

Gobernanza algorítmica en el sector asegurador: protección del consumidor financiero y estabilidad del mercado

Autores: Luisa Herrera, Maribel Sandoval, Laura Lucía Cagua Gamboa, Juan Miguel Tofiño Hurtado, Juan David Vergara Melo, Carlos Andrés Rodríguez Herrán, Juan Camilo Castaño Buitrago, Benjamin Chong-Castillo y William Alexander López Sandoval¹.

Síntesis: Andrea Signorino Barbat²

Con gran gusto y honor, pasaré a redactar una síntesis del importante artículo desarrollado por el Grupo de trabajo de Nuevas Tecnologías, Prevención y Seguros de ACOLDESE (sección

¹ 1. Luisa Fernanda Herrera Sierra. Abogada de la Universidad Externado de Colombia, Candidata a doctorado de Queen Mary University of London, LL.M. en Derecho de la Propiedad Intelectual y candidata a doctora en Derecho (PhD in Law) por Queen Mary University of London. Senior Managing Partner de G Herrera Abogados & Asociados, Vice-Chair del Grupo de Trabajo de Nuevas Tecnologías, Prevención y Seguros de AIDA Mundial y docente del Departamento de Riesgos y Seguros de la Universidad Externado de Colombia.

2. Maribel Sandoval Varón. Abogada de la Universidad del Rosario. Actualmente se desempeña como consultora del sector asegurador, enfocada en la articulación entre regulación, innovación tecnológica y prácticas de cumplimiento para la transformación digital de la industria. Especialista en Derecho de Seguros por la Pontificia Universidad Javeriana, especialista en Derecho del Seguro por la Universidad de Salamanca y con Maestría en Derecho Informático y Nuevas Tecnologías de la Universidad Externado de Colombia. Correo electrónico: maribel.sandoval@gmail.com.

3. Laura Lucía Cagua Gamboa. Doctora en Derecho por la Università di Roma Tor Vergata y por la Universidad Externado de Colombia. Correo electrónico: lauraluciagagua@gmail.com.

4. Juan Miguel Tofiño Hurtado. Especialista en Seguros por la Universidad Externado de Colombia. Correo electrónico: cyberjurista@hotmail.com.

5. Juan David Vergara Melo. Abogado, especialista en Derecho de las Fintech por la Universidad Externado de Colombia y candidato a magíster en Derecho y Economía por la Universidad de Buenos Aires, Argentina. Correo electrónico: juandavidvergaramelo@outlook.com.

6. Carlos Andrés Rodríguez Herrán. Especialista en Responsabilidad Civil y del Estado por la Universidad de La Sabana y especialista en Derecho de Seguros por la Pontificia Universidad Javeriana. Correo electrónico: catoli2011@hotmail.com.

7. Juan Camilo Castaño Buitrago. Especialista en Responsabilidad y Daño Resarcible por la Universidad Externado de Colombia y especialista en Derecho de Seguros por la Pontificia Universidad Javeriana. Correo electrónico: jccbuitrago@gmail.com.

8. Benjamin Chong-Castillo. Especialista en Derecho de Seguros por la Universidad de Salamanca y candidato a magíster en Derecho Comercial y Financiero por la Universidad Santo Tomás. Miembro de AIDA, Sección Colombia. Correo electrónico: benjaminchongcastillo@gmail.com.

9. William Alexander López Sandoval. Magíster en Derecho de Seguros por la Pontificia Universidad Javeriana. Correo electrónico: William_lopez@javeriana.edu.co.

² **Andrea Signorino Barbat.** Doctora (PhD) en Derecho Privado por la Universidad de Salamanca, España, y doctora en Derecho y Ciencias Sociales por la Universidad de la República Oriental del Uruguay. Directora académica del Postgrado Internacional en Derecho de Seguros de la Universidad de Montevideo. Presidenta del Grupo de Trabajo de Nuevas Tecnologías, Prevención y Seguros de AIDA Mundial y CILA, miembro del Comité Ejecutivo de AIDA Mundial y expresidenta de CILA. Especialista en Derecho de Seguros y Reaseguros, autora de diversas publicaciones académicas en la materia. Correo electrónico: andreassignorino@gmail.com.

colombiana de AIDA) como aporte al homónimo Grupo internacional de trabajo de CILA bajo mi dirección.

El mismo analiza el creciente uso de sistemas de inteligencia artificial (IA) y herramientas automatizadas en el sector asegurador, destacando su impacto a lo largo de toda la cadena de valor del seguro, desde el diseño de productos y la suscripción de riesgos hasta la gestión de siniestros y la detección de fraude. Estas tecnologías ofrecen beneficios significativos en términos de eficiencia, reducción de costos, personalización de servicios y mejora en la evaluación del riesgo. Sin embargo, también introducen riesgos relevantes de carácter jurídico, técnico y organizacional, especialmente cuando las decisiones automatizadas afectan derechos del consumidor financiero, como el acceso al seguro, la determinación de primas o la resolución de reclamaciones.

El texto propone abordar estos desafíos a través del concepto de gobernanza algorítmica, entendido como un marco amplio que incluye tanto sistemas de inteligencia artificial como otros sistemas automatizados avanzados que intervienen en la toma de decisiones. Este enfoque trasciende lo meramente tecnológico o normativo, al plantear la necesidad de una arquitectura integral de control que combine principios jurídicos, estándares técnicos, políticas organizacionales, mecanismos de supervisión humana, al igual que herramientas de gestión del riesgo.

Uno de los aportes centrales del artículo es caracterizar los riesgos algorítmicos —tales que sesgos, errores y fallas— como riesgos estructurales, por su carácter sistemático, escalable y, en muchos casos, opaco. Estos riesgos pueden reproducirse masivamente afectando a grandes grupos de consumidores, lo que exige un enfoque preventivo, no únicamente correctivo. En el ámbito asegurador, la dificultad radica en distinguir entre la legítima segmentación del riesgo (propia de la técnica actuarial) y prácticas discriminatorias derivadas del uso de variables proxy o datos sesgados.

El artículo desarrolla un enfoque multinivel de regulación, que articula distintos niveles: internacional, transversal, sectorial, organizacional, técnico. Cada uno cumple una función específica dentro del sistema de gobernanza, desde la formulación de principios globales hasta la implementación de políticas internas y estándares operativos. Este enfoque reconoce la complejidad del ecosistema digital así como la necesidad de coordinación entre reguladores, supervisores, aseguradoras y proveedores tecnológicos.

En este marco, se identifican principios fundamentales de la gobernanza algorítmica, tales como:

- Transparencia y explicabilidad, que permiten comprender el funcionamiento y los efectos de los sistemas;
- No discriminación, para evitar impactos adversos sobre grupos vulnerables.
- Trazabilidad y auditabilidad, que posibilitan reconstruir decisiones automatizadas.
- Seguridad y robustez, frente a fallas técnicas y riesgos cibernéticos.
- Supervisión humana significativa, que garantice control efectivo sobre las decisiones.
- Responsabilidad (accountability), que asegure la imputación jurídica de los resultados.
- Proporcionalidad, que adapte las exigencias regulatorias al nivel de riesgo del sistema.

El análisis se extiende a la incidencia concreta de estos sistemas en el contrato de seguro, evidenciando cómo la automatización transforma la relación entre asegurador y asegurado. En particular, se destacan riesgos como la discriminación indirecta en la suscripción, el perfilamiento excesivo basado en grandes volúmenes de datos, la hiperpersonalización que puede debilitar el principio mutualista del seguro. Asimismo, se identifican retos en la gestión de siniestros, donde decisiones automatizadas pueden dificultar la comprensión e impugnación por parte del asegurado.

El artículo también aborda la dimensión organizacional, señalando que la incorporación de IA redefine la estructura de gobierno corporativo de las aseguradoras, al introducir nuevos riesgos relacionados con la opacidad de los modelos, la dependencia de proveedores tecnológicos y la

ciberseguridad. En este contexto, la gobernanza algorítmica se convierte en un elemento clave para garantizar la estabilidad operativa, el cumplimiento normativo y la confianza en el mercado.

Finalmente, se proponen estándares mínimos de gobernanza, como la implementación de evaluaciones de impacto, auditorías periódicas de sesgos, mecanismos de supervisión humana, obligaciones de información al consumidor y sistemas robustos de trazabilidad. Estas medidas buscan equilibrar el desarrollo tecnológico con la protección de los derechos del consumidor financiero y la preservación de la estabilidad del sistema asegurador.

En conclusión, el artículo sostiene que la gobernanza algorítmica no es un complemento opcional, sino una condición estructural para el funcionamiento del sector asegurador en la era digital. Solo mediante una arquitectura integral y multinivel es posible aprovechar los beneficios de la inteligencia artificial sin comprometer la equidad, la transparencia y la confianza en el mercado.

Sin dudas, el presente trabajo resulta en un aporte excepcional para la debida gobernanza en el sector asegurador en el contexto de la revolución tecnológica, sector que no debe descuidar sino defender su mayor activo que es el asegurado, pues sin asegurados debidamente atendidos la industria de seguros no tiene sentido de existir.

Dra Andrea Signorino Barbat

Presidente del Grupo de trabajo de CILA Nuevas tecnologías, prevención y seguros

INTRODUCCIÓN

El uso de sistemas de inteligencia artificial y de herramientas automatizadas avanzadas se ha extendido progresivamente en la industria aseguradora, impactando distintas fases de la actividad: desde el diseño y distribución de productos, la suscripción y tarificación de riesgos, hasta la administración de pólizas, la gestión de siniestros y la detección de fraude. (Eling & Lehmann,

2018; Owens et al., 2022; Revista Ibero-Latinoamericana de Seguros, 2025). Lo anterior, permite optimizar procesos, mejorar la evaluación del riesgo, reducir costos operativos, detectar fraudes y prestar un servicio más eficiente. (EIOPA, 2021; McKinsey & Company, 2025; Kennedys, 2025; Bhattacharya et al., 2025).

De la mano de dicha incorporación, sobrevienen riesgos jurídicos, técnicos y organizaciones relevantes, específicamente cuando las decisiones automatizadas inciden en el acceso al seguro, la determinación de la prima, la configuración de coberturas, la gestión del siniestro o la explicación de decisiones adversas para el asegurado. (EIOPA, 2021; EIOPA, 2025; NAIC, 2023; Eling et al., 2022).

Entre dichos riesgos se encuentran la opacidad decisional, los sesgos algorítmicos, el uso de variables indirectas potencialmente discriminatorias, la dificultad de trazabilidad, la afectación de la transparencia contractual, la fragmentación de la cadena de valor mediante terceros tecnológicos y el debilitamiento de la capacidad de supervisión. (Szlajen, 2025; Toreini et al., 2022; FSB, 2025; IAIS, 2025)

Bajo ese contexto, el artículo se dividirá en tres partes, en primer lugar, se aborda la gobernanza algorítmica en el sector asegurador desde un enfoque multinivel de regulación, identificando los principales riesgos estructurales asociados a sesgos, errores, fallas, opacidad y falta de trazabilidad. En un segundo punto, se analiza la incidencia de los sistemas algorítmicos en la cadena de valor del contrato de seguro, especialmente en la suscripción, tarificación, diseño de productos, gestión de siniestros, detección de fraude y deberes de información frente al consumidor financiero. En una tercera parte, desde la perspectiva organizacional, se estudiará la gobernanza algorítmica incluyendo sus sistemas internos de gestión de inteligencia artificial, control de riesgos, subcontratación tecnológica, ciberseguridad algorítmica, supervisión humana y deberes de diligencia tecnológica.

Por último, y con un criterio propositivo, se plantearán principios y estándares mínimos de gobernanza algorítmica (noción que será definida posteriormente) que contribuyan a una utilización responsable de la inteligencia artificial y de los sistemas automatizados en seguros, fortaleciendo la transparencia, explicabilidad, no discriminación, auditabilidad, seguridad, supervisión humana y rendición de cuentas como condiciones necesarias para proteger al asegurado y preservar la estabilidad del mercado. (OECD, 2019; UNESCO, 2021; NIST, 2023; EIOPA, 2025).

CAPÍTULO I

GOBERNANZA ALGORÍTMICA EN EL SECTOR ASEGURADOR: DESDE UN ENFOQUE MULTINIVEL DE REGULACIÓN

La introducción de esta obra definió la gobernanza algorítmica como una categoría comprensiva, que incluye tanto los sistemas de inteligencia artificial en sentido estricto como los sistemas automatizados avanzados que, sin capacidades de aprendizaje, operan con un grado relevante de autonomía decisional en la actividad aseguradora. Este capítulo ofrece el marco conceptual y regulatorio sobre el que se proyectarán el contrato de seguro (Capítulo II) y la organización del asegurador (Capítulo III). Su tesis es que la gobernanza algorítmica en el sector asegurador no debe entenderse como un conjunto accesorio de buenas prácticas tecnológicas, sino como una arquitectura regulatoria, técnica y organizacional necesaria para prevenir que los sesgos, errores, fallas, opacidades, dependencias tecnológicas y riesgos sistémicos derivados de la automatización afecten al consumidor financiero y comprometan la estabilidad del mercado asegurador.

Esa arquitectura integra dos dimensiones inseparables: la *gobernanza de algoritmos* -las reglas, controles y estándares sobre el diseño, entrenamiento, validación, implementación y monitoreo de los sistemas-, y la *gobernanza por algoritmos* -el modo en que estos participan en decisiones sobre

consumidores, contratos, precios, coberturas y reclamaciones- . La IA generativa añade un riesgo diferencial, pues aun sin adoptar la decisión puede condicionar el juicio humano con resúmenes o borradores cuyo contenido jurídico o técnico solo sean sólidos en apariencia; sus salidas no validadas no deben emplearse para negar, limitar o condicionar derechos del asegurado. De ahí que la intervención humana significativa exija perfiles idóneos —técnicos, actuariales, jurídicos y comerciales— en todo el ciclo de vida del sistema, y que en Colombia el análisis se lea a la luz del régimen de protección al consumidor financiero de la Ley 1328 de 2009.

1. Sesgos, errores y fallas en sistemas automatizados como riesgo estructural

Cuando un sistema automatizado determina quién accede a una cobertura, a qué precio, bajo qué condiciones y si procede una indemnización, sus sesgos, errores y fallas dejan de ser incidencias técnicas y se convierten en un *riesgo estructural*, derivado del propio modo de operar de la tecnología en la cadena de valor del seguro. Los sesgos pueden originarse en los datos de entrenamiento, en variables proxy correlacionadas con categorías protegidas o en su uso fuera de contexto, y tienden a reproducirse de forma estable sobre colectivos amplios (NIST, 2023, Sección 3); por ello, distinguir la segmentación actuarial legítima de la discriminación algorítmica indebida es uno de los desafíos centrales de la gobernanza. Los errores incluyen desajustes entre el modelo y la realidad y la degradación del desempeño en el tiempo (*model drift*); las fallas van desde interrupciones operativas hasta la manipulación adversarial y la información incorrecta producida por sistemas generativos, agravadas por la opacidad de la “caja negra”. Su carácter sistemático, escalable y opaco exige una arquitectura preventiva, y no solo correctiva. Y como los sistemas sin capacidad de aprendizaje pueden producir efectos equivalentes, el perímetro de la gobernanza algorítmica debe construirse en función del impacto de las decisiones automatizadas sobre el consumidor y el mercado, y no de la etiqueta tecnológica que se adscriba al sistema.

2. La gobernanza algorítmica como necesidad estructural del sector asegurador

La gobernanza algorítmica es, así, una exigencia estructural del sector, con un doble fundamento: el seguro es una actividad de interés público, sometida a autorización, regulación y supervisión, y sus decisiones más sensibles —suscripción, tarificación, gestión de siniestros, detección de fraude— dependen cada vez más de sistemas cuya lógica no siempre es comprensible ni revisable. Ofrece un marco común para alinear tres planos: la relación contractual entre asegurador y asegurado, regida por la buena fe, la transparencia y el equilibrio económico; la organización interna del asegurador, con responsabilidades indelegables aun cuando los sistemas sean provistos por terceros; y la supervisión sectorial. Frente a la dispersión normativa, opera como categoría integradora que articula los regímenes existentes sin sustituirlos. Por la naturaleza transversal y sistémica de los riesgos que atiende, requiere un enfoque multinivel.

3. Enfoque multinivel de regulación y su interacción funcional

Los organismos internacionales y supervisores sectoriales convergen en arquitecturas que combinan normas vinculantes, estándares técnicos y *soft law* según el nivel de riesgo (FSB, 2024; IAIS, 2025; EIOPA, 2025; OECD, 2025). Se distinguen cinco niveles. El *internacional y de soft law* reúne los principios de la OCDE, la UNESCO y la IAIS y los pronunciamientos de EIOPA, que fijan un lenguaje técnico-normativo común. El *transversal de regulación dura* comprende normas generales como el Reglamento (UE) 2024/1689, que califica de alto riesgo los sistemas de evaluación de riesgos y fijación de precios en seguros de vida y salud; en Colombia, la Ley 1581 de 2012, la Ley 1266 de 2008 y el proyecto de ley de IA con enfoque basado en riesgos (Proyecto de Ley 043 de 2025 Senado / 324 de 2025 Cámara; cf. CONPES 4144, 2025). El *sectorial* regula el seguro como actividad de interés público: en Colombia, los artículos 335 y 150, numeral 19,

literal d, de la Constitución Política, la Ley 1328 de 2009 y la regulación de la Superintendencia Financiera, cuya Circular Básica Jurídica (Circular Externa 006 de 2025) ofrece un anclaje en ciberseguridad e inteligencia artificial, aunque no un régimen integral de supervisión algorítmica (EIOPA, 2025; IAIS, 2025; NAIC, 2023). El *organizacional* abarca las políticas, el gobierno corporativo, los controles internos y la gestión de proveedores de cada asegurador, y es objeto principal del Capítulo III. El *técnico y de estandarización* traduce los principios en requisitos verificables mediante el AI Risk Management Framework del NIST y la norma ISO/IEC 42001:2023 (NIST, 2023; ISO/IEC, 2023).

La interacción entre estos niveles no es jerárquica, sino funcional: cualquiera de ellos, desarrollado aisladamente, pierde eficacia protectora. De ello se sigue una distribución funcional de responsabilidades: al regulador le corresponde el marco general; al supervisor, su aplicación y verificación; al asegurador, su implementación proporcional; y a los proveedores tecnológicos, obligaciones acordes con su rol efectivo en la decisión automatizada.

4. Principios transversales de la gobernanza algorítmica

El enfoque multinivel se vuelve operativo mediante principios transversales. La *transparencia y explicabilidad* exigen informar de forma clara sobre la presencia del sistema, su rol y los factores principales del resultado, con explicaciones fieles a su funcionamiento real, para que el asegurado pueda controvertir la decisión y el supervisor evaluarla. La *no discriminación y equidad* admiten diferenciar riesgos con factores actuariales legítimos, pero no reproducir desigualdades mediante variables proxy ni excluir sistemáticamente a grupos vulnerables, lo que exige controles *ex ante* y *ex post* (NAIC, 2023; Cole & McCullough, 2021; cf. EIOPA, 2025). La *trazabilidad y auditabilidad* requieren registros sobre datos, parámetros, versiones, decisiones y cambios que

permitan reconstruir y auditar cada decisión conforme a estándares verificables (ISO/IEC, 2023; NIST, 2023). La *seguridad y robustez* aseguran un funcionamiento estable, resistente a ataques y con continuidad operativa. La *supervisión humana*, graduada según el impacto, preserva la atribuibilidad de la decisión y la posibilidad de corregirla. La *responsabilidad o accountability* imputa a actores determinados el deber de responder: el asegurador conserva un núcleo indelegable, sin perjuicio de la responsabilidad de desarrolladores y proveedores. La *proporcionalidad* modula las exigencias según la criticidad del sistema, su impacto, la sensibilidad de los datos y la autonomía decisional, sin desincentivar la innovación. Estos principios son interdependientes: la transparencia es condición de la rendición de cuentas; la trazabilidad, de la auditabilidad; la supervisión humana, de la efectividad de la responsabilidad; y la proporcionalidad, del balance entre todos ellos.

5. Interoperabilidad, automatización, analítica avanzada y riesgos estructurales/sistémicos asociados

Estos principios se aplican en entornos interoperables, automatizados a escala y basados en analítica avanzada, donde una decisión defectuosa puede afectar a miles de consumidores antes de ser advertida y la capacidad predictiva crece junto con la opacidad. De ello emergen riesgos estructurales y sistémicos: la concentración tecnológica en pocos proveedores críticos (FSB, 2024, 2025); la homogeneización de modelos, que en escenarios de estrés puede generar respuestas procíclicas (FSB, 2024; BIS, 2025); la fragmentación del mutualismo por hiperpersonalización; la manipulación adversarial y el envenenamiento de datos; y la opacidad relacional, por la que el consumidor deja de saber quién decide y cómo pedir revisión. Como estos riesgos se amplifican mutuamente, deben gestionarse en conjunto y también en clave macroprudencial.

6. Recomendaciones de gobernanza y estándares mínimos para el mercado asegurador

Del análisis se derivan estándares mínimos, articulados en clave multinivel. En *transparencia*, un deber expreso de informar al consumidor financiero sobre la intervención de sistemas algorítmicos en decisiones que le afecten, con sus factores principales y la vía para pedir revisión humana, que desarrolla el Capítulo II. En *no discriminación*, evaluaciones previas de impacto con análisis de variables proxy para sistemas de suscripción, tarificación o siniestros, y facultades del supervisor para exigir correcciones o suspenderlos. En *trazabilidad*, estándares de registro y auditoría interna, supervisora y, en supuestos definidos, independiente (NIST, 2023; ISO/IEC, 2023). En *seguridad*, integración con los marcos de ciberseguridad y resiliencia operativa; la tercerización se aborda en el Capítulo III. En *supervisión humana*, supuestos de revisión significativa —continua, por muestreo o a solicitud del afectado— como garantía material y no como trámite simbólico. En los planos *sectorial y sistémico*, la incorporación de la dimensión algorítmica a la supervisión basada en riesgos, con herramientas SupTech, y el monitoreo agregado de la concentración y homogeneización tecnológica (FSB, 2024, 2025; IAIS, 2025; BIS, 2025). Todo ello, modulado por la *proporcionalidad*. Estos estándares no equivalen a un marco regulatorio nuevo, sino a una orientación para articular las piezas existentes y cerrar brechas mediante la coordinación de los cinco niveles.

Algunas reflexiones

El capítulo construyó la gobernanza algorítmica sobre una categoría amplia, cuyo perímetro se define por el impacto de la decisión y no por la etiqueta tecnológica del sistema. Esa amplitud evita zonas sin control, pero deja abierta una pregunta: ¿deben gobernarse igual todos los sistemas que caben en ella? Cuatro reflexiones sugieren que no, y todas convergen en un mismo destinatario.

La primera concierne a la naturaleza del sistema. Los sesgos, errores y fallas descritos en el anteriormente en este texto no se manifiestan igual en un sistema algorítmico sin IA, en uno de IA no generativa, en uno de IA generativa o en uno de IA neuro simbólica (Tabla 1). La IA generativa añade riesgos que nacen del lenguaje —alucinaciones, fundamentos inventados, explicaciones persuasivas pero falsas—, hasta el punto de que el NIST la trata como un perfil de riesgo propio (NIST, 2024). La proporcionalidad no dependería, entonces, solo del impacto de la decisión, sino también del tipo de sistema que la produce.

Tabla 1. Tipos de sistema algorítmico: qué son, riesgos y controles

Tipo	Qué es	Ejemplo en seguros	Riesgo característico	Control clave
Sistema algorítmico sin IA	Ejecuta reglas, fórmulas o tablas fijadas de antemano por personas; no aprende de los datos.	Motor que marca mora cuando la prima vence; tarifa por tabla actuarial.	Regla errónea, discriminatoria o desactualizada aplicada en masa.	Control de cambios, pruebas y explicación de la regla aplicada.
IA no generativa	Aprende patrones de datos históricos para clasificar, puntuar	Scoring de fraude; modelo que estima	Sesgos en los datos, variables proxy, deriva del	Calidad de datos, monitoreo de sesgos, explicabilidad y

Tipo	Qué es	Ejemplo en seguros	Riesgo característico	Control clave
	o predecir; no crea contenido nuevo.	sinistralidad o fija precio.	modelo, puntaje opaco.	humano con autoridad para apartarse del modelo.
IA generativa	Produce contenido nuevo (textos, resúmenes, respuestas) a partir de instrucciones, por cálculo probabilístico.	Chatbot de atención; asistente que resume un expediente o redacta una carta de objeción.	Alucinaciones, fundamentos inventados, explicaciones persuasivas pero falsas, filtración de datos.	Verificación de fuentes, registro de instrucciones y salidas, revisión humana antes de afectar derechos.
IA neurosimbólica	Combina el aprendizaje de redes neuronales con razonamiento sobre reglas y conocimiento explícitos.	Sistema que contrasta los hechos del siniestro con las cláusulas y exclusiones	Errores o vacíos en las reglas codificadas; tecnología aún en maduración.	Validación jurídica de las reglas, trazabilidad del razonamiento y revisión humana de la conclusión.

Tipo	Qué es	Ejemplo en seguros	Riesgo característico	Control clave
		codificadas de la póliza.		

De ello se desprende la segunda: elegir el tipo y modelo de IA es, en sí mismo, un acto de gobernanza. Para fijar parámetros, la IA no generativa resulta menos riesgosa. Para determinar coberturas, la IA generativa solo parece adecuada si es de razonamiento avanzado o, incluso, neuro simbólica, y está sometida a revisión humana (Tabla 2). Es la tensión entre precisión y explicabilidad que el Capítulo II examina en el contrato de seguro.

Tabla 2. Tipo de sistema más prudente según el uso asegurador

Uso asegurador	Tipo de sistema más prudente	Razón
Calcular prima base	Sin IA (modelo actuarial y reglas) o IA no generativa explicable	Requiere estabilidad, validación y auditabilidad.
Estimar probabilidad de fraude	IA no generativa explicable, combinada con reglas	Detecta patrones, pero exige controlar falsos positivos.
Clasificar documentos de reclamación	IA no generativa, o IA generativa como apoyo con validación humana	Agiliza el trámite; no decide derechos.

Uso asegurador	Tipo de sistema más prudente	Razón
Interpretar cobertura	Sin IA (motor de reglas) con revisión humana; eventualmente IA neuro simbólica	Implica interpretación contractual y efectos jurídicos.
Redactar explicación al asegurado	IA generativa, siempre revisada por una persona	Debe basarse en una decisión trazable y correcta.

La tercera atañe a quién controla. El capítulo exige intervención humana significativa en todo el ciclo de vida del sistema, pero formula el principio como supervisión humana, que opera sobre todo frente a resultados. Si el riesgo nace en el diseño, el principio debería entenderse como de intervención humana, a cargo de perfiles que comprendan a la vez la lógica del algoritmo, los requerimientos técnicos del sistema y su marco jurídico, como plantea el Capítulo III.

La cuarta toca la propia arquitectura del enfoque. Si la interacción entre niveles no es jerárquica sino funcional, la idea de “nivel” sugiere una verticalidad que el capítulo mismo descarta. La expresión “multiplano”, en la que cada plano agrupa sus instituciones, entidades y normas, describiría con más fidelidad esa arquitectura, en sintonía con los planos contractual, organizacional y de supervisión que recorren el artículo.

Ese destinatario común es el consumidor financiero. En Colombia, sus principios y derechos, contenidos en la Ley 1328 de 2009, ofrecen el criterio para medir si el sistema elegido, su control y su arquitectura cumplen la función protectora que justifica la gobernanza algorítmica, proyección que desarrolla el Capítulo II.

Cierre y transición

La gobernanza algorítmica del sector asegurador es, ante todo, una respuesta jurídico-regulatoria al carácter estructural de los riesgos de la automatización, que articula instrumentos internacionales, regulación transversal y sectorial, dispositivos organizacionales y estándares técnicos bajo los principios de transparencia, no discriminación, trazabilidad, seguridad, supervisión humana, responsabilidad y proporcionalidad, con la doble finalidad de proteger al consumidor financiero y preservar la estabilidad del mercado asegurador. Sobre este marco, el Capítulo II analizará su incidencia en el contrato de seguro —suscripción, tarificación, siniestros y deberes de información— y el Capítulo III, su dimensión organizacional —gestión de IA, subcontratación tecnológica, ciberseguridad algorítmica y gobierno corporativo—. La continuidad entre los tres capítulos refleja la propia estructura de la gobernanza algorítmica multinivel: una arquitectura única, articulada en planos diferenciados pero recíprocamente dependientes.

Capítulo II. GOBERNANZA ALGORÍTMICA EN EL CONTRATO DE SEGURO

La incorporación de sistemas algorítmicos en la actividad aseguradora no supone únicamente una mejora en la eficiencia de sus operaciones, sino que transforma las condiciones en las que se evalúa el riesgo, se configura la oferta contractual y se decide sobre el cumplimiento de las prestaciones (Eling y Lehmann, 2018). Cuando la aceptación del tomador, la prima o la respuesta a una reclamación dependen de una herramienta automatizada, el problema jurídico no se agota en la fiabilidad de la tecnología; también exige establecer si el resultado respeta la buena fe, los deberes de información y las garantías del consumidor financiero (EIOPA, 2025). En Colombia, estas cuestiones deben examinarse a partir del régimen del contrato de seguro, la Ley 1328 de 2009 y las

disposiciones sobre tratamiento de datos personales de la Ley 1581 de 2012, sin que exista todavía una regulación contractual integral y específica de las decisiones algorítmicas.

1. Suscripción, tarificación y diseño de productos

La suscripción comprende la valoración del riesgo que realiza el asegurador para determinar si lo asume y en qué condiciones. Los sistemas de inteligencia artificial permiten analizar grandes cantidades de información para calcular la probabilidad de que ocurra un siniestro. Sin embargo, también pueden utilizar datos que, aunque estén relacionados estadísticamente con determinados resultados, no justifican por sí solos un trato diferente entre los asegurados (Eling, Nuessle y Staubli, 2022). La distinción resulta fundamental, porque el seguro presupone diferenciar riesgos y fijar primas de acuerdo con ellos; lo que exige control no es la segmentación en sí misma, sino su eventual utilización para reproducir desigualdades o excluir injustificadamente a determinados consumidores. Así, incluso cuando el modelo prescinde de categorías expresamente protegidas, variables como el lugar de residencia o ciertos patrones de consumo pueden funcionar como indicadores indirectos de ellas (Barocas, Hardt y Narayanan, 2023). De ahí que la revisión de los resultados no pueda limitarse a examinar los datos declarados, sino que deba considerar sus efectos sobre grupos de asegurados (EIOPA, 2021, 2025).

A esta dificultad se añade el perfilamiento del tomador mediante información obtenida de dispositivos conectados, registros de comportamiento y fuentes digitales. La disponibilidad de más datos no elimina las exigencias de finalidad y transparencia en su tratamiento, previstas en la Ley 1581 de 2012, particularmente cuando el consumidor desconoce las inferencias que determinan la oferta recibida. Además, la llamada “hiperpersonalización” de las primas puede fragmentar progresivamente los grupos de riesgo y comprometer la naturaleza mutualista del seguro, en la medida en que la determinación individual de las primas llegue a traducirse en barreras económicas de acceso para quienes presentan perfiles “menos favorables” (Eling, Nuessle y Staubli, 2022). Por

tanto, la eficiencia predictiva debe valorarse junto con sus consecuencias sobre la inclusión y la función económica del aseguramiento.

La automatización incide igualmente en el diseño de coberturas, exclusiones y deducibles. En este punto, la dificultad consiste en asegurar que las condiciones ofrecidas sean comprensibles y respondan a una delimitación verificable del riesgo. De forma paralela, la propia IA comienza a constituir una fuente de riesgos asegurables, por ejemplo, frente a errores de sistemas automatizados, daños derivados de productos tecnológicos o afectaciones de datos (Lior, 2022). La eventual cobertura mediante seguros de responsabilidad civil, riesgos cibernéticos o productos especializados exige precisar el hecho cubierto, las exclusiones y los criterios para acreditar el siniestro; no puede presumirse que toda póliza tradicional comprende, sin más, cualquier daño vinculado con estos sistemas (Weil et al., 2024).

2. Gestión automatizada de siniestros y consecuencias jurídicas

En la ejecución del contrato, los sistemas algorítmicos pueden clasificar reclamaciones, detectar inconsistencias, estimar pérdidas y recomendar la aceptación u objeción de un siniestro (Eling et al., 2022). Estas funciones permiten acelerar procedimientos repetitivos, pero su incidencia jurídica cambia cuando la recomendación determina materialmente la decisión de la aseguradora. En particular, una alerta de fraude o una puntuación de riesgo no equivalen, por sí solas, a la demostración de un incumplimiento contractual ni justifican automáticamente la negativa de una prestación. Por ello, la decisión debe apoyarse en los hechos del caso y en las condiciones aplicables de la póliza, y debe poder explicarse al asegurado de manera que este conozca sus fundamentos y pueda controvertirlos (Owens et al., 2022; EIOPA, 2025).

La dificultad aumenta cuando los datos utilizados para entrenar estos sistemas incorporan decisiones históricas de rechazo de reclamaciones que no han sido suficientemente verificadas o reproducen patrones asociados con determinados grupos de asegurados. En estos casos, los errores

o sesgos pueden extenderse a múltiples reclamaciones, mientras que la falta de transparencia sobre el funcionamiento del sistema dificulta identificar los criterios que determinaron cada decisión. Frente a estos riesgos, resulta necesario establecer mecanismos de control sobre los sistemas de inteligencia artificial utilizados por las aseguradoras, incluidos aquellos desarrollados o suministrados por terceros (NAIC, 2023). Con todo, la intervención de un proveedor tecnológico no desvincula a la aseguradora de las decisiones que adopta en ejecución del contrato de seguro. En consecuencia, el uso de estas herramientas no modifica, por sí sola, los presupuestos de la responsabilidad contractual, cuyo análisis exige establecer la existencia de una obligación, su incumplimiento, el daño y la relación de causalidad correspondiente. La complejidad técnica del sistema no puede convertirse, por tanto, en una justificación para excluir el examen de la conducta de la aseguradora ni de las consecuencias jurídicas de sus decisiones.

Esta distinción también permite evitar que la supervisión humana se convierta en una exigencia meramente formal. La revisión de una decisión automatizada debe estar a cargo de una persona que cuente con la información y las competencias necesarias para examinar sus fundamentos, cuestionar sus resultados y, cuando corresponda, corregirlos o apartarse de ellos. De lo contrario, la intervención humana se limitaría a ratificar una decisión sin que exista un control efectivo sobre los criterios que la sustentan. La intensidad de esta supervisión debe ser proporcional a las consecuencias de la decisión, pues la clasificación automatizada de documentos no plantea los mismos riesgos que la negativa a reconocer una indemnización o la modificación sustancial de las condiciones de cobertura (EIOPA, 2025; IAIS, 2025).

3. Transparencia, información y protección del asegurado

Los deberes de información y debida diligencia frente al consumidor financiero, previstos en la Ley 1328 de 2009, comprenden tanto la etapa precontractual como la celebración y ejecución del

contrato de seguro. En escenarios automatizados, no basta con informar que la aseguradora utiliza inteligencia artificial, pues esa advertencia general no permite comprender las razones por las cuales se rechazó una solicitud, se determinó una prima o se objetó una reclamación. La transparencia exige, por tanto, que el consumidor pueda conocer la intervención del sistema en las decisiones que le afectan, identificar los principales factores considerados y disponer de mecanismos efectivos para solicitar su aclaración o revisión (Goodman y Flaxman, 2017). Esto no supone revelar el código fuente ni la totalidad de los parámetros técnicos del modelo, sino proporcionar información comprensible y suficiente sobre los fundamentos de la decisión concreta (Owens et al., 2022).

La inteligencia artificial generativa plantea dificultades adicionales cuando se utiliza en asistentes conversacionales y canales de atención al consumidor. Estos sistemas pueden suministrar información incorrecta sobre las coberturas, omitir exclusiones o indicar procedimientos que no corresponden, con consecuencias sobre la conducta del asegurado y el ejercicio oportuno de sus derechos. Un ejemplo de esta problemática se encuentra en el caso *Moffatt v. Air Canada* (2024 BCCRT 149), en el que el Civil Resolution Tribunal de Columbia Británica examinó la responsabilidad de una empresa por la información errónea proporcionada mediante un asistente virtual disponible en su página web.

En este contexto, la gobernanza algorítmica debe traducirse en mecanismos que permitan garantizar el cumplimiento de las obligaciones del asegurador. La documentación de las decisiones automatizadas, la evaluación de posibles sesgos, la revisión humana de resultados adversos y la conservación de las comunicaciones con los consumidores constituyen instrumentos relevantes para prevenir riesgos y facilitar el control sobre el funcionamiento de estos sistemas (EIOPA, 2025; IAIS, 2025). Su implementación no pretende restringir la incorporación de nuevas tecnologías en

la actividad aseguradora, sino asegurar que su utilización resulte compatible con las obligaciones contractuales y legales de las entidades, de manera que el consumidor conserve la posibilidad efectiva de comprender y controvertir las decisiones que afectan sus derechos.

CAPÍTULO III. LA GOBERNANZA ALGORÍTMICA DEL ASEGURADOR

El análisis de la gobernanza algorítmica debe proyectarse también sobre la dimensión interna y organizacional de las entidades aseguradoras. La incorporación de sistemas de inteligencia artificial y otras herramientas automatizadas no supone únicamente una innovación tecnológica, sino que modifica los procesos de gobierno corporativo, administración de riesgos, control interno y toma de decisiones. De esta forma, la IA adquiere relevancia para la estabilidad operativa, el cumplimiento regulatorio y la protección del consumidor financiero (IAIS, 2025; EIOPA, 2025).

Desde esta perspectiva, la gobernanza algorítmica del asegurador comprende el conjunto de mecanismos jurídicos, técnicos y organizacionales destinados a dirigir, supervisar y controlar el diseño, implementación, operación y monitoreo de los sistemas algorítmicos utilizados por la entidad. Su alcance comprende tanto los sistemas que inciden directamente en el contrato de seguro como aquellos empleados en funciones actuariales, cumplimiento normativo, auditoría, ciberseguridad, detección de fraude, administración integral de riesgos y gobierno corporativo (EIOPA, 2025; Sáinz & Contreras, 2019; Palacios Sánchez, 2016).

En este ámbito, la gobernanza puede analizarse mediante una secuencia funcional: los sistemas algorítmicos intervienen en procesos relevantes de la entidad, dicha intervención genera riesgos

organizacionales y operativos, estos requieren mecanismos permanentes de control, y, finalmente, tales controles deben insertarse en una estructura capaz de atribuir responsabilidades.

3.1. Sistemas algorítmicos en la gestión aseguradora

La expresión sistemas algorítmicos se utiliza en un sentido funcional para comprender herramientas capaces de procesar grandes cantidades de información, automatizar tareas y generar inferencias, clasificaciones, recomendaciones o decisiones que inciden materialmente en la actividad aseguradora. Se trata de una categoría amplia que comprende mecanismos tradicionales de automatización y sistemas de IA, incluyendo aprendizaje automático, redes neuronales, *deep learning* e inteligencia artificial generativa (Russell & Norvig, 2022; Hurbans, 2020; Nicoletti, 2021).

La IAIS, siguiendo la definición de la OECD, caracteriza la IA como un sistema basado en máquinas que genera inferencias para producir predicciones, recomendaciones, contenidos o decisiones capaces de influir en entornos físicos o virtuales. Desde la perspectiva de la gobernanza, resultan particularmente relevantes los grados de autonomía y adaptación que estos sistemas pueden desarrollar una vez desplegados, pues su comportamiento puede evolucionar respecto de los parámetros originalmente aprobados y exigir mecanismos de monitoreo durante todo su ciclo de vida (IAIS, 2025).

Su utilización constituye una evolución del proceso de digitalización de una actividad históricamente basada en el análisis de información. Actualmente, los sistemas algorítmicos

intervienen en suscripción, tarificación, administración de pólizas, evaluación actuarial, atención al cliente, gestión de siniestros, cumplimiento y prevención del fraude, permitiendo ampliar la capacidad analítica, automatizar procesos y reducir costos operativos (EIOPA, 2021; IAIS, 2025). La evidencia sectorial muestra, además, una expansión significativa de su utilización precisamente en suscripción, fijación de precios, fraude y reclamaciones (Cole, Fier & Marzen, 2026).

Su relevancia jurídica aparece cuando sus resultados condicionan la aceptación de riesgos, las primas, las coberturas o la resolución de reclamaciones. Al mismo tiempo, su despliegue se encuentra crecientemente vinculado con infraestructura de nube, datos y soluciones desarrolladas por proveedores externos. Por ello, la gobernanza debe comprender tanto los sistemas utilizados internamente como las tecnologías y servicios de terceros incorporados a procesos relevantes de la aseguradora (EIOPA, 2019, 2021).

3.2. Riesgos organizacionales y operativos asociados al uso de sistemas algorítmicos

La creciente autonomía y capacidad adaptativa de estos sistemas transforma la naturaleza de los riesgos enfrentados por las aseguradoras. El desarrollo de arquitecturas más complejas, incluida la IA agéntica, evidencia que el riesgo ya no depende únicamente de la calidad técnica del modelo, sino también de su grado de autonomía y de la forma en que interactúa con datos, usuarios y otros sistemas durante su ciclo de vida (Russell & Norvig, 2022; Tekale, 2025; IAIS, 2025).

Uno de los principales riesgos corresponde a los sesgos algorítmicos, que pueden originarse tanto en desigualdades contenidas en los datos como en decisiones adoptadas durante la selección de

variables, entrenamiento o parametrización del modelo. En seguros, la dificultad radica en distinguir entre una diferenciación actuarial legítima y aquella que reproduce exclusiones injustificadas mediante variables aparentemente neutrales que funcionan como *proxies* de características protegidas (EIOPA, 2019; Prince & Schwarcz, 2020; Chong-Castillo, 2025; IAIS, 2025).

Junto con ello pueden presentarse errores vinculados con la calidad de los datos, programación, interoperabilidad, degradación del modelo o cambios en el entorno. En sistemas generativos pueden surgir, además, alucinaciones y, en arquitecturas con mayor autonomía, desviaciones funcionales respecto de los objetivos establecidos. Una característica relevante de estos errores es su escalabilidad, pues una deficiencia puede reproducirse de manera sistemática sobre numerosas decisiones antes de ser identificada (IAIS, 2025).

La opacidad algorítmica constituye otro riesgo relevante. Algunos modelos dificultan reconstruir los factores que determinaron un resultado específico dando lugar al denominado fenómeno de “caja negra”, lo que restringe su revisión y complica la atribución de responsabilidades cuando afectan a asegurados o beneficiarios (EIOPA, 2025). A ello se suman riesgos de ciberseguridad, tales como ataques adversariales, manipulación o envenenamiento de datos, y los derivados de la dependencia de proveedores tecnológicos, incluida la pérdida efectiva de capacidad de supervisión asociada al denominado *reverse outsourcing* (EIOPA, 2019; IAIS, 2025).

Finalmente, la utilización de infraestructuras, proveedores o modelos comunes introduce una posible dimensión sistémica. La concentración, criticidad y limitada sustituibilidad de determinados proveedores pueden permitir que una falla se propague a varias entidades

simultáneamente, de manera que el riesgo algorítmico trascienda a la aseguradora individual y alcance al mercado (FSB, 2025).

3.3. Mecanismos de control y mitigación del riesgo algorítmico

Debido a que estos riesgos pueden materializarse durante todo el ciclo de vida del sistema, su tratamiento exige mecanismos permanentes de prevención, detección y corrección. La gobernanza no puede limitarse a validar técnicamente un modelo al momento de su implementación, sino que debe combinar supervisión humana, trazabilidad y explicabilidad, monitoreo continuo e integración con los sistemas generales de gestión de riesgos (IAIS, 2025; EIOPA, 2025).

La supervisión humana busca impedir que decisiones con relevancia jurídica o económica queden completamente sustraídas del juicio humano. El Reglamento (UE) 2024/1689 exige para determinados sistemas de alto riesgo una supervisión efectiva y la posibilidad de ignorar, invalidar o revertir sus resultados (art. 14). Sin embargo, la mera presencia de una persona no garantiza control material, especialmente ante el riesgo de *automation bias*. La literatura ha advertido que una supervisión meramente formal puede generar una falsa sensación de seguridad cuando el operador carece de conocimientos, información o autoridad para cuestionar el sistema (Green, 2022; Fink, 2025). De ahí que la intervención significativa requiera capacidades técnicas, jurídicas y operativas suficientes (IAIS, 2025).

La trazabilidad permite reconstruir cómo se produjo una recomendación o decisión. La conservación de registros sobre datos, versiones, eventos e intervenciones facilita la auditoría y la

eventual determinación de responsabilidades, y constituye un presupuesto para la transparencia y explicabilidad (Reglamento UE 2024/1689, arts. 12 y 19; IAIS, 2025). Las técnicas de *Explainable Artificial Intelligence* buscan precisamente facilitar la comprensión de los resultados y fortalecer la confianza en decisiones automatizadas, aunque ciertos modelos requieran medidas compensatorias de supervisión, auditoría y control de datos cuando su explicabilidad sea limitada (Owens et al., 2022; EIOPA, 2025; IAIS, 2025).

Estos mecanismos deben incorporarse a las estructuras ordinarias de gobierno corporativo, auditoría y administración de riesgos. EIOPA sostiene que los principios tradicionales de gobierno continúan siendo aplicables a la IA, mientras que el *AI Risk Management Framework* del NIST propone gestionar sus riesgos mediante funciones permanentes de gobierno, identificación, medición y tratamiento (EIOPA, 2025; NIST, 2023). De igual forma, DORA exige marcos de resiliencia tecnológica y continuidad operativa, mientras que el Reglamento de IA incorpora evaluaciones preventivas de impacto para determinados sistemas de alto riesgo (Reglamento UE 2022/2554; Reglamento UE 2024/1689, art. 27).

3.4. Gobernanza organizacional y responsabilidad de la aseguradora

Los controles anteriores requieren una estructura que determine quién supervisa, quién decide y quién responde. La gobernanza algorítmica constituye así el marco organizacional que distribuye funciones y responsabilidades para garantizar que los sistemas utilizados por la aseguradora permanezcan sometidos a mecanismos efectivos de rendición de cuentas.

La IAIS exige líneas claras de responsabilidad y una comprensión suficiente de los riesgos tecnológicos por parte de los órganos de dirección, de manera que puedan cuestionar resultados y adoptar medidas correctivas. Esta exigencia constituye una proyección de los principios tradicionales de gobierno corporativo, en ese sentido, ICP 7 y ComFrame mantienen la responsabilidad de las entidades y de sus órganos de administración respecto de una gestión sana y prudente, aun cuando las decisiones se encuentren apoyadas por tecnologías automatizadas (IAIS, 2024; IAIS, 2025).

La responsabilidad organizacional se proyecta tanto sobre los datos como sobre los proveedores tecnológicos. Frente al riesgo de discriminación, la exclusión de variables sensibles no resulta suficiente si otras variables funcionan como *proxies*, por lo que la supervisión debe abarcar también los resultados y sus efectos sobre distintos grupos de consumidores (Prince & Schwarcz, 2020; EIOPA, 2025).

Frente a la externalización, la contratación de terceros tampoco permite desprenderse de las obligaciones regulatorias. DORA mantiene la responsabilidad de las entidades financieras cuando utilizan servicios tecnológicos externos, mientras IAIS y EIOPA exigen diligencia debida, mecanismos contractuales y capacidad efectiva de supervisión (Reglamento UE 2022/2554, art. 28; IAIS, 2025; EIOPA, 2025; FSB, 2025). En Colombia, esta lógica encuentra puntos de contacto con categorías tradicionales de selección y vigilancia de terceros. El artículo 2347 del Código Civil y la Sentencia C-1235 de 2005 permiten identificar la relevancia jurídica de esos deberes, sin que ello implique equiparar automáticamente a todo proveedor tecnológico con una persona sometida a dependencia de la aseguradora.

Finalmente, la ausencia de un régimen específico de responsabilidad por daños derivados de IA no significa que tales perjuicios queden sin mecanismos de reparación, pues pueden analizarse a partir de las categorías tradicionales de responsabilidad civil y de las obligaciones propias de la actividad aseguradora. A ello se suma el papel que el seguro puede desempeñar como mecanismo de transferencia y gestión de los riesgos derivados de sistemas de IA, cuestión que es relevante ante la pluralidad de actores que pueden intervenir en su diseño, implementación y utilización (Tapia Hermida, 2021; Lior, 2022; Jiménez Mahecha, 2023). La utilización de IA no desplaza, por tanto, las obligaciones regulatorias, contractuales y de diligencia de la aseguradora respecto de los sistemas que incorpora a sus procesos, sin perjuicio de eventuales responsabilidades concurrentes de desarrolladores y proveedores. No obstante, la evolución tecnológica evidencia la conveniencia de avanzar hacia reglas más específicas de explicación, impugnación y control de decisiones automatizadas (Woolcott, Cabrera & Navarro, 2026).

CONCLUSIONES

El análisis realizado permite concluir que la gobernanza algorítmica en el sector asegurador no constituye una respuesta exclusivamente tecnológica, sino una arquitectura jurídica, técnica y organizacional destinada a ordenar el uso de sistemas automatizados cuya incidencia se extiende sobre el mercado, el contrato de seguro y la propia estructura de las entidades. Su perímetro, por ello, no debe depender exclusivamente de que una herramienta sea calificada formalmente como inteligencia artificial, sino de la función que desempeña, su grado de autonomía y el impacto material que sus resultados pueden producir sobre consumidores y organizaciones.

La utilización de estos sistemas puede mejorar la evaluación de riesgos, la tarificación, la gestión de siniestros, la detección de fraude y la eficiencia operativa, sin embargo, también puede amplificar sesgos, errores, opacidad y dependencias tecnológicas. En la relación contractual, ello exige preservar la transparencia, la posibilidad de controvertir decisiones adversas y la diferenciación entre una segmentación actuarial legítima y prácticas discriminatorias derivadas de datos o variables *proxy*. La eficiencia predictiva no puede constituir, por sí sola, una justificación suficiente para decisiones que afecten derechos del consumidor financiero.

Desde la perspectiva organizacional, la gobernanza debe acompañar todo el ciclo de vida de los sistemas mediante mecanismos proporcionales de supervisión humana, trazabilidad, explicabilidad, monitoreo, auditoría y resiliencia operativa. Estos controles no deben operar como obligaciones documentales aisladas, sino integrarse a los sistemas ordinarios de gobierno corporativo, gestión de riesgos y control interno de las aseguradoras.

La utilización de proveedores tecnológicos tampoco permite diluir las responsabilidades de la entidad. La aseguradora conserva sus propias obligaciones de supervisión, diligencia y protección del consumidor respecto de los sistemas que incorpora a su operación, sin perjuicio de las responsabilidades concurrentes que puedan corresponder a desarrolladores u otros actores. De este modo, la gobernanza algorítmica articula una cadena que conecta decisión, riesgo, control y responsabilidad.

Por último, el ordenamiento colombiano dispone ya de normas sobre protección del consumidor financiero, datos personales, responsabilidad, gobierno corporativo y gestión de riesgos que ofrecen puntos de partida para abordar estas problemáticas, pero todavía carece de un marco

sectorial integral que articule específicamente su aplicación a las decisiones algorítmicas en seguros. El reto no consiste necesariamente en sustituir las instituciones existentes, sino en adaptarlas y coordinarlas mediante criterios de proporcionalidad, transparencia, supervisión y rendición de cuentas que permitan aprovechar las ventajas de la automatización sin comprometer la protección del asegurado ni la estabilidad del mercado.

BIBLIOGRAFÍA

Chong-Castillo B. (2025). Sesgos en los modelos algorítmicos de inteligencia artificial dentro del sector asegurador: La necesaria adopción de principios éticos para garantizar el respeto a derechos humanos de los asegurados. (2025). *Revista Ibero-Latinoamericana De Seguros*, 34(62), 127-138. <https://doi.org/10.11144/Javeriana.ris62.smai>

Cole, C.R., Fier, S.G. & Marzen, C. (2026). Artificial Intelligence and Insurance Regulation. *Journal of Insurance Regulation (NAIC)*, (45-3). <https://doi.org/10.52227/27364.2026>

Congreso de la República de Colombia. (1887). *Código Civil de Colombia* (arts. 1602–1604, 2341, 2347, 2356). <https://www.suin-juriscol.gov.co/viewDocument.asp?id=1871304>

Corte Constitucional de Colombia. (2005). *Sentencia C-1235 de 2005* (M.P. Rodrigo Escobar Gil). <https://www.corteconstitucional.gov.co/relatoria/2005/c-1235-05.htm>

EIOPA. (2019). Big data analytics in motor and health insurance: a thematic review. https://www.eiopa.europa.eu/document/download/becbbe3a-ba4c-47b9-870a-63872fef3986_en?filename=Big%20Data%20Analytics%20in%20motor%20and%20health%20insurance%3A%20A%20thematic%20review.pdf

EIOPA. (2021). *Artificial intelligence governance principles. Towards ethical and trustworthy artificial intelligence in the European insurance sector.* <https://www.eiopa.europa.eu/system/files/2021-06/eiopa-ai-governance-principles-june-2021.pdf>

EIOPA. (2025). *Opinion on artificial intelligence governance and risk management.* https://www.eiopa.europa.eu/publications/opinion-artificial-intelligence-governance-and-risk-management_en

Financial Stability Board. (2025). *Monitoring adoption of artificial intelligence and related vulnerabilities in the financial sector.* FSB. <https://www.fsb.org/uploads/P101025.pdf>

Fink, M. (2025). Human oversight under Article 14 of the EU AI Act en Malgieri, G., Gonzalez Fuster, G., Mantelero, A., & Zancir-Fortuna, G. (Eds.) (2026). *The EU Artificial Intelligence Act: A thematic commentary.* (1st ed.) Hart Publishing, Part III: High-Risk AI Systems, Chapter 18. <https://ssrn.com/abstract=5147196>

Green, B. (2022). The flaws of policies requiring human oversight of government algorithms. *Computer Law & Security Review*, 45, Artículo 105681. <https://doi.org/10.1016/j.clsr.2022.105681>

Hurbans, R. (2020). *Grokking artificial intelligence algorithms*. Manning Publications.

IAIS (2024). *Insurance core principles and common framework for the supervision of internationally active insurance groups (ICPs and ComFrame)*.
<https://www.iais.org/uploads/2025/06/IAIS-ICPs-and-ComFrame-December-2024.pdf>

IAIS (2025). *Application paper on the supervision of artificial intelligence*.
<https://www.iais.org/2025/07/the-iais-publishes-application-paper-on-the-supervision-of-artificial-intelligence/>

Jiménez Mahecha, L. F. (2023). *Inteligencia artificial: responsabilidad contractual y extracontractual*. Asuntos Legales. <https://www.asuntoslegales.com.co/analisis/luisa-fernanda-jimenez-mahecha-3586461/inteligencia-artificial-responsabilidad-contractual-y-extracontractual-3804316>

Lior, A. (2022). Insuring AI: The role of insurance in artificial intelligence regulation. *Harvard Journal of Law & Technology*, 35(2), 467–530.
<https://jolt.law.harvard.edu/assets/articlePDFs/v35/2.-Lior-Insuring-AI.pdf>

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>

Nicoletti, B. (2021). *Insurance 4.0. Benefits and Challenges of Digital Transformation*. Palgrave Macmillan.

Owens, E., Sheehan, B., Mullins, M., Cunneen, M., Ressel, J., & Castignani, G. (2022). Explainable artificial intelligence (XAI) in insurance. *Risks*, 10(12), Artículo 230. <https://doi.org/10.3390/risks10120230>

Palacios Sánchez, F. (ed.) (2016). *Seguros: Temas esenciales*. ECOE Ediciones – Universidad de La Sabana.

Prince, A. E. R., & Schwarcz, D. (2020). Proxy discrimination in the age of artificial intelligence and big data. *Iowa Law Review*, 105(3), 1257–1318. <https://ilr.law.uiowa.edu/print/volume-105-issue-3/proxy-discrimination-in-the-age-of-artificial-intelligence-and-big-data>

Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, sobre la resiliencia operativa digital del sector financiero (DORA). *Diario Oficial de la Unión Europea*, L 333, 27.12.2022, pp. 1–79.

Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial). *Diario Oficial de la Unión Europea*, L, 2024/1689, 12.7.2024.

Russell, S. & Norvig, P. (2022). *Artificial intelligence: A modern approach* (4th ed.). Pearson.

Sáinz Martínez, J.P. & Contreras Buzeta (coords.) (2019). *Derecho de seguros y reaseguro en América Latina*. Tirant Lo Blanch.

Tapia Hermida, A. J. (2021). La responsabilidad civil derivada del uso de la inteligencia artificial y su aseguramiento. *Revista Ibero-Latinoamericana de Seguros*, 30(54), 107–146. <https://doi.org/10.11144/Javeriana.ris54.rcdu>

Tekale, K. M. (2025). Agentic AI in Insurance: Moving Beyond Generative AI to Autonomous Decision-Making. *AIJCST*, 7(5), 42–54. <https://doi.org/10.63282/3117-5481/AIJCST-V7I5P104>

Woolcott Oyague, O. D., Cabrera Peña, K. I., & Navarro Reyes, D. (2026). Hacia una adaptación de la responsabilidad civil a la inteligencia artificial y su proyección en Colombia. *Novum Jus*, 20(1), 259–287. <https://doi.org/10.14718/NovumJus.2026.20.1.9>

Barocas, S., Hardt, M. y Narayanan, A. (2023). *Fairness and machine learning: Limitations and opportunities*. MIT Press.

EIOPA. (2021). *Artificial intelligence governance principles: Towards ethical and trustworthy artificial intelligence in the European insurance sector*.

EIOPA. (2025). *Opinion on artificial intelligence governance and risk management*.

Eling, M. y Lehmann, M. (2018). The impact of digitalization on the insurance value chain and the insurability of risks. *The Geneva Papers on Risk and Insurance*, 43, 359–396.

Goodman, B. y Flaxman, S. (2017). European Union regulations on algorithmic decision-making and a “right to explanation”. *AI Magazine*, 38(3), 50–57.

IAIS. (2025). *Application paper on the supervision of artificial intelligence*.

Ley 1328 de 2009. Diario Oficial de Colombia, 15 de julio de 2009.

Ley 1581 de 2012. Diario Oficial de Colombia, 17 de octubre de 2012.

Lior, A. (2022). Insuring AI: The role of insurance in artificial intelligence regulation. *Harvard Journal of Law & Technology*, 35(2), 467–529.

Moffatt v. Air Canada, 2024 BCCRT 149.

NAIC. (2023). Model bulletin on the use of artificial intelligence systems by insurers.

Owens, E., Sheehan, B., Mullins, M., Cunneen, M., Ressel, J. y Castignani, G. (2022). Explainable artificial intelligence (XAI) in insurance. *Risks*, 10(12), 230.

Weil, G., Pistillo, M., Van Arsdale, S., Ikegami, J., Onuma, K., Okawa, M. y Osborne, M. A. (2024). Insuring emerging risks from AI. Oxford Martin AI Governance Initiative.