Hacia una gobernanza corporativa de la inteligencia artificial: propuesta de implementación desde el deber fiduciario en Colombia

Autores
Melissa Salazar Cuartas y Jorge Armando Devia Rey
Título a obtener: Magister en Derecho Corporativo

Tutor
Mario Fernando Avila Cristancho

Universidad del Rosario

Facultad de Jurisprudencia

Maestría en Derecho Corporativo

Bogotá - Colombia

Año 2026

Hacia una gobernanza corporativa de la inteligencia artificial: propuesta de implementación desde el deber fiduciario en Colombia

Towards the Corporate Governance of Artificial Intelligence: An Implementation Proposal from the Perspective of Fiduciary Duties in Colombia

Melissa Salazar Cuartas - Jorge Armando Devia Rey

Resumen

El presente artículo de reflexión analiza el impacto de la inteligencia artificial en el gobierno corporativo y en el alcance del deber fiduciario de los administradores bajo el artículo 24 de la Ley 222 de 1995 en Colombia. Desde un enfoque jurídico-analítico y reflexivo, se sostiene que la delegación en sistemas algorítmicos no exime la responsabilidad, sino que exige mayores niveles de supervisión. Se identifica que el principal riesgo radica en la ausencia de marcos de gobernanza adecuados. Como aporte, se propone un modelo de implementación que articula control, gestión del riesgo y documentación como elementos centrales de la diligencia empresarial.

Abstract

This article presents a reflective legal analysis of the impact of artificial intelligence on corporate governance and on the scope of directors' fiduciary duties under Article 24 of Colombian Law 222 of 1995. From a legal-analytical perspective, it argues that reliance on algorithmic systems does not exempt corporate decision-makers from liability, but instead requires enhanced standards of oversight and supervision. The study identifies the absence of adequate governance frameworks as one of the principal legal and organizational risks associated with the corporate adoption of artificial intelligence. As its main contribution, the article proposes an implementation model that integrates oversight, risk management, and documentation as core components of corporate diligence and responsible governance.

Palabras Clave
Inteligencia artificial – Gobierno corporativo – Deber fiduciario – Responsabilidad empresarial

Keywords
Artificial Intelligence – Corporate Governance – Fiduciary Duties – Corporate Liability

La incorporación de sistemas de inteligencia artificial en las organizaciones ha generado nuevas discusiones jurídicas en torno a la toma de decisiones corporativas, la supervisión empresarial y el alcance de los deberes de los administradores. La creciente utilización de herramientas algorítmicas en procesos estratégicos, operativos y de análisis de información ha evidenciado la necesidad de revisar si los modelos tradicionales de gobierno corporativo ofrecen respuestas suficientes frente a los riesgos derivados de estas tecnologías.

En este contexto, el presente artículo de reflexión analiza el impacto de la inteligencia artificial en el deber fiduciario de los administradores desde la perspectiva del artículo 24 de la Ley 222 de 1995 y su relación con la gobernanza corporativa en Colombia. El artículo desarrolla una lectura interpretativa del deber de diligencia y supervisión frente al uso corporativo de sistemas de inteligencia artificial y, a partir de ello, formula una propuesta práctica de implementación orientada a órganos de administración, juntas directivas y áreas de cumplimiento. Para tal efecto, se adopta un enfoque jurídico-analítico sustentado en revisión doctrinal, análisis normativo y construcción de un modelo de gobernanza aplicable al contexto empresarial colombiano.

1. La inteligencia artificial y las empresas

Los avances tecnológicos actuales en inteligencia artificial están modificando por completo la manera que las empresas y los gobiernos manejan la información respecto de los servicios que prestan en la actualidad. Todavía, aunque esta innovación es disruptiva tiene aspectos éticos y legales para tener en cuenta.

La inteligencia artificial con el paso de los años se ha estado consolidando como una herramienta clave, convirtiéndose en un instrumento fundamental para operar o desarrollar estrategias en las empresas y grandes corporaciones a nivel mundial. Una de las ventajas que debemos resaltar es la capacidad para procesar grandes cantidades de datos, logrando aprender y ejecutar patrones que pueden resultar complejos y demorados para el ser humano, así mismo, esta evolución tecnológica logra ofrecer soluciones en tiempo real, transformando diferentes sectores, como el financiero, de la salud, manufacturación, y el comercio electrónico. Hoy en día, las empresas utilizan la inteligencia artificial para automatizar tareas repetitivas y para impulsar la innovación, optimizar la eficiencia operativa y mejorar la experiencia del cliente.

Un área clave donde la inteligencia artificial ha tenido un impacto significativo es en la toma de decisiones corporativas. Los sistemas de aprendizaje automático permiten a las empresas analizar datos históricos y en tiempo real para prever tendencias del mercado, evaluar riesgos y personalizar los servicios ofrecidos de acuerdo con el comportamiento de los usuarios, esto, según las necesidades específicas de los clientes. Por ejemplo, en el sector financiero, las nuevas tecnologías se utilizan para detectar transacciones sospechosas, segmentación y prevenir fraudes, mientras que en la manufactura se implementa para predecir fallos en máquinas y optimizar la cadena de suministro.

Se debe indicar que actualmente existen diferentes tipos de inteligencia artificial, una de ellas, la Inteligencia Artificial Generativa (IAG), siendo esta de gran interés para el sector empresarial y corporativo, teniendo en cuenta que puede generar beneficios al momento de llevar a cabo diferentes análisis para facilitar la toma de decisiones esenciales para las compañías. Las herramientas de la IAG utilizan modelos de lenguaje y generadores de contenido visual, lo cual, ha sido implementado en el marketing, el diseño personalizado y la redacción de informes empresariales, no obstante, su implementación plantea importantes

desafíos éticos y legales, como garantizar la transparencia en los resultados generados y prevenir el uso indebido de esta tecnología.

Es así como este tipo de tecnología está siendo utilizado en diferentes áreas corporativas, como es el caso de la gestión del talento humano, la IAG ha transformado los procesos de reclutamiento, evaluación de desempeño y capacitación de empleados. Los algoritmos son capaces de filtrar candidatos con base en sus competencias, identificar áreas de mejora en los equipos de trabajo y diseñar programas de formación personalizados, no obstante, el uso de esta tecnología puede tener sesgos discriminatorios, lo que subraya la necesidad de un diseño y uso ético de estas herramientas.

La inteligencia artificial ya no es una tecnología para el futuro sino una herramienta actual y esencial que se está utilizando en la estrategia corporativa. De la optimización de operaciones a la mejora en la toma de decisiones en general, la IAG está cambiando radicalmente la forma en que las empresas se organizan en un mercado mundial, por tanto, es crucial que las compañías cumplan estrictas regulaciones éticas, específicamente en los procesos que integran sus operaciones, aún más cuando incluyen IAG en la toma de decisiones.

Desde nuestro punto de vista, es necesario que se desarrollen políticas internas sobre la guía de responsabilidad, pero no solo enfocada en los sujetos sino también en el desarrollo e implementación de esta tecnología. Por lo cual, se examinará los enfoques con que las corporaciones avanzan en la IAG para su utilización y, sobre ello, presentar los desafíos que esto representa, explorando tanto las oportunidades como los riesgos.

1.1. Uso de la inteligencia artificial generativa en la toma de decisiones

En la actualidad, las empresas han adoptado la IAG en sus procesos para mejorar diversas actividades en áreas diferentes, desde marketing y talento humano hasta la elección de toma de decisiones estratégicas en los modelos de la empresa.

Por ejemplo, en lo que respecta al marketing, grandes corporaciones han utilizado IAG para desarrollar campañas publicitarias personalizadas. Los sistemas se basan en qué datos extrae del consumidor como preferencias y educación, cuando compra, etc., para construir contenido de texto e imagen que vaya dirigida a los miembros de una audiencia en específico. Este enfoque no solo optimiza los esfuerzos de marketing, sino que también mejora la experiencia del cliente al ofrecer mensajes altamente personalizados (Davenport & Ronanki, 2018).

Así mismo, en el ámbito de la salud, empresas han utilizado IAG, aprovechando su capacidad de procesar datos y producir resultados, para impulsar la creación y desarrollo de nuevos medicamentos. Los modelos generativos analizan bases de datos masivas sobre compuestos químicos y enfermedades, proponiendo nuevas moléculas que podrían ser eficaces en el tratamiento de algunas enfermedades o ciertas condiciones de salud. Este proceso, que solía tomar años en ejecutarse, ahora puede efectuarse en muy corto tiempo, lo que representa un avance significativo en la investigación médica (Rai et al., 2019).

Otro ejemplo que se puede mencionar es en el sector financiero, donde los bancos han adoptado el uso y herramientas de IAG para mejorar sus servicios de atención al cliente. En este caso, la tecnología usada genera y redacta respuestas automáticas en correos electrónicos y chats en línea, lo que genera una mayor capacidad de respuesta siendo esta una de las maneras más ágiles para el cliente, precisando para la compañía soluciones a las consultas realizadas. De igual manera, el uso de esta tecnología en este sector también se ha usado para generar reportes financieros personalizados para clientes corporativos, facilitando la toma de decisiones basada en datos.

De igual forma en el sector de la manufactura, las empresas han implementado dentro de sus procesos y operaciones la inteligencia artificial generativa para optimizar la producción. Una aplicación de las nuevas tecnologías se puede observar en las simulaciones virtuales de procesos de fabricación, permitiendo así identificar posibles fallas, logrando proponer soluciones antes de implementar cambios en las operaciones. Esto no solo reduce costos, sino que también mejora la calidad del producto final.

La incorporación de la IAG en la toma de decisiones corporativas plantea beneficios significativos, pero también genera interrogantes sobre transparencia, sesgos algorítmicos y protección de datos personales. En este contexto, se revisarán algunos casos, que serán un pilar de análisis para la guía de implementación que estamos desarrollando para las empresas, con el objetivo de tener una ruta de implementación de la IAG y cuáles serán esos pasos que garantizarán el respeto a los derechos fundamentales, planteando los límites y responsabilidades que deberán tener los administradores.

1.2. Análisis comparativo de casos reales

A continuación, se presenta un análisis que compara sistemáticamente varios estudios de caso empresariales con hallazgos sobre gobernanza, riesgos y beneficios de la IAG en la toma de decisiones corporativas. Se adoptan tres dimensiones analíticas: (a) naturaleza de la decisión impactada (estratégica vs operativa); (b) marcos de gobernanza utilizados (comités, auditorías, estándares); y (c) resultados y riesgos (beneficios cuantificables y externalidades no intencionadas).

Caso	Naturaleza de decisión impactada	Mecanismos de gobernanza observados	Beneficios reportados	Riesgos observados	Fuentes (ejemplos)
Csaszar et al. (experimentos LLMs)	Decisiones **estratégicas**: evaluación de planes de negocio, selección de emprendimientos	Experimentos controlados; comparación IA vs humanos; recomendaciones de validación humana y métricas de desempeño	LLMs producen análisis estratégicos de calidad comparable/better → mayor velocidad y escala en evaluación.	Sobreconfianza, riesgo de outputs no verificables, sesgos en datos de entrenamiento.	Csaszar, Ketkar & Kim (2024). *Artificial Intelligence and Strategic Decision-Making*. https://arxiv.org/abs/2408.08811
AstraZeneca (Ethics-Based Auditing, EBA)	Decisiones de **priorización R&D** y uso de modelos predictivos	Ethics-based auditing (EBA); comités, playbooks, auditorías internas/externas	Mejora en gobernanza, armonización de estándares, mayor control sobre riesgos éticos	Costo y complejidad de implementación; coordinación en organización descentralizada.	Mökander et al. (2024). *Operationalising AI governance through EBA*. https://arxiv.org/abs/2407.06232
JPMorgan (COiN — Contract Intelligence)	Decisiones **contractuales / legales** (revisión masiva de contratos)	Integración operativa + trazabilidad; controles humanos sobre revisiones finales	Reducción enorme de horas de revisión; mayor velocidad y consistencia	Riesgo de error no detectado; responsabilidad por decisiones automatizadas si falta supervisión.	JPMorgan Chase: Saving 360,000 Hours with Contract Intelligence AI — https://greendata.io/insights/jpmorgan-chase-coin-contract-intelligence?utm_source=
Amazon (forecasting / cadena de suministro)	Decisiones **operativas**: inventario, reposición, logística	Modelos predictivos integrados en S&OP; monitorización y métricas de performance	Reducción de stockouts; optimización logística; mejoras en ventas y eficiencia.	Dependencia de datos; cascadas de error si datos sesgados o corruptos.	Amazon/— https://aws.amazon.com/es/solutions/case-studies/amazon-pharmacy-case-study/?utm_source=
Netflix (recomendación)	Decisiones de **producto y programación** (qué contenidos producir/mostrar)	AB testing, métricas de engagement; gobernanza de experimentos y equipos mixtos	Aumento de retención, optimización de inversión en contenido.	Potencial sesgo en recomendaciones; creación de "burbujas" de consumo; decisiones estratégicas sesgadas.	Gómez-Uribe & Hunt (2015). *The Netflix recommender system*; Netflix Research — https://research.netflix.com/
Siemens (mantenimiento predictivo)	Decisiones **operativas/ingeniería**: mantenimiento, disponibilidad equipos	Integración de modelos de machine learning con plataformas industriales IoT (MindSphere); validación técnica de modelos; supervisión humana en la toma de decisiones críticas; protocolos de calidad de datos.	Reducción de tiempos de inactividad (downtime); optimización de costos de mantenimiento; mayor disponibilidad y vida útil de los equipos; mejora en la eficiencia operativa.	Dependencia de la calidad y confiabilidad de los datos; riesgos operativos y de seguridad física ante fallos de predicción; posibles impactos económicos por sobreconfianza en los modelos algorítmicos.	Siemens Digital Industries. MindSphere – Case Studies on Predictive Maintenance. https://new.siemens.com/global/en/products/software/mindsphere/case-studies.html
BBVA (IA Responsable)	Decisiones **financieras / crédito / operativas**	Marco interno, validación de modelos, comités, protocolos de apelación	Mejora gobernanza, reducción de sesgo en scoring (cuando se aplica correctamente)	Riesgo reputacional y regulatorio si no se aplica trazabilidad y explicabilidad.	BBVA — Marco IA Responsable: https://www.bbva.com/es/que-es-la-inteligencia-artificial-responsable/

El análisis comparado de casos corporativos evidencia que la adopción de IAG en la toma de decisiones no resulta siendo estándar y plana, sino que responde a factores sectoriales, regulatorios y organizativos. Como se sintetizó en el cuadro precedente, las empresas tienden a implementar mecanismos de gobernanza híbrida humano–IA, donde la tecnología aporta velocidad, escala y consistencia, mientras que la supervisión humana asegura trazabilidad, transparencia y responsabilidad ética (Shrestha, Ben-Menahem & von Krogh, 2019).

La revisión de experiencias tan diversas como las de AstraZeneca, JPMorgan Chase, Amazon, Netflix, Siemens y BBVA muestra una convergencia clara en los beneficios derivados de la IAG, eficiencia operativa, innovación, reducción de costos y optimización de procesos, pero también en riesgos comunes como el exceso de confianza en los algoritmos, los sesgos derivados de los datos y los desafíos de responsabilidad legal y reputacional (D'Angelo et al., 2022). Tal como señalan Shrestha et al. (2019), la eficacia de los modelos híbridos humano–IA podría depender de mantener la supervisión humana activa y la validación constante de las recomendaciones algorítmicas.

En la misma línea, Jobin, Ienca y Vayena (2019) destacan que la convergencia en principios éticos globales —transparencia, justicia, responsabilidad y privacidad es indispensable para optimizar la adopción de IAG a nivel mundial. Por su parte, Floridi y Cowls (2019) subrayan que la gobernanza tecnológica efectiva exige combinar principios abstractos con mecanismos verificables, de modo que las organizaciones puedan pasar de la ética declarativa a la ética aplicada mediante estándares auditable y estructuras de control interno.

En consecuencia, el estudio comparado desarrollado en este capítulo permite concluir que, aunque la IAG puede llegar a potenciar las capacidades estratégicas y operativas de las corporaciones, su integración sostenible requiere estructuras de control interno robustas, estándares éticos verificables y marcos regulatorios adaptativos. Este cierre refuerza la necesidad de avanzar hacia un modelo de gobernanza corporativa de la IAG, analizado desde todos los ángulos y con una estrategia clara para su implementación.

2. Ética en el uso de la inteligencia artificial generativa

Respecto al uso de la IA, la ética se configura como un aspecto fundamental que se debe tener en cuenta en el debate del uso de las nuevas tecnologías, ya que, la tecnología y automatización está influyendo significativamente en la toma de decisiones, teniendo en cuenta que su uso conlleva el procesamiento de grandes volúmenes de información personal. Su uso e implementación con un alto estándar ético evita riesgos como la discriminación algorítmica. Por ello es primordial contar con marcos éticos claros que promuevan un desarrollo tecnológico sostenible y responsable.

En el contexto empresarial, la ética juega un papel crítico al construir confianza con los consumidores. Según el artículo publicado por Deloitte "AI ethics: A business imperative", las empresas que en sus operaciones implementan principios éticos claros en el uso de la inteligencia artificial pueden lograr fidelizar de forma más fehaciente a los consumidores.

Es así, como adoptar principios éticos en el uso de la IAG es un tema crucial en el panorama tecnológico actual, teniendo en cuenta que, las nuevas tecnologías y desarrollos tienen la capacidad de crear contenido nuevo y original, como textos, imágenes o música, revolucionando sectores como el entretenimiento, la educación y los negocios. Por tanto, su implementación debe garantizar que su uso se haga de una manera responsable y alineada con los valores sociales.

Con esto, se pretende que los usuarios puedan comprender cómo y por qué se generan ciertos resultados, lo que implica ofrecer explicaciones claras sobre los algoritmos utilizados y las fuentes de datos empleadas en el entrenamiento de los modelos y sistemas.

Por consiguiente, se hace indispensable para abordar dicho problema, la implementación de procesos rigurosos de auditoría y supervisión ética que aseguren la inclusión y equidad en los resultados generados en el uso de IAG, para lo cual, la capacitación al personal y estipular reglas claras con limites en creación y configuración de su uso para las compañías es fundamental.

Así mismo, la protección de los datos personales también es un pilar fundamental en el uso ético de la IAG. En muchas ocasiones, estos sistemas se entrenan con grandes volúmenes de datos que pueden incluir información personal sensible, sobre el particular, es menester que las empresas y organizaciones cumplan con las regulaciones de protección de datos tanto a nivel nacional como internacional, como es el caso del Reglamento General de Protección de Datos (GDPR) en Europa o la Ley 1581 de 2012 en Colombia, garantizando que para el tratamiento de datos, se cuente con el consentimiento informado de los titulares.

Por esto consideramos es fundamental reforzar la ética por parte de las compañías y los gobiernos corporativos con el objetivo de respetar los derechos de los titulares del dato, incluyendo, los principios como la minimización de los datos, donde solo se debe recolectar los datos idóneos y necesarios para los fines establecidos. Por tanto, el uso ético de la IAG exige, además, medidas de seguridad contundentes para prevenir el acceso no autorizado y la exposición de información confidencial.

La responsabilidad es una parte clave del debate ético sobre la IAG. No solo recae en quienes diseñan estos sistemas, sino también en las empresas que los incorporan a sus procesos. Ambos actores deben hacerse cargo de las consecuencias que estas tecnologías pueden tener en la sociedad, lo que incluye anticipar cuándo podrían usarse con fines indebidos, como para cometer fraudes digitales, y tomar medidas para evitarlo.

En ese escenario, recursos como los códigos de conducta para el desarrollo de IAG y las políticas éticas dentro de las organizaciones pueden orientar a los distintos participantes hacia un uso más prudente y consciente de la tecnología.

2.1. Ética aplicada a la protección de datos personales en Colombia en el uso de IAG

Las aplicaciones éticas y legales de la gestión de datos personales son la piedra angular de un nuevo desarrollo tecnológico hacia el desarrollo basado en la ética de tecnologías en el campo de áreas emergentes como la IAG.

En Colombia, este principio se expresa a través del derecho de habeas data y la Ley 1581 de 2012, con su implementación y obligaciones normativas que especifican responsabilidades para recopilar y procesar datos, con consideración por la privacidad de los datos y la confianza ciudadana. Un punto relevante en este proceso es el consentimiento informado: las personas deben ser completamente informadas y de manera abierta sobre el propósito y el alcance del procesamiento de sus datos, así como sobre cómo se aseguran sus derechos de acceso, modificación o eliminación de sus datos.

Además, nos impone una obligación ética y legal estándar de implementar controles de seguridad técnicos y administrativos para prevenir el acceso no autorizado, fugas de datos y/o divulgación inapropiada de información, lo cual se puede llevar a cabo con la ayuda de parámetros como el cifrado, el control de acceso y auditorías periódicas.

Con la IAG, las evaluaciones de impacto sobre el procesamiento de datos son especialmente relevantes, así como el papel de la IA en identificar y contener riesgos éticos, legales y reputacionales relacionados con modelos algorítmicos. Estas acciones ayudan a eliminar sesgos, proporcionar privacidad y demostrar que las autoridades competentes siguen cumpliendo. La ética relacionada con la protección de datos y el contexto colombiano no solo debe ir más allá de la regulación; también implica la expectativa de compromisos organizacionales asumidos por las compañías hacia la transparencia, la seguridad y el respeto de los derechos de los ciudadanos. Dichas prácticas no solo van a procurar proteger a los usuarios, también servirán como base para crear un espacio más seguro y responsable.

Teniendo en cuenta todo lo expuesto, es esencial indicar que dentro de las acciones que las empresas o compañías deben implementar, se encuentran establecer procesos y procedimientos internos orientados a demostrar un compromiso ético relacionado con la adopción de inteligencia artificial, en este sentido, las empresas deben centrarse en prevenir posibles riesgos, mitigar su impacto y establecer mecanismos de control efectivos para abordar cualquier irregularidad que pueda surgir.

3. La aplicación de la inteligencia artificial en la toma de decisiones corporativas.

La inteligencia artificial, especialmente la generativa, está destinada a revolucionar la toma de decisiones en las empresas. Ya no se ve solo como un software para automatizar tareas, sino como un apoyo estratégico que define las prioridades, la asignación de recursos y los riesgos desde el nivel corporativo. Este cambio obliga a reconsiderar lo que es una buena gobernanza corporativa, ya que las decisiones no solo dependerán del juicio humano. Ahora, los sistemas que incorporan datos, modelos algorítmicos y revisión humana se unen para validar los hallazgos (Raisch & Krakowski, 2023).

En la práctica, los ejecutivos y los comités ejecutivos se encuentran en una posición complicada al necesitar tanto implementar oportunidades de inteligencia artificial, como una mejor predicción, velocidad de respuesta y personalización, como gestionar riesgos nuevos o ampliados que pueden implicar sesgos, opacidad o responsabilidad legal y reputacional (Stix et al., 2024). Todas estas tensiones impulsan la gobernanza de la inteligencia artificial en las agendas del CAIO, CEO y los consejos de administración corporativos.

Por lo tanto, es imperativo entender cómo la gobernanza de la IA impacta las decisiones estratégicas en las organizaciones y cómo los marcos de gobernanza, los controles internos y la cultura organizacional necesitan ajustarse para apoyar decisiones responsables, éticas y eficientes.

No obstante, la incorporación de la IAG transforma los procesos internos de gestión, pero a su vez plantea interrogantes jurídicos de especial relevancia respecto de la atribución de responsabilidad dentro de la estructura empresarial. Si las decisiones estratégicas comienzan a depender, total o parcialmente, de sistemas algorítmicos, resulta necesario examinar hasta qué punto los deberes tradicionales de los administradores, particularmente los de diligencia, lealtad y supervisión, conservan su alcance original o requieren una reinterpretación acorde con los nuevos riesgos tecnológicos.

En este sentido, la discusión ya no se limita a la eficiencia operativa o al aprovechamiento de oportunidades derivadas de la inteligencia artificial. También comprende la necesidad de determinar quién debe liderar su implementación, quién responde frente a eventuales errores, sesgos o afectaciones a terceros, y qué mecanismos de control deben adoptarse para asegurar un uso compatible con el interés social de la empresa. Bajo esta perspectiva, la inteligencia artificial deja de ser un asunto exclusivamente tecnológico para convertirse en una cuestión central del gobierno corporativo y de la responsabilidad fiduciaria.

4. Responsabilidad fiduciaria y gobernanza de la inteligencia artificial

La incorporación de sistemas de inteligencia artificial en las organizaciones ha trasladado las discusiones sobre innovación tecnológica al núcleo del gobierno corporativo. Cuando los procesos empresariales comienzan a depender de herramientas algorítmicas capaces de influir en decisiones estratégicas, evaluación de riesgos, tratamiento de información o estructuras de supervisión interna, surge la necesidad de reinterpretar el alcance de los deberes fiduciarios de los administradores frente a entornos cada vez más automatizados. En este contexto, la inteligencia artificial no constituye únicamente una herramienta técnica, sino un fenómeno capaz de impactar la atribución de responsabilidad, la rendición de cuentas y los mecanismos internos de gobernanza corporativa.

4.1. Deber fiduciario y nuevos estándares de gobernanza en la adopción de inteligencia artificial

La incorporación de sistemas de inteligencia artificial en la toma de decisiones corporativas obliga a replantear el alcance tradicional de los deberes fiduciarios de los administradores.

En el contexto colombiano, el artículo 24 de la Ley 222 de 1995 exige actuar de buena fe, con lealtad y con la diligencia de un buen hombre de negocios. Sin embargo, cuando las decisiones estratégicas se apoyan en sistemas algorítmicos, surge la necesidad de interpretar estos deberes a la luz de nuevos riesgos asociados a la opacidad tecnológica, los sesgos automatizados y la pérdida de control decisorio.

El deber de cuidado ya no se agota en revisar información financiera, operativa o comercial. También comprende la obligación de evaluar la calidad de los datos utilizados, la confiabilidad de los modelos implementados y las limitaciones técnicas de los sistemas empleados. La literatura especializada ha advertido que los modelos de IA pueden reproducir sesgos estructurales, operar bajo lógicas poco transparentes o producir resultados difíciles de verificar, lo que exige una supervisión reforzada por parte de la administración (Selbst et al., 2019). En consecuencia, el administrador diligente no puede limitarse a aceptar resultados automatizados, sino que debe cuestionarlos, contrastarlos y valorar sus efectos sobre el interés social.

El deber de lealtad igualmente adquiere una nueva dimensión. La adopción de inteligencia artificial debe responder al beneficio de la sociedad y no únicamente a indicadores de eficiencia o rentabilidad inmediata. Existen escenarios en los que los sistemas algorítmicos pueden maximizar resultados económicos a costa de riesgos éticos, legales o reputacionales. Por ello, la doctrina ha señalado que la automatización no elimina la dimensión ética del gobierno corporativo, sino que la intensifica (Floridi et al., 2018).

Bajo esta lógica, también se transforma el estándar del "buen hombre de negocios". Dicho parámetro ya no puede reducirse a la experiencia comercial o al juicio gerencial clásico, sino que exige un nivel razonable de comprensión tecnológica. Es decir, exigirle a la administración la capacidad de entender el funcionamiento general de las herramientas que aprueba, sus límites y sus riesgos. Como señalan Rai et al. (2019), la integración efectiva de IA en las organizaciones requiere líderes capaces de interactuar críticamente con estos sistemas y no solo de adoptarlos.

En este escenario, la inteligencia artificial no sustituye la responsabilidad humana. Su función es instrumental y de apoyo, mientras que la decisión final continúa siendo atribuible a quienes ostentan el poder de dirección. Por ello, la delegación en sistemas automatizados no opera como eximente de responsabilidad, sino como ampliación del ámbito de supervisión exigible a los administradores.

Ahora bien, esa responsabilidad reforzada exige la existencia de un marco regulatorio interno que permita gobernar la tecnología. La implementación de sistemas de IA sin políticas, procedimientos y controles específicos puede constituir una forma de negligencia organizacional, al omitir medidas razonables frente a una herramienta de alto impacto (Calo, 2017). En otras palabras, no resulta jurídicamente neutro adoptar inteligencia artificial sin estructuras de gobernanza.

Uno de los principales riesgos de esa omisión es la falta de trazabilidad, cuando no existen protocolos claros, registros o responsables definidos, se dificulta reconstruir cómo se adoptó una decisión automatizada y qué variables influyeron en ella. A ello se suma la falta de explicabilidad, entendida como la posibilidad de justificar razonablemente los resultados del sistema frente a accionistas, autoridades o terceros afectados. La ausencia de trazabilidad y explicabilidad debilita la rendición de cuentas y compromete el cumplimiento del deber de diligencia (Floridi et al., 2018).

Igualmente, la inexistencia de controles internos reduce la capacidad de la administración para detectar errores, sesgos o desviaciones estratégicas. Sin reglas claras sobre uso permitido, validación de resultados, revisión humana y escalamiento de incidentes, la organización queda expuesta a decisiones automatizadas incompatibles con el interés social.

Estas deficiencias tienen impacto en el deber de diligencia de los administradores, teniendo en cuenta que sus decisiones deben ser adoptadas de buena fe, de manera informada y mediante procesos razonables. Si no existen políticas internas, auditorías o evidencia de supervisión tecnológica, dicha protección se debilita sustancialmente, pues la diligencia deja de poder demostrarse (Calo, 2017).

Desde una perspectiva práctica, lo anterior exige que las organizaciones adopten políticas corporativas sobre inteligencia artificial, definan responsables internos, documenten decisiones relevantes, establezcan mecanismos de validación humana y desarrollen controles periódicos sobre los sistemas implementados. También resulta indispensable promover una cultura organizacional que evite la confianza ciega en la automatización y preserve el juicio crítico en la toma de decisiones.

El artículo 24 de la Ley 222 de 1995 consagra un estándar de actuación basado en buena fe, lealtad y diligencia. Este estándar exige hoy una lectura funcional frente a tecnologías capaces de incidir materialmente en la conducta empresarial. La inteligencia artificial no reemplaza la norma: exige una lectura contemporánea de sus deberes.

En este nuevo escenario, el deber de cuidado comprende no solo la adopción de decisiones razonables, sino también la selección adecuada de herramientas tecnológicas, la comprensión suficiente de sus límites, la evaluación de riesgos previsibles y la existencia de controles efectivos sobre su uso. Del mismo modo, el deber de lealtad exige que la implementación de IA responda al interés social de la compañía y no únicamente a incentivos de eficiencia inmediata, ahorro de costos o automatización acrítica.

La responsabilidad tampoco se diluye en la tecnología. Por el contrario, la utilización de sistemas automatizados intensifica las exigencias de supervisión, documentación y rendición de cuentas. Conceptos desarrollados en este capítulo —como curaduría tecnológica, gobernanza transversal y *accountability*— reflejan que el administrador contemporáneo debe asumir una posición activa frente a la tecnología y no una confianza pasiva en sus resultados (OECD, 2023; Floridi et al., 2018).

Asimismo, la inteligencia artificial debe entenderse como asunto estratégico. Su capacidad de afectar productividad, competitividad, reputación, continuidad operativa y valor empresarial exige intervención de la alta dirección y de los órganos societarios competentes. Tratarla exclusivamente como tema del área técnica implica desconocer su incidencia real sobre la estructura de riesgos de la organización.

Desde una perspectiva práctica, esta redefinición del deber fiduciario exige incorporar la IA dentro de los procesos formales de decisión estratégica y gestión de riesgos, ello supone adoptar tecnologías útiles para la empresa, pero también establecer políticas internas, auditorías, líneas claras de responsabilidad, supervisión periódica y mecanismos de respuesta ante incidentes.

4.2. Supervisión y curaduría tecnológica en sistemas de inteligencia artificial

La creciente incorporación de sistemas de inteligencia artificial en la toma de decisiones empresariales plantea una cuestión central en materia de responsabilidad: ¿hasta dónde llega la obligación de los administradores cuando las decisiones son generadas, sugeridas o condicionadas por sistemas algorítmicos? En el marco del artículo 24 de la Ley 222 de 1995, la respuesta parte de un principio básico: la utilización de tecnología no desplaza los deberes fiduciarios de dirección, diligencia y control.

La delegación de funciones en herramientas tecnológicas no equivale a una transferencia de responsabilidad, aunque la organización utilice sistemas avanzados de análisis, predicción o automatización, la decisión final y sus consecuencias continúan vinculadas a quienes ostentan la capacidad de administración. En este sentido, la inteligencia artificial debe entenderse como un instrumento de apoyo y no como un sustituto del juicio empresarial. La literatura ha advertido que los sistemas algorítmicos pueden operar con sesgos, errores o criterios poco transparentes, lo que impide considerarlos agentes autónomos de decisión (Selbst et al., 2019).

De ello se desprende la imposibilidad de delegar completamente en la IA. Una delegación absoluta supondría aceptar decisiones sin validación humana, lo cual resulta incompatible con el deber de cuidado exigible a los administradores. La automatización no elimina la necesidad de supervisión; por el contrario, exige formas más rigurosas de vigilancia y control sobre los sistemas utilizados (Calo, 2017).

En este contexto adquiere relevancia la noción de curaduría tecnológica, entendida como el conjunto de acciones mediante las cuales la administración selecciona, supervisa, interpreta y corrige el funcionamiento de los sistemas de IA. No se trata únicamente de aprobar la adquisición de una herramienta, sino de monitorear su desempeño, revisar la calidad de sus resultados e intervenir cuando existan desviaciones, inconsistencias o riesgos relevantes.

La curaduría tecnológica se opone al uso pasivo de la inteligencia artificial. Mientras este último implica aceptar acríticamente los resultados generados por el sistema, la curaduría exige una interacción activa y responsable con la tecnología. Bajo esta lógica, cobra

importancia el enfoque *human-in-the-loop*, que preserva la intervención humana en decisiones relevantes como mecanismo de control y atribución de responsabilidad (Rai et al., 2019).

Para efectos del presente artículo, la curaduría tecnológica puede entenderse como una manifestación reforzada del deber de supervisión empresarial frente al uso corporativo de sistemas de inteligencia artificial. La expresión "curaduría" no se emplea en un sentido estrictamente técnico, sino como una analogía orientada a describir una función activa de selección, evaluación, monitoreo y eventual intervención sobre herramientas tecnológicas capaces de incidir en decisiones organizacionales relevantes. Bajo esta perspectiva, la administración no solo debe autorizar la implementación de sistemas algorítmicos, sino también comprender razonablemente sus alcances, verificar sus condiciones de funcionamiento y mantener capacidad de reacción frente a riesgos previsibles.

A diferencia de mecanismos tradicionales de supervisión o auditoría, la curaduría tecnológica supone una aproximación continua y dinámica frente al comportamiento de la herramienta implementada. Mientras la auditoría suele operar mediante controles periódicos o verificaciones posteriores, la curaduría incorpora una lógica permanente de acompañamiento y evaluación sobre el uso empresarial de la inteligencia artificial. Ello comprende, entre otros aspectos, la revisión de riesgos emergentes, la validación de criterios de funcionamiento, la supervisión de resultados y, en casos necesarios, la modificación, suspensión o retiro de sistemas que generen afectaciones incompatibles con el interés social, el cumplimiento normativo o los deberes fiduciarios de los administradores.

El alcance de la responsabilidad también depende del nivel de control que razonablemente puedan ejercer los administradores. Si bien no se les puede exigir conocimiento técnico especializado propio de desarrolladores o ingenieros, sí se espera una comprensión suficiente del funcionamiento general del sistema, sus límites, fuentes de error y riesgos jurídicos asociados. La ausencia de esta comprensión puede constituir una omisión del deber de diligencia, especialmente cuando se adoptan decisiones estratégicas basadas en herramientas no entendidas por quienes las autorizan.

Desde una perspectiva práctica, ello exige establecer procesos de validación de resultados, controles periódicos, definición clara de responsables internos y protocolos de escalamiento ante incidentes. Igualmente, los sistemas implementados deben guardar relación con la naturaleza de la empresa, pues la adopción de soluciones genéricas sin adecuación al contexto organizacional incrementa la probabilidad de errores y, con ello, la exposición jurídica.

La curaduría tecnológica cumple además una función probatoria. En eventuales controversias, los administradores deberán acreditar que no actuaron de forma pasiva frente a la tecnología, sino que ejercieron supervisión efectiva.

En consecuencia, la implementación de sistemas de inteligencia artificial exige mecanismos permanentes de supervisión, validación y control sobre las herramientas utilizadas. La curaduría tecnológica permite integrar esos procesos dentro de una lógica de gobernanza

activa, orientada a preservar trazabilidad, capacidad de reacción y control organizacional frente a decisiones asistidas por IA.

4.3. Dirección estratégica, control societario y rendición de cuentas en la gobernanza de la inteligencia artificial

La incorporación de inteligencia artificial en las organizaciones plantea una cuestión estructural de gobierno corporativo: ¿en qué nivel de la sociedad se origina la responsabilidad por su adopción, supervisión y control? La respuesta exige distinguir entre funciones operativas, estratégicas y de vigilancia, pues la IA no constituye una herramienta meramente técnica, sino un factor capaz de incidir en la estrategia empresarial, la gestión del riesgo y la sostenibilidad corporativa.

En el derecho societario colombiano, la estructura orgánica distribuye competencias entre la administración, la junta directiva y la asamblea general de accionistas. Los administradores ejecutan la gestión ordinaria; la junta directiva orienta la estrategia y supervisa la marcha del negocio; y la asamblea ejerce funciones de deliberación y control. Bajo este esquema, la gobernanza de la inteligencia artificial no puede quedar reducida al nivel operativo, dado que sus efectos exceden el ámbito tecnológico e impactan decisiones relevantes para la compañía.

Por ello, la junta directiva emerge como el principal órgano llamado a liderar esta materia. Su papel no se limita a autorizar la adquisición de herramientas de IA, sino que comprende la definición de políticas corporativas, criterios de uso, niveles de tolerancia al riesgo tecnológico y mecanismos de supervisión. La doctrina contemporánea ha señalado que los órganos de dirección deben asumir una participación activa frente a tecnologías emergentes con potencial impacto reputacional, financiero y regulatorio (OECD, 2023).

Desde esta perspectiva, la responsabilidad estratégica se consolida en la junta directiva, mientras que la implementación operativa corresponde a la administración, esta distribución no fragmenta la responsabilidad, sino que la articula en distintos planos: ejecución por parte de la administración, supervisión por la junta y control institucional por la asamblea general. En consecuencia, la omisión de cualquiera de estos niveles puede comprometer la eficacia del modelo de gobernanza.

La asamblea general de accionistas también conserva un rol relevante, aunque indirecto. Su función principal se manifiesta mediante el examen de la gestión social, la valoración del desempeño de administradores y directivos, y la exigencia de información suficiente sobre decisiones estratégicas relacionadas con inteligencia artificial. En empresas donde la IA puede afectar el valor de la sociedad o incrementar riesgos relevantes, la capacidad de control informada de la asamblea adquiere especial importancia.

En este contexto, la rendición de cuentas se convierte en un eje esencial. Los informes de gestión deben incorporar información clara sobre el uso de sistemas de IA, los beneficios esperados, los riesgos identificados y las medidas adoptadas para mitigarlos. No se trata

únicamente de una práctica de transparencia, sino de una manifestación concreta del deber fiduciario y del deber de información frente a los accionistas.

Asimismo, la junta directiva debe exigir reportes periódicos a la administración sobre desempeño de los sistemas implementados, incidentes relevantes, cumplimiento normativo y resultados de auditoría. Tales reportes permiten ejercer control informado y documentar que las decisiones fueron adoptadas sobre bases razonables.

Desde una perspectiva probatoria, la adecuada documentación de esta materia: actas de junta, matrices de riesgo, reportes internos e informes de gestión, puede resultar determinante para demostrar diligencia en eventuales controversias. En entornos tecnológicos complejos, la responsabilidad no se evalúa solo por el resultado obtenido, sino también por la calidad del proceso de supervisión desplegado.

En este contexto, la gobernanza de la inteligencia artificial requiere una articulación permanente entre dirección estratégica, supervisión organizacional y mecanismos de rendición de cuentas. La participación de la junta directiva, la administración y la asamblea permite integrar el uso de IA dentro de estructuras formales de control corporativo y gestión del riesgo.

4.4. Protección de datos personales, accountability y deber fiduciario en sistemas de inteligencia artificial

En entornos corporativos, la utilización de sistemas de inteligencia artificial plantea una tensión jurídica relevante entre la innovación tecnológica y las obligaciones derivadas del tratamiento de datos personales. Cuando estas herramientas procesan información de clientes, trabajadores, proveedores o terceros, surge la necesidad de determinar cómo se articula el deber fiduciario de los administradores con el cumplimiento del régimen de protección de datos, especialmente en escenarios donde los procesos automatizados carecen de plena transparencia.

El problema adquiere mayor intensidad cuando los sistemas de IA operan sobre datos sensibles, perfiles comportamentales o grandes volúmenes de información. En tales casos, no solo se incrementa el riesgo de accesos indebidos, tratamientos excesivos o decisiones automatizadas lesivas, sino también la exposición a sanciones administrativas y daños reputacionales. Por ello, la responsabilidad de los administradores no se limita al uso eficiente de la tecnología, sino que comprende la obligación de garantizar que su implementación respete los estándares legales aplicables.

El tratamiento de datos personales mediante inteligencia artificial debe sujetarse a principios tradicionales como legalidad, finalidad, necesidad, proporcionalidad, seguridad y confidencialidad. La utilización de tecnologías avanzadas no suspende estas exigencias; por el contrario, las refuerza. La literatura ha advertido que los sistemas de IA, al requerir grandes volúmenes de datos para entrenamiento, aprendizaje o mejora continua, aumentan el riesgo de uso indebido de la información y de afectaciones a los titulares (Greenleaf, 2018).

En este contexto cobra especial relevancia el principio de accountability o responsabilidad demostrada. Este estándar implica que las organizaciones no solo deben cumplir la normativa de protección de datos, sino también estar en capacidad de acreditar dicho cumplimiento mediante evidencia verificable. En materia de inteligencia artificial, ello supone trazabilidad sobre los datos utilizados, documentación de decisiones automatizadas, controles internos y auditorías periódicas (OECD, 2023).

Trasladado al ámbito societario, el *accountability* representa una manifestación reforzada del deber fiduciario. No basta con implementar sistemas técnicamente funcionales; los administradores deben asegurar que su operación sea compatible con los derechos de los titulares de la información y con las obligaciones regulatorias vigentes. En otras palabras, la diligencia empresarial también se mide por la capacidad de prevenir, gestionar y demostrar cumplimiento frente al uso de datos.

La relación con autoridades de control, como la Superintendencia de Industria y Comercio, resulta especialmente significativa. En Colombia, la autoridad no solo verifica requisitos formales, sino la existencia real de políticas internas, medidas de seguridad, procedimientos de atención de titulares y esquemas preventivos de gestión del riesgo. En ese sentido, la ausencia de controles efectivos puede interpretarse como incumplimiento del deber de diligencia y agravar la exposición sancionatoria (SIC, 2020).

Desde una perspectiva práctica, las organizaciones que emplean IA deben realizar evaluaciones de impacto sobre privacidad, especialmente cuando se utilicen datos sensibles o se adopten decisiones automatizadas relevantes. Asimismo, deben implementar políticas claras sobre minimización de datos, anonimización, límites de finalidad, acceso restringido y conservación segura de la información.

Igualmente, resulta indispensable establecer mecanismos de auditoría interna y monitoreo continuo. Tales instrumentos permiten detectar desviaciones, documentar decisiones, corregir fallos y generar evidencia sobre la gestión responsable del sistema. En eventuales investigaciones administrativas o controversias judiciales, esta documentación puede ser decisiva para acreditar diligencia empresarial.

Finalmente, los administradores deben asumir una supervisión activa sobre el tratamiento de datos en sistemas de IA, integrando las áreas jurídicas, tecnológica y de cumplimiento.

En definitiva, el uso de inteligencia artificial exige integrar la protección de datos personales dentro de los mecanismos corporativos de control, supervisión y cumplimiento normativo. La trazabilidad de la información, las auditorías internas y la capacidad de demostrar medidas preventivas se convierten en elementos esenciales para una gestión responsable de sistemas algorítmicos en entornos empresariales.

4.5. Riesgos jurídicos derivados del uso de sistemas de inteligencia artificial licenciados o públicos

La adopción empresarial de sistemas de inteligencia artificial provistos por terceros —especialmente bajo modelos SaaS, licencias empresariales o plataformas abiertas— plantea desafíos relevantes en materia de responsabilidad y control. Cuando la organización depende de infraestructuras externas para procesar información o apoyar decisiones estratégicas, surge una pregunta central: ¿hasta qué punto los administradores conservan el dominio jurídico sobre los datos, los procesos y los riesgos asociados al sistema utilizado?

La cuestión resulta especialmente sensible cuando se introducen datos personales, información confidencial o insumos estratégicos en plataformas cuya operación, almacenamiento o arquitectura técnica escapan al control directo de la empresa. En estos escenarios, la externalización tecnológica no elimina los deberes fiduciarios de los administradores; por el contrario, exige una diligencia reforzada en la selección, supervisión y uso de proveedores tecnológicos.

Desde la perspectiva del deber de diligencia, la contratación de herramientas de IA suministradas por terceros exige evaluar razonablemente los riesgos asociados al proveedor, especialmente cuando las decisiones empresariales dependen de dichos sistemas.

Uno de los principales riesgos jurídicos es la pérdida de control de la información. Las plataformas externas pueden implicar almacenamiento en servidores de terceros, tratamiento automatizado para mejora del servicio, reutilización de datos o transferencias internacionales de información. Tales dinámicas pueden comprometer la confidencialidad empresarial y generar incumplimientos en materia de protección de datos si no existen controles adecuados (Greenleaf, 2018).

A ello se suma la dependencia tecnológica de terceros, fenómeno que puede limitar la autonomía organizacional. Cuando procesos críticos dependen de un proveedor externo, la empresa reduce su capacidad de intervención frente a fallos, cambios unilaterales del servicio, interrupciones operativas o modificaciones técnicas no previstas. Este escenario se relaciona con riesgos de *vendor lock-in* y asimetría de información, donde el proveedor conserva mayor conocimiento y capacidad de control que el usuario corporativo (Rai et al., 2019).

Desde el plano contractual, también surgen riesgos relevantes. Muchos proveedores incorporan cláusulas de limitación de responsabilidad, exclusiones por errores del sistema o restricciones sobre disponibilidad del servicio. En la práctica, ello puede trasladar al usuario corporativo gran parte del riesgo jurídico derivado de decisiones adoptadas con apoyo de la herramienta. Así, incluso cuando el sistema es suministrado por un tercero, las consecuencias frente a clientes, accionistas o autoridades pueden recaer principalmente sobre la empresa usuaria.

Estos riesgos poseen además una dimensión reputacional. Filtraciones de datos, decisiones discriminatorias, respuestas erróneas o uso indebido de plataformas abiertas pueden afectar la confianza de clientes, inversionistas y demás grupos de interés. La literatura ha destacado

que la legitimidad empresarial en entornos digitales depende cada vez más de la capacidad de gestionar tecnologías emergentes de forma ética y responsable (Floridi et al., 2018).

Frente a este panorama, el deber de cuidado exige adoptar medidas preventivas concretas. En primer lugar, realizar procesos de *due diligence* tecnológica que incluyan revisión de términos contractuales, políticas de privacidad, estándares de seguridad, ubicación de datos y antecedentes del proveedor. En segundo lugar, establecer políticas internas que definan qué tipo de información puede cargarse en estas plataformas y en qué condiciones, restringiendo especialmente datos sensibles o estratégicos.

Desde una perspectiva contractual, los administradores deben procurar, en la medida de lo posible, cláusulas que distribuyan razonablemente los riesgos entre proveedor y usuario, evitando que la totalidad de la responsabilidad recaiga sobre la organización. Cuando ello no sea viable, al menos deben conocer los riesgos asumidos y adoptar medidas internas para mitigarlos.

Es así, como en términos reputacionales, la organización debe estar preparada para responder con transparencia frente a incidentes relacionados con el uso de IA. Ello exige protocolos de gestión de crisis, canales de comunicación claros y capacidad de reacción oportuna ante errores, filtraciones o controversias derivadas del sistema implementado.

En consecuencia, el uso empresarial de sistemas de inteligencia artificial suministrados por terceros exige combinar evaluación contractual, controles internos y supervisión continua sobre los riesgos tecnológicos asumidos. La dependencia de proveedores externos, el manejo de información sensible y las limitaciones operativas de estas plataformas convierten la gestión del riesgo tecnológico en una dimensión relevante de la administración corporativa.

4.6. Impacto organizacional de la inteligencia artificial, atribución de responsabilidad y gobernanza transversal.

Desde una perspectiva organizacional, la inteligencia artificial ofrece beneficios evidentes en términos de productividad, eficiencia operativa y generación de valor. Herramientas capaces de automatizar procesos, mejorar predicciones y optimizar decisiones pueden traducirse en reducción de costos y mayor competitividad (Brynjolfsson & McAfee, 2017; Davenport & Ronanki, 2018). Sin embargo, estos beneficios económicos no eliminan una cuestión jurídica central: ¿quién responde cuando las decisiones adoptadas con apoyo de IA producen daños, incumplimientos o riesgos relevantes para la sociedad?

Para comprender esta atribución de responsabilidad conviene distinguir distintos niveles dentro de la organización. Por una parte, se encuentran quienes diseñan, implementan o administran técnicamente la herramienta; por otra, quienes ejecutan procesos soportados por IA; y finalmente, quienes toman decisiones estratégicas basadas en los resultados generados por dichos sistemas. Aunque estas funciones puedan distribuirse internamente, la responsabilidad jurídica no se fragmenta de manera equivalente.

La doctrina sociotécnica ha señalado que las decisiones asistidas por IA continúan siendo decisiones organizacionales, pues los sistemas operan dentro de parámetros definidos por personas y al servicio de objetivos empresariales determinados (Rai et al., 2019). En ese sentido, la IA no puede concebirse como sujeto autónomo de responsabilidad, sino como instrumento inserto en la estructura decisoria corporativa. La diferencia entre quien implementa la tecnología y quien decide utilizarla resulta esencial. La implementación técnica puede corresponder a áreas especializadas; sin embargo, la determinación de adoptar, mantener o confiar en un sistema de IA recae en la administración y en los órganos de dirección. Tal decisión supone asumir los riesgos asociados a errores, sesgos, fallos operativos o consecuencias jurídicas derivadas del uso del sistema.

Adicionalmente, la automatización puede generar una falsa apariencia de objetividad, incentivando la aceptación acrítica de resultados algorítmicos y reduciendo el escrutinio humano. La literatura ha advertido este fenómeno como una fuente de riesgo relevante (Selbst et al., 2019).

En este contexto, la respuesta adecuada no consiste en rechazar la inteligencia artificial, sino en establecer modelos de gobernanza transversal, la implementación responsable de IA requiere liderazgo estratégico desde la alta dirección, participación del área jurídica y de cumplimiento, intervención técnica especializada y mecanismos internos claros de supervisión.

El liderazgo principal debe recaer en administradores y junta directiva, quienes tienen la capacidad de definir políticas corporativas, asignar recursos y establecer límites de uso. El área de *compliance* cumple una función decisiva al traducir estos lineamientos en controles normativos, protocolos internos y esquemas preventivos. Por su parte, las áreas tecnológicas ejecutan la implementación operativa, mantenimiento y monitoreo de las herramientas utilizadas.

La gobernanza transversal exige, además, coordinación entre estas áreas. La ausencia de roles claros o la fragmentación funcional puede generar vacíos de control, dificultar la atribución de responsabilidades y debilitar la capacidad de respuesta ante incidentes. Por ello, resultan recomendables comités interdisciplinarios, matrices de responsabilidad, políticas internas sobre IA y canales de reporte periódico a la administración.

Desde una perspectiva práctica, también es necesario documentar el grado de intervención humana en decisiones relevantes, establecer procesos de validación de resultados, revisar impactos jurídicos y evaluar periódicamente si los beneficios obtenidos compensan los riesgos asumidos. La eficiencia tecnológica no puede analizarse aisladamente de los costos legales, reputacionales o regulatorios que una mala implementación puede generar.

En síntesis, la inteligencia artificial exige estructuras internas capaces de coordinar supervisión, cumplimiento y toma de decisiones estratégicas. Por ello, la IA no debe entenderse como un asunto exclusivamente técnico, sino como una materia transversal que

involucra a la administración, las áreas de cumplimiento y los órganos de dirección corporativa.

5. Propuesta de implementación para la gobernanza corporativa de la inteligencia artificial

Luego del análisis desarrollado en los capítulos precedentes sobre el impacto de la inteligencia artificial en la toma de decisiones corporativas, los deberes fiduciarios de los administradores y la necesidad de estructuras adecuadas de gobernanza, resulta pertinente avanzar hacia una dimensión aplicada del problema. En efecto, identificar riesgos jurídicos y organizacionales constituye apenas una primera etapa; el verdadero desafío consiste en traducir tales hallazgos en mecanismos internos capaces de orientar una adopción responsable de estas tecnologías dentro de la empresa.

Con este propósito, se formula una propuesta de implementación para la gobernanza corporativa de la inteligencia artificial, concebida como una herramienta práctica dirigida a órganos de administración, juntas directivas y áreas de cumplimiento. El modelo integra criterios jurídicos, organizacionales y operativos, con el fin de facilitar procesos de adopción tecnológica compatibles con el deber de diligencia, la gestión de riesgos y la creación sostenible de valor.

5.1. Justificación y necesidad de un modelo práctico de implementación

La incorporación de sistemas de inteligencia artificial en las organizaciones exige revisar la capacidad de las estructuras tradicionales de gobierno corporativo para responder a nuevos riesgos tecnológicos. Entre ellos se encuentran los sesgos algorítmicos, la opacidad decisoria, las afectaciones a datos personales, la dependencia tecnológica y los eventuales escenarios de responsabilidad. En este contexto, uno de los principales desafíos consiste en traducir tales riesgos en mecanismos internos de prevención, supervisión y control efectivos.

No basta, por tanto, con reconocer que la inteligencia artificial introduce retos relevantes para la gestión corporativa. También es necesario convertir ese diagnóstico en estructuras organizacionales, protocolos internos y herramientas de seguimiento que permitan incorporar innovación sin sacrificar control, legalidad ni responsabilidad. La sola identificación del riesgo, sin medidas concretas de respuesta, puede situar a la organización en escenarios de vulnerabilidad operativa y jurídica.

Esta necesidad se hace especialmente visible cuando la adopción tecnológica avanza con mayor rapidez que la actualización de los modelos internos de gobernanza. En tales supuestos, la implementación de herramientas de inteligencia artificial suele responder a objetivos de eficiencia, reducción de costos o ventaja competitiva, sin acompañarse de políticas corporativas claras, matrices de riesgo o delimitación suficiente de responsabilidades internas.

En el caso colombiano, esta situación adquiere particular relevancia si se considera que el régimen societario vigente ya impone a los administradores deberes de buena fe, lealtad y diligencia, especialmente a través del artículo 24 de la Ley 222 de 1995. Tales deberes no desaparecen frente al uso de nuevas tecnologías; por el contrario, exigen anticipar riesgos previsibles, adoptar decisiones informadas y establecer mecanismos razonables de vigilancia sobre procesos capaces de impactar el interés social de la compañía.

Desde esta perspectiva, la inteligencia artificial no constituye únicamente un asunto tecnológico, sino una materia vinculada con el deber fiduciario contemporáneo. La adopción de sistemas automatizados para apoyar decisiones empresariales obliga a fortalecer prácticas de supervisión, documentación y trazabilidad. La diligencia empresarial moderna no se mide exclusivamente por resultados financieros, sino también por la capacidad de gobernar responsablemente herramientas tecnológicas complejas.

Aunque existen avances regulatorios y mayor atención institucional sobre la materia, en el ámbito empresarial persisten dificultades para traducir tales desarrollos en instrumentos operativos de aplicación interna, especialmente en organizaciones medianas o en estructuras que no cuentan con áreas especializadas de innovación o cumplimiento digital. Subsiste así una brecha entre los marcos generales de gobernanza y su implementación cotidiana.

Con fundamento en lo anterior, se propone un modelo práctico de implementación para la gobernanza corporativa de la inteligencia artificial, concebido como herramienta orientadora para organizaciones que buscan incorporar estas tecnologías bajo criterios de responsabilidad, control y creación sostenible de valor.

El modelo se estructura en dos componentes complementarios: una lista estratégica de verificación dirigida a órganos de dirección y alta gerencia, y una hoja de ruta progresiva de implementación a 90, 180 y 365 días, orientada a consolidar un esquema maduro de supervisión continua.

Más que un simple instrumento técnico, la propuesta busca demostrar que la innovación y el cumplimiento no son objetivos incompatibles. Por el contrario, una ventaja competitiva sostenible depende cada vez más de la capacidad de adoptar inteligencia artificial con criterios sólidos de gobernanza, previsión jurídica y responsabilidad estratégica.

5.2. Propuesta de marco corporativo para la adopción responsable de inteligencia artificial

El análisis desarrollado en los capítulos anteriores permite concluir que la incorporación de inteligencia artificial en las organizaciones requiere mecanismos internos capaces de ordenar su uso, distribuir responsabilidades y reducir riesgos relevantes para la empresa. En ese contexto, el modelo que aquí se presenta tiene una finalidad eminentemente práctica: servir como guía para estructurar procesos corporativos de adopción, supervisión y mejora continua de estas tecnologías.

La propuesta se concibe como una herramienta flexible, aplicable a organizaciones de distinta dimensión, sector económico o nivel de madurez digital. No pretende imponer un esquema único de actuación, sino ofrecer criterios mínimos de referencia que puedan adaptarse según la complejidad operativa, el tipo de decisiones automatizadas y el grado de exposición jurídica o reputacional de cada empresa.

Su diseño responde a una lógica preventiva. En lugar de intervenir únicamente cuando surgen incidentes, el modelo busca anticipar riesgos mediante controles previos, definición de competencias internas, revisión periódica y documentación suficiente de los procesos relacionados con inteligencia artificial. De esta forma, la gobernanza tecnológica se integra a los sistemas ordinarios de administración y control empresarial.

Para facilitar su implementación, la propuesta se divide en dos componentes complementarios, así:

5.2.1. Parte A. Lista estratégica de verificación

Comprende un conjunto de aspectos que la organización debería revisar antes y durante el uso de sistemas de inteligencia artificial. Entre ellos se incluyen la identificación de riesgos, políticas internas, tratamiento de datos, trazabilidad, supervisión humana, relación con proveedores, criterios ESG y reporte a órganos de dirección.

Nº	Ítem de verificación	Objetivo	Evidencia / Documentación	Responsable
1	Evaluación de riesgos y beneficios	Garantizar que la IA generativa aporta valor y minimiza riesgos éticos/legales	Matriz de riesgos firmada por la junta	Comité de Riesgos / CEO
2	Política corporativa de uso de IA	Definir límites, casos permitidos y prohibidos	Documento aprobado por la Junta Directiva	Director de Cumplimiento
3	Transparencia algorítmica	Conocer fuentes de datos y sesgos potenciales	Informe técnico del proveedor o equipo interno	CTO / CDO
4	Protección de datos personales	Cumplimiento de normativas (GDPR, Ley 1581/2012 en Colombia)	Actas de auditoría de datos	Oficial de Privacidad
5	Trazabilidad de decisiones asistidas por IA	Poder justificar cada recomendación generada por IA	Registro de decisiones y fuente algorítmica	Comité de Auditoría
6	Capacitación ética y técnica del personal	Asegurar que los tomadores de decisiones entienden la tecnología	Plan de formación anual	Gerencia de Talento Humano
7	Evaluación continua de proveedores de IA	Evitar dependencia de soluciones opacas o no certificadas	Informe de due diligence	Comité de Compras
8	Simulación de incidentes y crisis	Prepararse ante errores de la IA o fugas de datos	Registro de simulacros	Comité de Continuidad de Negocio
9	Revisión periódica de impacto	Medir beneficios y riesgos reales frente a lo proyectado	Informe trimestral a la junta	Comité de Estrategia
10	Alineación con principios ESG	Integrar el uso de IA en sostenibilidad y responsabilidad social	Informe ESG anual	CEO / Director de Sostenibilidad

5.2.2. Parte B. Hoja de ruta progresiva de implementación (90, 180 y 365 días)

Establece una secuencia gradual de acciones orientadas a pasar de un diagnóstico inicial a un modelo consolidado de gobernanza. Esta metodología permite priorizar medidas urgentes en el corto plazo, fortalecer capacidades internas en una etapa intermedia y consolidar procesos maduros de supervisión continua en el largo plazo.

La utilidad del modelo radica en que traduce principios generales de responsabilidad corporativa en acciones verificables dentro de la empresa. Así, la inteligencia artificial deja de ser únicamente una decisión tecnológica para convertirse en un proceso institucional sujeto a dirección, control y rendición de cuentas.

Plazo	Acciones clave	Responsable(s)	Métricas de éxito
0–90 días (Inicio y diagnóstico)	- Realizar diagnóstico de uso actual de IA en la empresa. - Identificar procesos donde la IA generativa puede aportar valor. - Definir y aprobar política interna de uso de IA. - Formar un comité de IA con miembros de TI, legal, riesgos y negocio.	CEO, CTO, Director Legal	- Política aprobada. - Comité conformado. - Informe de diagnóstico entregado.
90–180 días (Despliegue controlado)	- Implementar pilotos controlados de IA en 1-2 áreas. - Establecer sistema de trazabilidad y documentación de decisiones. - Realizar capacitación técnica y ética a directivos y personal clave. - Definir protocolos de auditoría interna.	CTO, Comité de IA, Talento Humano	- Pilotos operativos. - 100% de directivos capacitados. - Protocolos de auditoría definidos.
180–365 días (Escalado y gobernanza continua)	- Extender el uso de IA a otras áreas con base en resultados del piloto. - Implementar revisiones trimestrales de riesgos y beneficios. - Integrar métricas de IA en informes ESG y de gestión. - Simular escenarios de riesgo (ej. sesgo, fuga de datos).	CEO, Comité de IA, Auditoría Interna	- 80% de áreas críticas con IA implementada. - Informes trimestrales presentados. - Simulacro realizado y evaluado.

El modelo presentado ofrece una ruta estructurada para pasar de la intención de adoptar inteligencia artificial a un esquema real de gobernanza interna. Seguidamente, se desarrollan los fundamentos jurídicos y funcionales que justifican cada uno de sus componentes.

5.3. Alcance jurídico y funcional del modelo propuesto

El valor principal del modelo planteado no reside únicamente en su utilidad operativa, sino en su capacidad para traducir exigencias jurídicas y principios de buen gobierno corporativo en medidas concretas de aplicación empresarial, es decir, permite convertir deberes generales de diligencia, supervisión y control en acciones verificables dentro de la organización, reduciendo así la distancia entre la regulación abstracta y la gestión cotidiana de la inteligencia artificial.

Desde la perspectiva del derecho societario colombiano, el artículo 24 de la Ley 222 de 1995 exige a los administradores actuar de buena fe, con lealtad y con la diligencia de un buen hombre de negocios. En entornos tecnológicos, este estándar implica adoptar decisiones informadas, prever riesgos razonablemente identificables y establecer controles proporcionales frente a procesos que puedan comprometer el interés social de la compañía.

El modelo propuesto busca precisamente facilitar el cumplimiento práctico de tales deberes.

5.3.1. Alcance funcional de la Parte A: lista estratégica de verificación

En primer lugar, se encuentra la verificación de riesgos y beneficios, etapa en la que la organización analiza su modelo de negocio, las áreas donde pretende implementar inteligencia artificial y el nivel de exposición derivado de su uso. En esta fase resulta indispensable identificar el alcance de las decisiones que serán asistidas por IA, pues la responsabilidad no será uniforme en todos los casos, sino que dependerá del tipo de decisión y de riesgos asociados como errores operativos, sesgos, uso indebido de datos personales, afectaciones reputacionales o impactos sobre terceros.

Con base en ello, se requiere la construcción de una matriz de riesgo diseñada conforme a las características de la empresa, su actividad económica y el tipo de tecnología que desea incorporar. Para su adecuada elaboración conviene la participación de distintas áreas mediante un equipo multidisciplinario y su validación por la junta directiva o el máximo órgano competente. Desde la perspectiva del gobierno corporativo, este paso permite evidenciar una actuación diligente, pues la ausencia de evaluación previa puede facilitar la imputación de riesgos previsibles posteriormente materializados.

Identificados los riesgos, corresponde definir políticas internas claras que establezcan usos permitidos y prohibidos, lineamientos legales aplicables y niveles de supervisión humana según la criticidad de cada proceso. A mayor exposición al riesgo, mayor debe ser la intensidad de los controles adoptados.

No obstante, el valor de estas políticas no radica únicamente en su existencia documental, sino en su implementación efectiva. Para ello, deben contar con aprobación orgánica, adecuada divulgación interna e integración con los procesos empresariales. Solo de esa manera se convierten en mecanismos reales de control y en una primera línea de defensa frente a contingencias derivadas del uso de inteligencia artificial.

Otro componente relevante es la transparencia algorítmica. Las compañías no requieren comprender el funcionamiento técnico del sistema en profundidad, pero sí conocer elementos suficientes para cuestionarlo y supervisarlo. Esto supone identificar el origen de los datos, el tipo de modelo utilizado y sus principales limitaciones. En la práctica, se traduce en exigir a proveedores o equipos técnicos reportes comprensibles para la alta dirección. La transparencia no elimina la complejidad tecnológica, pero reduce la dependencia ciega y fortalece la capacidad de control de los administradores.

Un punto igualmente esencial es la protección de datos personales, dado que los sistemas de IA operan mediante recolección y análisis de información. Su implementación exige identificar qué datos se utilizan, especialmente si son sensibles, limitar su tratamiento a lo necesario, establecer controles de acceso y seguridad, y realizar auditorías periódicas. Este componente no puede tratarse como un asunto aislado del área jurídica, sino integrarse desde el diseño del sistema, con suficiente documentación que permita demostrar cumplimiento.

La trazabilidad de decisiones asistidas por IA representa un cambio relevante en los procesos corporativos. Ya no basta con conocer el resultado final, sino que resulta necesario reconstruir cómo se adoptó la decisión. En términos prácticos, ello implica registrar la herramienta utilizada, la información procesada y la validación humana correspondiente. La trazabilidad permite acreditar control, razonabilidad y supervisión frente a eventuales controversias.

Dentro del plan de implementación también es fundamental la capacitación del personal. Directivos y colaboradores deben comprender qué puede hacer la inteligencia artificial, cuáles son sus límites y cómo interactuar con ella de forma diligente. Esta formación debe abarcar aspectos técnicos básicos, así como criterios éticos, legales y de responsabilidad organizacional.

Uno de los riesgos menos visibles en la implementación de inteligencia artificial es la dependencia frente a proveedores externos. Muchas organizaciones utilizan soluciones desarrolladas por terceros, lo que introduce riesgos asociados a continuidad del servicio, opacidad tecnológica, manejo de datos y limitaciones contractuales. Por ello, la evaluación continua de proveedores no debe entenderse como una revisión exclusiva del momento de contratación, sino como un mecanismo permanente de control.

En la práctica, este proceso inicia con ejercicios de debida diligencia orientados a revisar condiciones contractuales, cláusulas de responsabilidad, políticas de tratamiento de datos y estándares de seguridad. Posteriormente, exige revisiones periódicas que permitan detectar cambios en el funcionamiento del sistema, nuevas dependencias tecnológicas o variaciones en el manejo de la información. Su resultado debe reflejarse en informes actualizados que faciliten decisiones informadas sobre continuidad, modificación o sustitución del proveedor, y que además acrediten control sobre terceros.

Otro componente esencial corresponde a la simulación de incidentes y crisis. Los sistemas de IA pueden fallar, generar respuestas incorrectas o afectar a terceros, por lo que no basta con prevenir riesgos: también es necesario prepararse para responder a ellos. En términos prácticos, ello implica diseñar escenarios realistas —como filtraciones de datos, decisiones automatizadas erróneas o sesgos relevantes— y desarrollar simulacros con participación de las áreas involucradas.

El valor de estos ejercicios radica en que permiten identificar debilidades operativas, fallos de comunicación y vacíos decisorios antes de que ocurra un incidente real. Cada simulacro debe documentarse mediante informes o actas, los cuales constituyen evidencia útil de gestión del riesgo y fortalecen la capacidad de respuesta institucional.

La revisión periódica de impacto busca evitar la pérdida progresiva de control sobre tecnologías ya implementadas. Su finalidad es verificar si la inteligencia artificial está generando los beneficios esperados y si los riesgos inicialmente identificados continúan siendo adecuadamente gestionados. Para ello, conviene elaborar reportes periódicos que

incluyan indicadores de desempeño, eventos de riesgo, errores detectados y ajustes adoptados.

Lo relevante no es solo producir estos informes, sino asegurar que lleguen a la junta directiva o al órgano estratégico competente. Ello mantiene la supervisión en el más alto nivel organizacional y permite ajustar, limitar o suspender el uso de la tecnología cuando deje de generar valor o incremente riesgos relevantes.

Finalmente, la alineación con principios ESG incorpora una dimensión externa de responsabilidad corporativa. La organización no solo debe evaluar la eficiencia de la inteligencia artificial, sino también su impacto social, reputacional y de gobierno. En la práctica, esto supone incluir información sobre uso de IA en informes de sostenibilidad o gestión, abordando materias como transparencia, prevención de sesgos, protección de datos y estándares éticos.

En conjunto, esta primera parte convierte la gobernanza de la IA en un proceso institucionalizado y documentable, fortaleciendo la posición de la administración frente a eventuales cuestionamientos sobre diligencia o supervisión insuficiente.

5.3.2. Alcance funcional de la Parte B: hoja de ruta 90, 180 y 365 días

La primera fase de implementación, proyectada entre 0 y 90 días, tiene como finalidad establecer una base organizacional sólida antes de desplegar herramientas de inteligencia artificial. Iniciar procesos sin un diagnóstico claro puede generar más riesgos que beneficios, especialmente cuando no existen lineamientos internos ni responsables definidos.

El punto de partida consiste en identificar cuál es el estado actual del uso de IA dentro de la empresa. En muchos casos, estas herramientas ya se utilizan de forma dispersa en áreas como mercadeo, servicio al cliente o talento humano, sin supervisión centralizada. Detectar estos usos permite dimensionar riesgos existentes y no solo los futuros.

Posteriormente, corresponde evaluar en qué procesos la inteligencia artificial puede generar valor real para el negocio. Esto evita implementaciones motivadas únicamente por tendencias tecnológicas y orienta la adopción hacia necesidades concretas de la organización.

De manera paralela, debe aprobarse una política interna de uso de IA, destinada a fijar reglas básicas, límites operativos y criterios iniciales de control. Asimismo, resulta recomendable conformar un comité interdisciplinario con participación de áreas de tecnología, legal, riesgos y negocio, encargado de coordinar decisiones y supervisar la implementación.

El resultado esperado de esta etapa es una estructura mínima de gobernanza compuesta por diagnóstico inicial, política aprobada y responsables claramente definidos. Sin estos elementos, las fases posteriores tienden a desarrollarse de forma desordenada y con mayores niveles de exposición al riesgo.

La segunda fase de implementación, proyectada entre 90 y 180 días, corresponde al tránsito de la planeación a la ejecución, procurando que la adopción tecnológica se realice sin pérdida de control. Su objetivo principal es desarrollar pilotos limitados, y no soluciones definitivas, en una o dos áreas donde la inteligencia artificial pueda generar valor y donde los riesgos resulten manejables.

La selección de estos procesos debe responder a criterios estratégicos: potencial de mejora operativa, posibilidad de medición y baja exposición crítica frente a eventuales errores. La lógica de esta etapa consiste en aprender antes de escalar.

Durante esta fase adquiere especial relevancia la trazabilidad de decisiones asistidas por IA. Desde el momento en que la herramienta interviene en procesos corporativos, la organización debe registrar su uso, los datos empleados y la validación humana correspondiente. Más que un requisito técnico complejo, se trata de instaurar una cultura temprana de documentación y control.

De forma paralela, la capacitación del personal se convierte en eje central. Directivos y usuarios clave deben comprender el funcionamiento básico del sistema, sus límites y los criterios adecuados de interacción. Esta formación reduce errores y promueve un uso crítico de la tecnología.

Asimismo, conviene definir protocolos de auditoría interna que establezcan cómo se supervisará el uso de la inteligencia artificial, qué controles se aplicarán y cómo se detectarán desviaciones. Con ello, el control deja de ser reactivo y se incorpora desde el inicio de la implementación.

El resultado esperado de esta etapa es conocimiento práctico verificable: pilotos operativos, personal capacitado y mecanismos iniciales de supervisión que permitan avanzar hacia fases posteriores con mayor seguridad organizacional.

La tercera fase de implementación, proyectada entre 180–365 días, representa el paso de la experimentación al uso estructurado de la inteligencia artificial dentro de la organización. En esta etapa, el objetivo ya no es probar herramientas, sino consolidar un modelo estable de gobernanza tecnológica.

El escalamiento no debe ser automático, sino sustentado en los resultados obtenidos durante la fase anterior. Esto exige analizar qué procesos funcionaron adecuadamente, qué riesgos se materializaron y qué ajustes resultan necesarios antes de ampliar el uso de la tecnología a nuevas áreas.

La expansión debe realizarse de forma progresiva, priorizando procesos estratégicos donde la inteligencia artificial pueda generar mayor valor sin comprometer el control interno. De esta manera, el crecimiento del sistema se acompaña de supervisión suficiente.

Uno de los componentes centrales de esta fase es la revisión periódica de riesgos y beneficios, basada ya en la experiencia real de operación. Estas evaluaciones permiten verificar si la tecnología está generando los resultados esperados o si ha introducido riesgos adicionales. Conviene que sus resultados sean reportados trimestralmente a la alta dirección, manteniendo la supervisión en el nivel estratégico.

Asimismo, resulta conveniente integrar métricas de IA dentro de informes de gestión y reportes ESG, de modo que la tecnología deje de verse como elemento aislado y pase a formar parte de la estrategia corporativa.

En esta etapa también cobran relevancia las simulaciones de riesgo, mediante escenarios como sesgos decisorios, errores del sistema o fugas de datos, con el fin de medir la capacidad real de respuesta institucional.

El resultado esperado es una organización que no solo utiliza inteligencia artificial, sino que la gobierna mediante controles periódicos, reportes estratégicos y capacidad efectiva de reacción frente a contingencias.

El plan de implementación en 90, 180 y 365 días no es una simple distribución temporal de actividades. Es una estrategia que responde a una necesidad real: evitar que la adopción de inteligencia artificial se convierta en un proceso desordenado o riesgoso.

Su valor radica en que permite avanzar de manera progresiva, reduciendo la incertidumbre en cada etapa. Primero se entiende, luego se prueba y finalmente se escala. Este orden no es arbitrario, es lo que permite mantener el control.

5.3.3. Función probatoria y relevancia estratégica del modelo

Uno de los principales aportes de la propuesta radica en su utilidad probatoria. En escenarios de responsabilidad administrativa, societaria o reputacional, no basta invocar buena fe en la adopción tecnológica; suele ser necesario acreditar procesos internos de análisis, supervisión y respuesta. El modelo facilita esa demostración mediante matrices de riesgo, políticas aprobadas, informes periódicos, registros de decisiones, auditorías internas y evidencia de capacitación, los cuales pueden servir como soporte objetivo del cumplimiento del deber de diligencia por parte de administradores y órganos de dirección.

Al mismo tiempo, el esquema posee relevancia estratégica. Una organización que gobierna adecuadamente su inteligencia artificial no solo reduce contingencias jurídicas, sino que fortalece confianza interna, reputación externa, calidad decisoria y sostenibilidad competitiva.

En síntesis, la propuesta convierte principios generales de gobierno corporativo en una metodología concreta de implementación, integrando la inteligencia artificial como proceso sujeto a dirección, control y rendición de cuentas.

5.4. Consideraciones finales sobre gobernanza corporativa e inteligencia artificial

La incorporación de inteligencia artificial en el ámbito empresarial confirma que la innovación tecnológica ya no puede analizarse al margen del gobierno corporativo. La IA incide en decisiones estratégicas, estructuras de riesgo, relaciones con terceros, tratamiento de información y generación de valor, por lo que su adopción exige respuestas institucionales desde los órganos de dirección y administración.

La principal tensión jurídica no radica en el uso mismo de la tecnología, sino en la ausencia de mecanismos adecuados para gobernarla. Cuando la inteligencia artificial se implementa sin políticas internas, criterios de supervisión, trazabilidad suficiente o asignación clara de responsabilidades, los beneficios potenciales de eficiencia pueden verse desplazados por contingencias jurídicas, reputacionales y operativas.

En este contexto, el deber fiduciario contemporáneo adquiere una proyección renovada. La diligencia exigible a los administradores comprende no solo decisiones comerciales razonables, sino también la capacidad de identificar riesgos tecnológicos previsibles, exigir controles adecuados y promover esquemas internos de vigilancia continua. Innovar sin supervisar difícilmente resulta compatible con una administración prudente.

La propuesta desarrollada en este capítulo parte de esa premisa. Gobernar la inteligencia artificial no significa frenar la innovación, sino encauzarla dentro de parámetros compatibles con el interés social de la empresa, la protección de terceros y la sostenibilidad corporativa. En tal sentido, políticas internas, comités interdisciplinarios, auditorías y métricas de seguimiento constituyen instrumentos razonables de estabilidad institucional.

En términos empresariales, las organizaciones que incorporan tempranamente criterios de gobernanza tecnológica suelen fortalecer su competitividad, mejorar la confianza de inversionistas y reducir costos asociados a litigios, sanciones o crisis reputacionales. La gobernanza de la IA no debe entenderse, entonces, como obstáculo al crecimiento, sino como condición para un desarrollo sostenible y jurídicamente más seguro.

Desde la perspectiva jurídica colombiana, el marco societario vigente ofrece bases suficientes para exigir comportamientos diligentes frente al uso empresarial de estas tecnologías, particularmente a partir de los deberes previstos en el artículo 24 de la Ley 222 de 1995.

En definitiva, la inteligencia artificial no desplaza la responsabilidad humana dentro de la empresa; por el contrario, la hace más visible y exigente. Cuanto mayor sea la capacidad tecnológica de una organización, mayor deberá ser también su capacidad de dirección, control y rendición de cuentas. Ese constituye hoy el verdadero parámetro de responsabilidad empresarial frente a la inteligencia artificial.

Conclusiones

La incorporación de la inteligencia artificial en la gestión empresarial no constituye únicamente un avance tecnológico, sino una transformación estructural del gobierno corporativo y de los estándares jurídicos que rigen la actuación de los administradores. A lo largo de este artículo se ha evidenciado que la inteligencia artificial, en particular la generativa, ha dejado de ser una herramienta operativa para convertirse en un elemento que incide directamente en la toma de decisiones estratégicas, la gestión del riesgo, el tratamiento de la información y la generación de valor dentro de las organizaciones.

Este cambio obliga a replantear el alcance tradicional del deber fiduciario. En el contexto colombiano, el artículo 24 de la Ley 222 de 1995 mantiene su vigencia como parámetro normativo, pero su contenido material exige una reinterpretación funcional acorde con entornos donde las decisiones se encuentran mediadas por sistemas algorítmicos. La diligencia del "buen hombre de negocios" ya no puede entenderse únicamente en términos de experiencia empresarial o juicio gerencial, sino que incorpora la obligación de comprender, supervisar y controlar herramientas tecnológicas capaces de influir en la conducta corporativa.

En este escenario, la inteligencia artificial no desplaza la responsabilidad humana. Por el contrario, la intensifica. La delegación en sistemas automatizados no constituye un mecanismo de exoneración, sino una ampliación del ámbito de control exigible a los administradores. Conceptos como la curaduría tecnológica, la trazabilidad de decisiones y el accountability evidencian que la responsabilidad contemporánea no se limita a adoptar decisiones correctas, sino a demostrar que estas fueron tomadas mediante procesos informados, supervisados y razonables.

Asimismo, el análisis desarrollado permite concluir que uno de los principales riesgos jurídicos no radica en el uso de la tecnología en sí mismo, sino en su implementación sin estructuras adecuadas de gobernanza. La ausencia de políticas internas, mecanismos de supervisión, delimitación de responsabilidades y sistemas de control no solo incrementa la exposición a riesgos operativos, sino que debilita la capacidad de los administradores para acreditar el cumplimiento de su deber de diligencia.

En este contexto, la gobernanza de la inteligencia artificial se requiere como una exigencia jurídica y organizacional, y no como una buena práctica opcional. La intervención de la junta directiva, la articulación de funciones entre áreas estratégicas, técnicas y de cumplimiento, así como la integración de criterios éticos, regulatorios y operativos, resultan indispensables para garantizar un uso responsable de estas tecnologías dentro de la empresa.

A partir de esto, el artículo propone una guía de implementación que permite traducir principios abstractos de gobierno corporativo en mecanismos concretos de aplicación empresarial. La lista estratégica de verificación y la hoja de ruta progresiva constituyen herramientas que facilitan la identificación de riesgos, la asignación de responsabilidades, la documentación de procesos y la supervisión continua del uso de inteligencia artificial.

El valor de esta propuesta no es únicamente operativo, sino también jurídico. En escenarios de responsabilidad, la existencia de matrices de riesgo, políticas aprobadas, auditorías, registros de decisiones y evidencia de capacitación puede constituir un soporte determinante para acreditar la diligencia de los administradores. De esta forma, la gobernanza tecnológica se convierte en un mecanismo de prevención, pero también en un instrumento probatorio.

Por lo anterior, la incorporación de inteligencia artificial no puede analizarse como una disyuntiva entre innovación y control, sino como un problema de dirección empresarial. La adopción tecnológica solo resulta jurídicamente adecuada cuando se encuentra acompañada de mecanismos efectivos de supervisión, gestión de riesgos y rendición de cuentas. La ausencia de estos elementos no limita la innovación, pero sí incrementa la exposición de la organización a escenarios de responsabilidad.

En definitiva, la inteligencia artificial redefine el alcance del deber fiduciario de los administradores al exigir una actuación más informada, estructurada y responsable frente a los riesgos tecnológicos. Su implementación no modifica el sujeto de la responsabilidad, pero sí eleva las condiciones bajo las cuales esta se ejerce, incorporando deberes de supervisión, control y documentación sobre procesos decisorios asistidos por sistemas algorítmicos. En este contexto, la diligencia deja de evaluarse únicamente por el resultado de las decisiones y pasa a examinarse a partir de la forma en que estas fueron adoptadas, lo que impone a los administradores la obligación de demostrar que actuaron con criterios razonables de gobernanza, gestión del riesgo y control tecnológico.

Referencias

Brynjolfsson, E., & McAfee, A. (2017, July 18). The business of artificial intelligence: What it can—and cannot—do for your organization. Harvard Business Review.

Calo, R. (2017). Artificial Intelligence Policy: A Primer and Roadmap. UC Davis Law Review, 51, 399–435. https://ssrn.com/abstract=3015350.

D'Angelo, C. A., Floridi, L., & Cenci, A. (2022). Corporate digital responsibility: Organizational governance to promote ethical AI. Journal of Business Ethics, 183(4), 931–950. https://doi.org/10.1007/s10551-021-04996-1

Davenport, T. H., & Ronanki, R. (2018). Artificial intelligence for the real world. Harvard Business Review, 96(1), 108–116.

Deloitte. (2019). *AI ethics: A business imperative for boards and C-suites*. Deloitte. Recuperado de https://web.archive.org/web/20230320150220/https://www2.deloitte.com/us/en/pages/regulatory/articles/ai-ethics-responsible-ai-governance.html

Floridi, L., & Cowls, J. (2019). A unified framework of five principles for AI in society. Harvard Data Science Review, 1(1). https://doi.org/10.1162/99608f92.8cd550d1

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., & Vayena, E. (2018). AI4People—An ethical framework for a good AI society. Minds and Machines, 28(4), 689–707. https://doi.org/10.1007/s11023-018-9482-5

Greenleaf, G. (2018). Global data privacy laws 2017: 120 national data privacy laws. Privacy Laws & Business International Report, 145, 10–13. https://ssrn.com/abstract=2993035

Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. Nature Machine Intelligence, 1(9), 389–399. https://doi.org/10.1038/s42256-019-0088-2

Ley 222 de 1995 (Colombia), artículo 24.

Rai, A., Constantinides, P., & Sarker, S. (2019). Editor's comments: Next-generation digital platforms: Toward human–AI hybrids. MIS Quarterly, 43(1), iii–ix. https://aisel.aisnet.org/misq/vol43/iss1/2/

Raisch, S., & Krakowski, S. (2023). Toward AI governance. Information Systems Frontiers, 25(4), 1123–1139. https://doi.org/10.1007/s10796-022-10251-y

Selbst, A. D., Boyd, D., Friedler, S. A., Venkatasubramanian, S., & Vertesi, J. (2019). Fairness and abstraction in sociotechnical systems. Proceedings of the Conference on Fairness, Accountability, and Transparency (FAT*), 59–68. https://doi.org/10.1145/3287560.3287598

Shrestha, Y. R., Ben-Menahem, S. M., & von Krogh, G. (2019). Organizational decision-making structures. California Management Review, 61(4), 66–83. https://doi.org/10.1177/0008125619862257

Stix, C., Ashurst, C., & Floridi, L. (2024). AI governance: A systematic literature review. AI and Ethics, 4(2), 167–189. https://doi.org/10.1007/s43681-023-00282-9

Superintendencia de Industria y Comercio (SIC). (2020). Guía para la implementación del principio de responsabilidad demostrada (accountability)

OECD. (2023). The state of implementation of the OECD AI Principles four years on. OECD Artificial Intelligence Papers, No. 3. https://doi.org/10.1787/835641c9-en