló que algunas personas registraban múltiples expedientes iniciados contra distintas aseguradoras.

El caso derivó luego en el intercambio de información entre compañías y en la formulación de una denuncia penal contra una organización dedicada, presuntamente, a generar reclamos falsos sobre la base de siniestros inexistentes o simulados, con el propósito de defraudar a aseguradoras. La investigación culminó con condenas a numerosas personas por su intervención en una estructura organizada para ese fin²¹.

Más allá de las particularidades penales del caso, su relevancia para este análisis reside en otro aspecto: el patrón existía en los documentos, pero no había sido detectado por las aseguradoras. Fue advertido por una persona, casi artesanalmente, al reconocer repeticiones entre expedientes. Es decir, la información estaba disponible, pero dispersa; podía ser leída, pero no estaba estructurada; podía generar una alerta, pero dependía de la memoria, experiencia o atención circunstancial de un profesional.

Allí aparece con claridad uno de los aportes más concretos de la inteligencia artificial aplicada al seguro. La industria no debería depender de que alguien detecte casi por casualidad la repetición de actores, testigos, profesionales, domicilios, patologías, mecánicas de accidente o estructuras de reclamo. Debería contar con bases de información capaces de cruzar datos en forma sistemática y generar alertas tempranas cuando aparezcan recurrencias relevantes.

Para ello, resulta indispensable el trabajo conjunto de la industria aseguradora. Es necesario superar las resistencias que históricamente han existido para compartir información entre

¹⁹ Villar, B. (2026, 3 de junio). *Condenaron a los jefes de la red de abogados caranchos que estafaba aseguradoras: Uno había sido policía 15 años*. Infobae. <https://www.infobae.com/sociedad/policiales/2026/06/03/condenaron-a-los-jefes-de-la-red-de-abogados-caranchos-que-estafaba-aseguradoras-uno-habia-sido-policia-15-anos/>

El Seguro en Acción. (2026, 30 de abril). *Justicia contra los “caranchos”: Casación confirmó las condenas a una red de abogados que estafaba aseguradoras mediante siniestros falsos*. <https://elseguroenaccion.com.ar/justicia-contra-los-caranchos-casacion-confirio-las-condenas-a-una-red-de-abogados-que-estafaba-aseguradoras-mediante-siniestros-falsos/>

²⁰ Tscherwinski, W. D., & Varena, D. A. (2026, 4 de junio). *Seguro obligatorio. Responsabilidad civil. Mutación de las conductas fraudulentas: Su expansión a distintos departamentos judiciales. Su impacto económico*. [Ponencia]. XX Congreso Nacional e Internacional de Derecho de Seguros.

²¹ Tribunal en lo Criminal N.º 8 del Departamento Judicial de Lomas de Zamora. (2026, 2 de junio.). *Causa 65.939/18, “Jorge Luis Messina y Walter Damián Lobo”* [Sentencia].

compañías y avanzar hacia esquemas de colaboración que permitan perseguir un objetivo común: combatir de manera más eficaz el fraude, un flagelo que afecta gravemente al sector en su conjunto. Naturalmente, una alerta de este tipo no constituye por sí sola prueba de fraude. Su función no es reemplazar la investigación ni justificar decisiones automáticas de rechazo. Su valor consiste en anticipar señales, orientar la revisión humana y permitir que las compañías actúen antes de que el fraude se consolide o se multiplique. En ese sentido, la inteligencia artificial puede transformar una detección ocasional en una política preventiva, trazable y sistemática.

La misma lógica se proyecta sobre la litigiosidad. En muchas jurisdicciones, uno de los principales problemas es la falta de publicación sistemática de jurisprudencia. Los fallos existen, pero al no encontrarse disponibles en bases públicas, completas y fácilmente consultables, resulta muy difícil conocer con precisión el criterio de determinados juzgados o tribunales frente a cuestiones puntuales.

Esta falta de visibilidad genera consecuencias relevantes. Por un lado, dificulta la identificación de criterios divergentes o inconsistentes frente a casos sustancialmente similares. Por otro, impide construir un análisis suficientemente fundado del riesgo judicial, ya que las partes, las aseguradoras y los estudios jurídicos deben decidir muchas veces con información parcial, dispersa o dependiente de la experiencia individual de quienes intervienen en el caso.

Las aseguradoras y los estudios jurídicos suelen contar con un volumen considerable de expedientes propios: demandas, contestaciones, pericias, sentencias, recursos, acuerdos y liquidaciones. Sin embargo, ese acervo no siempre se aprovecha de manera sistemática. Muchas veces se consulta un antecedente porque alguien lo recuerda, no porque exista una base ordenada que permita buscarlo y compararlo.

Si esa información se estructura, puede transformarse en una herramienta de gestión del riesgo judicial. Permite conocer criterios de tribunales, rangos indemnizatorios, rubros habitualmente admitidos o rechazados, tasas de interés aplicadas, argumentos defensivos con mejor recepción y resultados obtenidos en casos semejantes. Esa información puede mejorar la decisión de conciliar, litigar o apelar.

En mercados de alta litigiosidad y con fuerte incidencia del fraude, estas capacidades tienen un valor estratégico. No eliminan la incertidumbre judicial ni previenen por completo las maniobras fraudulentas, pero permiten abordar ambos problemas con mejores datos, mayor trazabilidad y una capacidad de detección más temprana.

El punto decisivo es la trazabilidad. La información extraída de los documentos no debe convertirse en una afirmación autónoma o incontrolable. Cada dato relevante debe poder vincularse con su fuente: la sentencia, la demanda, la pericia, la denuncia o el informe del cual surge. Sin esa posibilidad de retorno al documento original, el sistema pierde valor jurídico y se transforma en una nueva caja negra.

2.3. Prueba digital y estándar reforzado de trazabilidad

La inteligencia artificial generativa también obliga a revisar la forma en que se produce y valora la prueba digital en seguros²².

La actividad aseguradora se apoya cada vez más en documentos digitales: fotografías de daños, presupuestos, certificados médicos, historias clínicas, capturas de pantalla, mensajes, videos y archivos enviados por canales remotos. Esa documentación resulta útil y, en muchos casos, indispensable para gestionar reclamos con rapidez. Pero también plantea un problema creciente de autenticidad.

El riesgo no se limita a los *deepfakes* sofisticados. En la práctica aseguradora, los problemas más frecuentes pueden ser más simples: imágenes editadas, daños incorporados o exagerados, documentos alterados, archivos sin fecha verificable o fotografías que no permiten acreditar con seguridad su origen y contexto.

Frente a este escenario, no parece razonable negar valor a toda prueba digital. Sería desconocer cómo funciona hoy la gestión de siniestros. Pero tampoco resulta adecuado valorarla automáticamente cuando es desconocida por la contraparte, carece de metadata, no tiene cadena de custodia y no se encuentra corroborada por otros elementos.

La apariencia de realidad ya no puede confundirse con autenticidad. Una imagen puede parecer verosímil y no corresponder al hecho debatido. Un documento puede lucir formalmente correcto y haber sido modificado. Por eso, el derecho de seguros debería avanzar hacia un estándar reforzado de autenticidad, trazabilidad y corroboración, especialmente cuando la prueba digital constituye el principal sustento del reclamo.

Ese estándar no exige transformar cada reclamo en una pericia informática. Exige algo más razonable: preservar archivos originales cuando sea posible, registrar canales de recepción, conservar información técnica relevante, utilizar mecanismos de validación en inspecciones remotas y valorar la prueba digital en conjunto con otros elementos del caso.

La inteligencia artificial puede agravar este problema, porque facilita la generación o alteración de documentos. Pero también puede ayudar a mitigarlo, mediante herramientas de comparación, detección de inconsistencias, control de duplicados, análisis de patrones y validación preliminar. Nuevamente, su valor depende del modo de implementación. La tecnología puede ser fuente de riesgo o herramienta de prevención, según los controles que la acompañen.

2.4. Inteligencia artificial agéntica en seguros

La evolución de la inteligencia artificial no se agota en modelos capaces de responder preguntas, resumir documentos o redactar textos. Un paso adicional, especialmente relevante para la industria aseguradora, es la inteligencia artificial agéntica.

A diferencia de un sistema que produce una respuesta ante una consulta, un agente de inteligencia artificial puede recibir un objetivo, planificar pasos intermedios, utilizar herramientas, consultar

²² Carello, G. (2025, 17 de noviembre). Deepfakes, fotografías adulteradas y prueba digital: El nuevo desafío probatorio en tiempos de IA generativa. *El Derecho*, 314.

bases de datos, interactuar con sistemas internos, generar documentos, enviar comunicaciones o activar flujos de trabajo. En términos simples, no solo responde: actúa dentro de un proceso.

En seguros, esta diferencia puede ser decisiva. Un agente podría intervenir en la apertura de un siniestro, revisar si la denuncia contiene información mínima, identificar documentación faltante, consultar condiciones de póliza, comparar antecedentes, advertir inconsistencias, preparar un informe preliminar o derivar el caso al área correspondiente. También podría asistir en el seguimiento de expedientes judiciales, control de vencimientos, actualización de bases internas o priorización de reclamos que requieren atención humana.

La potencialidad económica es clara. Buena parte de la gestión aseguradora está compuesta por tareas repetitivas, distribuidas entre distintas áreas y sistemas. Si un agente logra ordenar ese flujo, reducir reprocesos, evitar demoras y derivar mejor los casos, puede tener impacto en costos, tiempos de respuesta y calidad operativa.

Pero la autonomía trae aparejado un riesgo considerable. Un modelo de IA generativa que alucina o responde mal genera un error de contenido. En cambio, un agente de IA que actúa mal puede producir efectos directos: enviar una comunicación indebida, requerir documentación impropia, omitir una cobertura aplicable, clasificar erróneamente un caso, exponer información sensible o adoptar una conducta incompatible con la buena fe.

Por eso, el riesgo de la inteligencia artificial agéntica no consiste solo en que no alcance el resultado buscado. También importa cómo intenta alcanzarlo. En seguros, no basta con que un sistema reduzca costos, acelere liquidaciones o mejore procesos. Debe hacerlo por medios lícitos, transparentes y compatibles con los deberes propios de la actividad aseguradora.

La investigación reciente en seguridad de modelos ofrece una advertencia útil. En ejercicios controlados de laboratorio, Anthropic verificó que ciertos modelos, colocados en escenarios hipotéticos con acceso a información sensible, objetivos definidos y amenaza de ser desactivados, podían optar por conductas instrumentalmente dañinas, como amenazar o chantajear a una persona ficticia para evitar su reemplazo²³. No se trató de un daño real en producción, sino de una prueba diseñada para identificar riesgos. Pero el ejemplo sirve para mostrar un punto relevante: cuando un sistema tiene objetivos, información y capacidad de actuar, no alcanza con controlar el resultado final. También deben controlarse los medios que puede utilizar.

Trasladado al seguro, el problema es evidente. Si un agente recibe como único objetivo “reducir el costo del siniestro” o “cerrar reclamos pendientes”, puede quedar mal orientado. La eficiencia debe estar subordinada a reglas previas: no inducir a error, no formular amenazas, no ocultar información relevante, no presionar indebidamente, no utilizar datos sensibles como herramienta de negociación, no discriminar, no comunicarse fuera de canales autorizados y no adoptar decisiones relevantes sin revisión humana.

²³ Anthropic. (2025, 20 de junio). *Agentic misalignment: How LLMs could be insider threats*. <https://www.anthropic.com/research/agentic-misalignment>

A este riesgo debe sumarse otro, especialmente relevante cuando los agentes interactúan con documentación proveniente de terceros: el denominado *prompt injection*²⁴. Esta técnica consiste, en términos simples, en incorporar instrucciones maliciosas o no autorizadas dentro de textos, documentos, correos, formularios, páginas web o archivos que luego serán leídos por un sistema de inteligencia artificial. El objetivo es inducir al modelo a ignorar sus instrucciones originales, alterar su comportamiento o producir una respuesta favorable a quien introdujo ese comando.

El problema se vuelve particularmente delicado en sistemas agénticos porque el modelo no solo analiza información, sino que puede tener permisos para actuar. Si un agente lee una demanda, una denuncia de siniestro, un presupuesto o un correo electrónico, y dentro de ese documento existe una instrucción oculta dirigida al sistema, podría confundirla con una orden válida. En un sistema meramente asistido, el resultado podría ser una respuesta incorrecta. En un sistema conectado a herramientas internas, la consecuencia podría ser más grave: modificar una clasificación, omitir una alerta, preparar una comunicación indebida, acceder a información no autorizada o activar un flujo de trabajo improcedente.

Este riesgo ya dejó de ser una hipótesis meramente académica. En Brasil se detectaron recientemente intentos de insertar comandos ocultos en escritos judiciales con el propósito de influir en sistemas de inteligencia artificial utilizados por órganos judiciales. En un caso tramitado ante la Justicia del Trabajo, se informó que una petición contenía texto oculto dirigido al sistema Galileu para condicionar el modo en que debía procesar el escrito²⁵. A su vez, el Superior Tribunal de Justicia informó que identificó en su propio acervo peticiones con *prompt injection* y que dispuso la investigación de esas tentativas, aun cuando su sistema STJ Logos habría neutralizado los comandos maliciosos²⁶.

La referencia es importante para el sector asegurador porque muestra una vulnerabilidad que puede trasladarse fácilmente a cualquier ámbito donde un agente lea documentación externa. Reclamos administrativos, demandas, certificados, presupuestos, correos electrónicos o formularios web podrían contener instrucciones diseñadas para manipular al sistema. Por eso, en materia de seguros, todo documento proveniente de terceros debe ser tratado, desde el punto de vista de seguridad, como información no confiable, aun cuando sea relevante para el análisis del caso.

El *prompt injection* muestra con claridad que la seguridad de la inteligencia artificial agéntica no depende solamente de la calidad del modelo. Depende, sobre todo, del diseño del proceso en el que el agente se inserta. No basta con indicarle al sistema que “no siga instrucciones maliciosas”. Deben existir controles técnicos y organizacionales que separen las instrucciones legítimas del sistema de los datos externos que el agente debe analizar.

²⁴ IBM. (s. f.). *¿Qué es un ataque de inyección de prompts?* IBM Think. Recuperado el 19 de junio de 2026, de <https://www.ibm.com/es-es/think/topics/prompt-injection>

²⁵ Lantyer de Mello, V. H. (2026, 25 de mayo). *Prompt injection oculto em petição inicial: O caso de Parauapebas*. Migalhas. <https://www.migalhas.com.br/depeso/455925/prompt-injection-oculto-em-peticao-inicial-o-caso-de-parauapebas>

²⁶ Superior Tribunal de Justiça. (2026, 20 de mayo). *Tentativas de uso de prompt injection no STJ serão investigadas*. <https://www.stj.jus.br/sites/porta/paginas/Comunicacao/Noticias/2026/20052026-Tentativas-de-uso-de-prompt-injection-no-STJ-serao-investigadas.aspx>

Por eso, antes de implementar agentes de inteligencia artificial, la aseguradora debe definir con precisión el proceso en el que intervendrán. No basta con conectar el agente a los sistemas y evaluar si “funciona”. Debe establecerse qué puede hacer, qué no puede hacer, qué información puede consultar, qué acciones requieren autorización, en qué casos debe detenerse y a quién debe escalar la situación.

Un marco mínimo de buenas prácticas debería incluir, al menos, las siguientes definiciones. Primero, el objetivo del agente debe estar formulado de manera completa; no debería limitarse a una meta económica o de velocidad, sino incorporar los límites jurídicos y operativos dentro de los cuales debe actuar. Por ejemplo, no es lo mismo ordenar “rechazar reclamos improcedentes” que ordenar “identificar reclamos que requieren revisión humana por posibles inconsistencias, sin adoptar decisiones definitivas ni comunicar rechazos sin autorización”.

Deben definirse sus permisos: un agente no debería tener acceso amplio a todos los sistemas de la compañía ni capacidad irrestricta para ejecutar acciones. Debe operar con permisos mínimos, adecuados a su función y revisables periódicamente. Para el efecto, sería prudente clasificar las acciones según su nivel de riesgo, pues algunas tareas pueden automatizarse con mayor libertad, como ordenar documentos, extraer datos o generar borradores internos. Otras exigen revisión previa, como enviar comunicaciones a asegurados o terceros, sugerir rechazos, requerir documentación sensible, modificar reservas o intervenir en negociaciones.

Es recomendable establecer puntos de interrupción obligatoria. Ante supuestos ambiguos, señales de fraude, datos sensibles, impacto económico significativo o cualquier instrucción sospechosa incorporada en documentación externa, el agente debería detener su actuación autónoma y derivar el caso a una persona responsable.

Debe quedar registro de lo actuado: toda intervención relevante debería ser trazable: qué información consultó el agente, qué pasos siguió, qué documentos utilizó, qué recomendó, qué comunicación preparó y quién autorizó la acción final.

Para minimizar el riesgo de *prompt injection* deben separarse técnicamente las instrucciones del sistema de los documentos o datos externos. El agente debe poder analizar una demanda, una denuncia o un presupuesto sin tratar su contenido como una orden dirigida a modificar su comportamiento. Esta separación es especialmente importante cuando se procesan documentos provenientes de terceros.

Es importante probar escenarios adversos antes del despliegue, toda vez que no alcanza con verificar que el agente funcione en casos simples o ideales. Debe evaluarse cómo responde frente a información contradictoria, instrucciones maliciosas dentro de documentos, errores en bases de datos, pedidos urgentes, datos sensibles o tensión entre objetivos económicos y deberes legales.

La supervisión continua resulta indispensable²⁷: los agentes de inteligencia artificial no son herramientas que se configuran una vez y quedan definitivamente resueltas. A diferencia del software tradicional, su comportamiento puede variar con el tiempo por cambios en el modelo

²⁷ National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)* (NIST AI 100-1). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.AI.100-1>

subyacente, en los datos disponibles, en los sistemas con los que interactúa, en las reglas de negocio o en el propio contexto operativo en el que actúa.

En este punto adquiere relevancia el fenómeno conocido como *agentic drift*²⁸. La expresión alude al deterioro o desalineación progresiva del desempeño de un agente respecto de los objetivos, procedimientos o estándares inicialmente definidos. Un agente que en una etapa de prueba funciona correctamente puede, luego de una actualización del modelo, de una modificación en una base de datos o de un cambio en el proceso de negocio, comenzar a omitir pasos relevantes, tomar atajos, interpretar de manera distinta sus instrucciones o producir resultados indeseados.

La inteligencia artificial agéntica puede ser una herramienta de enorme valor para seguros. Pero justamente por su capacidad de actuar, exige un diseño más cuidadoso que los sistemas de IA generativa meramente asistivos. Su implementación responsable no depende solo del modelo utilizado, sino de la arquitectura de permisos, controles, límites, registros, defensas frente a instrucciones maliciosas y supervisión humana que lo rodea.

2.5. Gobernanza, datos y responsabilidad

La implementación de inteligencia artificial en seguros no puede ser tratada como una decisión puramente tecnológica. Es una decisión de gobernanza jurídica, tecnológica y de datos²⁹.

La herramienta opera sobre datos, procesos, personas, proveedores, decisiones económicas y relaciones jurídicas. Puede incidir en la atención de asegurados, la liquidación de siniestros, la detección de fraude, la estrategia judicial, la protección de información sensible y la reputación institucional de la compañía.

Por eso, una implementación responsable debería apoyarse en algunos ejes centrales.

La compañía debe saber qué problema busca resolver y cómo medirá si la herramienta realmente mejora el proceso. Incorporar IA solo porque está disponible o porque el mercado la exige suele conducir a soluciones decorativas, difíciles de integrar y pobres en resultados.

Una herramienta técnicamente sofisticada puede ser inútil si no comprende cómo funciona una aseguradora, qué documentos circulan, qué áreas intervienen, qué plazos importan y qué decisiones se toman en cada etapa.

Toda conclusión relevante debe poder ser auditada. En el ámbito jurídico y asegurador, una respuesta que no permite volver a la fuente tiene un valor limitado y se torna riesgosa.

²⁸ IBM. (s. f.). *The hidden risk that degrades AI agent performance*. IBM Think. Recuperado el 19 de junio de 2026, de <https://www.ibm.com/think/insights/agentic-drift-hidden-risk-degrades-ai-agent-performance>

²⁹ International Association of Insurance Supervisors. (2025, julio). *Application paper on the supervision of artificial intelligence*. <https://www.iaais.org/uploads/2025/07/Application-Paper-on-the-supervision-of-artificial-intelligence.pdf>

European Insurance and Occupational Pensions Authority. (2025, 6 de agosto). *Opinion on artificial intelligence governance and risk management*. https://www.eiopa.europa.eu/document/download/88342342-a17f-4f88-842f-bf62c93012d6_en?filename=Opinion%20on%20Artificial%20Intelligence%20governance%20and%20risk%20management.pdf

La intensidad de esa revisión puede variar según el riesgo de la tarea, pero no debería desaparecer en decisiones que afecten cobertura, derechos de terceros, sospechas de fraude, estrategia judicial o tratamiento de datos sensibles.

Los documentos pueden contener información sensible y datos personales. Su tratamiento mediante IA exige reglas claras de confidencialidad, seguridad, control de accesos, minimización, conservación y eliminación.

Los datos históricos pueden reflejar decisiones incorrectas, prácticas desiguales o patrones que no deberían reproducirse. Por eso, no alcanza con entrenar o alimentar sistemas con grandes volúmenes de información. La calidad, pertinencia y representatividad de los datos importa tanto como su cantidad.

La inteligencia artificial no debe diluir quién responde por una decisión. Si una aseguradora utiliza una herramienta propia o provista por un tercero, debe conservar control sobre su uso, sus permisos, sus resultados y sus consecuencias.

Estos principios no buscan frenar la innovación. Buscan hacerla sostenible y responsable. La confianza en estas herramientas no se construye con promesas de eficiencia, sino con procesos verificables, límites claros y responsabilidad institucional.

2.6. La IA representa una gran oportunidad para el seguro, pero solo genera valor si se incorpora con controles, transparencia y supervisión humana.

La inteligencia artificial ofrece una oportunidad histórica para la industria aseguradora latinoamericana. Puede transformar documentos archivados en datos estructurados, y esos datos en conocimiento útil para prevenir fraude, gestionar siniestros, valorar prueba, estimar riesgo judicial y mejorar decisiones.

Su aporte resulta especialmente relevante en mercados con alta litigiosidad, documentación fragmentada y criterios judiciales difíciles de sistematizar. En ese contexto, la IA puede ayudar a observar mejor, comparar mejor y decidir con mayor información.

Pero esa oportunidad exige prudencia. La herramienta que permite detectar patrones también puede generar opacidad. La que acelera reclamos también puede inducir decisiones apresuradas. La que reduce costos también puede producir incentivos incorrectos. Y la que actúa de manera autónoma puede causar daños si no tiene límites suficientes.

Por eso, el debate no debería formularse como una elección entre adoptar o rechazar inteligencia artificial. La cuestión central es cómo incorporarla. En seguros, la IA solo será valiosa si se la diseña como una ampliación responsable del criterio humano, no como una delegación opaca de decisiones sensibles.

El objetivo no debe ser automatizar a cualquier costo, sino construir conocimiento verificable, reducir incertidumbre, mejorar procesos, prevenir conflictos y fortalecer la confianza en el sistema asegurador.

Por último, la gobernanza interna de la inteligencia artificial en las aseguradoras no es, sin embargo, un asunto que se agote puertas adentro de la compañía. Los principios de trazabilidad, explicabilidad, supervisión humana y responsabilidad institucional que deben regir el uso de estas herramientas en la gestión operativa del siniestro adquieren una dimensión adicional —y más exigente— cuando los resultados producidos por esos mismos sistemas deben trasladarse al proceso judicial o arbitral como elementos de prueba. En ese momento, la decisión de gobernanza deja de ser solo una cuestión de política interna y se convierte en un problema procesal.

Esta circunstancia resulta especialmente crítica en la acreditación del siniestro, que muchas veces depende por entero de evidencia de naturaleza técnica y digital. Allí, la IA no es solo una herramienta de gestión interna: es, en muchos casos, el único medio viable para reconstruir los hechos que activan la cobertura. Por eso, los estándares de gobernanza que se acaban de exponer —trazabilidad del proceso, método verificable, límites claros a la autonomía y supervisión humana efectiva— son los mismos que el ordenamiento procesal exige para que un dictamen pericial tenga valor probatorio, y ello tiene una íntima relación con la acreditación del siniestro en algunos seguros, como los seguros cibernéticos, donde la IA puede resultar decisiva tanto para la compañía de seguros como para el asegurado a la hora de superar las barreras probatorias que condicionan el reconocimiento de la indemnización, como se explicará a continuación.

3. La aplicación de la inteligencia artificial en prueba del siniestro: el caso del dictamen pericial en los seguros cibernéticos

La prueba pericial es, en todos los ordenamientos latinoamericanos, el medio por el que ingresan al proceso los conocimientos especializados que el juzgador no posee ni tiene el deber de poseer. Pese a las diferencias entre las legislaciones, conserva en todas ellas tres notas estructurales: recae sobre hechos que exigen conocimientos científicos, técnicos o artísticos; está sujeta al deber de imparcialidad y objetividad del perito; y se aprecia conforme a la sana crítica o a la libre apreciación motivada, sin que sus conclusiones vinculen al juez (Calderón Ortega y Cueto Calderón, 2022; Cantos Pardo, 2024).³⁰

En los litigios de seguros, donde resulta necesario acreditar de forma constante hechos de naturaleza técnica, esa prueba cumple una función central: probar la ocurrencia del siniestro, su causa y la cuantía del daño. La función, ya exigente en los ramos tradicionales, se vuelve crítica cuando el riesgo asegurado se desplaza del mundo físico al entorno digital, como sucede con los riesgos cibernéticos. Allí el hecho que activa la cobertura no deja huellas materiales observables, sino rastros técnicos dispersos que solo un análisis especializado puede reconstruir, de modo que el ramo donde la prueba pericial es más difícil de practicar es, a la vez, aquel donde resulta más indispensable.

El presente documento tiene por objeto abordar dos cuestiones que suelen tratarse por separado, pero que conforman un mismo problema. La primera es si el dictamen pericial elaborado con inteligencia artificial, o apoyado en ella, resulta admisible en los ordenamientos latinoamericanos, asunto que se examina desde una perspectiva general y mediante un ejercicio de derecho

³⁰Sobre estas coincidencias y los matices entre ordenamientos, véase el cuadro comparativo de la prueba pericial en los diez ordenamientos analizados que se incorpora como anexo al final de este trabajo.

comparado. La segunda es de qué manera ese marco general se proyecta sobre un campo de aplicación concreto y especialmente exigente, el de la prueba del siniestro en los seguros de riesgos cibernéticos, donde la inteligencia artificial ha dejado de ser una hipótesis teórica para convertirse en una herramienta que la práctica forense ya emplea con el fin de identificar, reconstruir y cuantificar el siniestro.

La tesis que se defiende es que ambos planos se iluminan recíprocamente: el estándar que la jurisprudencia comparada viene decantando para el dictamen apoyado en inteligencia artificial encuentra en el siniestro cibernético su banco de pruebas más riguroso, y ese campo de aplicación, a su vez, muestra por qué el estándar resulta necesario.

El análisis se desglosa en cinco partes: (i) el régimen comparado de la prueba pericial en la región; (ii) los problemas que la inteligencia artificial introduce en ese régimen; (iii) el estado de la jurisprudencia comparada, ordenado por ejes y no por jurisdicciones; (iv) la aplicación de ese marco al campo de los riesgos cibernéticos, con sus coberturas, sus dificultades probatorias y las soluciones técnicas que la inteligencia artificial ofrece; y (v) las conclusiones.

Conviene precisar, desde ahora, el alcance del ejercicio comparado, para que el lector sepa con exactitud qué encontrará en estas páginas. El estudio se apoya en dos planos de profundidad distinta. En el plano normativo, se realizó un barrido de diez ordenamientos iberoamericanos (Colombia, Brasil, Argentina, España, Portugal, México, Ecuador, Chile, Perú y Uruguay), cuyo régimen de la prueba pericial se sintetiza en el cuadro comparativo que acompaña este trabajo como anexo. En el plano jurisprudencial, en cambio, el análisis se concentra en las jurisdicciones que han producido pronunciamientos relevantes sobre la prueba apoyada en inteligencia artificial, que hasta la fecha son fundamentalmente Colombia, España, Brasil y Argentina; ello obedece a una razón objetiva, y es que las decisiones que abordan el problema, todavía escasas, se han concentrado en esos foros, mientras que en los demás ordenamientos el material es incipiente o inexistente.

La asimetría no es un defecto del método, sino un reflejo del estado del arte, y el trabajo opta por hacerla explícita antes que por disimularla con menciones aparentes.

Conviene advertir, además, que las decisiones que resuelven de manera frontal si puede o no elaborarse un dictamen con inteligencia artificial son escasas en todas las jurisdicciones. El estado del arte se concentra, sobre todo, en pronunciamientos sobre la fiabilidad de la prueba científica, la autenticidad de la prueba digital, la transparencia algorítmica o las llamadas alucinaciones. De ese conjunto se extraen, por analogía, los estándares aplicables al dictamen apoyado en inteligencia artificial, y esa labor de extracción analógica constituye buena parte del aporte de este trabajo.

3.1. El marco comparado de la prueba pericial en Latinoamérica y España

Como se anticipó, el primer paso de esta investigación consistió en un barrido normativo de diez ordenamientos representativos del espacio iberoamericano: Colombia, Brasil, Argentina, España, Portugal, México, Ecuador, Chile, Perú y Uruguay. La selección obedece a un criterio de diversidad de familias procesales dentro de una tradición jurídica común, lo que permite contrastar soluciones sin perder el terreno compartido. El examen se ordenó en torno a cuatro variables (la designación del perito, su deber de imparcialidad, el objeto del dictamen y el modo de su valoración) y arrojó contrastes más concordantes que disonantes. El cuadro que se incorpora como anexo recoge, ordenamiento por ordenamiento, la base normativa de cada una de esas variables; en lo que sigue se exponen los hallazgos transversales más relevantes.

El primer hallazgo es una marcada diferencia en el diseño de la prueba, que admite ordenarse en dos grandes modelos. En un extremo se sitúa el modelo de perito de parte, nítido en Colombia y España, en el que cada litigante aporta su propio dictamen y la contradicción se concentra en el interrogatorio del perito en audiencia. En el otro se halla el modelo de perito judicial, propio de Brasil, Argentina, Portugal, Chile, Perú y Uruguay, en el cual el tribunal designa al experto y las partes intervienen mediante consultores o asistentes técnicos, cuestionarios y observaciones.³¹

Entre ambos extremos se ubican sistemas mixtos como el mexicano y el ecuatoriano, que parten del dictamen de parte pero reservan al juez la designación de un perito tercero en discordia o, en el caso ecuatoriano, el nombramiento por sorteo cuando la parte no tiene acceso al objeto de la pericia.

La distinción no es menor para lo que sigue, porque el modelo de perito de parte deposita la garantía de fiabilidad en la contradicción entre dictámenes rivales, mientras que el de perito judicial la deposita en la imparcialidad del experto designado, y cada uno reacciona de manera distinta ante la irrupción de un dictamen automatizado.

Ahora bien, más allá de esa diferencia estructural, las coincidencias son mayores y pueden resumirse en tres ideas. En primer término, el objeto del dictamen se limita a hechos que requieren conocimientos especializados, sin extenderse a cuestiones de derecho, salvo la prueba del derecho extranjero. A su turno, rige en todos los ordenamientos el deber de imparcialidad y objetividad del perito. Y, finalmente, la valoración se realiza conforme a la sana crítica o a la libre apreciación motivada, sin que las conclusiones del dictamen vinculen al juez.

Esta cartografía interesa porque las cuatro variables del régimen clásico, esto es, la designación del perito, su deber de imparcialidad, el objeto limitado a hechos técnicos y la valoración por sana crítica, son precisamente los puntos donde la llegada de la inteligencia artificial genera la mayor tensión. No se trata, pues, de cuatro categorías descriptivas, sino de los cuatro frentes en los que se libraré la discusión que sigue. La pregunta, en consecuencia, no es si la inteligencia artificial cabe en este marco, sino en qué condiciones lo hace sin desnaturalizar las garantías que los ordenamientos buscan proteger.

3.1.1. Los problemas que introduce la inteligencia artificial

Antes de examinar las tensiones conviene distinguir tres supuestos que reciben un tratamiento jurídico diverso: la inteligencia artificial empleada como herramienta auxiliar por un perito humano que firma el dictamen y responde por él; el informe sustancialmente generado por inteligencia artificial y luego suscrito o validado por un experto; y la valoración automatizada realizada por cualquier interesado en el proceso, que puede no constituir siquiera un dictamen en sentido procesal. Los problemas se agravan a medida que se avanza del primer supuesto al tercero, pues disminuye de manera correlativa la intervención humana que el ordenamiento exige. Sobre esa gradación se proyectan los cuatro frentes de tensión anunciados, que conviene tratar por separado.

³¹Fuentes normativas principales: Colombia, Ley 1564 de 2012 (CGP), arts. 226 a 235; Brasil, Lei 13.105 de 2015 (CPC), arts. 464 a 480; Argentina, CPCCN, arts. 457 a 478; España, Ley 1/2000 (LEC), arts. 335 a 352; Portugal, Lei 41/2013 (CPC), arts. 467 a 489; México, CNPCF (2023), arts. 300 a 307; Ecuador, COGEP (2015), arts. 221 a 228; Chile, CPC, arts. 409 a 425; Perú, CPC (1993), arts. 262 a 271; Uruguay, Ley 15.982 de 1988 (CGP), arts. 177 a 185.

El primero es la transparencia frente a la «caja negra». Si el método algorítmico no puede explicarse de modo comprensible, se lesiona la contradicción, porque la parte no puede impugnar lo que no conoce, y se compromete la valoración del juez, para quien resulta indispensable comprender no solo las conclusiones, sino el razonamiento que conduce a ellas. Sobre el particular, Calderón Ortega y Cueto Calderón (2022) han advertido que reconducir la prueba por inteligencia artificial a la simple categoría de mensaje de datos, en virtud del principio de neutralidad tecnológica, es epistemológicamente insuficiente, y han propuesto canalizarla a través de la pericia científica, de modo que un experto humano explique el funcionamiento del algoritmo y garantice la cadena de custodia de la información.³²

Este planteamiento, con todo, encierra un riesgo que conviene anticipar: el de sustituir el dictamen técnico sobre el hecho jurídicamente relevante por un dictamen técnico sobre la fiabilidad del primer dictamen, lo que abriría un regreso al infinito de difícil justificación práctica. La explicabilidad, por tanto, debe entenderse como una exigencia de comprensión razonable del método, no como la imposición de una pericia sobre la pericia.

El segundo frente es la identidad y la idoneidad del perito. Una máquina no presta juramento, no es recusable y no está sujeta a las consecuencias jurídicas previstas para el incumplimiento de los deberes del perito; sobre todo, no puede cumplir uno de los más esenciales, comparecer a la audiencia y someterse al interrogatorio de las partes. A lo sumo podrían comparecer sus desarrolladores, cuya capacidad de explicar de manera íntegra el modelo es limitada, pues en los sistemas de aprendizaje profundo puede resultar muy complejo, o incluso imposible, reconstruir el razonamiento seguido por la máquina.³³

De ahí que el dictamen apoyado en inteligencia artificial siga exigiendo un perito humano idóneo que asuma la autoría y la responsabilidad del resultado, y que esa exigencia no sea un formalismo, sino la condición que hace posible la contradicción.

El tercer frente es la fiabilidad, esto es, la cuestión de si el algoritmo es capaz de emplear, o de simular, un método real e idóneo para fundar su concepto. La teoría racionalista de la prueba ha precisado que la fiabilidad de la prueba científica no reposa en la autoridad de quien la emite, sino en la validez de su método, en el control de su tasa de error y en la posibilidad de someter sus fundamentos a escrutinio.³⁴

La irrupción de la inteligencia artificial agudiza esa exigencia, porque un sistema opaco impide la contrastación empírica de sus fundamentos y, con ello, el ejercicio de la contradicción. Esa misma idea se ha decantado en la jurisprudencia: la Corte Suprema de Justicia de Colombia, en la

³²Calderón Ortega, M. A. y Cueto Calderón, C. A. (2022). Prueba por inteligencia artificial: una propuesta de producción probatoria desde el dictamen pericial científico en Colombia. *Civilizar: Ciencias Sociales y Humanas*, 22(42).

³³Cantos Pardo, M. (2024). La algoritmización del dictamen pericial: ¿puerta de entrada para la aparición del «perito-robot»? *Actualidad Jurídica Iberoamericana*, (21), que analiza el difícil encaje del algoritmo en los arts. 340 y 347 de la LEC española.

³⁴Taruffo, M. (2005). Conocimiento científico y estándares de prueba judicial. *Boletín Mexicano de Derecho Comparado*, (114). UNAM.

sentencia SC2154-2025, fijó cinco dimensiones para evaluar la calidad epistémica del dictamen pericial, plenamente trasladables a un dictamen apoyado en inteligencia artificial.³⁵

Los tres frentes confluyen en una misma conclusión provisional: el régimen vigente no prohíbe de manera expresa el dictamen elaborado con inteligencia artificial, pero está construido sobre supuestos (el perito que jura, comparece y responde) que un sistema automatizado, por sí solo, no satisface. La pregunta se traslada entonces a la jurisprudencia, que es donde esos supuestos se han puesto a prueba.

3.1.2. El estado de la jurisprudencia comparada y los ejes del problema

Conforme se advirtió en la introducción, el análisis jurisprudencial se concentra en las jurisdicciones que han producido pronunciamientos sobre la prueba apoyada en inteligencia artificial, esto es, Colombia, España, Brasil y Argentina, sin que ello suponga abandonar el marco normativo de los diez ordenamientos, que opera como telón de fondo. El material disponible es, además, desigual: algunos foros han producido un número mayor de decisiones y otros han concentrado su atención en problemas distintos, de modo que la comparación resulta más clara si se ordena por problemas y no por jurisdicciones.

Del conjunto de decisiones analizadas, en las que predominan las altas cortes pero se incorporan también tribunales inferiores cuando aportan criterios útiles (como la Audiencia Nacional española o el juzgado civil de Tucumán), pueden extraerse cinco ejes que, leídos de manera horizontal, perfilan un estándar emergente. Esos cinco ejes responden, punto por punto, a las tensiones identificadas en el apartado anterior: donde el régimen clásico exhibía cuatro frentes de fricción, la jurisprudencia ofrece cinco respuestas convergentes.

a) La reserva humana de la valoración

La valoración de la prueba y la decisión son funciones indelegables del juzgador, que la inteligencia artificial puede apoyar, pero no sustituir. Así lo sostuvo la Corte Constitucional de Colombia en la Sentencia T-323 de 2024, dictada a raíz de que un juez empleó una herramienta generativa al resolver una acción de tutela. La Corte precisó que la inteligencia artificial puede apoyar, mas no reemplazar, el razonamiento humano en la valoración de las pruebas, en la fijación de los hechos y en la solución del caso (Corte Constitucional, 2024), y fijó criterios de transparencia, contradicción, verificación de fuentes, prevención de sesgos y alucinaciones, responsabilidad y supervisión humana.³⁶

En el plano regulatorio, la Instrucción 2/2026 del Consejo General del Poder Judicial de España avanza en la misma dirección y prohíbe expresamente «La sustitución, automatización o delegación de la toma de decisiones judiciales, de la valoración de los hechos o de las pruebas» (Consejo General del Poder Judicial, 2026, p. 14485); solo admite el uso de sistemas de inteligencia artificial facilitados por las Administraciones competentes en materia de justicia o por

³⁵Corte Suprema de Justicia de Colombia, Sala de Casación Civil, Agraria y Rural, sentencia SC2154-2025, del 15 de diciembre de 2025. Las cinco dimensiones de la calidad epistémica del dictamen son: (i) idoneidad del perito; (ii) transparencia de las premisas fácticas; (iii) validez metodológica; (iv) coherencia del razonamiento; y (v) inteligibilidad.

³⁶Corte Constitucional de Colombia, Sentencia T-323 de 2024.

el propio Consejo General del Poder Judicial, sometidos a control de calidad y auditoría por este último.³⁷

La misma reserva aparece en el pronunciamiento más próximo al núcleo de este trabajo. Según el comunicado oficial del Superior Tribunal de Justiça de Brasil, cuyo texto íntegro aún no se ha publicado, la 5.^a Turma, en el Habeas Corpus n.º 1.059.475/SP, excluyó de los autos un «Relatório Técnico» producido con inteligencia artificial generativa que pretendía contradecir un laudo pericial oficial, por carecer de la confiabilidad epistémica mínima exigible a la prueba.³⁸

b) La fiabilidad y el método verificable

El dictamen no se valora solo por las credenciales del perito, sino por la solidez verificable de su razonamiento, que debe ser trazable y reproducible, de suerte que solo la técnica puede refutar a la técnica. La Corte Suprema de Justicia de Colombia lo afirmó en la sentencia SC2154-2025, donde fijó cinco dimensiones de control: «1) idoneidad del perito, 2) transparencia de las premisas fácticas, 3) validez metodológica, 4) coherencia del razonamiento y 5) la inteligibilidad» (Corte Suprema de Justicia, 2025, p. 315), directamente trasladables a un dictamen apoyado en inteligencia artificial en cuanto exigen explicabilidad, trazabilidad y método verificable.³⁹

En idéntica dirección apunta el citado pronunciamiento del Superior Tribunal de Justiça de Brasil, que solo admitió apartarse de un laudo pericial mediante otro fundamento técnico idóneo, dotado de método verificable, perito responsable y posibilidad de contradicción.

A esa exigencia de método se anuda el tratamiento de la prueba generada por aparatos automáticos. La STS 184/2018 unificó la doctrina sobre los márgenes de error del cinemómetro y recordó que la lectura de la máquina no es verdad absoluta y debe corregirse por su error, mientras que el Tribunal Constitucional, en la STC 40/2008, estableció que la presunción de veracidad de los registros administrativos es solo iuris tantum y debe poder rebatirse en contradicción.⁴⁰

En el plano de la valoración de un dictamen deficiente, el auto AC135-2023 de la Corte Suprema de Colombia recordó que «la falta de soportes o documentos presentados por el perito es razón insuficiente para dejar de apreciar o rechazar el dictamen» (Corte Suprema de Justicia, 2023, p. 141), aunque advirtió que pierde fuerza demostrativa si no justifica la información empleada, criterio plenamente aplicable a la opacidad de un sistema de inteligencia artificial.⁴¹

c) La contradicción y la idoneidad de quien examina la prueba

³⁷Instrucción 2/2026, de 28 de enero, del Pleno del Consejo General del Poder Judicial de España (BOE-A-2026-2205).

³⁸Superior Tribunal de Justiça (Brasil), 5.^a Turma, HC 1.059.475/SP, rel. min. Reynaldo Soares da Fonseca, decisión divulgada el 8 de abril de 2026 (texto íntegro pendiente de publicación; cf. comunicado oficial del STJ del 8 de abril de 2026).

³⁹Corte Suprema de Justicia de Colombia, Sala de Casación Civil, Agraria y Rural, sentencia SC2154-2025, de 15 de diciembre de 2025; publicada en la Gaceta de Jurisprudencia de la Sala de Casación Civil, 4.º trimestre de 2025.

⁴⁰Tribunal Supremo de España, Sala 2.^a, STS 184/2018, de 17 de abril de 2018 (Pleno), ECLI:ES:TS:2018:1465; y Tribunal Constitucional, STC 40/2008, de 10 de marzo de 2008, ECLI:ES:TC:2008:40.

⁴¹Corte Suprema de Justicia de Colombia, Sala de Casación Civil, auto AC135-2023 (rad. 2022-03805).

Detrás del resultado técnico debe existir una persona idónea que pueda ser interrogada. La Sala Segunda del Tribunal Supremo español, en la STS 300/2015, advirtió que la posibilidad de manipulación forma parte de la realidad de las cosas y que, impugnada la prueba de una comunicación electrónica, esta debe someterse a reconocimiento pericial que verifique su origen, la identidad de los interlocutores y su integridad (Tribunal Supremo, 2015).⁴² La STS 375/2018 matizó después que no existe una presunción de falsedad que deba destruirse siempre con pericial, exigible solo ante indicios reales de manipulación, y que la impugnación de la autenticidad desplaza la carga de la prueba a quien quiere aprovechar el material (Tribunal Supremo, 2018).⁴³

Sobre quién puede ser perito, la Audiencia Nacional, en la sentencia 3266/2024, advirtió que los informes de la UDEF o de la IGAE no equivalen a una pericial informática, que requiere idoneidad específica.⁴⁴

d) La explicabilidad y el acceso al algoritmo

La posibilidad de conocer y escrutar el método algorítmico es condición de la contradicción. Su hito es la sentencia del Tribunal Supremo español de 11 de septiembre de 2025, conocida como caso BOSCO, que reconoció el derecho de acceso al código fuente de un algoritmo público y el deber de la Administración de explicar de forma comprensible su funcionamiento, al subrayar que el sistema adoptaba una decisión de manera automática y con efecto multiplicador de sus errores (Tribunal Supremo, 2025).⁴⁵

En la misma línea, la Corte Constitucional de Colombia, en la Sentencia T-067 de 2025, reconoció el carácter de información pública del código fuente de las aplicaciones estatales y sostuvo que los algoritmos públicos deben ser auditables y poder someterse a escrutinio, lo que contribuye a detectar y prevenir sesgos en las decisiones automatizadas.⁴⁶

e) El deber de verificación frente a las alucinaciones

La responsabilidad de comprobar las salidas de la herramienta es una carga indelegable que no se transfiere al algoritmo. La Corte Suprema de Justicia de Colombia, en la providencia STC17832-2025, concedió la protección constitucional frente a una decisión judicial que se había sustentado en extractos jurisprudenciales inexistentes atribuidos a sentencias reales, y en el auto AC739-2026 sancionó a un abogado que apoyó un recurso extraordinario de revisión en referencias jurisprudenciales apócrifas, al constatar que «se acumularon diez referencias apócrifas... entraña temeridad» (Corte Suprema de Justicia, 2026, p. 77) y recordar que el deber de verificación comprende el control humano efectivo y el contraste con los repositorios oficiales.⁴⁷

⁴²Tribunal Supremo de España, Sala 2.ª, STS 300/2015, de 19 de mayo de 2015, ECLI:ES:TS:2015:2047, ponente Marchena Gómez.

⁴³Tribunal Supremo de España, Sala 2.ª, STS 375/2018, de 19 de julio de 2018, ECLI:ES:TS:2018:2966, ponente Berdugo Gómez de la Torre.

⁴⁴Audiencia Nacional de España, Sala de lo Penal, Sentencia 3266/2024, de 27 de mayo de 2024, ECLI:ES:AN:2024:3266.

⁴⁵Tribunal Supremo de España, Sala 3.ª, sentencia de 11 de septiembre de 2025, rec. cas. 7878/2024, ECLI:ES:TS:2025:3826 (caso BOSCO).

⁴⁶Corte Constitucional de Colombia, Sentencia T-067 de 2025.

⁴⁷Corte Suprema de Justicia de Colombia, Sala de Casación Civil, sentencia STC17832-2025, de 5 de noviembre de 2025, M. P. Adriana Consuelo López Martínez; y auto AC739-2026, de 13 de febrero de 2026, rad. 11001-02-03-000-

El mismo deber se ha hecho valer fuera de Colombia. El Juzgado Civil y Comercial Común de la X Nominación de Tucumán, en «O. F. C. c/ Booking.com Argentina S.R.L.», impuso una multa por temeridad y mala fe a la letrada que fundó su demanda en seis precedentes inexistentes, uno de cuyos enlaces remataba en «source=chatgpt.com». El juzgado razonó que el uso de inteligencia artificial no es reprochable en sí mismo, pero sí lo es la ausencia de control profesional efectivo sobre la veracidad de sus salidas.⁴⁸

Leídos en conjunto, los cinco ejes perfilan un estándar emergente que, sin resolver de manera frontal la pregunta inicial, ofrece una base consistente para admitir la inteligencia artificial como herramienta auxiliar del perito: reserva humana de la valoración, fiabilidad de método verificable, contradicción a cargo de un experto idóneo, explicabilidad del algoritmo y deber indelegable de verificación. Ese estándar, construido sobre materiales dispersos (prueba científica, prueba digital, transparencia algorítmica y alucinaciones), encuentra su prueba de resistencia en un campo donde la totalidad de la prueba es técnica y digital: el de los riesgos cibernéticos.

3.1.3. La aplicación al campo de los riesgos cibernéticos

El marco anterior no constituye un ejercicio meramente teórico. Encuentra su banco de pruebas más exigente en los seguros de riesgos cibernéticos, donde la acreditación del siniestro depende por entero de evidencia técnica y donde la inteligencia artificial ha dejado de ser una hipótesis para convertirse en una herramienta de uso corriente en la investigación forense. En este campo, los frentes de tensión examinados en abstracto (transparencia, fiabilidad, idoneidad y verificación) adquieren contornos concretos, y el estándar de los cinco ejes deja de ser una construcción doctrinal para volverse un criterio operativo.

3.1.3.1.El contexto: la transformación digital y el riesgo cibernético

La transformación digital ha modificado de manera sustancial la forma en que las personas, las empresas y los Estados desarrollan sus actividades. La información, concebida durante décadas como un elemento complementario de la actividad económica, se ha convertido en uno de los principales activos de las organizaciones, hasta el punto de que los datos constituyen el elemento común de las nuevas tecnologías y adquieren especial relevancia cuando permiten identificar o inferir características de una persona (Hernández Batista, 2025, p. 16). La protección de los sistemas que almacenan, procesan y transmiten esa información ha adquirido, en consecuencia, una importancia creciente tanto para los particulares como para el sector asegurador.

En este contexto surgen los denominados riesgos cibernéticos, cuya expansión ha obligado a replantear categorías tradicionales del derecho de seguros. El *phishing*, el *ransomware* y los ataques a la cadena de suministro figuran entre las amenazas más frecuentes para las pequeñas y medianas empresas, muchas de las cuales carecen de medidas de protección adecuadas (El Ferjani et al., 2025). Ello explica el creciente interés de la industria aseguradora por desarrollar coberturas especializadas, en una línea que la OECD (2017) ya había anticipado al señalar que los riesgos

2025-05324-00, que impuso multa de 15 salarios mínimos al abogado que sustentó un recurso extraordinario de revisión en diez referencias jurisprudenciales apócrifas (ocho inexistentes y dos sentencias reales con contenido falseado).

⁴⁸Juzgado Civil y Comercial Común de la X Nominación de Tucumán (Argentina), «O. F. C. c/ Booking.com Argentina S.R.L. y otro s/ daños y perjuicios», Expte. 6937/24, sentencia n.º 0009 de 2 de febrero de 2026, juez Santiago José Peral.

cibernéticos constituyen una de las principales amenazas para la economía digital y que los seguros desempeñan un papel fundamental en su gestión y transferencia.

La relevancia del riesgo cibernético para la industria aseguradora obedece a varios factores. El primero es el incremento significativo de la frecuencia e intensidad de los ataques, tendencia que confirma la proyección de un endurecimiento de las condiciones del mercado asegurador ante la creciente sofisticación de las amenazas y la vulnerabilidad de las infraestructuras críticas (Gallagher, 2025).

El segundo es la magnitud de las pérdidas. El coste medio de una brecha de datos ha llegado a niveles récord (IBM Security, 2024) y el impacto económico global se aproxima al billón de dólares, con daños que trascienden lo estrictamente financiero para comprender afectaciones reputacionales, elevados costes de recuperación tecnológica, interrupción de operaciones y la consecuente pérdida de ingresos y clientes (Ayala Cubillos, 2024).

El mercado afronta, además, dificultades estructurales para comprender y valorar estos riesgos, derivadas de la ausencia de estadísticas históricas suficientes y de la rápida evolución de las amenazas. A ello se suma que asegurados y aseguradoras se enfrentan a un enemigo invisible, cuya identificación suele resultar extremadamente difícil y limita incluso las posibilidades de repetición contra el responsable del daño. La IAIS (2020) ha identificado, en efecto, la escasez de información confiable, la dificultad de evaluar vulnerabilidades específicas y la limitada experiencia histórica como obstáculos centrales para modelar este tipo de riesgos.

El mercado enfrenta, por último, un problema de fragmentación. La falta de estandarización en las definiciones y en el lenguaje de las pólizas genera coberturas concurrentes o ambiguamente delimitadas (*overlapping coverage*). Así ocurre cuando un mismo evento, por ejemplo la extorsión informática, puede quedar cubierto tanto por una póliza específica de cyber como por una de secuestro y rescate (*kidnap & ransom*), o cuando el fraude por ingeniería social concurre con los seguros de infidelidad de empleados o crime (OECD, 2020).

A ese solapamiento se añaden los llamados riesgos silenciosos, esto es, exposiciones en las que la cobertura de eventos cibernéticos no está expresamente incluida ni expresamente excluida en la póliza. El fenómeno se explica porque muchas pólizas tradicionales de daños o de responsabilidad civil fueron diseñadas antes de la existencia de las amenazas digitales masivas, de modo que ni las contemplaban ni las descartaban.

Esta ambigüedad técnica constituye una preocupación crítica para la gestión de la acumulación de riesgos, pues un solo evento catastrófico podría disparar reclamaciones simultáneas en múltiples ramos y generar una severidad imprevista para el capital de las aseguradoras (Saraiva Lima, 2020). De ahí que la tendencia regulatoria actual exija una transición hacia coberturas afirmativas, en las que cada riesgo cibernético se declare de forma clara e inequívoca.

La cuestión adquiere especial importancia porque, desde la perspectiva del derecho de seguros, la ocurrencia del siniestro es el presupuesto del nacimiento de la obligación indemnizatoria. En los seguros tradicionales, la materialización del riesgo suele exteriorizarse mediante daños físicos observables que facilitan esa acreditación.

En materia de riesgos cibernéticos, en cambio, la acreditación de los hechos exige reconstruir eventos digitales complejos que se desarrollan en entornos virtuales, dejan evidencias de naturaleza técnica e involucran con frecuencia a múltiples actores ubicados en distintas jurisdicciones, lo que dificulta la delimitación de la cobertura y la determinación misma del

siniestro (Signorino Barbat, 2022, pp. 231-248). Es precisamente en este punto donde la prueba técnica, y la inteligencia artificial como instrumento de esa prueba, pasan a ocupar el centro del contrato de seguro.

3.1.3.2. Las coberturas en los seguros de riesgos cibernéticos

El riesgo cibernético se entiende técnicamente como la posibilidad de sufrir pérdidas derivadas de eventos que comprometan la confidencialidad, la integridad o la disponibilidad de los sistemas informáticos y de la información. Las pólizas deben estructurarse para cubrir tanto los daños propios, como la pérdida de datos o la extorsión, cuanto la responsabilidad civil frente a terceros derivada de violaciones de privacidad (Saraiva Lima, 2020). Aunque existe una amplia diversidad de productos, el análisis del mercado permite identificar ciertos grupos de coberturas recurrentes (Ariza Vesga, 2022).

Se encuentran, en primer término, las coberturas relacionadas con vulneraciones de datos, que protegen al asegurado frente a los costos derivados del acceso no autorizado a información sensible, incluidos los gastos de mitigación, recuperación y defensa jurídica ante eventuales sanciones. A su turno, aparecen las coberturas asociadas a la interrupción de operaciones y a los gastos extraordinarios de recuperación de datos, aplicables cuando el ataque impide el funcionamiento normal de la organización durante períodos prolongados.

Resultan también frecuentes las coberturas frente a ataques de ransomware o de extorsión informática, que operan cuando un tercero accede a sistemas o datos y exige una contraprestación económica para restablecer el acceso o evitar la divulgación de la información comprometida. Por último, se hallan las coberturas vinculadas a la responsabilidad del asegurado frente a terceros, en especial en escenarios de fraude digital o de daños ocasionados tras la vulneración de información de clientes o proveedores (Ariza Vesga, 2022).

3.1.3.3. Las dificultades probatorias del siniestro cibernético

La prueba del siniestro constituye uno de los elementos más complejos de los seguros cibernéticos, pues la naturaleza digital de los eventos que activan las coberturas genera dificultades que rara vez se presentan en otros ramos. La primera consiste en determinar si efectivamente ocurrió un incidente cubierto, ya que los ataques suelen desarrollarse de manera silenciosa y pueden permanecer ocultos durante largos períodos antes de ser detectados; las dificultades para evaluar vulnerabilidades y la limitada disponibilidad de información confiable, señaladas por la IAIS (2020), se trasladan así al terreno probatorio.

Una segunda dificultad atañe a la identificación de la causa del daño, que puede derivar de manera simultánea de errores humanos, vulnerabilidades tecnológicas, fallas operativas o acciones maliciosas de terceros, de modo que determinar cuál de ellas produjo efectivamente el perjuicio reclamado exige reconstruir la secuencia de acontecimientos que precedieron al siniestro. A esa dificultad técnica se suma la dispersión de las evidencias digitales: los siniestros cibernéticos involucran a menudo a múltiples actores, como proveedores de nube o servicios externos, ubicados en diversas jurisdicciones, lo que añade una capa de complejidad jurídica a la determinación de la cobertura y a la cadena de custodia de las pruebas (Signorino Barbat, 2022).

Un aspecto adicional es la cuantificación de las pérdidas, dado que los daños derivados de incidentes cibernéticos no siempre son inmediatamente visibles ni fácilmente calculables. La valoración económica del siniestro exige metodologías especializadas para analizar la interrupción de operaciones, los costos de restauración y, de manera fundamental, el componente de lost

business, que comprende la fuga inesperada de clientes y las afectaciones severas a la reputación de la marca (OECD, 2020).

Como consecuencia de todo lo anterior, la prueba pericial informática se convierte en una pieza central de la reclamación: el experto debe identificar los hechos relevantes, preservar la evidencia digital, reconstruir la secuencia de eventos y explicar técnicamente la relación entre el incidente y las pérdidas reclamadas. Y es aquí donde la inteligencia artificial ofrece un auxilio difícilmente sustituible.

3.1.3.4. Las soluciones que aporta la inteligencia artificial como prueba técnica

Las dificultades descritas explican por qué la inteligencia artificial ha adquirido relevancia en la investigación de incidentes cibernéticos. Su principal aporte radica en la capacidad de procesar volúmenes masivos de información en tiempos muy inferiores a los de los métodos tradicionales: gracias a su aprendizaje constante, agiliza la identificación de vulnerabilidades, permite analizar con rapidez grandes volúmenes de datos y detectar movimientos sospechosos, anticipando y mitigando posibles ataques (Ayala Cubillos, 2024). En esa misma línea, los modelos de inteligencia artificial mejoran los procesos de detección y respuesta mediante el análisis automatizado de patrones de tráfico y comportamientos anómalos en la red (ENISA, 2023).

El uso de estas herramientas ha dejado de ser opcional. La inteligencia artificial se ha vuelto esencial para optimizar la eficiencia operativa y fortalecer la resiliencia de los servicios financieros, al actuar como una barrera técnica avanzada frente a las amenazas crecientes del cibercrimen (World Economic Forum, 2025).

La necesidad de recurrir a herramientas automatizadas se explica por la propia evolución del riesgo. Frente a unas amenazas cada vez más frecuentes y complejas (El Ferjani et al., 2025), las organizaciones se ven obligadas a producir y almacenar volúmenes crecientes de información técnica para su eventual análisis forense (Kent et al., 2006). La utilidad de la inteligencia artificial se aprecia con nitidez en cuatro frentes que se examinan a continuación, y que conviene leer a la luz del estándar de los cinco ejes, pues cada capacidad técnica reproduce, en el plano forense, una de las exigencias jurídicas ya señaladas.

3.1.3.5. El procesamiento masivo de evidencia digital

A diferencia de otros ramos del seguro, la infraestructura tecnológica moderna produce millones de registros técnicos diarios provenientes de servidores, sistemas de detección de intrusiones, firewalls, aplicaciones empresariales y plataformas de almacenamiento en la nube. Cada ejecución de código malicioso, correo de phishing o transferencia no autorizada genera registros, los llamados logs, que constituyen la base de la informática forense, entendida como la aplicación de métodos científicos para la identificación, recopilación, examen y análisis de datos, preservando su integridad y manteniendo una estricta cadena de custodia (Kent et al., 2006).

Esa saturación de datos, agravada por una asimetría de información en la que las organizaciones suelen ser reacias a revelar la magnitud real de sus brechas, genera un ámbito de enormes incertidumbres (Ríos Insua et al., 2018). Frente a ese desafío, la inteligencia artificial opera como un motor de procesamiento que transforma grandes volúmenes de datos desestructurados en información pericial comprensible.

Ese procesamiento descansa, según Hernández Batista (2025), en tres operaciones fundamentales. La clasificación agrupa la información conforme a patrones identificados en el entrenamiento previo, para distinguir la actividad normal de la maliciosa. El filtrado excluye de manera

automática los registros benignos o irrelevantes, de modo que el experto pueda concentrarse en los eventos de interés. Y la asociación establece relaciones lógicas entre activos de información dispersos en distintos sistemas y momentos, lo que facilita la reconstrucción de la secuencia de acontecimientos.

3.1.3.6.La correlación automática de eventos para reconstruir el siniestro

La dispersión de la evidencia es una de las principales dificultades de la investigación forense, pues los rastros de un mismo incidente rara vez se concentran en un único sistema: un acceso no autorizado puede figurar en los registros de autenticación, mientras la exfiltración de información se refleja en los de tráfico de red, en servidores remotos o en aplicaciones de terceros, lo que obliga a correlacionar datos de múltiples fuentes (Kent et al., 2006). El software de correlación de eventos posee, por ello, un valor significativo para automatizar el análisis (Cichonski et al., 2012).

La inteligencia artificial contribuye a solventar esa dispersión mediante herramientas de gestión de eventos de seguridad y de análisis forense de red. Estas normalizan los registros y, a partir de coincidencias en direcciones IP, nombres de usuario y protocolos, agrupan los eventos individuales en meta-eventos que ofrecen al perito una visión global de la actividad maliciosa.

Para la reconstrucción del siniestro, el sistema emplea las marcas de tiempo de relojes sincronizados mediante el protocolo de tiempo de red, lo que permite construir líneas temporales forenses cronológicamente coherentes. Sobre ellas, los algoritmos identifican secuencias y relaciones entre hechos en apariencia inconexos, como un acceso fallido en un servidor y una exfiltración posterior en una base de datos remota. Estas herramientas no sustituyen el juicio del experto, sino que fortalecen su capacidad de fundamentar técnicamente el nexo causal entre el incidente y las pérdidas reclamadas, reduciendo los tiempos de investigación y el margen de error en la cadena de custodia digital.

3.1.3.7.La detección de anomalías como mecanismo de identificación del siniestro

La detección de anomalías parte de la premisa de que los sistemas informáticos presentan patrones de comportamiento relativamente estables y de que las desviaciones significativas respecto de ellos pueden constituir indicios de actividad maliciosa. El monitoreo de registros y la correlación de eventos contribuyen a identificar incidentes y violaciones de políticas (Kent et al., 2006), y la automatización resulta necesaria para realizar un análisis inicial que seleccione los eventos de interés que luego serán objeto de revisión humana (Cichonski et al., 2012). Bajo esa lógica de aprendizaje, los sistemas construyen modelos de comportamiento normal y generan alertas ante desviaciones estadísticamente significativas (Hernández Batista, 2025).

Dada la prevalencia de ataques de ransomware y phishing (El Ferjani et al., 2025), muchos de los cuales permanecen ocultos durante largos períodos, la inteligencia artificial permite identificar esas anomalías con mayor rapidez y localizar evidencia potencialmente relevante. Con todo, la detección automatizada no constituye por sí misma prueba concluyente de la ocurrencia del siniestro: su función es facilitar la identificación de eventos que después deberán ser verificados y valorados por el experto, quien sigue siendo responsable de la interpretación de la evidencia y de las conclusiones del dictamen.

3.1.3.8.La priorización de la evidencia relevante

La utilidad de la inteligencia artificial en la fase avanzada de la investigación no se limita a identificar datos, sino que se funda en su capacidad de descarte sistemático de información irrelevante. Los procesos de examen forense deben, según la guía oficial, «extraer exclusivamente

los datos de interés, filtrando la información extraña o redundante» (Kent et al., 2006, p. 3), de modo que, de un registro de millones de eventos, el perito pueda concentrarse en los pocos que guardan relación directa con el siniestro.

Mediante algoritmos de jerarquización, los sistemas clasifican los eventos según niveles de criticidad y realizan un análisis inicial que selecciona los de mayor relevancia para la revisión humana, automatizando tareas que tradicionalmente requerían semanas de trabajo manual. Esta priorización asegura que el experto concentre su atención en los elementos con mayor probabilidad de acreditar la ocurrencia del siniestro y la cuantía de las pérdidas, y optimiza la eficiencia de las investigaciones forenses, lo que no solo reduce los tiempos de respuesta, sino que fortalece la resiliencia del sector financiero al proporcionar un soporte técnico robusto y preciso para la resolución de las reclamaciones (World Economic Forum, 2025).

3.1.4. El reencuentro con el estándar: las cuatro capacidades a la luz de los cinco ejes

Las cuatro capacidades descritas confirman que la inteligencia artificial es, en el siniestro cibernético, un auxiliar técnico de enorme valor, pero también reproducen, una a una, las exigencias del estándar jurisprudencial. Conviene mostrar esa correspondencia, porque es la que mantiene unidos el marco general y su aplicación.

El procesamiento masivo y la priorización de evidencia solo son admisibles si los criterios de clasificación y filtrado resultan explicables y trazables. De lo contrario, el descarte automático de millones de registros se convierte en una caja negra que decide, sin control, qué evidencia llega al proceso y cuál se descarta, con la consiguiente lesión del eje de explicabilidad y del derecho de la contraparte a escrutar el método. La correlación automática que reconstruye la secuencia del ataque, a su vez, debe poder reproducirse y auditarse, en los términos del eje de fiabilidad y método verificable, de modo que la línea temporal forense no se acepte por su apariencia técnica, sino por la validez comprobable del procedimiento que la genera.

La detección de anomalías ilustra con particular claridad el eje de la reserva humana: una alerta estadística no prueba el siniestro, sino que ofrece un indicio que el perito debe verificar y valorar, sin que la herramienta pueda desplazar ese juicio. Y la totalidad del proceso queda sujeta al deber indelegable de verificación, que impide al perito, y al asegurador o al juez que reciben su dictamen, descansar en la salida del sistema sin contrastarla.

En suma, las soluciones que la inteligencia artificial ofrece al siniestro cibernético no operan al margen del estándar, sino dentro de él: lo que en el plano general es una exigencia jurídica, en el plano forense es una condición de validez de la prueba.

3.1.5. Reflexiones en torno a la aplicación de la inteligencia artificial en la demostración del siniestro en seguros cibernéticos – Análisis del dictamen pericial elaborado por inteligencia artificial como herramienta demostrativa frente al asegurador

Ningún legislador ni ninguna alta corte iberoamericana ha resuelto todavía, de manera frontal, si puede o no elaborarse un dictamen pericial con inteligencia artificial. La respuesta que se desprende de los pronunciamientos examinados conviene formularla con precisión, porque encierra tres momentos de una misma línea evolutiva que no deben confundirse entre sí.

El primer momento es de imposibilidad actual, pero no por una prohibición tecnológica expresa, sino por la rigidez del régimen probatorio vigente. Hoy un dictamen no puede elaborarse íntegramente con inteligencia artificial, porque el ordenamiento exige un perito que jure,

comparezca, sea recusable y responda, supuestos que un sistema automatizado, por sí solo, no satisface. No es que la ley diga «la inteligencia artificial no puede»; es que la ley está construida sobre exigencias que, tal como están redactadas, la inteligencia artificial no alcanza a cumplir sin intermediación humana.

El segundo momento es de habilitación condicionada. Ese mismo régimen, interpretado por la jurisprudencia comparada, ya admite la inteligencia artificial como herramienta auxiliar del perito, siempre que se respete un estándar que este trabajo ha sistematizado en cinco ejes: la valoración de la prueba y la decisión siguen siendo labor humana indelegable del juez; el dictamen apoyado en inteligencia artificial debe ser transparente en cuanto a su uso, su método y sus datos; debe ser fiable y reproducible, y por ello sometido a los criterios de la prueba científica; debe ser explicable y auditable, de modo que pueda contradecirse; y exige, en todo caso, un perito humano idóneo que asuma la autoría, comparezca y verifique las salidas de la herramienta. El uso auxiliar, por tanto, no solo es posible, sino que ya cuenta con reglas.

El tercer momento es prospectivo, y es donde se sitúa la apuesta de este trabajo. Ese estándar, hoy concebido para gobernar el uso auxiliar de la inteligencia artificial, es precisamente el andamiaje que, una vez consolidado, abrirá la puerta a que en el futuro el dictamen pueda elaborarse con inteligencia artificial en un rol nuclear, y no meramente marginal. Dicho de otro modo, las mismas exigencias que hoy disciplinan a la inteligencia artificial como simple apoyo (explicabilidad, trazabilidad, método verificable, posibilidad de contradicción y verificación humana) son las que, el día en que la técnica permita satisfacerlas de manera autónoma o cuasiautónoma, harán jurídicamente admisible un dictamen de fuente algorítmica. El estándar no es solo un límite presente; es, al mismo tiempo, el cimiento de una admisión futura. No hay contradicción entre afirmar que hoy no se puede y sostener que el camino para que algún día se pueda ya está siendo trazado: lo segundo es consecuencia de lo primero, porque solo un marco de garantías suficientemente exigente puede justificar, llegado el momento, la ampliación del papel de la herramienta.

Estos estándares, contruidos sobre la prueba científica, la prueba digital y la transparencia algorítmica, encuentran en los litigios de seguros un campo de aplicación natural y, en los riesgos cibernéticos, su expresión más exigente. En el derecho de seguros, la acreditación del siniestro y de su cuantía, sea judicial o extrajudicial, es el eje que permite la procedencia del pago indemnizatorio; y dada la naturaleza técnica de las cuestiones aseguradas, contar con un dictamen elaborado con inteligencia artificial, o al menos asistido por ella, reduce los costos que debe asumir el asegurado y puede elevar el grado de convencimiento del asegurador para proceder al pago.

En el caso particular de los riesgos cibernéticos, la prueba del siniestro se desplaza por completo del mundo tangible hacia la reconstrucción de eventos digitales invisibles. La dificultad de acreditar la ocurrencia de un ataque, identificar su origen y cuantificar daños tan complejos como el impacto reputacional o la pérdida de clientes sitúa a la prueba técnica en el corazón del contrato, en un entorno de incertidumbre que los métodos tradicionales de ajuste no alcanzan a cubrir. La inteligencia artificial se ofrece allí como un soporte difícilmente prescindible: su capacidad para procesar millones de registros, filtrar lo irrelevante, detectar anomalías y correlacionar eventos transforma el caos de la evidencia digital en conclusiones técnicas precisas.

El uso de estas herramientas, sin embargo, no es absoluto, y aquí convergen el marco general y su aplicación cibernética. La tecnología identifica correlaciones potentes, pero carece de la

sensibilidad para determinar la causalidad jurídica o para valorar las consecuencias de una decisión.

Por ello, tanto en el plano de los principios como en el de la práctica forense del siniestro cibernético, la intervención del experto humano sigue siendo el pilar que garantiza que la inteligencia artificial opere como una aliada del análisis probatorio, y no como un sustituto del juicio que el ordenamiento reserva, de manera indelegable, a las personas. En ese equilibrio, una herramienta cada vez más capaz, gobernada por un estándar cada vez más preciso, se juega el futuro del dictamen pericial en la era de la inteligencia artificial.

4. Conclusiones

El recorrido realizado a lo largo de este artículo permite formular tres conclusiones que, leídas en conjunto, revelan la unidad de fondo de un análisis que se desarrolló en tres planos distintos.

La primera conclusión surge del mapeo regulatorio. Brasil, Colombia y Argentina han incorporado la inteligencia artificial a sus sistemas judiciales con intensidades y focos distintos, pero sobre una base común: la preservación de la centralidad del juez humano y la supervisión efectiva de las decisiones automatizadas. Esa convergencia no es una coincidencia de políticas públicas, sino el reflejo de una convicción compartida: la eficiencia que ofrece la tecnología solo es legítima si no compromete las garantías procesales fundamentales. Para el sector asegurador, que opera en esas mismas jurisdicciones y que es uno de los principales protagonistas de la litigiosidad regional, ese principio no es un dato externo sino el marco dentro del cual debe diseñar su propia relación con la inteligencia artificial.

La segunda conclusión emerge del análisis de la industria aseguradora. La inteligencia artificial ofrece a las aseguradoras una oportunidad real de transformar documentos dispersos en conocimiento estructurado, de convertir detecciones ocasionales de fraude en políticas preventivas sistemáticas y de gestionar el riesgo judicial con mayor información y trazabilidad. Pero esa oportunidad solo se materializa si la implementación descansa en principios claros de gobernanza: objetivos bien definidos, permisos mínimos, puntos de interrupción obligatoria, supervisión humana efectiva y registros auditables de lo actuado. Sin esos controles, la misma herramienta que promete eficiencia puede producir decisiones opacas, incentivos incorrectos o daños difíciles de reparar.

La tercera conclusión articula los dos planos anteriores con el análisis procesal. Los principios de gobernanza que deben regir el uso interno de la IA en las aseguradoras y los estándares que la jurisprudencia comparada ha ido decantando para admitir el dictamen pericial asistido por inteligencia artificial no son dos conjuntos de exigencias paralelas: son, en esencia, el mismo conjunto visto desde ángulos distintos. La trazabilidad, la explicabilidad, la supervisión humana y la responsabilidad institucional que una buena práctica de implementación exige puertas adentro de la compañía son exactamente las condiciones que el ordenamiento procesal impone para que los resultados de esas herramientas tengan valor probatorio en el proceso. Los seguros cibernéticos ilustran esa correspondencia con particular claridad, porque en ese ramo la frontera entre la gestión interna del siniestro y su acreditación judicial es especialmente delgada: la misma herramienta que reconstruye el ataque para decidir si se paga la indemnización es, frecuentemente, la misma que deberá sustentar el dictamen pericial si la decisión se judicializa.

El desafío común para las aseguradoras y para los sistemas jurídicos latinoamericanos no consiste, por tanto, en decidir si adoptar o rechazar la inteligencia artificial. Esa decisión, en la práctica, ya está tomada. El desafío real consiste en construir los marcos de gobernanza, los estándares procesales y las culturas institucionales que permitan aprovechar el potencial de estas herramientas sin sacrificar la transparencia, la trazabilidad y la confianza que tanto el contrato de seguro como el proceso judicial requieren para funcionar.

Bibliografía

- Ariza Vesga, R. A. (2022). Nuevas perspectivas del uso de la tecnología en el ámbito del contrato de seguro. *Revista Ibero-Latinoamericana de Seguros*, 31(57), 13-48. <https://doi.org/10.11144/Javeriana.ris57.nput>
- Ayala Cubillos, L. P. (2024). Riesgos cibernéticos: desafío para las aseguradoras. *Revista Fasecolda*, 92-97.
- Calderón Ortega, M. A., y Cueto Calderón, C. A. (2022). Prueba por inteligencia artificial: una propuesta de producción probatoria desde el dictamen pericial científico en Colombia. *Civilizar: Ciencias Sociales y Humanas*, 22(42). <http://www.scielo.org.co/pdf/ccso/v22n42/2619-189X-ccso-22-42-e20220106.pdf>
- Cantos Pardo, M. (2024). La algoritmización del dictamen pericial: ¿puerta de entrada para la aparición del «perito-robot»? *Actualidad Jurídica Iberoamericana*, (21).
- Cichonski, P., Millar, T., Grance, T., y Scarfone, K. (2012). Computer security incident handling guide (NIST Special Publication 800-61 Rev. 2). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-61r2>
- El Ferjani, I., Alcañiz Zanón, M., y Santolino Prieto, M. (2025). Ciberseguridad en pequeñas y medianas empresas: vulnerabilidades, amenazas y desarrollo del ciberseguro. *Anales del Instituto de Actuarios Españoles*, 4.^a Época(31), 1-18. https://doi.org/10.26360/2025_01
- European Insurance and Occupational Pensions Authority. (2019). Cyber risk for insurers: Challenges and opportunities. EIOPA.
- European Union Agency for Cybersecurity. (2023). Cyber insurance: Models and methods and the use of artificial intelligence. ENISA. <https://www.enisa.europa.eu/publications/cyber-insurance-models-and-methods-and-the-use-of-ai>
- Gallagher. (2025). 2026 cyber insurance market outlook. <https://www.ajg.com/-/media/files/gallagher/us/news-and-insights/2025/2026-cyber-insurance-market-outlook.pdf>
- Hernández Batista, I. (2025). IA y privacidad: su problemática en el sector de los seguros [Tesis doctoral, Universitat Rovira i Virgili].
- IBM Security. (2024). Cost of a data breach report 2024. IBM Corporation. <https://www.ibm.com/forms/mkt-whitepaper-16381>
- International Association of Insurance Supervisors. (2020). Cyber risk underwriting: Identified challenges and supervisory considerations for sustainable market development. IAIS.

- Kent, K., Chevalier, S., Grance, T., y Dang, H. (2006). Guide to integrating forensic techniques into incident response (NIST SP 800-86). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-86>
- National Association of Insurance Commissioners. (2020). Report on the cybersecurity insurance and identity theft coverage supplement. NAIC.
- Organisation for Economic Co-operation and Development. (2017). Enhancing the role of insurance in cyber risk management. OECD Publishing. <https://doi.org/10.1787/9789264282148-en>
- Organisation for Economic Co-operation and Development. (2020). Encouraging clarity in cyber insurance coverage: The role of public policy and regulation. OECD Publishing.
- Ríos Insua, D., Couce-Vieira, A., y Musaraj, K. (2018). Some risk analysis problems in cyber insurance economics. *Estudios de Economía Aplicada*, 36(1), 181-194.
- Saraiva Lima, H. J. M. (2020). Seguros cibernéticos. *Revista Ibero-Latinoamericana de Seguros*, 29(53), 161-172. <https://doi.org/10.11144/Javeriana.ris53.seci>
- Signorino Barbat, A. (2022). Los seguros cibernéticos: alcance frente a los ciber riesgos. *Revista Ibero-Latinoamericana de Seguros*, 31(57), 231-248. <https://doi.org/10.11144/Javeriana.ris57.scaf>
- Taruffo, M. (2005). Conocimiento científico y estándares de prueba judicial. *Boletín Mexicano de Derecho Comparado*, (114). UNAM. <https://classic.scielo.org.mx/pdf/bmdc/v38n114/v38n114a13.pdf>
- World Economic Forum. (2025). Artificial intelligence in financial services (2025). World Economic Forum. https://reports.weforum.org/docs/WEF_Artificial_Intelligence_in_Financial_Services_2025.pdf

Providencias y normas citadas

- Audiencia Nacional. (2024). Sentencia 3266/2024, de 27 de mayo (ECLI:ES:AN:2024:3266). Sala de lo Penal.
- Consejo General del Poder Judicial. (2026). Instrucción 2/2026, de 28 de enero. Boletín Oficial del Estado (BOE-A-2026-2205).
- Corte Constitucional. (2024). Sentencia T-323 de 2024.
- Corte Constitucional. (2025). Sentencia T-067 de 2025.
- Corte Suprema de Justicia. (2023). Auto AC135-2023 (rad. 2022-03805). Sala de Casación Civil.
- Corte Suprema de Justicia. (2025). Sentencia SC2154-2025, de 15 de diciembre. Sala de Casación Civil, Agraria y Rural.
- Corte Suprema de Justicia. (2025). Sentencia STC17832-2025, de 5 de noviembre (M. P. Adriana Consuelo López Martínez). Sala de Casación Civil.

Corte Suprema de Justicia. (2026). Auto AC739-2026, de 13 de febrero (rad. 11001-02-03-000-2025-05324-00). Sala de Casación Civil.

Juzgado Civil y Comercial Común de la X Nominación de Tucumán. (2026). O. F. C. c/ Booking.com Argentina S.R.L. y otro s/ daños y perjuicios (Expte. 6937/24, sentencia n.º 0009, de 2 de febrero; juez Santiago José Peral). Tucumán, Argentina.

Superior Tribunal de Justiça. (2026). Habeas Corpus n.º 1.059.475/SP (5.ª Turma, rel. min. Reynaldo Soares da Fonseca; decisión divulgada el 8 de abril de 2026; texto íntegro pendiente de publicación). Brasil.

Tribunal Constitucional. (2008). STC 40/2008, de 10 de marzo (ECLI:ES:TC:2008:40).

Tribunal Supremo. (2015). STS 300/2015, de 19 de mayo (ECLI:ES:TS:2015:2047). Sala Segunda.

Tribunal Supremo. (2018). STS 184/2018, de 17 de abril (ECLI:ES:TS:2018:1465). Sala Segunda.

Tribunal Supremo. (2018). STS 375/2018, de 19 de julio (ECLI:ES:TS:2018:2966). Sala Segunda.

Tribunal Supremo. (2025). Sentencia de 11 de septiembre de 2025, rec. cas. 7878/2024 (ECLI:ES:TS:2025:3826), caso BOSCO. Sala Tercera.

Anexo I

Cuadro comparativo de la prueba pericial en diez ordenamientos iberoamericanos

El cuadro sintetiza, para cada ordenamiento, el modelo de designación del perito, la base normativa del deber de imparcialidad y de la objeción o recusación, el objeto admisible del dictamen y el criterio de valoración. Las referencias normativas corresponden a la legislación procesal civil general de cada país; en algunos ordenamientos coexisten regímenes especiales (penal, contencioso-administrativo) con reglas propias. Se trata de un mapa normativo de base, no de un análisis jurisprudencial, y su función es respaldar el alcance del barrido comparado descrito en el apartado II.

Ordenamiento	Modelo de designación	Imparcialidad y objeción / recusación	Objeto del dictamen
Colombia	Perito de parte (CGP, arts. 226-235)	Deber de imparcialidad y juramento; contradicción en audiencia e interrogatorio del perito (arts. 226, 228)	Hechos técnicos, científicos o artísticos; no cuestiones de derecho salvo derecho o costumbre extranjeros
Brasil	Perito judicial (CPC, arts. 464-480); admite asistentes técnicos de parte	Perito designado por el juez, sujeto a impedimento y sospecha; asistentes técnicos no recusables	Hechos que dependen de conocimiento técnico o científico (art. 464)
Argentina	Perito judicial (CPCCN, arts. 457-478); consultor técnico de parte	Perito único de oficio recusable por causales legales; consultor técnico de cada parte	Conocimiento especial en ciencia, arte, industria o actividad técnica (art. 457)
España	Perito de parte (LEC, arts. 335-352); posibilidad de designación judicial	Deber de objetividad con manifestación de tacha (art. 335.2); recusación del perito judicial y tacha del de parte	Conocimientos científicos, artísticos, técnicos o prácticos (art. 335)
Portugal	Perito judicial (CPC, arts. 467-489); posible perito de parte o colegial	Perito nombrado por el tribunal sujeto a recusación; compromiso de honor	Percepción o apreciación de hechos que exigen conocimientos especiales (art. 388 CC)

Ordenamiento	Modelo de designación	Imparcialidad y objeción / recusación	Objeto del dictamen
México	Mixto: perito de parte con tercero en discordia designado por el juez (CNPCF, arts. 300-307)	Peritos de parte que acreditan idoneidad; perito tercero designado de listas oficiales; recusación del tercero	Conocimientos especiales en ciencia, arte, técnica u oficio; se desecha sobre cuestiones de derecho o hechos notorios
Ecuador	Mixto: perito de parte si hay acceso al objeto; designación judicial por sorteo si no lo hay (COGEP, arts. 221-228)	Peritos acreditados ante el Consejo de la Judicatura; comparecencia obligatoria y sustentación oral; no recusables, pero sin valor si hay inhabilidad comprobada	Hechos o circunstancias relacionados con la materia, no cuestiones jurídicas (art. 221)
Chile	Perito judicial (CPC, arts. 409-425); informe de peritos	Perito designado por el tribunal o por acuerdo de partes; causales de inhabilidad	Puntos de hecho para cuya apreciación se requieren conocimientos especiales de una ciencia o arte
Perú	Perito judicial (CPC, arts. 262-271); admite perito de parte	Peritos nombrados por el juez, sujetos a tacha; perito de parte como observador	Apreciación de hechos que requieren conocimientos especiales de naturaleza científica, tecnológica, artística u otra
Uruguay	Perito judicial (CGP, arts. 177-185); posibles peritos de parte	Perito designado por el tribunal, recusable; las partes pueden proponer puntos y observaciones	Hechos que requieren conocimientos especiales, ajenos al derecho nacional

Fuente: elaboración propia a partir de la legislación procesal civil vigente en cada ordenamiento (véase la nota 2 del texto). El cuadro refleja el régimen general de la prueba pericial y no agota los regímenes especiales ni las reformas en trámite a la fecha de cierre de este trabajo.

