

El compliance en la era de inteligencia artificial en el sector bancario de Venezuela

Eddy Yafranci iv Ferrer Bravo¹; Arianna Petit²; Yanine Revilla³

Resumen

La presente investigación tiene como objetivo general analizar el compliance en la era de la Inteligencia Artificial (IA) en el sector bancario de Venezuela. Este estudio se fundamentó en la necesidad de modernizar las unidades de compliance ante el surgimiento de amenazas disruptivas como el phishing automatizado y los deepfakes, así como la exigencia de dar fiel cumplimiento a la Resolución N.º 010.25 de la SUDEBAN (2025) o cualquier otra normativa aplicable. Esta investigación se desarrolla bajo un enfoque cualitativo, de carácter descriptivo y con un diseño no experimental, en la cual se utilizaron como instrumentos de recolección de datos la entrevista semiestructurada y la revisión documental como técnica de observación. Como resultados, se determinó que la inteligencia artificial estrecha (ANI) es el único modelo con madurez operativa para la banca nacional, destacando el machine learning y el procesamiento de lenguaje natural como pilares de eficiencia. Asimismo, se concluye que la adopción estratégica de estas tecnologías permite transitar de un compliance reactivo a una gestión proactiva y multidimensional. No obstante, la implementación debe regirse por los principios de explicabilidad algorítmica y supervisión humana bajo el protocolo “Maker/Checker”, asegurando que la responsabilidad jurídica institucional permanezca indelegable y alineada con los estándares de seguridad jurídica internacional, a fin de garantizar idóneas acciones preventivas y correctivas de acuerdo con el compliance.

Palabras clave: compliance, inteligencia artificial, sector bancario.

Cómo citar: Ferrer, E., Petit, A., Revilla, Y. (2026). El compliance en la era de inteligencia artificial en el sector bancario de Venezuela. En Del Castillo, G., Miranda, N. (Eds.). *Lex nova: fronteras jurídicas y desafíos globales*. High Rate Consulting/Universidad Andina del Cusco. <https://doi.org/10.38202/lexnova7>

1. <https://orcid.org/0000-0002-3859-2289>, eddyferrerb@gmail.com | Abogado Summa Cum Laude (LUZ). Licenciado en Ciencia Política y Administrativa, mención: Ciencia Política (URU) con Diplomado en Docencia para la Educación Superior, Especialista en Metodología de la Investigación y Magister en Banca y Finanzas. Profesor de las Escuelas de Derecho y Ciencias Políticas de la Universidad Rafael Urdaneta.
2. <https://orcid.org/0000-0001-6671-4979>, arianna.petit.81022@uru.edu | Doctora en Ciencia Políticas (URBE). MSc. En Gerencia de Empresa mención: Gerencia Financiera (LUZ). Economista. (LUZ).
3. <https://orcid.org/0000-0001-7755-5264>, profesorayanirevi@gmail.com | Doctora en Ciencias Gerenciales; Doctora en Ciencias Humanas, MSc. En Gerencia de Empresa mención Gerencia Financiera, Especialista en Métodos de investigación, y en Educación superior, MBA en administración de empresas, Ingeniero Industrial, Contador Público, Profesora de la Universidad del Zulia, Universidad Rafael Urdaneta, Universidad Yacambú.

Compliance in the era of artificial intelligence in the banking sector of Venezuela

Abstract

The general objective of this research is to analyze compliance in the era of Artificial Intelligence (AI) in the banking sector of Venezuela. This study was based on the need to modernize Compliance units in the face of the emergence of disruptive threats such as automated phishing and deepfakes, as well as the requirement to faithfully comply with SUDEBAN (2025) Resolution N° 010.25 or any other applicable regulations. This research is developed under a qualitative approach, of a descriptive nature with a non-experimental design, in which the semi-structured interview and the documentary review as an observation technique were used as a data collection instrument. As a result, it was determined that Narrow Artificial Intelligence (ANI), is the only model with operational maturity for national banking, highlighting Machine Learning and Natural Language Processing as pillars of efficiency, it is also concluded that the strategic adoption of these technologies allows moving from a reactive compliance to a proactive and multidimensional management. However, the implementation must be governed by the principles of algorithmic explainability and human supervision under the “Maker/Checker” protocol, ensuring that institutional legal responsibility remains non-delegable and aligned with international legal security standards, in order to guarantee appropriate preventive and corrective actions according to compliance.

Keywords: compliance, artificial intelligence, banking sector.

Introducción

En la actualidad, el sistema financiero global atraviesa una transformación disruptiva impulsada por la Inteligencia Artificial (IA), la cual se erige como una fuerza tecnológica capaz de revolucionar los procesos legales y administrativos a escala mundial. Ahora bien, en el contexto latinoamericano, esta tendencia responde a la necesidad de modernizar infraestructuras frente al auge de las *fintechs* y a marcos regulatorios cada vez más complejos.

Sin embargo, en el caso particular de Venezuela, la adopción de estas herramientas enfrenta un escenario singular determinado por la presión normativa liderada por la Superintendencia de las Instituciones del Sector Bancario (SUDEBAN, 2021, citado por Ferrer Bravo, 2023), que contrasta con una realidad de desinversión tecnológica, obsolescencia de plataformas y fuga de talento especializado.

Esta asimetría ha derivado en una gestión de cumplimiento normativo (*compliance*) predominantemente manual y reactiva. El *compliance* es el conjunto de procedimientos y buenas prácticas que adoptan las organizaciones para identificar y clasificar los riesgos operativos y legales a los que

se enfrentan, a fin de establecer mecanismos internos de prevención, gestión, control y reacción frente a posibles incumplimientos de leyes o normas éticas.

En tal sentido, el sector bancario está entrando en una fase de transformación crítica impulsada por la inteligencia artificial (IA), donde la supervisión ya no se limita a auditorías periódicas, sino que evoluciona hacia una gestión de riesgos tecnológica continua.

Los sistemas tradicionales de control, diseñados bajo paradigmas estáticos, hoy resultan insuficientes para procesar volúmenes masivos de operaciones en tiempo real, lo que genera síntomas críticos como una elevada tasa de “falsos positivos” y una notable lentitud en la generación de reportes de actividades sospechosas (RAS).

Mientras la banca nacional enfrenta procesos humanos caracterizados por su lentitud y altos costos, el panorama de riesgos ha evolucionado hacia amenazas potenciadas por la propia IA, tales como el phishing automatizado y la creación de deepfakes para la suplantación de identidad, incrementando exponencialmente el riesgo legal y repu-

tacional ante delitos de legitimación de capitales y financiamiento al terrorismo (LC/FT/FPADM).

Ante la imposibilidad humana de supervisar este entorno con la celeridad requerida, la integración de la inteligencia artificial estrecha (ANI) se presenta no solo como una opción de eficiencia operativa, sino como un requisito de seguridad jurídica. Por ello, la aplicación de algoritmos de machine learning para el análisis conductual, el procesamiento de lenguaje natural (PLN) para la interpretación semántica de normativas y el reconocimiento inteligente de caracteres (ICR) para la digitalización de expedientes, ofrece el potencial de transformar el cumplimiento reactivo en una gestión proactiva y predictiva.

Fundamentación teórica

Por consiguiente, desde el contexto teórico, la banca en Venezuela, sin perjuicio del grave retroceso a nivel tecnológico y de infraestructura, se encuentra en constante evolución y adaptación a las nuevas tecnologías, en donde la inteligencia artificial (IA), a partir de la vigencia de la Resolución N.º 001.21 de la SUDEBAN (2021), ha venido a regular las alianzas entre las instituciones bancarias y las instituciones de tecnología financiera del sector bancario (ITFB), con el objeto de que estas últimas puedan ofrecer productos y servicios financieros a los bancos, basados en la inteligencia artificial, el aprendizaje automático, el análisis avanzado de datos, la tecnología de registros distribuidos, la computación en la nube, entre otros, para lograr entornos de control y procesos eficaces de gestión del riesgo de tecnología de la información y mitigar problemas propios de la actividad bancaria.

Al respecto, la Resolución N.º 001.21 regula los servicios financieros prestados a través de nuevas tecnologías, ofrecidos por las instituciones de tecnología financiera del sector bancario (ITFB), en cualesquiera de sus modalidades, a las instituciones bancarias, así como su organización, operación y funcionamiento. A tales fines, para entender el concepto de inteligencia artificial, se presenta la Tabla 1, con un listado de las principales definiciones de la misma.

En el contexto bancario, la inteligencia artificial puede ser usada para realizar diversos análisis; por ejemplo: 1) descriptivos, que buscan explicar qué ha pasado y generalmente son los más frecuentes; 2) predictivos, aquellos cuya finalidad es anticipar qué va a pasar, y 3) prescriptivos, los que recomiendan qué hacer para conseguir una meta determinada.

Tabla 1.
Definiciones de IA

Base conceptual	Definiciones
Resolución 001.21 de la SUDEBAN (2021)	Tecnologías utilizadas para emular características o capacidades ligadas de manera exclusiva al intelecto humano.
Pérez-Ugena (2024)	Disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico.
Herrera-Ortiz et al. (2024)	La IA viene a constituirse en una parte de la informática o la computación que busca emular las acciones propias de un ser humano inteligente; es decir, una persona que ha desarrollado sus capacidades cognitivas para asumir labores complejas que ameritan el uso del pensamiento y la lógica racional.
Reglamento sobre IA del Parlamento Europeo y el Consejo de la Unión Europea (2024).	Aquellos sistemas definidos por el software que se desarrolla, empleando ciertas técnicas o estrategias, y que puede, para un conjunto determinado de objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa
AEB (2019). Asociación Española de Banca	Disciplina cuya finalidad es la automatización en la toma de decisiones y ejecución de estrategias, acciones y tácticas mediante el uso de sistemas informáticos en aplicación de técnicas matemáticas para el manejo de grandes volúmenes de datos.

Hoy en día, la inteligencia artificial es una herramienta común en actividades frecuentes como la búsqueda en internet, el reconocimiento facial, las recomendaciones de las redes sociales (mediante algoritmos o instrucciones sistematizadas) o la determinación de trayectos en aplicaciones de navegación. En este caso, la SUDEBAN (2021, citado por Ferrer Bravo, 2023) presentó una definición restrictiva de la inteligencia artificial, tomando en cuenta que dicho concepto es de evolución rápida gracias a la concentración y mayor disponibilidad de datos y a la mejora de la tecnología, que permite gestionar grandes volúmenes y fuentes de datos, demostrando una gran capacidad para detectar patrones, aunque no es capaz de aprender de manera asociativa como los humanos, quienes son capaces de realizar análisis bajo una panorámica amplia y asociar todos sus conocimientos.

El futuro desafío de la inteligencia artificial radica en su capacidad para comprender y reaccionar al entorno de manera más profunda, con el fin de mejorar la capacidad tecnológica y económica de

las sociedades, siempre manteniendo el bienestar y beneficio de las personas como objetivo principal, siendo esto último una contextualización flexible de ese concepto. Esa normativa implica que las instituciones de tecnología financiera del sector bancario (ITFB) pueden ofrecer servicios financieros utilizando tecnologías avanzadas, como la inteligencia artificial, para mejorar la interacción entre los clientes y las instituciones bancarias sin la necesidad de intervención humana, previa autorización de la Superintendencia de las Instituciones del Sector Bancario, basada en la Resolución N.º 001.21 (SUDEBAN, 2021).

Si bien la inteligencia artificial brinda oportunidades innovadoras, también genera riesgos importantes en virtud de su capacidad para procesar datos masivamente y sus algoritmos de aprendizaje automático; la IA puede tomar decisiones automatizadas que afectan directamente a las personas y a la sociedad. En tal sentido, se reconoce que la inteligencia artificial se divide en inteligencia artificial estrecha (débil) e inteligencia artificial general (fuerte).

Para Scarcello (2018), la IA fuerte es aquella considerada como realmente pensante, es decir, que tiene la autonomía y capacidad mental humana, pudiendo hacer más tareas que aquellas para las que fue diseñada. A la fecha, no existe una IA fuerte conocida, por lo que es solo una cuestión teórica. Por otro lado, la IA débil es aquella dotada de la capacidad de simular procesos mentales del cerebro humano por medio de computadoras, cumpliendo trabajos específicos. De estos tipos de inteligencia artificial, la IA estrecha o débil se centra en realizar una única tarea específica, como identificar imágenes, revisar documentos o traducir idiomas. Estos sistemas no aprenden por sí mismos y solo pueden hacer lo que se les ha programado, estando limitados a su área de especialización.

Por tal motivo, el estudio de la aplicabilidad de la IA en el cumplimiento normativo bancario venezolano se centró exclusivamente en la inteligencia artificial estrecha (o débil), dado que es el único tipo de IA maduro y operativamente disponible en la actualidad, ya que estos sistemas, definidos por su capacidad de automatizar tareas específicas (como el monitoreo transaccional, el análisis de documentos o la detección de patrones de fraude) mediante algoritmos de machine learning y redes neuronales, son los que proporcionan una solución real e inmediata para la mejora de la eficiencia y la gestión de riesgos (compliance) en el sector bancario.

Asimismo, para Carranza Bravo (2010), las técnicas de la inteligencia artificial son soportes valiosos

y poderosos para abordar los nuevos paradigmas de la tecnología, ya que son capaces de considerar la información cualitativa y, a partir de ella, diseñar e implementar modelos estadísticos y computacionales que asistan a los decisores en la resolución de diversos problemas.

Dentro de las técnicas de la inteligencia artificial se encuentra el procesamiento de lenguaje natural (NLP), el cual implica que una de las tareas fundamentales de la inteligencia artificial es la manipulación de lenguajes naturales usando herramientas de computación; en esta, los lenguajes de programación juegan un papel importante, ya que forman el enlace necesario entre los lenguajes naturales y su manipulación por una máquina. El NLP consiste en la utilización de un lenguaje natural para comunicarnos con la computadora, debiendo esta entender las oraciones que le sean proporcionadas. El uso de estos lenguajes naturales facilita el desarrollo de programas que realicen tareas relacionadas con el lenguaje o, bien, desarrollar modelos que ayuden a comprender los mecanismos humanos relacionados con el lenguaje.

Por otro lado, el reconocimiento inteligente de caracteres (ICR), para IBM (2023), es una tecnología de OCR avanzada que lleva la extracción de datos tradicional al siguiente nivel al permitir que las máquinas reconozcan y procesen texto escrito a mano. El ICR utiliza algoritmos avanzados de aprendizaje automático (ML) e inteligencia artificial (IA) para identificar e interpretar texto escrito a mano. El ICR puede reconocer diferentes estilos de escritura, fuentes y tamaños, y es ampliamente utilizado en industrias donde la información escrita a mano, como formularios, cheques, encuestas o cualquier documento que implique texto de forma libre, necesita ser digitalizada.

De acuerdo con lo expuesto, la Agencia Española de Protección de Datos y el Supervisor Europeo de Protección de Datos (2020) exponen que el aprendizaje automático (machine learning o ML) es una rama específica de la IA, aplicada a la resolución de problemas específicos y limitados, como tareas de clasificación o predicción. A diferencia de otros tipos de IA que intentan emular la experiencia humana (por ejemplo, sistemas expertos), el comportamiento de los sistemas de aprendizaje automático no está definido por un conjunto predeterminado de instrucciones. Los modelos de machine learning se entrenan utilizando conjuntos de datos, razón por la cual, durante su entrenamiento, los sistemas se adaptan de forma autónoma a los patrones encontrados en las diferentes variables de un conjunto de datos dado, creando correlaciones.

Tabla 2.
Funcionalidades de la IA en el derecho

Funcionalidades de la IA en el Derecho	Principales exponentes	Premisa
Sistemas expertos jurídicos	"Martínez Bahena (2013) Lancho Pedrera (2003) Escudero Molina (2023)"	Son sistemas computacionales que podrían plantear posibles soluciones a determinados asuntos jurídicos aplicando el conocimiento experto, así como explicar sus razonamientos.
Procesamiento inteligente de documentos (IDP)	"Microsoft (2024) Ayerdi (2025) Amazon Web Services (2024)"	Es una solución de software que captura, transforma y procesa datos de documentos (por ejemplo, correo electrónico, texto, Word, PDF o documentos escaneados).
Análisis predictivo e investigación jurídica	"Correa (2025) García (2024) Celis Correa (2023)"	El uso de inteligencia artificial en el derecho ofrece numerosos beneficios, entre los cuales, destacan la eficiencia en la gestión de casos, la mejora en la precisión de la revisión documental, la posibilidad de tomar decisiones más informadas y la reducción de errores humanos.
Prevención de riesgos de LC/FT/FPADM y reducción de riesgos legales	"Villegas Ruiz (2021) Gómez Cáceres y López Zeballos (2002) Resolución 010.25 SUDEBAN (2025)"	El manejo del riesgo es la operación de análisis que una empresa u organización realiza para prever y manejar las incertidumbres que depara el futuro.

De lo anterior, se desprende que las funcionalidades de la IA en el ámbito jurídico (reflejado en la anterior Tabla 2) se estructuran en torno a tres ejes fundamentales: los sistemas expertos, el procesamiento inteligente de documentos (IDP) y el análisis predictivo. Mientras los sistemas expertos actúan como soportes de decisión mediante motores de inferencia que replican el razonamiento lógico, el IDP permite la captura y transformación de datos cualitativos en información estructurada mediante el uso de tecnologías como el OCR y el Procesamiento de Lenguaje Natural (PLN). Asimismo, el análisis predictivo utiliza grandes volúmenes de datos históricos para anticipar resultados legales y comportamientos futuros.

Por ello, estas funcionalidades no solo optimizan la eficiencia operativa, sino que constituyen un pilar para la reducción de riesgos legales y la prevención de delitos relacionados con la legitimación de capitales, el financiamiento al terrorismo y el financiamiento a la proliferación de armas de destrucción masiva (en adelante, LC/FT/FPADM), al permitir la detección temprana de anomalías y patrones sospechosos que escapan a la supervisión manual tradicional.

El cumplimiento normativo como acciones de idoneidad legal.

El cumplimiento normativo emerge no solo como una obligación legal, sino como una disciplina estratégica y proactiva que integra la prevención, detección y respuesta a las infracciones, abarcando

tanto el marco legal obligatorio como las mejores prácticas éticas, y que se extiende a todos los niveles y actores de una organización.

Por su parte, Castagnino (2019) define el cumplimiento normativo o Corporate Compliance, también conocido como “compliance empresarial” o “cumplimiento empresarial”, como el conjunto de acciones preventivas ejercidas por la empresa, que procuran garantizar que esta, sus accionistas, directivos, gerentes, empleados y agentes vinculados cumplan con la normativa aplicable y ejecuten sus actividades con ética. Dentro del cumplimiento normativo se encuentra el denominado compliance program o autorregulación corporativa (self-policing interno), que implica que la entidad empresarial se autorregula en la medida en que sus órganos corporativos establecen reglas, protocolos y modos de proceder en su negocio específico. Por ello, la autorregulación nace del propio seno de la entidad comercial, atendiendo a sus necesidades corporativas.

Asimismo, Vaudo (2022) establece que el compliance corporativo, junto con la autorregulación que realiza la propia empresa, persigue constituirse en garantía de la adopción de medidas de prevención y control de situaciones adversas, corrección y autogestión de riesgos, para garantizar un buen gobierno en el tráfico jurídico de la empresa y el cumplimiento de sus fines comerciales.

Por otro lado, dentro de las normas legales en materia de cumplimiento normativo se encuentran el Decreto con rango, valor y fuerza de Ley de Instituciones del Sector Bancario (2014), la Resolución

N.º 010/2025 emanada de la Superintendencia de las Instituciones del Sector Bancario (2025), y, a nivel internacional, las Normas ISO 37301 (2021), ISO 31000 (2018) e ISO 27001 (2022), las cuales se detallan en la siguiente Tabla 3.

Tabla 3.
Normas ISO aplicables al cumplimiento normativo y gestión de riesgos

Norma ISO	Objeto
ISO 37301: Sistemas de Gestión de Compliance	Es la norma que establece los requisitos para implantar un sistema de cumplimiento eficaz en la organización. Con esta norma, se busca establecer la base normativa para que el uso de algoritmos no vulnere la transparencia corporativa.
ISO 31000: Gestión del Riesgo	Proporciona principios y un marco de referencia para identificar, analizar y evaluar riesgos de cualquier naturaleza. En virtud de que IA utiliza los principios de esta norma para calcular matemáticamente la probabilidad de ocurrencia de delitos como la LC/FT/FPADM.
ISO 27001: Seguridad de la Información	Es la norma principal para garantizar la confidencialidad, integridad y disponibilidad de los datos, su propósito es proteger los activos de información mediante un sistema de gestión de seguridad.

Todas esas normas, incluyendo las Normas ISO, constituyen el marco de referencia internacional que valida la idoneidad de la inteligencia artificial en la banca venezolana, generando la base para gestionar técnicamente la automatización de tareas y garantizar que esta sea segura y ética.

Ahora bien, el cumplimiento normativo busca la reducción de riesgos legales, ya que el manejo del riesgo es la operación de análisis que una empresa u organización realiza para prever y gestionar las incertidumbres que depara el futuro. Por tanto, un compliance program efectivo debe contar con un proceso de análisis de riesgo sólido, un adecuado uso de los recursos corporativos designados y revisiones constantes de los riesgos identificados o potenciales.

Metodología

Esta investigación está estructurada bajo un enfoque cualitativo con alcance descriptivo, debido a que existe un análisis teórico de las características del compliance en la era de la Inteligencia

Artificial, que pueden ser utilizadas para fortalecer los sistemas de prevención y detección en la banca venezolana, como parte de los procesos de cumplimiento normativo y acciones preventivas de idoneidad legal.

Por otro lado, el diseño del estudio es no experimental, transeccional descriptivo y de campo. En cuanto a la población, estuvo compuesta por las instituciones bancarias que operan en Venezuela y se encuentran bajo la supervisión de la SUDEBAN (2025).

La muestra de la presente investigación fue de tipo intencional y estuvo constituida por el Banco de Venezuela (BDV) y el Banco Nacional de Crédito (BNC), seleccionados por su posición en el ranking bancario compilado por el portal especializado Banca y Negocios (2026): en el caso del BDV, por ocupar el primer puesto en resultado neto mensual al corte de marzo de 2026; y, en el caso del BNC, por formar parte de los tres primeros bancos privados en total de activos al corte del 31 de marzo de 2026.

A continuación, se detalla la Tabla 4, referente a la población de la investigación.

Tabla 4.
Población y Unidades Informantes

Institución Financieras	Áreas Seleccionadas	Muestra (cantidad)
Banco de Venezuela	Cumplimiento Normativo / Tecnología (TI) / Legal /	3 personas
Banco Nacional de Crédito		7 personas

Asimismo, se utilizó la entrevista estructurada (aplicada a inicios de 2026), la cual consiste en que el entrevistador tiene una lista de veinticuatro preguntas abiertas definidas previamente y se limita estrictamente a ellas; en consecuencia, se elaboró una guía de entrevista. Posteriormente, se realizó el análisis de las respectivas respuestas.

Al respecto, se entrevistaron de forma virtual a colaboradores de esas entidades bancarias que forman parte de las áreas de cumplimiento (LC/FT/FPADM), legal, TI y riesgo, en cargos de gerentes y/o vicepresidentes de dichas dependencias. Las preguntas fueron elaboradas para lograr entender, desde la perspectiva de cada sujeto de estudio, sus conocimientos en técnicas de IA, funcionalidades y su relación con el cumplimiento normativo, especialmente con la mitigación de riesgos.

Análisis y discusión de resultados

Se destaca que este apartado se desarrolló mediante la triangulación analítica de datos realizada a partir de veinticuatro preguntas dirigidas a profesionales del sector bancario venezolano, contrastadas con los postulados teóricos que fundamentan cada elemento de análisis, en concatenación con la interpretación o hermenéutica del investigador, evitando sesgos o apreciaciones subjetivas, lo que permitió construir un cuerpo de hallazgos sistemático y coherente sobre las oportunidades, limitaciones y condiciones de implementación de la inteligencia artificial en la gestión del cumplimiento normativo. Por consiguiente, la presente discusión organiza estos hallazgos en torno a ejes temáticos que atraviesan las distintas preguntas y que, en su conjunto, dibujan un mapa comprehensivo del estado del arte en la materia (Villegas Ruiz, 2021).

De la detección reactiva a la anticipación estratégica

Uno de los hallazgos más sólidos que emerge del análisis es el reconocimiento generalizado de que el aprendizaje automático transforma sustancialmente la capacidad de detección de patrones complejos de legitimación de capitales, superando las limitaciones inherentes a los sistemas basados en reglas tradicionales. Los participantes coinciden en señalar que esta transformación opera a través de dos mecanismos específicos que merecen ser destacados, tal como desarrollan Microsoft (2024) y Correa (2025), quienes explican que la IA es una fuerza transformadora, incluyendo el ámbito legal.

El primer mecanismo es la capacidad de análisis multidimensional de variables interconexas, que, a diferencia de los sistemas tradicionales que evalúan cada transacción de forma aislada con base en umbrales predefinidos, permite la observación simultánea de múltiples variables que, consideradas en su conjunto, revelan patrones que el análisis lineal no puede detectar (Scarcello, 2018). En este sentido, los participantes describen este fenómeno como un desplazamiento desde la lógica de la regla explícita hacia la lógica de la correlación estadística, donde el sistema identifica asociaciones entre variables que ningún programador podría haber anticipado al momento de diseñar las reglas de monitoreo.

El segundo mecanismo es la adaptabilidad dinámica. En este punto, los participantes explican que un sistema basado en aprendizaje automático aprende de las decisiones pasadas del banco, de modo que aquellas operaciones que han sido consistentemente calificadas como seguras dejan de generar alertas, concentrando los recursos de investi-

gación en aquellas transacciones que efectivamente presentan características anómalas, ya que este mecanismo aborda directamente uno de los problemas más persistentes del cumplimiento bancario: la fatiga por falsos positivos, que desgasta a los equipos analíticos y reduce su capacidad de identificar verdaderos casos sospechosos (AEB, 2019).

Sin embargo, los participantes introducen un matiz que resulta fundamental para la discusión: la efectividad de estos mecanismos no es automática ni está garantizada por la mera adopción tecnológica. Por ello, la reducción de falsos positivos depende críticamente de las premisas que el modelo incorpora en su análisis. En este sentido, los participantes señalan que las variables de mayor valor predictivo no son exclusivamente transaccionales, sino que incluyen dimensiones contextuales como el comportamiento histórico del cliente, su entorno operativo y la trayectoria de sus relaciones bancarias previas. Esta observación sugiere que la calidad del modelo predictivo está directamente vinculada a la riqueza y diversidad de los datos que se le suministran.

En estrecha relación con lo anterior, los participantes advierten que la adaptabilidad del algoritmo frente a nuevas tipologías de delitos financieros no es ilimitada, especialmente en el contexto venezolano. Un diagnóstico recurrente es que el entorno financiero local se caracteriza por una dinámica delictiva que no es estática, sino que se desplaza a la velocidad de la inflación, las fluctuaciones del mercado cambiario y la irrupción de nuevas plataformas digitales. Esta especificidad implica que las tipologías de legitimación de capitales en Venezuela cambian con una rapidez impulsada por variables macroeconómicas que escapan a la lógica transaccional tradicional (Vaudo, 2022).

La promesa y los límites del procesamiento de lenguaje natural

El análisis de las preguntas relativas al procesamiento de lenguaje natural revela una tensión similar entre el potencial transformador de la tecnología y las condiciones que limitan su aplicación efectiva. Por ello, en el ámbito del análisis normativo, los participantes reconocen que el procesamiento de lenguaje natural puede acelerar significativamente la revisión de Gacetas Oficiales y normativas emitidas por la SUDEBAN (2025). Sin embargo, la precisión de estas herramientas aparece como un punto de cautela recurrente, ya que, tal como señala García (2024), la IA debe ser capaz de evitar sesgos discriminatorios.

A este respecto, los participantes señalan que

el procesamiento de lenguaje natural puede producir interpretaciones de los documentos que no necesariamente se corresponden con el espíritu de la norma o con las solicitudes regulatorias (Microsoft, 2024). A ello se suma el fenómeno de las alucinaciones, mediante el cual el sistema genera información aparentemente verosímil, pero inexistente, como la consideración de artículos que no forman parte del texto normativo. Por lo tanto, en un dominio como el cumplimiento bancario, donde la precisión interpretativa es innegociable, estas limitaciones imponen la necesidad de una revisión humana de los resultados generados por el sistema, como explica Ayerdi (2025), quien señala que la IA puede ser utilizada para analizar o procesar información, transformando procesos manuales a fin de reducir gastos.

Esta cautela se extiende al ámbito de la gestión documental, ya que los participantes coinciden en que el procesamiento inteligente de documentos puede optimizar la clasificación y validación de expedientes de clientes mediante dos vías concretas. La primera es la curación del expediente, entendida como la validación automática de que la documentación presentada es correcta, está completa y se encuentra vigente. La segunda es la reducción drástica de los tiempos de revisión manual, lo que libera recursos humanos para actividades de mayor valor analítico, dando cumplimiento a lo expuesto por Amazon Web Services (2024), ya que estas tecnologías utilizan redes neuronales para emular la capacidad humana en el reconocimiento y procesamiento de datos. Sin embargo, también aquí los participantes insisten en que la efectividad de estas optimizaciones depende de un aprendizaje guiado por el especialista en cumplimiento, quien debe consolidar su conocimiento técnico sobre el algoritmo para asegurar que la clasificación documental responda a los criterios relevantes para la gestión del riesgo.

En el caso de los asistentes virtuales o chatbots aplicados a la fase de debida diligencia y atención al cliente, los participantes introducen un criterio de valoración que trasciende lo operativo. El aporte de un chatbot, señalan, no reside en su capacidad conversacional per se, sino en su integración con el esquema regulatorio y con las variables de riesgo del sujeto obligado. Un asistente virtual que no honre la naturaleza del enfoque basado en riesgo, por más fluida que sea su interacción con el cliente, no agregaría valor real al proceso de cumplimiento. Esta observación es particularmente relevante porque sitúa la discusión sobre chatbots en el terreno de la legitimidad regulatoria y no solo en el terreno de la eficiencia operativa.

Los desafíos de la extracción automatizada de datos

El análisis de las preguntas sobre reconocimiento óptico de caracteres y reconocimiento inteligente de caracteres revela que los desafíos técnicos para lograr una extracción confiable de datos desde documentos de identidad y RIF no se concentran en el algoritmo propiamente dicho, sino en la cadena de valor que antecede al procesamiento algorítmico. Los participantes identifican tres eslabones críticos en esta cadena.

El primer eslabón es la calidad del documento fuente, que puede estar deteriorado físicamente por el paso del tiempo, presentar marcas de uso, manchas o roturas que afectan la legibilidad de los caracteres. El segundo es la estandarización del formato, afectada por la coexistencia de múltiples diseños oficiales emitidos a lo largo de distintos años, con variaciones en tipografías, disposición de los campos y elementos de seguridad. El tercero es la calidad de la captura digital, que depende del equipo utilizado, las condiciones de iluminación, el ángulo de toma y la pericia del operador que realiza el escaneo o la fotografía del documento.

Estos eslabones son confirmados por Holdsworth (2023) de IBM, cuando explica que las técnicas de OCR permiten convertir datos en formato texto, garantizando la calidad de la imagen y reduciendo la entrada manual y redundante de datos.

Los participantes añaden un desafío adicional que resulta particularmente relevante para la debida diligencia: el presunto forjamiento de documentación. Un sistema de reconocimiento óptico de caracteres puede leer perfectamente los caracteres de un documento falso y, sin embargo, el resultado de esa extracción será confiable solo en un sentido técnico, pero no en un sentido operativo para la vinculación del cliente. Esta observación sugiere que la confiabilidad de la extracción no es únicamente una cuestión de precisión óptica, sino también de validación de autenticidad.

Validación humana y protocolos de supervisión

Uno de los hallazgos más consistentes a lo largo de toda la triangulación es la insistencia en que los protocolos de validación humana no son un complemento opcional de la automatización, sino una condición de su legitimidad. En el caso específico del reconocimiento de caracteres manuscritos, los participantes proponen distintos niveles de supervisión que operan de manera complementaria.

El primer nivel opera por excepción, activándose solo cuando el sistema detecta baja confianza en

su propio resultado o cuando identifica ambigüedades en el texto manuscrito. Este enfoque reconoce que el reconocimiento automatizado no opera en un registro binario de acierto o error, sino en un espectro de probabilidades, y que el punto en el cual esa probabilidad deja de ser aceptable debe estar definido de antemano por la institución.

Asimismo, el segundo nivel opera por segregación de funciones, mediante el esquema conocido como Maker/Checker, donde un operador ejecuta la digitalización y extracción asistida por el sistema, mientras que un segundo operador revisa, con base en muestras, que los resultados se hayan registrado en los campos correspondientes. Esta lógica de doble control, ampliamente difundida en el sector financiero, reduce el riesgo de sesgos individuales o descuidos.

Un tercer nivel opera por revisión terminal, donde un especialista evalúa la coherencia global del resultado obtenido, no campo por campo sino en su conjunto. Este nivel es particularmente relevante cuando la documentación tiene consecuencias jurídicas significativas, pues el criterio del especialista actúa como un filtro final que detecta errores que el sistema automatizado, por su propia naturaleza, no puede identificar.

La arquitectura de la integración tecnológica

El análisis de las preguntas sobre integración del procesamiento inteligente de documentos con los sistemas core bancarios revela una fractura conceptual significativa entre los participantes. Por un lado, emerge una visión que rechaza frontalmente cualquier tipo de vinculación con el core, argumentando que se trata de una plataforma de alto impacto cuya integración con sistemas periféricos introduce riesgos que superan los beneficios potenciales. Esta postura refleja una cultura tecnológica donde el aislamiento del sistema central se concibe como garantía de estabilidad operativa.

Por otro lado, se presenta una visión que no solo acepta la integración, sino que la diseña en términos técnicos precisos. Los participantes que adoptan esta postura proponen la implementación de APIs bidireccionales que permitan una interconexión rigurosa entre el core y el sistema de procesamiento inteligente de documentos. Este modelo no se limita a transferir información de un sistema a otro, sino que incorpora lógica de negocio: el sistema tiene la capacidad de detener el flujo automáticamente cuando detecta coincidencias o errores que requieren intervención especializada. De este modo, la integración no sacrifica el control en aras de la fluidez; por el contrario, introduce puntos de

pausa inteligentes donde la máquina cede el paso al humano.

Los participantes que se pronuncian a favor de la integración añaden una dimensión que va más allá de la arquitectura de software. Señalan que el flujo de información debe ser auditable por los entes reguladores, lo que implica que los expedientes digitalizados no pueden ser alterados sin dejar rastro y que la institución debe poder probar la autenticidad y custodia de los documentos. Esta dimensión forense de la integración es particularmente relevante en un contexto donde los reguladores examinan no solo la calidad de la gestión del riesgo, sino también la integridad de los registros que documentan esa gestión. En tal sentido, en este punto resultan relevantes las regulaciones de la ISO 27001 (2022) sobre seguridad de la información, por cuanto constituye una norma base para proteger los activos de información sensible en cualquier organización.

El análisis predictivo y la redefinición del oficial de cumplimiento

Uno de los hallazgos de mayor alcance estratégico es la redefinición del rol del oficial de cumplimiento que posibilita el análisis predictivo. Los participantes describen este cambio como un tránsito desde una función reactiva de auditoría hacia una función proactiva de estrategia. El oficial de cumplimiento, en esta nueva configuración, siguiendo la opinión de Celis Correa (2023), deja de ser alguien que revisa lo ocurrido para convertirse en alguien que anticipa escenarios, calcula probabilidades y define movimientos antes de que los riesgos se materialicen.

Esta transformación se sostiene sobre la capacidad del análisis predictivo para cuantificar la incertidumbre que el banco está dispuesto a asumir. Tradicionalmente, el apetito de riesgo solía ser una declaración de principios flotando en documentos de política, sin un anclaje operativo preciso. El análisis predictivo permite traducir esa tolerancia al riesgo en umbrales numéricos que alimentan los sistemas de alerta y las decisiones de vinculación de clientes. Ahora bien, el enfoque basado en riesgo, tantas veces invocado pero difícil de operacionalizar, encuentra aquí un mecanismo concreto de aplicación.

Los participantes identifican que el espectro de decisiones habilitado por el análisis predictivo va desde la no vinculación de un prospecto cuando el nivel de incertidumbre supera el umbral definido, hasta la aplicación de una debida diligencia intensificada que mitigue riesgos emergentes antes de que se materialicen. Entre ambos extremos, el

análisis predictivo permite graduar la intensidad del escrutinio según la probabilidad estimada de que el cliente o la transacción presenten irregularidades. Esta gradualidad constituye una de las ganancias más significativas respecto de los sistemas basados en reglas binarias, donde la decisión solía ser todo o nada.

Un aspecto particularmente relevante que emerge del análisis es la capacidad del análisis predictivo para detectar la intención antes de la acción. Esta formulación, propuesta por uno de los participantes, señala el verdadero desafío del fraude: este no es un mero patrón observable, sino una conducta intencional que solo se manifiesta plenamente en el momento de su ejecución.

Los modelos predictivos no leen mentes, pero pueden identificar correlaciones entre variables observables y la probabilidad de que exista una intención fraudulenta aún no exteriorizada. Detectar la intención antes de la acción es, por definición, el horizonte inalcanzable para cualquier sistema basado exclusivamente en reglas, que solo reacciona cuando la acción ya ocurrió.

Los participantes advierten que esta capacidad predictiva tiene límites que no deben ser ignorados. Un participante señala la diferencia entre predecir el incumplimiento de un crédito por razones económicas legítimas y predecir la intención fraudulenta. La primera es una cuestión de capacidad de pago, que puede modelarse con datos financieros. La segunda implica un engaño activo desde el origen, cuya inferencia es mucho más compleja y está sujeta a mayores márgenes de error. Esta observación es valiosa porque desmonta una posible ingenuidad: predecir el fraude no es equivalente a predecir el incumplimiento, y los modelos que funcionan bien para lo segundo pueden ser inadecuados para lo primero.

La solución que proponen los participantes no es abandonar los modelos predictivos, sino subordinarlos a un marco de gobernanza que incluya auditorías periódicas para detectar sesgos discriminatorios, especialmente aquellos que afectan a sectores vulnerables o minorías. Esta solución reconoce que los sesgos no son un error técnico que pueda corregirse con una actualización de software, sino una cuestión de diseño institucional, de rendición de cuentas y de distribución de responsabilidades.

El marco regulatorio y sus silencios

El análisis de las preguntas sobre la Resolución N.º 010.25 de SUDEBAN (2025) revela un diagnóstico compartido por los participantes: la norma representa un avance significativo en la modernización

del marco regulatorio bancario venezolano, pero presenta vacíos que podrían frenar precisamente las innovaciones que busca habilitar.

En el terreno de las fortalezas, los participantes destacan la exigencia de detección de alertas en tiempo real, lo que implica un reconocimiento normativo de que la prevención del delito financiero no puede operar sobre bases retrospectivas o con desfases temporales significativos. También señalan la vinculación digital del cliente, que remueve un obstáculo normativo que durante años frenó la digitalización del onboarding bancario. El robustecimiento de la tecnología biométrica como factor de autenticación, junto con la firma electrónica y las contraseñas de uso único, completa el cuadro de fortalezas.

Sin embargo, el vacío más importante señalado por los participantes es la ausencia de reglas claras sobre inteligencia artificial y criptoactivos. Esta doble omisión no es menor. La inteligencia artificial, como ha quedado documentado a lo largo de esta discusión, está transformando la detección de patrones, la calificación de riesgo y la gestión documental. La ausencia de un marco regulatorio específico genera incertidumbre sobre qué tipo de modelos son aceptables, qué requisitos de transparencia deben cumplir y qué responsabilidad recae sobre la institución cuando un algoritmo produce un error. Los participantes advierten que esta falta de claridad podría llevar a las instituciones bancarias a dudar en implementar modelos de aprendizaje automático avanzados por temor a sanciones discrecionales.

En este contexto de vacío normativo, los participantes ven en las normas ISO 37301 (sistema de gestión de compliance) y 31000 (gestión del riesgo) un puente útil para demostrar la idoneidad de los sistemas de inteligencia artificial ante el regulador. La alineación con estos estándares internacionales permite construir un expediente de diligencia que muestra que la institución ha identificado los riesgos de la tecnología, ha establecido controles proporcionales y mantiene una supervisión humana sobre los resultados automatizados. No se trata de que la ISO exima del cumplimiento de la ley local, sino de que el cumplimiento de estándares reconocidos internacionalmente constituye una evidencia sólida de que la institución actuó con la diligencia debida al implementar la tecnología.

Responsabilidad y ética en la era de la automatización

El análisis de las preguntas sobre responsabilidad jurídica y lineamientos éticos revela un consenso claro entre los participantes en torno a un

principio fundamental: la responsabilidad regulatoria final es indelegable y recae sobre el oficial de cumplimiento y la institución, no sobre los desarrolladores de algoritmos. El argumento que sustenta este consenso es sólido desde la perspectiva regulatoria, ya que el banco puede contratar a un tercero para desarrollar una herramienta de inteligencia artificial, pero no puede delegar en un tercero sus obligaciones regulatorias. En consecuencia, si un algoritmo mal diseñado produce decisiones discriminatorias o no detecta operaciones sospechosas, el banco podrá ejercer un reclamo contra el desarrollador por incumplimiento contractual, pero frente al regulador la responsabilidad seguirá siendo del banco.

En tal sentido, los participantes matizan esta posición al señalar que la responsabilidad se distribuye a lo largo de toda la cadena de valor de la inteligencia artificial. Quienes definen los objetivos del modelo, quienes seleccionan y preparan los datos de entrenamiento, quienes diseñan la arquitectura algorítmica, quienes validan los resultados antes de la puesta en producción, quienes monitorean su desempeño una vez operativo y quienes toman decisiones basadas en sus salidas, todos tienen una porción de responsabilidad proporcional a su capacidad de influir en el resultado final. Sin embargo, frente al regulador, la responsabilidad última se concentra en la figura del oficial de cumplimiento, quien actúa como interlocutor designado ante la superintendencia.

Otro principio destacable es la supervisión humana como garantía última de responsabilidad y corrección. La automatización no puede operar sin controles humanos que revisen sus decisiones, especialmente aquellas que afectan negativamente al cliente. La supervisión humana no es un complemento opcional de la automatización, sino un requisito ético que asegura la existencia de un punto de responsabilidad identificable cuando una decisión algorítmica produce un resultado cuestionable.

Conclusiones

La presente investigación permitió analizar el compliance en la era de la inteligencia artificial (IA) en el sector bancario de Venezuela. Este estudio se fundamentó en la necesidad de modernizar las unidades de compliance ante el surgimiento de nuevas dinámicas tecnológicas, lo cual no representa únicamente una actualización tecnológica, sino una reconfiguración necesaria del paradigma de cumplimiento normativo.

En principio, si se considera lo respectivo a las funcionalidades de la IA en el derecho, se conclu-

ye que herramientas como los sistemas expertos, el procesamiento inteligente de documentos (IDP) y el análisis predictivo constituyen un ecosistema de soporte que potencia, sin sustituir, la labor del profesional jurídico. Asimismo, se determinó que la IA permite transitar de un análisis de riesgos lineal y reactivo a uno multidimensional y preventivo en lo relativo al compliance. En tal sentido, el análisis predictivo se erige como la “piedra angular” de la prevención moderna de la legitimación de capitales, al permitir que las instituciones financieras actúen bajo un enfoque basado en riesgos dinámico, anticipando tipologías delictivas mediante la identificación de patrones que resultan imperceptibles para la supervisión humana tradicional.

En cuanto a las tecnologías específicas aplicables al sector bancario venezolano, se concluye que el machine learning (ML) y el procesamiento de lenguaje natural (PLN) son pilares de la eficiencia operativa, ambos dentro de la inteligencia artificial estrecha. El ML ha demostrado ser vital para la reducción de “falsos positivos”, optimizando la carga de trabajo de las unidades de cumplimiento al filtrar el ruido transaccional. No obstante, esta investigación arrojó una conclusión crítica sobre el PLN: a pesar de su capacidad para la revisión masiva de datos y su análisis, persiste el riesgo de “alucinaciones” algorítmicas. Por tal motivo, la tecnología debe ser implementada bajo un esquema de “aprendizaje supervisado”, donde el experto humano actúe como filtro de veracidad técnica y legal. Asimismo, el reconocimiento de caracteres (OCR/ICR) enfrenta en Venezuela el desafío de la baja calidad de soportes físicos deteriorados, lo que obliga a la adopción de protocolos mixtos de validación.

Sobre las implicaciones legales, de gobernanza y ética, la conclusión más trascendental que arroja esta investigación es la ratificación de que la responsabilidad jurídica institucional es indelegable, ya que, a pesar del nivel de autonomía que pueda alcanzar un algoritmo, el control final y la consecuencia legal recaen exclusivamente en el sujeto humano y en la persona jurídica bancaria. Por tal motivo, la gobernanza debe regirse por la doctrina del “buen padre de familia”, donde la institución es responsable de asegurar que el algoritmo sea explicable, transparente y libre de sesgos, a fin de que la ética en la IA bancaria venezolana se enfoque en la minimización de datos y el respeto a la privacidad, limitando la automatización a la información estrictamente necesaria para la relación financiera, evitando así vulneraciones a derechos fundamentales por perfilamientos indebidos.

De lo anterior y en relación con el objetivo de esta investigación, se concluye que el compliance en la

era de la inteligencia artificial (IA) en el sector bancario de Venezuela puede materializarse mediante técnicas de IA estrecha, bajo una estructura multidisciplinaria y resiliente. En tal sentido, es necesario que las entidades financieras creen un comité de ética e implementen protocolos de verificación tipo Maker/Checker para la inteligencia documental, a fin de responder de manera efectiva a los vacíos detectados en la práctica. La IA debe entenderse como un “asistente de alta precisión” que blinda a la institución ante riesgos emergentes, como los deepfakes y la ingeniería social automatizada, mediante el uso

de biometría dinámica y modelos defensivos.

La adopción estratégica de la IA en la banca venezolana no es una opción futura, sino un imperativo presente para garantizar la seguridad jurídica y la celeridad procedimental. La investigación demuestra que, si se implementa bajo principios de gobernanza sólida y supervisión humana experta, la IA tiene el potencial de transformar el cumplimiento normativo en una ventaja estratégica que proteja la integridad del sistema financiero nacional frente a las crecientes amenazas del crimen transnacional y la complejidad de los mercados globales.

Referencias

- Agencia Española de Protección de Datos y Supervisor Europeo de Protección de Datos (2020). *10 malentendidos sobre el machine learning (Aprendizaje Automático)* [10 Misunderstandings About Machine Learning (Artificial Intelligence)]. <https://www.aepd.es/guias/10-malentendidos-machine-learning.pdf>
- Amazon Web Services (2024). *¿Qué es el procesamiento inteligente de documentos (IDP)?* [What Is Intelligent Document Processing (IDP)?]. <https://aws.amazon.com/es/what-is/intelligent-document-processing/>
- Asamblea Nacional (2014). Decreto 1402, mediante el cual se dicta el decreto con Rango, Valor y Fuerza de Ley de Instituciones del Sector Bancario (Decree No. 1402, issuing the Decree with the Rank, Value and Force of Law on Banking Sector Institutions). Gaceta Oficial N.º 40.557. 8 de diciembre de 2014. Caracas, Venezuela.
- Asociación Española de Banca (2019). *El uso de la inteligencia artificial en el sector bancario* (The Use of Artificial Intelligence in the Banking Sector). <https://s1.aebanca.es/wp-content/uploads/2019/07/la-inteligencia-artificial-en-el-sector-bancario.pdf>
- Ayerdi, A. (2025). Las ventajas de aplicar la IA a la gestión documental (The Advantages of Applying AI to Document Management). Docuware. <https://start.docuware.com/es/blog/gestion-documental-ia>
- Banca y Negocios. (2026). *Ranking bancario - Marzo 2026* (Banking Ranking – March 2026). <https://www.bancaynegocios.com/ranking-bancario/>
- Carranza Bravo, P. (2010). Introducción a las técnicas de inteligencia artificial aplicadas a la gestión financiera empresarial (Introduction to Artificial Intelligence Techniques Applied to Business Financial Management). *Fides et Ratio: revista de difusión cultural y científica de la Universidad La Salle*, 4(4), 8 – 15. <http://www.scielo.org.bo/pdf/rfer/v4n4/v4n4a02.pdf>
- Castagnino, D. (2019). Una aproximación al concepto de corporate compliance (An Approach to the Concept of Corporate Compliance). *Revista Venezolana de Derecho Mercantil*, (3), 97–130. https://www.sovedem.com/_files/ugd/de1016_d5fd1af712aa43f08a67c45b8dda2b0e.pdf
- Celis Correa, J.A. (2023, agosto 22). Predicción judicial: la inteligencia artificial como aliada en el sistema legal (Judicial Prediction: Artificial Intelligence as an Ally in the Legal System). *Boletín Uniciencia* (31). <https://unicienciabga.edu.co/vive-la-u/egresados/boletines/342-articulo-7>
- Correa, C. (2025, marzo 21). El impacto de la IA en la gestión legal: una revolución en marcha (The Impact of AI on Legal Management: A Revolution Underway). [Webdox CLM Blog]. <https://www.webdoxclm.com/blog/el-impacto-de-la-ia-en-la-gestion-legal>
- Escudero Molina, J. (2023). *El sistema de codificación predictiva y expertos jurídicos en la valoración probatoria. Una aproximación entre el derecho y la inteligencia artificial* (The Predictive Coding System and Legal Experts in the Evaluation of Evidence: An Approach Between Law and Artificial Intelligence) [Tesis de Licenciatura, Institución Universitaria Tecnológico de Antioquia]. <https://dspace.tdea.edu.co/server/api/core/bitstreams/3a970e4f-4a2c-442f-bc00-f56d633bddea/content>
- Ferrer Bravo, E.Y. (2023, abril 13). El Servicio de Tecnología Financiera (Fintech) y las Instituciones de Tecnología del Sector Bancario (ITFB): Tendencia en Venezuela (The Financial Technology Service (Fintech) and Financial Technology Institutions of the Banking Sector (ITFB): A Trend in Venezuela). *Derecho y Sociedad Revista y Blog*. <https://www.derysoc.com/el-servicio-de-tecnologia-financiera-fintech-y-las-instituciones-de-tecnologia-del-sector-bancario-itfb-tendencia-en-venezuela/>
- García, M.L. (2024). UAX fomenta el pensamiento crítico sobre IA y justicia en su formación jurídica (UAX Promotes Critical Thinking on AI and Justice in Legal Education). Universidad Alfonso X El Sabio. <https://www.uax.com/noticias/la-uax-analiza-el-impacto-de-la-ia-en-la-justicia>
- Gómez Cáceres, D. & López Zeballos, J. (2002). *Riesgos financieros y operaciones internacionales* (Financial Risks and International Operations). ESIC Editorial.
- Herrera-Ortiz, J., Peña-Avilés, J., Herrera-Valdivieso, M., & Moreno-Morán, D. (2024). La inteligencia artificial y su impacto en la comunicación: recorrido y perspectivas (Artificial Intelligence and Its Impact on Communication: Evolution and Perspectives). *Telos: Revista de Estudios Interdisciplinarios en Ciencias Sociales*, 26(1), 278-296. <https://doi.org/10.36390/telos261.18>

- Holdsworth, J. (2023). ¿Qué es el reconocimiento óptico de caracteres (OCR)? (What Is Optical Character Recognition (OCR)?). IBM. <https://www.ibm.com/es-es/think/topics/optical-character-recognition>
- International Organization for Standardization (2018). *Gestión del riesgo - Directrices (ISO 31000:2018) [Risk Management — Guidelines (ISO 31000:2018)]*. <https://www.iso.org/standard/65694.html>
- International Organization for Standardization (2021). *Sistemas de gestión del cumplimiento - Requisitos con orientación para su uso (ISO 37301:2021) [Compliance Management Systems — Requirements with Guidance for Use (ISO 37301:2021)]*. <https://www.iso.org/standard/75080.html>
- International Organization for Standardization (2022). *Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información (ISO 27001:2022) [Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems (ISO 27001:2022)]*. <https://www.iso.org/es/norma/27001>
- Lancho Pedrera, F. (2003). Los sistemas expertos en el derecho (Expert Systems in Law). *Anuario de la Facultad de Derecho*, 21, 629-636. <https://dialnet.unirioja.es/servlet/articulo?codigo=854374>
- Martínez Bahena, G.C. (2013). La inteligencia artificial y su aplicación al campo del derecho (Artificial Intelligence and Its Application to the Field of Law). *Revista Alegatos*, (82), 827-846. <https://alegatos.azc.uam.mx/index.php/ra/article/view/205>
- Microsoft. (2024). *Procesamiento inteligente de documentos con Microsoft AI (Intelligent Document Processing with Microsoft AI)*. <https://www.microsoft.com/en-us/research/project/document-ai/>
- Parlamento Europeo y Consejo de la Unión Europea (2024, junio 13). Reglamento (UE) 2024/1689 por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n° 300/2008, (UE) n° 167/2013, (UE) n. o 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) [Artificial Intelligence Act: Regulation (EU) 2024/1689 Laying Down Harmonized Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144, and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)]. *Diario Oficial de la Unión Europea*, 2024/1689. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32024R1689>
- Pérez-Ugena, M. (2024). La inteligencia artificial: definición, regulación y riesgos para los derechos fundamentales (Artificial Intelligence: Definition, Regulation, and Risks to Fundamental Rights). *Revista de Derecho Público*, 72(1), 307-337. <https://doi.org/10.18543/ed.3108>
- Scarcello, F. (2018). Artificial intelligence. En: S. Ranganathan, M. Gribskov, S.S. Nakai y C. Schönbach (Eds.). *Encyclopedia of Bioinformatics and Computational Biology* (Vol. 1, pp. 287-293). Elsevier. <https://www.sciencedirect.com/science/chapter/referencework/abs/pii/B9780128096338203269>
- Superintendencia de las Instituciones del Sector Bancario (2021, junio 17). Resolución N.° 001-21 mediante la cual se dictan las normas que regulan los servicios de tecnología financiera (FINTECH) [Resolution No. 001-21 issuing the regulations governing financial technology (FINTECH) services]. *Gaceta Oficial* N.° 42.162. Caracas, Venezuela.
- Superintendencia de las Instituciones del Sector Bancario (2025, marzo 31). Normas relativas a la administración y fiscalización de los riesgos relacionados con la legitimación de capitales (Regulations concerning the management and supervision of risks related to money laundering). Resolución N.° 010.25. *Gaceta Oficial* N.° 43.098. Caracas, Venezuela.
- Vaudo, L. (2022). Cumplimiento organizacional y autorregulación normativa empresarial. Especial referencia a las instituciones del sistema financiero venezolano (Organizational Compliance and Corporate Regulatory Self-Regulation: Special Reference to Institutions of the Venezuelan Financial System). *Revista Venezolana de Legislación y Jurisprudencia*, (19), 177-196. <https://rvlj.com.ve/wp-content/uploads/2023/01/RVLJ-19-177-196.pdf>
- Villegas Ruiz, J. (2021). Introducción al estudio del derecho del cumplimiento normativo y análisis regulatorio de la empresa (Introduction to the Study of Compliance Law and Regulatory Analysis of the Company). *Revista de Derecho Mercantil*, (7), 153-196. http://www.ulpiano.org.ve/revistas/bases/artic/texto/RVDM/7/RVDM_2021_7_153-196.pdf