# Estudio de la exposición a riesgos de las entidades financieras por la adopción de sistemas de Inteligencia Artificial (IA) en sus actividades

Santiago Tabares Rodríguez

Escuela de Derecho

Universidad EAFIT

Pregrado en Derecho

Monografía

Asesora: Norma Cecilia Nieto

Medellín

2025

# Tabla de Contenido

## Resumen

En esta monografía se busca abordar el tema de los riesgos a los que se verían expuestas las entidades financieras en Colombia por el uso de sistemas de Inteligencia Artificial dentro de sus actividades cotidianas. La IA ha jugado un papel fundamental en los diferentes sectores económicos desde que se le ha dado aplicación comercial a principios del siglo XXI y cada vez es más claro que los sistemas algorítmicos y de machine learning modelan nuestras vidas cotidianas, por lo tanto, es común que surjan preocupaciones entre quienes no estamos incluidos en el desarrollo de estas tecnologías acerca de cuáles serán las posibles implicaciones en materia de privacidad, transparencia y derechos del consumidor. En este trabajo analizaré el marco regulatorio y legal en Colombia, así como las tendencias internacionales, que buscan responder a la pregunta de cómo deben abordar las instituciones los riesgos inherentes a la IA. Finalmente, se concluye el estudio con la premisa de que, aunque una regulación estricta no es deseable, pues puede obstaculizar la innovación tecnológica, es urgente la implementación de medidas que mitiguen los riesgos asociados al uso de la IA en el sector financiero, medidas que pueden alcanzarse a través de regulación especializada y flexible o a través del mecanismo del soft law. Posteriormente se

elabora una propuesta de medidas de mitigación a través de la adopción de buenas prácticas corporativas, y se estudian algunas instituciones de la responsabilidad civil que pueden dar respuesta a la cuestión de la adjudicación de los daños causados por un sistema de IA.

## 1. Introducción

En los últimos años, hemos visto como se ha incrementado la popularidad y el uso de los sistemas de Inteligencia Artificial (en adelante "IA") por parte tanto de las personas naturales como de las empresas, este incremento se ve representado en el aumento del valor total del mercado de la IA, según El Tiempo (2024) el mercado global de la IA duplicará su valor actual, llegando a los 1,27 billones de dólares (aproximadamente 1,14 billones de euros) para el año 2028. Este aumento representaría el 10% del mercado tecnológico global. Estas cifras representan el panorama de crecimiento y expansión que tiene la IA en el mundo, sin embargo, en este trabajo nos enfocaremos en el uso específico que los actores del Sistema Financiero dan a los sistemas de IA en sus actividades ordinarias.

En el marco del mercado financiero, la IA tiene una infinidad de aplicaciones que se ha visto reflejada en el aumento del uso de estos sistemas por parte de las entidades financieras, en Colombia las aplicaciones más comunes se han dado en la detección de fraude y ciberseguridad y en el incremento de la inclusión financiera (Asobancaria, 2024). Sin embargo, el verdadero potencial de la IA radica en su capacidad para recopilar, analizar y realizar recomendaciones a sus usuarios a partir de una enorme cantidad de datos. Este manejo de grandes cantidades de información (Big Data o Macrodatos) es especialmente relevante para las entidades financieras, puesto que estas deben recopilar, almacenar y utilizar; con arreglo a las normas vigentes, grandes

cantidades de información personal que incluye aspectos como los nombres, edades, números de identificación, ocupación, residencia, transacciones, bienes, deudas, etc.

Este manejo de información sensible, que además es utilizada para diversos fines como el rastreo de posibles situaciones de fraude u otros escenarios ilícitos, la calificación crediticia de los ciudadanos y la determinación del acceso al crédito representa una actividad de vital importancia para toda entidad financiera, por lo cual es natural que estas busquen formas de aumentar la eficiencia de recopilación y análisis de estos datos, es en este contexto en el cual la introducción de la IA en los servicios financieros representa una oportunidad de crecimiento para el sector financiero.

A pesar de esto, debemos tener en cuenta que la IA es una tecnología emergente, Webb (2019) define a la IA como una transformación significativa similar a la Revolución Industrial; es, en sus propias palabras, “la tercera era de la computación” (Webb, 2019, p. 13). Como tecnología emergente debemos entender que aún no es posible dimensionar en su totalidad los riesgos inherentes a su aplicación en los distintos escenarios de la economía global, sin embargo, a través de un ejercicio de inferencia razonable, es posible identificar los escenarios de riesgo a partir de la comprensión de cómo se construyen estos sistemas IA. Más adelante en la Sección 2 se identificarán los posibles riesgos a los que se enfrentan las entidades financieras con el uso cotidiano de la IA en sus actividades.

Otro punto problemático de este avance tecnológico es la poca – y en los casos existentes imprecisa – regulación acerca de este tema, aunque es cierto que, por regla general, el Derecho avanza a un paso más atrasado que las innovaciones tecnológicas y comerciales, en un campo como la IA la inseguridad jurídica puede traer consecuencias nefastas ya que los nuevos descubrimientos ocurren a un ritmo vertiginoso y es probable que, sin un marco general de principios éticos, los intereses

comerciales conduzcan a la IA a ser una herramienta de generación de riqueza sin consideración alguna por los componentes humanos del mercado. A pesar de esto, el escenario opuesto – una regulación rígida – no es deseable desde ningún punto de vista, ya que puede obstaculizar o detener la innovación tecnológica dentro de su jurisdicción, causando que el Estado que implementó dicha norma quede rezagado jurídica, tecnológica y económicamente del resto del mercado; o por el contrario puede ser una regulación que no responda a las necesidades de los desarrolladores, usuarios y consumidores finales, dejándolos en un estado de vulnerabilidad ante los posibles escenarios perjudiciales que se estudiarán en la Sección 2.

Por lo tanto, es de vital importancia para todos los actores contar con un marco jurídico claro que defina las reglas de juego en el uso de sistemas de IA. Una regulación inteligente, flexible y clara permitiría a los desarrolladores aplicar medidas correctivas a la IA incluso antes de su comercialización, a los usuarios, les permite conocer y reportar las posibles fallas y eximirse de responsabilidad, y a los consumidores, les asegura la protección debida frente a los demás actores del mercado.

Debo precisar que, cómo se verá más adelante, en un escenario regulatorio como el visto previamente las normas del derecho tradicional probablemente no sean la mejor solución, en especial por la necesidad de una regulación dinámica y flexible que responda a la velocidad con que se lanzan al mercado las nuevas innovaciones tecnológicas, y por lo tanto entraremos en un escenario donde se realza la importancia de los mecanismos de *soft law,* sin dejar de lado la importancia que tiene que los reguladores financieros conozcan y entiendan las implicaciones futuras de la aplicación de la IA por parte de los actores del sistema financiero.

## 2. Sección 1: la importancia de la IA en el sector financiero

### 2.1 Concepto de la IA en el sector financiero

Para iniciar con nuestro análisis, primero debemos entender de forma correcta qué se entiende por IA y, especialmente, dar una definición que logre poner en común los diferentes criterios usados por los expertos en la materia.

Para comenzar, Amy Webb, autora de *Nueve gigantes. Las máquinas inteligentes y su impacto en el rumbo de la humanidad*, define la IA de la siguiente manera: "En su forma más básica, la IA es un sistema que toma decisiones autónomas" (Webb, 2019, p.29).

En un trabajo académico denominado *Robotics, AI and the Future of Law,* escrito por varios académicos y editado por Marcelo Corrales, Mark Fenwick y Nikolaus Forgó, en el apartado escrito por Sam Wrigley de la Universidad de Helsinki se define la IA como aquellos programas que puedan realizar tareas que requerirían inteligencia humana, o computadores que piensen con una lógica humana (Corrales et al., 2018).

La Real Academia Española define la inteligencia artificial como una "disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o razonamiento lógico" (Real Academia Española, |RAE|, s.f., definición 1).

En el artículo *Inteligencia Artificial en la banca*, el gremio de las entidades financieras en Colombia Asobancaria define la IA como los "sistemas y algoritmos que crean máquinas capaces de resolver problemas para los cuales suele requerirse inteligencia humana" (Asobancaria, 2023, p.1).

Por su parte, la Superintendencia Financiera de Colombia ha definido la IA de la siguiente forma: "La IA se refiere a sistemas que muestran un comportamiento inteligente analizando su entorno y

actuando – con cierto grado de autonomía – para alcanzar objetivos específicos" (Superintendencia Financiera de Colombia, |SFC|, s.f.)

Finalmente, y con el objetivo de dar una definición precisa útil al ámbito financiero, en el mismo artículo previamente citado Asobancaria define a la IA en el sector financiero como el "conjunto de sistemas habilitados por tecnología para evaluar escenarios de servicio en tiempo real, operando datos recopilados de fuentes digitales y/o físicas para brindar recomendaciones, alternativas y soluciones personalizadas a los clientes en sus consultas o problemas, incluso aquellos muy complejos" (Asobancaria, 2023, p. 2).

Al ver la multiplicidad de definiciones y características que se atribuyen a la IA, es preciso que lleguemos a un concepto unificado extrayendo los elementos usuales a todas las definiciones. Así, es notorio como las descripciones tradicionales usan frecuentemente términos como "autonomía", "sistema" e "inteligencia" que resaltan las características fundamentales de la IA.

Por lo tanto, una definición propia de la IA y que será como se entenderá en este trabajo en adelante, es que la IA es todo aquel sistema que es capaz, de forma autónoma, de formular soluciones viables a través del análisis de datos recopilados de su entorno.

### 2.2 Aplicaciones de la IA en el sector financiero

Como vimos anteriormente, el uso de la IA por parte de las entidades financieras colombianas ha tenido un incremento significativo a lo largo de los últimos años, siendo el principal atractivo de estos sistemas su capacidad de gestión de grandes cantidades de datos (Big Data) lo que la hace ventajosa para estas entidades que, en su actividad ordinaria, deben gestionar grandes cantidades de información de forma rápida y exigente.

Estos sistemas tecnológicos pueden ser usados por las entidades financieras para una multiplicidad de objetivos, sin embargo, todas las actividades que las entidades financieras realizan pueden

resumirse como una forma de mitigación de riesgos. En efecto, las entidades financieras (y especialmente los bancos comerciales) se dedican esencialmente al negocio de la gestión de riesgos (Kurzgesagt, 2015, 1m20s).

Es así como, para comprender las actividades de las entidades financieras, es especialmente útil comprender los riesgos a los que se encuentran expuestas, para ello, usaremos el listado y definición que la Superintendencia Financiera de Colombia impone a sus regulados en su Circular Básica Contable y Financiera, en el Capítulo XXXI "SIAR", acrónimo de "Sistema Integral de Administración de Riesgos".

En esencia, las entidades financieras colombianas se encuentran expuestas a los siguientes riesgos:

- **Riesgo de crédito:** definido como aquella posibilidad de que la entidad financiera incurra en pérdidas y disminuya el valor de sus activos como consecuencia de que un deudor o contraparte incumpla sus obligaciones.
- **Riesgo de mercado:** definido como aquella posibilidad de que la entidad financiera incurra en pérdidas asociadas a la disminución del valor de sus portafolios y/o portafolios de terceros que administre, por efecto de variaciones en el precio de las inversiones en las cuales mantiene posiciones dentro o fuera del balance.
- **Riesgo operacional:** definido como aquella posibilidad de que la entidad financiera incurra en pérdidas por las deficiencias, fallas o inadecuado funcionamiento de los procesos, la tecnología, la infraestructura y el recurso humano, así como por la ocurrencia de acontecimientos externos a estos. Incluye el riesgo legal.
- **Riesgo de liquidez:** definido como aquella posibilidad de que la entidad financiera incurra en pérdidas asociadas a la contingencia de no poder cumplir plenamente de manera

oportuna y eficiente con los flujos de caja esperados e inesperados, vigentes y futuros, sin afectar el curso de las operaciones diarias o la condición financiera de la entidad.

- **Riesgo País:** definido como aquella posibilidad de que la entidad financiera incurra en pérdidas en virtud de las operaciones financieras en el exterior por causa de un detrimento de las condiciones económicas y/o sociopolíticas del país receptor de dichas operaciones, bien sea por limitaciones a las transferencias de divisas o por factores no imputables a la condición comercial y financiera del país receptor de la operación.

  (Superintendencia Financiera de Colombia, 2021b).

Definidos los riesgos a que están expuestas las entidades financieras, será más fácil entender de qué manera se están utilizando los sistemas de IA en la realización de las labores ordinarias de las entidades financieras, así, la IA es utilizada por las entidades financieras colombianas para las siguientes actividades:

1. Detección de transacciones fraudulentas.
2. Asesoría financiera personalizada (Banca personalizada).
3. Manejo del riesgo crediticio.
4. Automatización de procesos.

Para concluir, la adopción de la IA por parte de las entidades financieras colombianas tiene el potencial de convertirse en un avance significativo en todas las actividades de estas, incluyendo la gestión de riesgos. La capacidad de procesamiento de datos de esta nueva tecnología representa el mayor atractivo para las entidades financieras. Más adelante en la Sección 3 estudiaremos la aplicación concreta de la IA en las operaciones autorizadas que pueden realizar las entidades financieras y veremos como una adopción diligente de esta tecnología puede fortalecer al sistema financiero colombiano y adaptarlo a un entorno económico global en constante evolución.

## 3. Sección 2. Matriz de riesgos en el uso de la IA en el sector financiero

En esta sección, analizaremos uno a uno los principales riesgos derivados del uso de sistemas de IA por parte de las entidades financieras en sus actividades ordinarias, con el objetivo de construir una matriz de riesgos que permita realizar una fácil identificación de los problemas relacionados con la adopción de esta tecnología, y proponer se logren medidas preventivas y correctivas para mitigar estos riesgos.

### 3.1 Riesgo por uso de datos personales e infracción de la privacidad

Como hemos visto, para que una IA especializada en finanzas funcione correctamente requiere de una enorme cantidad de datos que alimenten sus procesos de *machine learning,* de forma que:

> El insumo crítico sigue siendo la abundancia y diversidad de datos. Para desarrollar modelos de IA que puedan "ver" a una persona y determinar qué servicios financieros específicos ofrecerle, se necesita una gran cantidad de datos de diferentes naturalezas: geográficos, económicos, históricos, entre tantos otros. Estos datos pueden provenir de diversas entidades, tanto públicas como privadas, así como de los propios colombianos que deseen compartir su información de manera voluntaria. (Asobancaria, 2024, p. 7)

Así, se hace evidente que, para poner en funcionamiento esta tecnología, las entidades financieras deben disponer de una enorme cantidad de datos, teniendo en cuenta que entre más datos son procesados más precisas son las decisiones de la IA, por ejemplo, una IA de banca personalizada

que funcione según las expectativas actuales del sector deberá recabar los datos privados[1] financieros del individuo, como su puntaje de crédito, sus ingresos y egresos, entre otros. Sin embargo, esta recolección y manejo deben sujetarse a las disposiciones de las leyes 1266 de 2008 y 1581 de 2012.

Entonces, debido a la complejidad de los sistemas de IA, se le dificulta a las entidades financieras el cumplir con sus responsabilidades en el manejo de los datos de sus clientes, en particular, con respecto a los principios de transparencia y confidencialidad estipulados en las leyes sobre protección de datos personales; a una entidad financiera puede dificultársele explicar de qué manera se están usando los datos privados de sus clientes dentro de un sistema de IA, o podría tener razones legítimas relacionadas con secretos comerciales que la compelen a no revelar la información sobre sus sistema de IA o como los "alimenta" con los datos de los clientes, además, existe la posibilidad de que se dé una captura ilegítima de los datos, esto es, que un sistema de IA programado para recabar y analizar datos se exceda en su labor, realizando un monitoreo excesivo del comportamiento de los clientes y/o potenciales clientes de la entidad, lo cual a su vez perjudicaría a las entidades financieras usuarias de esta tecnología, ya que podrían verse en incumplimiento del deber de responsabilidad demostrada consagrado en el artículo 19-A de la Ley 1266 de 2008 y, por lo tanto, verse sujetas a sanciones por parte de la Superintendencia Financiera.

### 3.2 Riesgo por uso indebido de propiedad intelectual

Además de las posibles infracciones al régimen de datos personales, es necesario estudiar la posibilidad de que la IA incurra en infracciones al régimen de propiedad intelectual en la ejecución de sus funciones, especialmente si tenemos en cuenta que, debido a la profundidad y complejidad

[1] **Artículo 3 literal h de la Ley 1266 de 2008:** Dato privado. Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

de las redes neuronales de los sistemas de IA, las entidades financieras (usuarias) y los desarrolladores (proveedores) pueden no tener la capacidad de entender correctamente todas las operaciones lógicas que tienen lugar en las redes neuronales que conforman la IA.

Respecto a esto, en Colombia la propiedad industrial e intelectual se rigen por la Decisión Andina 468 del 2000 (en adelante, DA-486 del 2000), la Ley 23 de 1982 y la Ley 1915 de 2018. Es importante traer a colación estas normas ya que, como bien dicen Agarwal et al. (2024) uno de los riesgos de la IA son las "infracciones de la propiedad intelectual, como violaciones de los derechos de autor e incidentes de plagio, ya que los modelos fundacionales suelen aprovechar datos basados en internet."

En particular, encontramos que los sistemas de IA pueden ser usados de forma desleal en casos de plagio, como, por ejemplo, el uso de una IA para parafrasear y ocultar así el uso de una obra protegida; o el uso de la IA para copiar marcas y/o formatos de otras entidades; e incluso puede ocurrir que se use de forma desleal un sistema de IA para analizar y copiar los secretos, estrategias y modelos comerciales y empresariales de la competencia, contraviniendo los artículos 260-265 de la DA-486 del 2000.

Y, finalmente, surge el interrogante acerca de las patentes. La IA es una tecnología disruptiva que no se ajusta a los marcos de la propiedad industrial, en efecto, el artículo 14 de la DA-486 del 2000 establece que: "Los Países Miembros otorgarán patentes para las invenciones, sean de producto o de procedimiento, en todos los campos de la tecnología, siempre que sean nuevas, tengan nivel inventivo y sean susceptibles de aplicación industrial."

Sin embargo, como ya hemos estudiado la importancia de los datos que otorga el usuario (entidad financiera) para modelar las decisiones de la IA, cabe hacerse las siguientes preguntas: ¿un sistema de IA modelado con un grupo específico de datos es patentable? ¿existe una diferencia entre la

propiedad del algoritmo y la de los datos utilizados? ¿la entidad financiera funge como "propietaria" de los datos de terceros? Y ¿cuál elemento, el algoritmo o los datos, pesa más a la hora de definir la novedad, inventiva y aplicabilidad industrial de un sistema IA, o su carácter de secreto empresarial en términos del artículo 260 de la DA-486 del 2000?

Todas estas preguntas merecen su propio trabajo investigativo y escapan a nuestros objetivos con este trabajo, con la formulación de estas solo se busca poner de presente los desafíos regulatorios que plantea la adopción de sistemas de IA por parte de las entidades financieras.

### 3.3 Riesgos de fraude y ciberseguridad

Dejando de lado las infracciones legales, ahora debemos tratar el tema de la ciberseguridad y el riesgo de fraude. La IA es una tecnología que cuenta con grandes capacidades generativas, así, es de conocimiento general el auge que han tenido las herramientas de IA generativa como ChatGPT, Grok, Dall-E, etc. Estas herramientas tienen la capacidad de generar contenido y de interactuar de una forma más directa con sus usuarios. Sin embargo, en el marco empresarial y, especialmente, en el financiero, existe el riesgo de que estas u otras herramientas de IA más sofisticadas sean utilizadas con ánimo ilícito, esto es lo que denominaremos riesgo de fraude.

El principal riesgo es la generación de deepfakes, que pueden ser de texto, de imágenes o de audio; un deepfake, según el LISA Institute (s.f.) es un archivo manipulado mediante un software de IA para que parezca auténtico, que busca inducir al error al receptor. Por lo tanto, en el marco de las operaciones financieras, encontramos que tanto la entidad financiera como sus clientes pueden ser receptores de esta información engañosa, por ejemplo, los clientes pueden ser víctimas de

phishing[2] para robar sus datos personales, usando a la IA para suplantar a una entidad financiera. O, por el otro lado, la entidad financiera puede ser objeto de engaño mediante la utilización de una IA para burlar sus filtros de seguridad, como el reconocimiento facial o por voz.

Por otro lado, la ciberseguridad misma de la entidad financiera puede verse en riesgo por el uso de sistemas de IA, siendo así que la entidad puede ser objeto de un ataque cibernético con IA, o de un ataque cibernético dirigido a la IA (envenenamiento de datos).

En primer lugar, los ataques cibernéticos con IA ocurren ya que, según Sardanyés (s.f.):

> Gracias al aprendizaje automático integrado dentro de la IA, esta tecnología, sin necesidad de inteligencia humana, es capaz de detectar vulnerabilidades y brechas de seguridad en los sistemas informáticos de manera más eficiente y a gran escala. Además de poder utilizarse para generar y distribuir malware y automatizar procesos de ataque.

Así, la IA puede ser usada por los ciberdelincuentes para "secuestrar" los sistemas de una entidad financiera y obligarla a realizar alguna acción, o ser usada con el objetivo preciso de dañar a la entidad y minar la confianza del público en el sistema financiero como, por ejemplo, borrando las bases de datos de las entidades o modificando los datos financieros que estas custodian.

En segundo lugar, los ataques dirigidos a la IA usan una técnica llamada "envenenamiento de datos" y buscan afectar a los sistemas de IA de las entidades financieras. Según IBM Corporation (2025) el envenenamiento ocurre cuando un individuo inyecta intencionadamente muestras engañosas o incorrectas en los conjuntos de datos de entrenamiento o de ajuste de una IA. Este ataque busca sesgar intencionadamente los resultados de la IA, afectando al usuario de esta e

[2] Siguiendo a Kosinski (2024) el phishing es la utilización de información fraudulenta para engañar a las personas y que se expongan a la ciberdelincuencia, por ejemplo, mediante la vulneración de sus datos personales.

induciéndolo a un comportamiento que podría no haber tomado si hubiese tenido acceso a la información veraz.

### 3.4 Riesgo de rendimiento y sesgos algorítmicos

Por último, debemos estudiar la posibilidad de que una entidad financiera se vea expuesta a riesgos de rendimiento de la IA, haciendo un especial énfasis en la problemática de los sesgos algorítmicos.

El riesgo de rendimiento es la posibilidad de que un sistema de IA falle en sus datos de salida, este riesgo puede materializarse por la ocurrencia de las siguientes contingencias:

1. Si el sistema de IA cuenta con algoritmos cuyas inferencias fallan por su diseño de código, esto, en pocas palabras, significa que el software de IA no cumple con unos estándares de calidad adecuados y que, en consecuencia, genera razonamientos ilógicos.
2. Si el sistema de IA es incapaz de mantener el ritmo de funcionamiento esperado. Este escenario es especialmente relevante para nuestro tema, puesto que el mercado financiero genera un enorme volumen de datos de forma continua, y un sistema de IA puede sufrir una sobrecarga por un exceso de datos de entrada, o porque el sistema demande un poder de cómputo superior al hardware disponible, o porque el consumo de energía eléctrica supere con creces la capacidad de la red.

Estos riesgos se ven exacerbados si la entidad financiera es excesivamente dependiente de la IA, incluso se puede llegar producir una incapacidad total de atender las necesidades de los clientes, o un paro total de las actividades de la entidad financiera si esta no somete sus sistemas a unos controles de calidad y a una supervisión humana constante.

Ahora bien, un componente especial de este riesgo que merece su propio apartado es la posibilidad de que una entidad financiera se vea afectada por un sesgo algorítmico.

Los algoritmos son la esencia de un sistema, son las instrucciones dadas por el programador al sistema y modelan el comportamiento y las respuestas de este, así, los algoritmos son una pieza vital de la tecnología actual debido a su versatilidad y utilidad (Capitani, 2022).

Con esta información, podemos a su vez entender el sesgo algorítmico como aquel que ocurre cuando los sesgos y prejuicios de los desarrolladores y usuarios se ven reflejados en los resultados que entrega una IA. Este riesgo puede ser intencionado o no intencionado, en este apartado nos referiremos al sesgo no intencionado, pues el sesgo intencionado se trata de forma más extensa en el apartado de riesgo de fraude y ciberseguridad.

Para ilustrar mejor este riesgo, veamos el caso de VisionAI, propiedad de Google, que ocurrió en 2020:

En 2020, investigadores de Algorithmwatch.org descubrieron que la herramienta VisionAI de Google presentaba un sesgo respecto a la raza de las personas, si se mostraba una imagen de una persona de raza negra sosteniendo un termómetro de los utilizados para medir la temperatura durante la pandemia de Covid-19, el sistema arrojaba que en la imagen había un arma de fuego; en cambio, si se mostraba la misma imagen y el mismo termómetro, pero aclarando el tono de piel de la mano, entonces el sistema infería que se trataba de un termómetro (Kayser-Bril, 2020).

En su libro, Webb (2019) explica que los sesgos se generan por la baja diversidad de los equipos que trabajan en el desarrollo de estos sistemas, compuestos en su mayoría por hombres, Webb también explica que debido a que los procesos de selección están en su mayoría automatizados (encargados a sistemas diseñados por este selecto grupo de desarrolladores) es una segregación que se agrava con el tiempo, tendiente a excluir a las mujeres y a las personas de razas negra e hispana, y también excluye a aquellos con formación adicional en áreas como ética o sociología,

pues su formación se considera irrelevante a pesar de que podría contribuir al manejo ético de la IA (p. 51)

Continuando con nuestro análisis, la plataforma IBM watsonx, que es la cartera de productos de IA de IBM, uno de los "gigantes" del mundo de la IA según Webb, establece las siguientes definiciones para los sesgos algorítmicos:

- **Sesgo de decisión:** "El sesgo de decisión se produce cuando un grupo se ve injustamente favorecido respecto a otro debido a las decisiones del modelo. Esto podría deberse a sesgos en los datos y también amplificarse como resultado del entrenamiento del modelo." (IBM Corporation, 2025b)
- **Sesgo de los datos para la IA:** ocurre cuando los sesgos históricos y sociales presentes en los datos se utilizan para entrenar y afinar el modelo, dando lugar a resultados que pueden representar injustamente o discriminar de otro modo a determinados grupos o individuos. (IBM Corporation, 2025c)
- **Sesgo de salida:** ocurre cuando el contenido generado puede representar de forma injusta a determinados grupos o individuos. (IBM Corporation, 2025d)

Con todo esto, nos es posible imaginar algunos ejemplos en el sector financiero colombiano que ilustren los posibles efectos negativos de un sesgo algorítmico en un sistema usado por una entidad financiera:

1. Escenarios donde un sistema de detecciones de fraudes o transacciones ilícitas genere alertas contra usuarios que tengan apellidos similares o iguales a los de personas condenadas por delitos, o que provengan de regiones afectadas por el conflicto.

2. Restricciones de acceso al crédito a personas por razones no relacionadas con su información crediticia, como su sexo, orientación sexual, etnia, nacionalidad, afiliación política o religiosa, etc.
3. Scoring de crédito incorrecto que perjudique a personas pertenecientes a sectores que históricamente no han tenido acceso al sistema financiero y, por lo tanto, no han generado un historial crediticio, como jóvenes, agricultores, empresas emergentes o personas pertenecientes a comunidades o territorios históricamente marginados.
4. Pérdida de oportunidades para la entidad financiera, por ejemplo, si se adopta una IA que analice la pertinencia y calidad de las garantías que presenten los clientes y un cliente presenta una garantía novedosa, la cual puede ser rechazada por la IA incluso si es una buena garantía al no estar contemplada en sus datos de entrenamiento.

De hecho, el mismo Gobierno Nacional ha reconocido el riesgo que implica el sesgo algorítmico en la adopción de sistemas de IA, en el Documento CONPES 4144 de 2025 que creó la Política Nacional de Inteligencia Artificial, el gobierno afirmó que:

> En el país se evidencia insuficiencia de conocimientos sobre los sesgos y los riesgos que estos generan en el ciclo de vida de los sistemas de IA. Resultados del ILIA (Cenia, 2023) muestran que solo el 3,8 % de mensajes en redes sociales corresponden a tópicos de IA y sesgos sociales. Por otro lado, se evidencia que sólo 29 % de las empresas colombianas encuestadas por PricewaterhouseCoopers analizan la forma en que sus algoritmos toman decisiones, siendo una proporción baja respecto a la velocidad de desarrollo y adopción de la IA (PricewaterhouseCoopers, 2024a).
>
> (Consejo Nacional de Política Económica y Social et al., 2025)

En conclusión, el sesgo algorítmico representa el mayor riesgo para una entidad financiera que adopta la IA debido a la frecuencia con la que puede ocurrir (esencialmente, en cada operación en que actúe la IA), sin embargo, como se definirá más adelante, las entidades pueden mitigar este riesgo al ser los titulares de los datos de entrenamiento, ya que pueden realizar un ejercicio de depuración de los datos que elimine aquellos irrelevantes a la hora de tomar una decisión financiera, como la raza o la orientación sexual. Esta depuración no debe ser exclusivamente practicada por los técnicos o programadores, que podrían replicar sus propios sesgos, es vital que intervenga un comité de ética u otros colaboradores que impriman una dimensión más humana. Esta depuración es tan vital que representa el principal punto de interés para el regulador, por la posibilidad de que un sesgo influya negativamente en la democratización del crédito, y, por lo tanto, representa el principal nicho regulatorio tanto por parte de las mismas entidades financieras como por parte de la Superintendencia Financiera de Colombia.

### 3.5 Mapa de riesgos y conclusiones

Analizados los principales riesgos a los que se expone una entidad financiera con la adopción de sistemas de IA, podremos elaborar un mapa de riesgos que permita identificar la gravedad de estos, contrastando la frecuencia con la que pueden ocurrir con el impacto que tendría su ocurrencia en la actividad o en el patrimonio de la entidad, para luego presentar un adelanto de las medidas correctivas que pueden aplicarse.

**Tabla 1**

*Mapa de riesgos por uso de sistemas de IA por parte de las entidades financieras*

| FRECUENCIA | | | | |
|---|---|---|---|---|
| ***Muy alta*** | | Captura ilegítima de datos | | Sesgo algorítmico |
| ***Alta*** | | Plagio de documentos | Plagio de secretos industriales | |
| ***Media*** | | Suplantación de la entidad financiera mediante phishing | | Fallas de rendimiento por causas externas (hardware, energía eléctrica, etc.) |
| ***Baja*** | Incapacidad de demostrar trazabilidad en el manejo de los datos personales | | Incertidumbre sobre quién es el propietario del modelo<br><br>Vulneración de los filtros de seguridad de la entidad financiera<br><br>Envenenamiento de datos | Ataque cibernético con utilización de IA<br><br>Fallas en el código |
| **IMPACTO** | ***Leve*** | ***Moderado*** | ***Severo*** | ***Catastrófico*** |

| *El riesgo es* | |
|---|---|
| ***Aceptable*** | ***Grave*** |
| ***Tolerable*** | ***Inaceptable*** |

Nota. Esta tabla es de elaboración propia, pero el formato y los colores se extrajeron del material del Diplomado en Comercio Exterior de la Universidad EAFIT del profesor Carlos Torres Muskus (comunicación personal, 1 de febrero de 2025).

Así, tenemos que los principales riesgos son aquellos relacionados con el rendimiento de la IA y con una excesiva captura de datos personales, por lo cual, las medidas correctivas más efectivas son aquellas que apunten al mejoramiento y solidez de los sistemas informáticos; este objetivo puede alcanzarse con el establecimiento de políticas y reglamentos internos de ciberseguridad en

la IA que pueden elaborar las entidades vigiladas que deseen implementar la IA, estos reglamentos deben construirse por un equipo multidisciplinario que incluya no solo a programadores y desarrolladores, sino también a expertos en ética, en datos y miembros de toda disciplina que intervenga en las actividades antes vistas. Desde el ámbito regulatorio por otro lado, la Superintendencia Financiera de Colombia puede ejercer su función de supervisión exigiendo a sus vigilados la presentación de estos reglamentos para dar su visto bueno a los mismos, poniendo una especial atención a las disposiciones sobre depuración de datos de entrada, infraestructura de soporte, pruebas y ensayos, supervisión humana y cumplimiento de las normas sobre datos personales y propiedad intelectual.

## 4. Sección 3. Marco regulatorio nacional e internacional

En esta sección, analizaremos las principales normas y estándares regulatorios nacionales e internacionales que regulan o mencionan el uso de la IA por parte de las entidades financieras, con el objetivo de realizar un estudio normativo de las disposiciones que podrían influenciar el comportamiento de los actores del sistema financiero.

### 4.1 Análisis de la normativa financiera colombiana

El sistema financiero, entendido por Baena Toro et al. (2016) como el "conjunto de entes conformado por las autoridades que gobiernan, regulan y supervisan, así como las que operan los mercados del ahorro, la inversión, el crédito y los servicios auxiliares de los mismos" (p. 74) tiene como función principal la de canalizar el ahorro de la sociedad permitiendo que circule el dinero a través de la realización de diversas operaciones.

Así mismo, Cárdenas (2020) establece lo siguiente “los mercados financieros más libres crean oportunidades, competencia y crecimiento, al tiempo que facilitan el desarrollo y funcionamiento de las instituciones” (p. 269)

Es así como, en Colombia, el sistema financiero y sus actores son objeto de una regulación especial, con unos elementos, instituciones y normas particulares a la materia financiera, tanto es que la Constitución Política le encomendó al Congreso de la República de forma especial la regulación en materia financiera, bursátil, aseguradora y cualquier otra actividad de captación de recursos del público en el artículo 150, numeral 19 literal d:

> **Artículo 150.** Corresponde al Congreso hacer las leyes. Por medio de ellas ejerce las siguientes funciones:
>
> 19. Dictar las normas generales, y señalar en ellas los objetivos y criterios a los cuales debe sujetarse el Gobierno para los siguientes efectos:
>
> d) Regular las actividades financiera, bursátil, aseguradora y cualquiera otra relacionada con el manejo, aprovechamiento e inversión de los recursos captados del público;

(Constitución Política de Colombia, 1991).

Por su parte, el artículo 189, numeral 24 de la Constitución estableció en cabeza del presidente el ejercicio de la inspección, vigilancia y control sobre las actividades mencionadas previamente:

> **Artículo 189.** Corresponde al Presidente de la República como Jefe de Estado, Jefe del Gobierno y Suprema Autoridad Administrativa:
>
> 24. Ejercer, de acuerdo con la ley, la inspección, vigilancia y control sobre las personas que realicen actividades financiera, bursátil, aseguradora y cualquier otra

> relacionada con el manejo, aprovechamiento o inversión de recursos captados del público. Así mismo, sobre las entidades cooperativas y las sociedades mercantiles. (Constitución Política de Colombia, 1991)

Estos mandatos constitucionales han sido desarrollados de forma sucesiva con el paso del tiempo, desde el ámbito legislativo, hoy en día contamos con que las principales normas en materia financiera y bursátil son el Estatuto Orgánico del Sistema Financiero (en adelante "EOSF") y la Ley 964 de 2005 para el sector bursátil.

Por el lado del ejecutivo, el presidente ejerce sus funciones a través del Ministerio de Hacienda y Crédito Público (en adelante "MHCP"), que prepara las leyes y decretos en materia financiera a través de la Unidad de Regulación Financiera URF, en virtud del artículo 2 del Decreto 4712 de 2008.

Sin embargo, desde la promulgación del Decreto 4327 de 2005, se creó la Superintendencia Financiera de Colombia (en adelante "SFC") mediante la fusión de la Superintendencia Bancaria y de la Superintendencia de Valores, siguiendo la tendencia internacional de unificar a los reguladores financieros y bursátiles en un solo ente público. La SFC está adscrita al MHCP y tiene como funciones principales promover la estabilidad del sistema financiero colombiano, promover la integridad y transparencia del mercado de valores y velar por la protección de los derechos de los consumidores financieros (inversionistas, ahorradores y asegurados).

En ejercicio de sus atribuciones, la SFC ha expedido toda una variedad de circulares externas que reglamentan e instruyen a las entidades financieras vigiladas en el ejercicio de su actividad, para este trabajo, las principales normas a analizar serán la Circular Básica Jurídica (en adelante "CBJ") o Circular Externa 029 de 2014, y la Circular Básica Contable y Financiera (en adelante "CBCF") o Circular Externa 100 de 1995.

Así mismo, el principal marco regulatorio en materia financiera, que regula las operaciones autorizadas a las entidades financieras, es el Decreto 2555 de 2010 que unifica la normativa financiera en un solo cuerpo normativo. Esta norma será objeto de un especial análisis, pues uno de los objetivos de nuestro trabajo es identificar las actividades autorizadas en las cuales las entidades financieras pueden querer implementar sistemas de IA.

### *4.1.1 Responsabilidades de las entidades financieras a la luz del Estatuto Orgánico del Sistema Financiero y la Ley 964 de 2005.*

En Colombia, la ley general que regula a los actores del sistema financiero es el Decreto Ley 663 de 1993, comúnmente conocido como el Estatuto Orgánico del Sistema Financiero, en esta norma se recogen las disposiciones sobre la intervención estatal en el sistema financiero, las autoridades de inspección y vigilancia, el funcionamiento, operación y el régimen sancionatorio a que están sujetas las entidades financieras. Para efectos de facilitar el estudio, analizaremos las normas del EOSF según el tipo de entidad para precisar en cuáles de las operaciones autorizadas por la ley es más probable la adopción de un sistema de IA.

**Establecimientos Bancarios.** Los establecimientos bancarios pueden efectuar las operaciones autorizadas por el artículo 7 del EOSF, si tenemos en cuenta las capacidades analíticas de la IA y el enfoque de gestión de riesgos, las operaciones autorizadas en que es más probable que se adopte un sistema IA son las siguientes:

- La compra y venta de letras de cambio y divisas, autorizada por el literal d, ya que la IA puede realizar seguimientos y predicciones de los tipos de cambio. (Zapata & Díaz, 2008)
- El otorgamiento de créditos, autorizado por el literal e, ya que, como vimos, la IA tiene un gran potencial a la hora de realizar estudios de riesgo de crédito.

- La aceptación de letras de cambio originadas en compraventas nacionales o internacionales, debido al potencial de la IA para llevar a cabo estudios de riesgo de mercado
- Las operaciones de leasing habitacional, leasing y arrendamiento sin opción de compra, como lo autorizan los literales n y o, por el potencial de la IA para llevar a cabo estudios de riesgo de crédito.
- El otorgamiento de avales y garantías, respaldado por el literal l, utilizando la IA para el estudio de crédito del avalado.

Además, los sistemas de IA pueden utilizarse para realizar los estudios de riesgo de mercado de las inversiones autorizadas por los artículos 8 y 9 del EOSF

**Corporaciones Financieras.** Las corporaciones financieras pueden efectuar las operaciones autorizadas por el artículo 11 del EOSF, que se orienta en gran medida a la promoción de la creación, reorganización, fusión, transformación y expansión de las empresas.

En relación con esto, los sistemas de IA pueden ser útiles a las corporaciones financieras para efectuar los estudios de riesgo de crédito y de mercado de las empresas, en las operaciones que le autoriza el artículo 12 del EOSF.

Además, las corporaciones financieras pueden otorgar créditos a terceros para financiar la adquisición de acciones y bonos convertibles en acciones de las sociedades anónimas nacionales, como lo autoriza el literal d del artículo 13 del EOSF.

**Compañías de Financiamiento.** Las compañías de financiamiento pueden efectuar las operaciones autorizadas por el artículo 24 del EOSF. Muchas de las cuáles pueden relacionarse con las autorizadas a los establecimientos bancarios. Las operaciones donde pueden adoptarse sistemas de IA son:

- El otorgamiento de préstamos
- La compraventa de títulos representativos de obligaciones emitidas por entidades de derecho público, en lo cual se puede adoptar un sistema de IA para efectuar el correspondiente estudio del riesgo de mercado
- La financiación mediante la aceptación de letras de cambio, en lo cual se puede adoptar un sistema de IA para el estudio de la idoneidad de las letras recibidas
- El otorgamiento de avales y garantías
- Las operaciones de factoring
- Operaciones de compra y venta de divisas
- Operaciones de leasing

**Cooperativas Financieras.** Las cooperativas financieras pueden realizar las operaciones autorizadas por el numeral 2 del artículo 27 del EOSF, estas operaciones se circunscriben al otorgamiento de determinados créditos (ordinarios y de fomento), la adquisición o descuento de créditos hipotecarios y la adquisición de títulos representativos de obligaciones emitidos por entidades de derecho público nacionales o sociedades anónimas nacionales.

**Sociedades Fiduciarias.** Las sociedades fiduciarias, como sociedades de servicios financieros, tienen una estructura diferente a las de los establecimientos de crédito previamente analizados. Así, estas pueden adoptar la IA en la realización de las siguientes actividades:

- Los estudios de crédito y mercado de las inversiones realizadas en virtud un encargo fiduciario, como lo autoriza el literal b del numeral 1 del artículo 29 del EOSF
- La prestación de servicios de asesoría financiera, como lo autoriza el literal f del numeral 1 del artículo 29 del EOSF, en este punto la IA tiene un especial potencial gracias a su

aplicación en la asesoría financiera personalizada, como lo ha mencionado Asobancaria (2023).

- El desarrollo de operaciones de inversión y/o colocación a cualquier título de sumas de dinero en desarrollo de los contratos de fideicomiso de inversión que celebre con sus clientes.

**Sociedades Comisionistas de Bolsa.** Aunque dentro del EOSF no se encuentra un listado concreto de las operaciones autorizadas a las sociedades comisionistas de bolsa, el derecho financiero colombiano si contempla que estos, como intermediarios del mercado de valores, pueden realizar actividades de intermediación de valores siempre que estén inscritas en el Registro Nacional de Agentes del Mercado de Valores RNAMV.

Así, siguiendo al Ministerio de Hacienda y Crédito Público y a la Superintendencia Financiera de Colombia (s.f.), con base en la información consignada en la Cartilla de Información del Mercado de Valores, trae una lista de las actividades que son consideradas como intermediación en este mercado. Dentro de las cuales, las que tienen un mayor potencial para la aplicación de la IA son la asesoría profesional para la compra y venta de valores inscritos en el Registro Nacional de Valores y Emisores RNVE o de valores extranjeros listados en un sistema local de cotizaciones de valores extranjeros (p.4) y la realización de operaciones por cuenta propia.

### *4.1.2 Estudio de las operaciones autorizadas a las entidades financieras por el Decreto 2555 de 2010*

Debido a que en el apartado anterior se estudiaron las operaciones autorizadas por el EOSF, en este apartado nos enfocaremos en las actividades de las Sociedades Comisionistas de Bolsa que no fueron contempladas por el mencionado Estatuto.

Así, el artículo 3 de la Ley 964 de 2005 en su literal c consagra la actividad de intermediación del mercado de valores y estableciendo en su parágrafo que las entidades que la practiquen serán vigiladas por el Estado.

Por su parte, el Decreto 2555 de 2010 consagra un régimen de autorización general para las SCB, permitiéndoles, entre otros, la realización de los siguientes actos (artículo 2.9.2.1.1.):

- Operaciones del mercado de valores por cuenta propia
- Administración de valores y/o portafolios de terceros
- Asesoría en actividades relacionadas con el mercado de capitales
- Otorgar financiación para la adquisición de valores

Sin embargo, para los efectos de este estudio, es de especial relevancia el numeral 4 del artículo 2.9.2.1.2. y el artículo 2.9.2.1.3, que le exige a las SCB la tenencia de una adecuada infraestructura tecnológica y profesional que le permita gestionar adecuadamente las operaciones y los intereses que adelanta.

### *4.1.3 Las leyes 1266 de 2008 y 1581 de 2012 sobre el tratamiento de datos personales*

Debido a la importancia que tienen los datos para los sistemas de IA, ya que es a través de los mismos que los desarrolladores y usuarios de la IA entrenan al sistema y le imponen los parámetros de conducta esperados, es de especial relevancia conocer las disposiciones normativas sobre el tratamiento de datos personales que existen en Colombia, dándoles un enfoque dirigido a los datos que manejan las entidades financieras y que pueden ser utilizados para el entrenamiento de los sistemas de IA adoptados por las mismas.

Así, la Ley Estatutaria 1581 de 2012 dictó las disposiciones generales para el tratamiento de datos personales, creando una serie de principios, derechos y deberes tanto de los titulares de la

información como de los operadores de esta. Sin embargo, dado que existe una regulación específica al sector financiero, nuestro análisis de esta ley se limitará a conocer la definición de "dato sensible" pues identificamos que estos son los datos que deben ser evitados a la hora de entrenar una IA, ya que pueden generar los mencionados sesgos algorítmicos.

Así, según el artículo 5 de la mencionada ley, los datos sensibles son aquellos cuyo uso indebido puede generar discriminación, contándose entre ellos los referentes a la raza o etnia, orientación sexual, política o religiosa; pertenencia a asociaciones o sindicatos, datos de salud y datos biométricos. Estos datos tienen un régimen de uso restringido, ya que los operadores de la información solo pueden darles uso en los escenarios contemplados en el artículo 6 de la mencionada ley, que son:

- La autorización explicita dada por el titular, salvo que no se requiere su autorización por mandato legal.
- El tratamiento sea necesario para salvar el interés vital del titular y este se encuentra jurídica o físicamente incapacitado (no es de interés para la realización de actividades financieras, excepto en casos especialísimos que deberían ser expresamente regulados como, por ejemplo, el otorgamiento de un crédito de forma urgente para la financiación de un procedimiento vital no cubierto por el Sistema General de Salud).
- Los datos sean tratados con fines humanitarios por una entidad sin ánimo de lucro, caso en el cual se prohíbe la comercialización de estos a terceros.
- Los datos necesarios para ejercer el derecho de defensa en un proceso judicial.
- Los datos tengan una finalidad histórica, estadística o científica; caso en el cual deberán adoptarse mecanismos que supriman la identidad de los titulares.

Estas clasificaciones son útiles a nuestro objeto de estudio ya que, como se verá más adelante en la Sección 4, una recomendación dada a las entidades financieras será la exclusión de los datos sensibles del conjunto de datos utilizados para el entrenamiento de una IA.

Por otro lado, el ordenamiento jurídico colombiano cuenta con una norma especial en materia del tratamiento de la información financiera y crediticia de las personas, esta es la Ley 1266 de 2008 cuya vigilancia y control recae en la SFC en virtud del artículo 17 de la misma. Por lo tanto, merece un especial análisis en nuestro estudio.

Así, esta ley aplica cuando se de el traslado de estos datos a un tercero en virtud del inciso final del artículo 2. Dado que en el entrenamiento y uso de la IA en las actividades financieras encontramos que la fuente de la información, que es la entidad financiera, traslada los conjuntos de datos a un tercero proveedor de la tecnología para su uso con finalidades de entrenamiento y posterior uso comercial, encontramos que esta ley aplica íntegramente al manejo de datos por parte de los sistemas de IA adoptados por las entidades financieras en Colombia.

Sin embargo, cabe resaltar que, en virtud de los recientes avances en materia de finanzas abiertas, el parágrafo del numeral 1 del artículo 6 de esta ley establece que no se requiere el consentimiento previo del titular de la información en la administración de los datos financieros y crediticios, pero si la atención y cumplimiento a las normas y principios establecidos en las leyes de protección de datos personales.

Por otro lado, los artículos 19A y 19B añadidos por la Ley 2157 de 2021 establecen que los operadores de la información deben estar en capacidad de demostrar a los titulares de la información:

- La naturaleza jurídica del operador, de la fuente y del usuario, y la adopción de las obligaciones de la ley 1266 de 2008.

- La naturaleza de los datos tratados y el tipo de tratamiento.
- Los riesgos potenciales
- La existencia de una organización interna proporcional al tamaño empresarial del operador enfocada en la adopción e implementación de las políticas y principios de la ley 1266 de 2008.
- La adopción de mecanismos internos de implementación de estas normas, y de procesos para la atención a los titulares de la información.

Por lo tanto, las entidades vigiladas por la SFC que deseen adoptar un sistema de IA, aunque deben dar íntegro cumplimiento a las disposiciones colombianas sobre tratamiento de datos personales, en principio no se exponen a un riesgo legal considerable por la sola adopción del sistema de IA, incluso si trasladan los datos que serán usados con fines de entrenamiento de la nueva tecnología; siempre que se garantice que la naturaleza de los datos es exclusivamente financiera y crediticia, salvaguardando la identidad de los titulares y excluyendo del entrenamiento de la IA los datos sensibles definidos por la Ley 1581 de 2012. Esto sin excluir las obligaciones generales sobre seguridad, confidencialidad y trazabilidad de los datos.

### *4.1.4 La gestión de riesgos por parte de las entidades financieras*

Como vimos previamente, la gestión de riesgos es una actividad clave por parte de las entidades financieras que les ha valido una especial regulación por parte de las autoridades de supervisión del sistema financiero, en Colombia esto se ha visto con la implementación del Capítulo XXXI de la Circular Básica Contable y Financiera de la SFC (en adelante “SIAR”) que contiene los lineamientos mínimos para la gestión de los riesgos asociados a la actividad financiera. La

importancia de conocer esta regulación radica en la creciente implementación de los sistemas de IA por parte de las entidades financieras colombianas.

A continuación, trataremos de clasificar los riesgos inherentes a la adopción de la IA en tres categorías: riesgo de crédito, riesgo de mercado y riesgo operacional. Esto nos permitirá tener un mejor entendimiento de las medidas correctivas que deben aplicarse en cada uno de los riesgos de la IA que se estudiaron en la Sección 2.

Encontramos entonces que, en lo referente al riesgo de crédito, la IA puede:

- Adolecer de sesgos algorítmicos que impidan un correcto estudio de crédito
- Causar un sobreendeudamiento de la entidad (este riesgo es exclusivo de los casos donde una entidad financiera ha delegado totalmente en una IA la aprobación y desembolso de los créditos sin contar con mecanismos humanos de supervisión).

En lo referente al riesgo operacional, la IA puede:

- Adolecer de fallos en los modelos representados en decisiones erróneas de crédito, inversión o detección de fraudes
- Incrementar la vulnerabilidad de la entidad a los ataques cibernéticos
- Crear una dependencia excesiva de la entidad de los sistemas de IA, transfiriendo efectivamente el riesgo sistémico de la entidad financiera a la IA.
- Excederse en las funciones de captura de información, infringiendo las disposiciones de protección de datos personales y propiedad intelectual.

En lo referente al riesgo de mercado, la IA puede:

- Realizar predicciones erróneas de tendencias del mercado, ya sea del precio de los valores en el mercado de capitales o de las tasas de interés en el mercado intermediado.

- Causar volatilidad en el mercado por la rapidez con la que la IA puede tomar decisiones de inversión.

Destaca entre toda la normativa del SIAR el numeral 4.3.1.3.1., que autoriza a las entidades financieras a tercerizar sus procesos siempre que no haya delegación de la profesionalidad. Esto es especialmente relevante pues nos da el principio general que debemos tener en cuenta en toda regulación en materia de IA, que esta no debe reemplazar a los componentes humanos de la actividad financiera, pues esta es una actividad que implica una profesionalidad y una confianza del público que no deben ser menospreciados y delegados sin más a un sistema informático que muchas veces es incomprensible para el público general.

Este numeral les exige a las entidades financieras realizar un análisis de los riesgos de la tercerización, definir los criterios de selección de los terceros proveedores y la inclusión de las siguientes cláusulas en los contratos celebrados con estos:

i. Obligaciones de las partes
ii. Niveles de servicio
iii. Operación en situaciones contingentes
iv. Gestión de los riesgos operacionales que puedan afectar el cumplimiento de las obligaciones del tercero
v. Acuerdos de confidencialidad sobre la información manejada y las actividades desarrolladas

(Superintendencia Financiera de Colombia, 1995).

### *4.1.5 Disposiciones regulatorias sobre el uso de tecnologías por parte de las entidades financieras*

Teniendo esto en cuenta, analizaremos ahora las disposiciones normativas y regulatorias que conciernen a la adopción de tecnologías de IA por parte de las entidades financieras.

En primer lugar, la Ley 964 de 2005, en el numeral 2 del literal b del artículo 1 de dicha ley, se menciona:

> **Artículo 1. Objetivos y criterios de la intervención.** El Gobierno Nacional ejercerá la intervención en las actividades de manejo, aprovechamiento e inversión de recursos captados del público que se efectúen mediante valores, con sujeción a los siguientes objetivos y criterios:
>
> b) Criterios de intervención:
>
> 2. Que la regulación y la supervisión del mercado de valores *se ajusten a las innovaciones tecnológicas* y faciliten el desarrollo de nuevos productos y servicios dentro del marco establecido en la presente ley.

[cursivas añadidas] (Ley 964 de 2005)

Por su parte, los numerales 3 y 4 del artículo 17 de la Ley 1266 de 2008 establecen que:

> **Artículo 17. Función de vigilancia.** (…)
>
> 3. Velar porque los operadores y fuentes cuenten con un sistema de seguridad y con las demás condiciones técnicas suficientes para garantizar la seguridad y actualización de los registros, evitando su adulteración, pérdida, consulta o uso no autorizado conforme lo previsto en la presente ley.
>
> 4. Ordenar a cargo del operador, la fuente o usuario la realización de auditorías externas de sistemas para verificar el cumplimiento de las disposiciones de la presente ley.
>
> (Ley 1266 de 2008)

Además, el EOSF cuenta con las siguientes disposiciones:

> **Artículo 46. Objetivos de la intervención.** (…)

b. Que en el funcionamiento de tales actividades se tutelen adecuadamente los intereses de los usuarios de los servicios ofrecidos por las entidades objeto de intervención y, preferentemente, el de ahorradores, depositantes, asegurados e inversionistas.

d. Que las operaciones de las entidades objeto de la intervención se realicen en adecuadas condiciones de seguridad y transparencia. (…)

h. Que el sistema financiero tenga un marco regulatorio en el cual cada tipo de institución pueda competir con los demás bajo condiciones de equidad y equilibrio de acuerdo con la naturaleza propia de sus operaciones.

**Artículo 49. Democratización del crédito.** (…)

Además, el Gobierno Nacional podrá dictar normas con el fin de evitar que en el otorgamiento de crédito por parte de las instituciones sometidas a la inspección y vigilancia de la Superintendencia Bancaria[3] se empleen prácticas discriminatorias relacionadas con sexo, religión, filiación política y raza u otras situaciones distintas a las vinculadas directamente con el riesgo de la operación y la capacidad de pago del solicitante. (…)

**Artículo 325. Naturaleza, objetivos y funciones.** (…)

c. Supervisar las actividades que desarrollan las entidades sometidas a su control y vigilancia con el objeto de velar por la adecuada prestación del servicio financiero, esto es, que su operación se realice en condiciones de seguridad, transparencia y eficiencia.

**Artículo 326. Funciones y facultades de la Superintendencia Bancaria.** (…)

5. Facultades de prevención y sanción. (…)

[3] Téngase en cuenta que, a partir del Decreto 4327 de 2005, se fusionaron las Superintendencias Bancaria y de Valores en la Superintendencia Financiera de Colombia. En virtud del artículo 93 del mencionado decreto, todas las referencias que hagan las disposiciones legales vigentes a la Superintendencia Bancaria, a la Superintendencia Bancaria de Colombia o a la Superintendencia de Valores se entenderán efectuadas a la Superintendencia Financiera de Colombia.

a. Emitir las órdenes necesarias para que se suspendan de inmediato las prácticas ilegales, no autorizadas e inseguras y se adopten las correspondientes medidas correctivas y de saneamiento cuando la Superintendencia considere que alguna institución sometida a su vigilancia ha violado sus estatutos o alguna disposición de obligatoria observancia, o esté manejando sus negocios en formas no autorizada o insegura. (…)

(Decreto Ley 663 de 1993)

De estas disposiciones, podemos entonces extraer que, aunque las entidades financieras están autorizadas para adoptar toda clase de nuevas tecnologías, se encuentran sometidas a la vigilancia de la SFC que, como organismo encargado de la estabilidad y solidez del sistema financiero colombiano, ejercerá sus facultades de supervisión y sanción si considera que una tecnología es violatoria de alguna norma financiera, haciendo un especial énfasis en la protección de los consumidores financieros.

Precisando aún más, aunque no existe una norma colombiana que regule de forma concreta la adopción de sistemas de IA por parte de las entidades financieras, si existe una autorización general a adoptar esta tecnología, esto lo encontramos en la Circular Básica Jurídica de la SFC, en el numeral 1.3 del Capítulo 1, Título 2, Parte 1 de la mencionada circular, denominado “Canales, medios, seguridad y calidad en el manejo de información en la prestación de servicios financieros”:

**Numeral 1.3.** (…)

Las entidades vigiladas pueden adoptar tecnologías como realidad aumentada, internet de las cosas, blockchain, inteligencia artificial, machine learning, big data, robots, entre otras, cuando lo consideren pertinente para mejorar la prestación de servicios a los consumidores financieros y optimizar sus procesos. Para el efecto, la entidad debe realizar una adecuada gestión de los riesgos

asociados a la tecnología adoptada, verificar de manera regular la efectividad de los controles implementados y dar cumplimiento a las normas vigentes en materia de protección de datos y habeas data.

(Superintendencia Financiera de Colombia, 2021a)

Esta norma de la CBJ será entonces nuestro marco para el posterior estudio y diseño de medidas de mitigación de riesgos en la adopción de la IA por parte de las entidades financieras, ya que contiene todos los elementos esenciales que debe tener una Política de Uso de IA y, aún más importante, nos dice qué elementos son considerados como importantes por la SFC en la adopción de las nuevas tecnologías, a saber, una política de IA debe contener:

- Plan de gestión de riesgos
- Existencia de controles y verificación de estos
- Énfasis en el cumplimiento de las disposiciones de tratamiento de datos personales.

### *4.1.6 Normas y estándares colombianos sobre el uso de la Inteligencia Artificial*

Aunque no existan disposiciones legales que traten expresamente el tema de la Inteligencia Artificial, el Estado colombiano no ha descuidado la necesidad de tener unos marcos regulatorios claros que permitan a las entidades mitigar los riesgos asociados a la adopción de la IA. En este apartado estudiaremos en concreto dos documentos expedidos por el Gobierno Nacional, que comparten entre sí que fueron expedidos por el Ejecutivo y que funcionan como instrumentos de soft law; estos documentos son el Marco Ético para la Inteligencia Artificial en Colombia, del Departamento Administrativo de la Presidencia y el Documento CONPES 4144 de 2025 que contiene la Política Nacional de Inteligencia Artificial.

**Marco Ético para la Inteligencia Artificial en Colombia.** Este documento, construido por el Departamento Administrativo de la Presidencia de la República, contiene en esencia 3 secciones que estudiaremos: una introducción donde destaca una serie de recomendaciones cuando se intenta regular la IA, un listado de principios a seguir en la adopción de la IA, y un listado de mecanismos para hacer efectivos estos principios.

El Marco Ético comienza reconociendo la creciente importancia de la IA en la economía global, declarado desde el inicio que la IA puede generar una exposición a escenarios desagradables como desinformación, sesgos, discriminación, inseguridad y afectaciones a la privacidad. Si bien el Marco Ético es una recomendación (no vinculante) dirigida a las entidades públicas, más adelante el DAPR aclara que los privados son bienvenidos a adoptar las recomendaciones de este.

Prosigue el documento destacando la importancia de que el Marco Ético se construya teniendo en cuenta los siguientes factores:

- Enfoque basado en riesgos
- Ciberseguridad como elemento fundamental
- Importancia de que el Marco Ético sea adoptado como buenas prácticas y no como norma taxativa
- Énfasis en la seguridad de los datos
- Control humano proporcional al nivel del riesgo

El Marco Ético continúa enlistando una serie de principios relevantes a la hora de regular la IA, para los efectos de nuestro estudio, los principios relevantes son:

1. Principio de Transparencia: la entidad que adopta la IA debe ser capaz de demostrar, de forma fiable, el cumplimiento normativo en el diseño, funcionamiento e impacto de la IA. Este principio abarca temas como la fuente y uso de los datos personales, el procedimiento

a seguir con inteligencias artificiales demasiado complejas que escapan a la comprensión de sus desarrolladores, la protección de la confidencialidad, la repartición clara de funciones desde el gobierno corporativo y la información a los usuarios.

2. Principio de Privacidad: la adopción de una IA debe estar precedida por el respeto a la esfera privada de las personas, esto quiere decir, debe haber autorización expresa al uso de los datos personales, debe limitarse la información entregada a los algoritmos a la necesaria sin incluir aspectos privados de la persona y deben existir procedimientos internos que aseguren la gestión del riesgo de privacidad.
3. Principio de Control Humano: aplicable a las IA autónomas, exige un nivel de control humano que sea proporcional al nivel de riesgo de la IA, en particular, en el control de las decisiones que toma una IA de cara al público general.
4. Principio de Seguridad: mediante el aseguramiento de los datos personales, la IA no debe afectar la salud física y mental de los seres humanos, monitoreando los riesgos de ciberseguridad y rendimiento y mitigando los sesgos que se identifiquen en el actuar de la IA.
5. Principio de Responsabilidad: los resultados dañinos que sean producto de una IA deben ser reparados; para tal efecto se presume la solidaridad de todos los participantes de la "cadena algorítmica" (diseñadores, desarrolladores y usuarios institucionales) desvirtuable solo mediante la prueba de una mayor negligencia de uno de los participantes.
6. Principio de No Discriminación: establece que las IA no deben considerar asuntos personales de los ciudadanos como el sexo, la raza, la religión, la edad, la procedencia, discapacidades, etc. Esto se mitiga a través de la depuración de los datos entregados a la IA.

El Marco Ético finaliza proponiendo una serie de mecanismos para asegurar la implementación de estos principios, destacando la depuración constante de los datos por parte de los seres humanos, la revisión periódica de los algoritmos, de su rendimiento y sus respuestas; y el análisis constante del impacto a la privacidad que causa la IA.

**Documento CONPES 4144 de 2025.** Teniendo en cuenta la gran importancia de la IA como una tecnología revolucionaria, el Gobierno Nacional decidió ajustar las políticas públicas sobre la materia y publicar el Documento CONPES 4144 de 2025 o Política Nacional de Inteligencia Artificial, en este CONPES el Gobierno estudió los antecedentes normativos en la materia y realizó un diagnóstico general de los problemas que tiene la IA en Colombia, para luego realizar una serie de recomendaciones de política pública. En este apartado analizaremos solo los puntos más relevantes al sector privado y a las particularidades del sistema financiero.

En la sección de antecedentes, el Gobierno trajo a colación el CONPES 3975 de 2019 que en su momento fue la política de transformación digital, vigente hasta 2022. Resaltó otros logros como la Hoja de Ruta para el Desarrollo y Aplicación de la IA en Colombia del Ministerio de las TIC y la misión de expertos que visitó Colombia entre el 2021 y el 2022, traída por el Departamento Nacional de Planeación.

En materia de ética y gobernanza, Colombia adoptó en 2019 las Recomendaciones OCDE sobre IA. En 2021 hizo lo mismo con las Recomendaciones de la UNESCO y también adoptó el Marco Ético que estudiamos con anterioridad, sin embargo, entre los diagnósticos se destaca la falta de un órgano central de gobernanza en materia de IA.

Sobre otros asuntos como la disponibilidad de datos de calidad para la IA, el Gobierno cita las leyes que regulan el tema de los datos abiertos y aclara que el Ministerio de las TIC mantiene una

vigilancia sobre este tema. En materia de riesgos y efectos no deseados de la IA, se reconoce que en Colombia no existen políticas o normas que traten el tema, pero se aclara que el Gobierno es consciente de que los riesgos de la IA están entre las principales preocupaciones de la economía global, al punto que el FMI lo coloca como la sexta principal preocupación en su Informe de Riesgos que estudiaremos más adelante. Finalmente, el Gobierno se pronuncia sobre la necesidad de generar seguridad y confianza, asegurar la protección de la propiedad intelectual y los datos personales y la necesidad de promover la adopción de la IA en todos los sectores.

En la sección de diagnóstico, el Gobierno identificó, entre otras, las siguientes problemáticas relacionadas al uso de la IA:

- Debilidades en la gobernanza y los principios éticos
- Poca infraestructura tecnológica que soporte a la IA
- Poca disponibilidad de datos de calidad
- Bajo nivel de adopción de la IA en el marco empresarial
- Alta vulneración de derechos, como la privacidad, la propiedad intelectual y los datos personales

Para solucionar estas problemáticas, el Gobierno propone en el CONPES 4144 una serie de acciones de política pública que listo a continuación:

1. La creación de un instrumento normativo que regule el tema de la gobernanza de la IA.
2. El mejoramiento del ecosistema de datos abiertos a través de la colaboración entre varias entidades públicas, que permita una mayor depuración, movilidad, protección y confianza en los datos existentes.
3. Actualizar el Modelo Nacional de Seguridad Digital a las nuevas tecnologías, este documento contendrá las capacidades mínimas de seguridad que permitan una adecuada

identificación, gestión, tratamiento y mitigación de los riesgos asociados a la IA y será especialmente dirigido al sector privado (Consejo Nacional de Política Económica y Social et al., 2025).

4. Monitoreo constante de las posibles vulneraciones a la propiedad intelectual por parte de sistemas de IA
5. La promoción de la adopción de la IA en el sector privado, a través del Ministerio de Comercio, Industria y Turismo.

Como podemos ver, a pesar de que este documento CONPES no trata específicamente el tema de la adopción de la IA por parte de las entidades financieras, si nos deja claro que el Gobierno no ha dejado pasar el tema de los riesgos asociados a la IA y que las entidades públicas están comenzando a movilizarse para regular esta nueva tecnología, si bien en el CONPES no hay instrucciones precisas dirigidas al MHCP o a la SFC, si nos permite predecir en dónde iniciarán las regulaciones estatales sobre esta nueva tecnología y cuáles son las tendencias del Gobierno, esta información será usada más adelante en la Sección 4 cuando se elabore una propuesta de regulación usando un modelo de buenas prácticas empresariales, más que una regulación taxativa que pueda frenar el desarrollo y adopción de la IA en Colombia.

### *4.1.7 La Circular Externa 002 del 21 de agosto de 2024 de la Superintendencia de Industria y Comercio y sus posibles efectos sobre las entidades del sistema financiero*

Debido al auge de los sistemas de IA y su adopción por parte de las empresas administradoras de datos personales, la Superintendencia de Industria y Comercio (en adelante “SIC”) expidió los Lineamientos sobre el Tratamiento de Datos Personales en Sistemas de Inteligencia Artificial dirigido a los sujetos vigilados por la SIC en su rol de Autoridad de Protección de Datos Personales.

Cabe aclarar que el artículo 17 de la Ley 1266 de 2008 estableció que, cuando la fuente, usuario u operador de los datos personales sea una entidad vigilada por la SFC, será esta Superintendencia y no la SIC la encargada de ejercer las facultades propias de la Ley 1266 de 2008, por lo cual, en principio, esta Circular de la SIC no atañe a nuestro objeto de estudio, que es la regulación financiera colombiana, sin embargo, no podemos descartar los pronunciamientos que sobre la materia han hecho otras autoridades administrativas, ya que estos pronunciamientos nos permiten discernir de qué manera los funcionarios públicos están entendiendo y regulando los sistemas de IA.

Así, a continuación, estudiaremos paso a paso los razonamientos y recomendaciones realizados por la SIC en esta Circular, teniendo presente que nuestro objetivo es extraer de la misma los principios generales de la regulación en materia de IA.

En primer lugar, la Circular reconoce la importancia económica que han adquirido los sistemas de IA, y declara que su propósito es el de brindar seguridad tanto a los administradores de los datos como a los titulares de estos mediante el establecimiento de unas políticas claras en la materia.

Continua la Circular estableciendo que las leyes 1266 de 2008 y 1581 de 2012 son "tecnológicamente neutrales", es decir, que sus postulados se aplican en toda operación y proceso de tratamiento de datos personales sin importar la clase de tecnología o entidad que esté utilizando los datos, incluyendo entonces a los sistemas de IA dentro del objeto de la norma.

Por lo tanto, la responsabilidad más importante de los destinatarios de estas normas es la prueba del principio de responsabilidad demostrada, establecido en el artículo 19A de la ley 1266 de 2008, que requiere que los administradores de datos personales demuestren la adopción de medidas útiles, oportunas, eficientes y demostrables de cumplimiento de la regulación en materia de datos personales.

Así, la SIC recomienda a sus vigilados la adopción del modelo de Privacidad desde el Diseño y por Defecto, a través de la técnica matemática de la privacidad diferencial, esto es, que se aplique un conjunto de técnicas matemáticas que permitan hacer analítica de datos sin revelar información sobre las personas que los proporcionaron. Esto quiere decir que al momento de seleccionar los datos de entrada (input) de entrenamiento de una IA, deben aplicarse técnicas que impidan la identificación del titular de los datos, en concordancia los principios de confidencialidad del artículo 4 literal f de la Ley 1266 de 2008 y artículo 4 literal h de la Ley 1581 de 2012.

Adicionalmente, la SIC establece que la identificación y clasificación de los riesgos; y la adopción de medidas de mitigación, son **elementos esenciales** del principio de responsabilidad demostrada; y que, dentro de la etapa de identificación, y previo al desarrollo de la IA, el administrador de datos personales debe realizar un estudio de impacto a la privacidad, que contenga como mínimo:

- Una descripción detallada de las operaciones de tratamiento de datos personales
- Una identificación y clasificación de los riesgos específicos para los derechos y libertades de los titulares de los datos
- Un listado de las medidas previstas para evitar la materialización de dichos riesgos, a través del diseño de software, medidas de seguridad, mecanismos de protección, etc.

Prosigue la SIC enfatizando que el artículo 4 literal d de la Ley 1581 de 2012 prohíbe el uso de datos parciales, incompletos, fraccionados o que conduzcan al error; y en que deben evitarse, a través de la adopción de medidas tecnológicas, humanas o de cualquier otra índole, los siguientes escenarios:

- Acceso indebido o no autorizado de datos personales
- Manipulación, destrucción, uso indebido o no autorizado de la información
- Circulación o suministro de la información a personas no autorizadas

Finalmente, la SIC diferencia entre los conceptos de dato accesible al público y dato de naturaleza pública, estableciendo un limitante a la captura de datos personales que resulta especialmente relevante a nuestro estudio ya que, como se mencionó previamente, una de las fuentes de las cuáles la IA extrae sus datos de entrada es el internet.

Así, la SIC establece que:

> El hecho de que los datos estén disponibles en internet no significa que cualquier persona puede tratarlos sin autorización previa, expresa e informada del Titular del Dato. De esta manera, los Administradores de Datos personales que recolecten Datos personales privados, semiprivados o sensibles en internet no están legitimados para apropiarse de dicha información y tratarla para cualquier finalidad que consideren apropiado sin la autorización previa, expresa e informada del Titular de la información.
>
> (Superintendencia de Industria y Comercio, 2024, p. 7)

Para concluir, vemos como resulta de vital importancia conocer las normas sobre la adopción de la IA, incluso las que no guardan una relación directa con el Derecho Financiero, pues ello nos permite dilucidar las tendencias regulatorias que están construyendo la regulación sobre la IA en Colombia. Aunque las instrucciones de la SIC se enfocan en la protección de datos personales y la privacidad, su análisis nos permite anticipar los posibles pronunciamientos de la SFC y dotar de este modo a las entidades financieras de una hoja de ruta que les permita adoptar las medidas de mitigación necesarias para protegerse del riesgo por uso indebido de datos personales e infracción de la privacidad.

### 4.2 Análisis de la normativa internacional

En este apartado, estudiaremos los pronunciamientos internacionales en materia de la adopción de la IA, emitidos tanto por las naciones u organismos multilaterales que ostentan el liderazgo en materia de IA como los Estados Unidos y la Unión Europea, como por las organizaciones internacionales que tienen por objeto la creación de estándares y recomendaciones de política pública en materia económica y financiera, como la OCDE y el FMI.

### *4.2.1 Recomendaciones de la OCDE sobre las tendencias regulatorias en materia de IA*

La Organización para la Cooperación y el Desarrollo Económico OCDE publicó en 2019 su Recomendación sobre la Inteligencia Artificial, donde consagra cinco principios claves que deben tenerse en cuenta en materia de regulación de la IA, dicha Recomendación fue adoptada por Colombia como bien lo enuncia el Documento CONPES 4144 de 2025 previamente analizado, es por ello por lo que el análisis y comprensión de estos principios es relevante a la hora de estudiar las tendencias regulatorias.

**Principio 1. Crecimiento Inclusivo, Desarrollo Sostenible y Bienestar.** Este principio establece que las partes interesadas[4] deben asegurar a través de sus mecanismos de administración el direccionamiento de la IA para que esta sea provechosa para el ser humano. Este principio enmarca además la necesidad de asegurar la reducción de las desigualdades económicas y sociales.

**Principio 2. Respeto del Estado de derecho.** Este principio, dirigido a los actores de la IA[5], busca asegurar que estos integren en el ciclo de vida de los sistemas de IA valores como la no

[4] Definido por la OCDE como "todas las entidades y personas que participan o se ven afectadas directa o indirectamente por los sistemas de IA." (OCDE, 2019, p. 4)
[5] Definido por la OCDE como "aquellos que desempeñan un papel activo en el ciclo de vida del sistema de IA, como las entidades y personas que despliegan y explotan la IA." (OCDE, 2019, p.4)

discriminación, la autonomía de las personas, la privacidad y protección de datos personales y el abordaje de la desinformación amplificada por la IA. El principio enuncia como fundamental la existencia de un mecanismo de intervención y supervisión humana en todas las fases del ciclo de vida de la IA que tenga por objetivo principal la identificación y el manejo de los riesgos inherentes a estos sistemas.

**Principio 3. Transparencia y Explicabilidad.** Según este principio, los actores de la IA deben ser capaces de suministrar información veraz y suficiente que permita una comprensión general de los sistemas de IA, esta información debería incluir entonces las fuentes de los datos de entrada, los procesos que subyacen a las predicciones de la IA y las recomendaciones o decisiones de esta, de tal forma que se permita a los afectados por una IA (tanto positiva como negativamente) conocer el porqué de sus resultados.

**Principio 4. Solidez, Seguridad y Protección.** Este principio está relacionado principalmente con la seguridad cibernética y el rendimiento del sistema de IA, así, sin importar la forma en que se utilicen, no deben plantear un riesgo excesivo a la seguridad, privacidad y protección de los seres humanos.

Este principio se materializa con la existencia de mecanismos que permitan la interrupción, corrección, desmantelamiento o reparación de los daños causados por un sistema de IA.

**Principio 5. Responsabilidad.** Este principio, dirigido a los actores de la IA, establece que estos son responsables por el funcionamiento de la IA en las actividades en las que se implemente de acuerdo con sus funciones.

Esto significa que los actores deben poder demostrar la trazabilidad de elementos como los datos, los procesos y decisiones de la IA, la existencia de un esquema de gestión de riesgos y la adopción

de políticas corporativas de debida diligencia en materia de riesgos relacionados con sistemas de IA, incluyendo el riesgo de sesgo algorítmico.

Estos principios comprenden entonces el marco ético general que las regulaciones de los países miembros de la OCDE que hayan adoptado la mencionada Recomendación deben seguir. Por lo tanto, dado que Colombia ha manifestado expresamente su adopción y ha iniciado recientemente su nueva Política Nacional de Inteligencia Artificial (CONPES 4144 de 2025), para un estudio de riesgo legal futuro como este es de vital importancia el conocimiento de estos.

### *4.2.2 Pronunciamientos del FMI sobre la adopción de la IA en el mercado financiero*

En octubre de 2024 el Fondo Monetario Internacional (en adelante "FMI") publicó su Reporte Global de Estabilidad Financiera, este es un documento mediante el cual el FMI busca analizar los riesgos a los que está expuesto el sistema financiero global con el objetivo de identificar las políticas públicas que deberían implementarse para prevenir posibles crisis financieras.

En este reporte, el Capítulo 3 se dedicó especialmente a los efectos de la aplicación de la IA en el mercado de capitales (desintermediado), sin embargo, como veremos más adelante, varias de las recomendaciones del FMI también son aplicables al mercado intermediado.

El Reporte del FMI resalta los usos más comunes dados a la IA en el mercado de capitales, como el monitoreo y reporte de riesgos, la rapidez en la toma de decisiones de inversión y la mayor efectividad en la asignación de los recursos; estas ventajas se resumen en el incremento de la eficiencia de los mercados principales, que es vista por el FMI como el principal avance que la IA puede ofrecer al sistema financiero.

Sin embargo, el FMI también identifica los riesgos implícitos de esta nueva tecnología, siendo los más importantes el incremento en la opacidad del mercado (es decir, que existe un mayor grado de dificultad para entender las operaciones y las tendencias del mismo), mayor dificultad en la supervisión de las actividades del mercado de capitales, mayor vulnerabilidad a los ataques cibernéticos y riesgo de experimentar dependencia excesiva de una entidad financiera con un único proveedor de tecnología.

Para la mitigación de estos riesgos, el FMI propone que los reguladores exijan a sus vigilados lo siguiente:

- El mapeo constante de las interdependencias entre los datos, los modelos, la infraestructura y los usos dados a las respuestas de los sistemas de IA utilizados.
- El mapeo constante de las relaciones con los proveedores de servicios de IA que sean críticos para el funcionamiento de la entidad, así como de la infraestructura esencial que soporta dichos sistemas.

Además, como buenas prácticas, se sugiere a las entidades financieras que adopten la IA contar con un sistema que limite el monto de dinero operable de forma directa por una IA sin supervisión humana, y se recomienda la creación de mecanismos que permitan la interrupción de la IA y aseguren la resiliencia de las áreas afectadas, es decir, que la entidad debe ser capaz de prestar sus servicios incluso sin el uso de sus sistemas de IA.

### *4.2.3 El Reglamento 2024/1689 de la Unión Europea sobre el uso de la IA*

El 13 de junio de 2024, la Unión Europea a través de su Parlamento estableció el Reglamento de Inteligencia Artificial aplicable a todos los estados miembros de la UE. Este Reglamento busca garantizar que los sistemas de IA cumplan con una serie de requisitos que permitan garantizar la

supervisión humana de los sistemas, la solidez técnica y seguridad de estos, la gestión de la privacidad y los datos y la transparencia de los sistemas de IA, entre otros fines. Este Reglamento ha sido reconocido por su intención humanista y se ha dicho que puede llegar a motivar otras normas similares en otros países (Asobancaria, 2024b)

Con base en el numeral (5)(b) del Anexo III de este Reglamento, las IA utilizadas para evaluar el riesgo de crédito son consideradas IA de alto riesgo, con excepción de si son utilizadas para detectar fraudes. Con el objeto de abarcar todos los escenarios posibles, analizaremos las disposiciones referentes a la IA de alto riesgo, aunque no todas las IA adoptadas por las entidades financieras sean de alto riesgo, ya que evaluando los requisitos más estrictos abarcaremos también los más simples.

Hay que tener en cuenta que las IA que evalúan los indicadores de fortaleza patrimonial de las entidades financieras no fueron consideradas como IA de alto riesgo y, por lo tanto, en este apartado no veremos referencias al control del riesgo de liquidez.

El Reglamento también define a los proveedores de IA como:

> Una persona física o jurídica, autoridad, órgano u organismo que desarrolle un sistema de IA o un modelo de IA de uso general o para el que se desarrolle un sistema de IA o un modelo de IA de uso general y lo introduzca en el mercado o ponga en servicio el sistema de IA con su propio nombre y marca, previo pago o gratuitamente.
>
> (Unión Europea, 2024, p. 46).

Entonces, las IA de alto riesgo, según el artículo 9, deben contar con un sistema de gestión de los riesgos asociados a la misma, que permita una adecuada identificación, evaluación, mitigación y tratamiento de estos, precisando que el deber de controlar los riesgos se limita con la evitabilidad y previsibilidad de estos.

Así, estas IA deben ser constantemente sometidas a pruebas (artículo 9 numeral 6) que deben determinar las medidas de mitigación de riesgos más adecuadas, y que certifiquen que los sistemas de IA funcionan de acuerdo con las normas y estándares impuestos por la organización o por la autoridad. Así mismo, debe existir un marco de gobernanza de los datos que son utilizados por la IA, que ponga especial énfasis en la depuración de estos y en el cumplimiento de las normas europeas sobre uso y tratamiento de los datos personales.

Sin embargo, previo a la puesta en funcionamiento del sistema, debe demostrarse que el proveedor de la IA realizó todas las evaluaciones de idoneidad, seguridad y gestión de riesgos, incluyendo una evaluación del posible impacto de la IA a los derechos fundamentales cuando el proveedor sea una autoridad o preste un servicio de interés público. Estos estudios deben custodiarse como documentación técnica y ser almacenados por el proveedor en desarrollo de un deber de conservación de documentos.

Además, el Reglamento es especialmente enfático en la necesidad de que exista una supervisión humana a lo largo de todo el proceso de adopción de la IA, especialmente si la IA es de alto riesgo, pues los humanos deben intervenir de forma directamente proporcional al nivel del riesgo y al grado de autonomía de la IA. Así, una IA destinada a redactar documentos internos no requerirá el mismo nivel de supervisión que una IA que redacte comunicados al público o a los inversionistas, que a su vez no requerirá tanta supervisión como una IA encargada de realizar el scoring de crédito de los clientes de la entidad financiera.

Por otro lado, en el marco de la ciberseguridad, el Reglamento establece el deber de evitar el envenenamiento de datos, los defectos del modelo de IA y los sesgos previos incrustados en el modelo.

Todos estos deberes impuestos por la UE a quienes deseen adoptar sistemas de IA de alto riesgo se traducen en una responsabilidad de los proveedores respecto a las actuaciones de la IA, sin embargo, los proveedores pueden demostrar la existencia de un Sistema de Gestión de Calidad que audite toda la cadena de la IA (artículo 17), desde el desarrollo inicial hasta el lanzamiento comercial, serán los órganos encargados de este sistema los que tengan la custodia de los documentos técnicos.

Además, establece una norma interesante en materia de responsabilidad, pues, aunque en principio se presume la solidaridad de todos los intervinientes en la cadena de la IA, especialmente en las IA complejas, establece que si uno de los intervinientes modifica de forma no autorizada la IA y dicha modificación produjo el resultado indeseado, se exime de responsabilidad al resto de los intervinientes.

Por parte de las autoridades competentes, el Reglamento las autoriza para solicitar a los proveedores la documentación técnica para verificar el cumplimiento de las regulaciones en materia de IA y sancionar a quienes incumplan con las disposiciones reglamentarias. Además, el Reglamento contempla la posibilidad de certificar determinados modelos de IA, incluso con el sello “CE”, que demuestren el cumplimiento de todas las disposiciones del Reglamento.

### *4.2.4 Reglamentación en los Estados Unidos*

Los Estados Unidos ostentan la posición dominante en el mercado global de la IA (Del Pozo & Rojas, 2025), con la IA teniendo un impacto equivalente al 14,5% del PIB de Norteamérica a 2017 (PricewaterhouseCoopers, s.f.). Estas cifras explican  por qué el Gobierno de los Estados Unidos ha sido cuidadoso en la regulación de esta nueva tecnología, ya que le representa una posición de dominio global y no desea perderla debido a la adopción de una regulación rígida, así, es de

importancia conocer los mecanismos de soft law que han regulado la IA en el Derecho estadounidense para conocer cuál es el tipo de normas que han permitido el crecimiento de la IA hasta alcanzar los niveles e importancia mencionados, en este apartado estudiaremos: la Orden Ejecutiva 14110 de la Administración Biden, el Marco de Gestión de Riesgos de IA (AI RMF 1.0) de la NIST y el Informe de la Cámara de Representantes con propuestas regulatorias sobre el tema.

**La Orden Ejecutiva 14110 y su derogatoria.** El 30 de octubre de 2023, el entonces presidente Joe Biden emitió la OE 14110 que buscaba el Uso y Desarrollo Seguro y Confiable de la Inteligencia Artificial en los Estados Unidos.

Dicha Orden Ejecutiva establecía todo un listado de evaluaciones, órdenes, guías y prácticas (Hunton Andrews Kurth LLP., 2025) que guiaban el actuar del Gobierno Federal de los Estados Unidos en materia de Inteligencia Artificial, los puntos más relevantes eran los siguientes:

- La Orden reconocía la importancia de la IA en el entorno económico actual, haciendo un especial énfasis en la utilización de la IA en los servicios financieros en la Sección 2 (e).
- Se emitían órdenes a varias agencias federales de los Estados Unidos para que realizaran estudios detallados de los riesgos asociados a la adopción de la IA. Incluso llegó al punto de solicitar a los particulares que entregaran la información recopilada hasta el momento sobre las vulnerabilidades y fallas de sus sistemas de IA.
- Ordenó al NIST (Instituto Nacional de Estándares y Tecnología por sus siglas en inglés) para que estableciera un nuevo marco de guías y buenas prácticas en la evaluación de los modelos de IA.

- Hizo un especial énfasis en la protección de la privacidad y el uso de los datos personales, en la creación de medidas contra la discriminación y la protección de los derechos de los consumidores.

A pesar de estas y otras innovaciones en la materia, esta Orden Ejecutiva, al ser una política bandera de la pasada administración Biden, fue revocada por el presidente Trump el pasado 20 de enero de 2025, con el objetivo declarado de eliminar barreras al desarrollo de la IA y asegurar el dominio estadounidense sobre el mercado global de la IA.

**Los Pronunciamientos del NIST.** El Instituto Nacional de Estándares y Tecnología NIST ha desarrollado un Marco de Gestión de Riesgos de la IA (AI RMF) que busca brindar a las organizaciones un insumo en la identificación, evaluación y manejo de los riesgos asociados al uso de la IA.

En este trabajo, nos enfocaremos en la sección 2 del AI RMF, estándar que publicó NIST en enero de 2023, debido a que esta sección contiene los elementos esenciales con que debe contar todo sistema de gestión de riesgos de la IA.

Así, encontramos que todo sistema de gestión de riesgos debe contener los siguientes elementos:

- Gobernanza: la entidad debe contar con códigos, procesos y personas responsables del uso de la IA, que aseguren la participación multidisciplinaria en todas las etapas del proceso de adopción de la IA. Este componente se satisface a través de prácticas de buen gobierno corporativo.
- Mapeo: la entidad debe contar con un mapa de riesgos asociados a la IA, que le permita establecer prioridades en la gestión de riesgos.

- Medición: la entidad debe contar con herramientas que permitan una correcta estimación del impacto que tendría la materialización de los riesgos identificados.
- Manejo: la entidad debe contar con un plan de mitigación, recuperación y comunicación en caso de materializarse uno o varios de los riesgos.

Estas recomendaciones, recogidas en el AI RMF 1.0 de enero de 2023, tiene por objetivo estandarizar la estructura de los modelos de gestión de riesgos asociados a la IA en los Estados Unidos y representa un insumo clave para nuestra propia propuesta de manejo de riesgo que enunciaremos más adelante en la Sección 4.

**El Informe de la Cámara de Representantes sobre el uso de la IA.** Atendiendo al estado de la regulación estadounidense en la materia y a la importancia estratégica de la IA, la Cámara de Representantes de los Estados Unidos recibió un informe con propuestas de regulación para asegurar la continuidad de la preeminencia de los Estados Unidos en el mercado global de la IA. Este informe trató de forma específica el uso de la IA en los servicios financieros, por lo que enfocaremos nuestro análisis en esta sección del mismo.

Así, los investigadores encontraron que la IA tiene el potencial de transformar las finanzas gracias a sus capacidades de analítica de datos, y que es por este potencial transformador que debe existir una regulación que promueva el desarrollo de la IA, proteja a los consumidores y asegure la estabilidad del sistema financiero.

El informe encontró tres escenarios desagradables en la adopción de la IA por parte de las entidades financieras:

- Debe asegurarse la calidad, seguridad y privacidad de los datos recolectados y utilizados en el entrenamiento de la IA, además,

- Debe asegurarse que la IA no se utiliza para vulnerar derechos de propiedad intelectual, como, por ejemplo, que sea utilizada para adquirir de forma ilegítima datos o secretos comerciales de la competencia.
- Si los datos de entrenamiento de la IA son incompletos o sesgados, puede generarse un sesgo difícil de detectar, que se retroalimenta a sí mismo, y que tiene un potencial de causar un daño permanente a la estabilidad y confianza en el sistema financiero, especialmente si los resultados de una IA son utilizados para tomar decisiones financieras (Congreso de los Estados Unidos, 2024).

El Informe sin embargo encontró que estos escenarios perjudiciales pueden reducirse con transparencia en el desarrollo y uso de la IA, y asegurando la diversidad de los equipos encargados de la ingeniería, el desarrollo y el testeo de la IA.

Asimismo, los actores del mercado financiero deben ser capaces de explicar los usos, limitaciones y correcciones realizadas a sus modelos de IA (recuérdese el principio de transparencia del Marco Ético colombiano); y deben asegurar la supervisión de un ser humano sobre las decisiones que toman los sistemas de IA.

Así, la IA es una tecnología con un gran potencial por sus múltiples aplicaciones por parte de las entidades financieras, entre estas se destacan el análisis rápido de la información del mercado, la detección del fraude y la asistencia personalizada; sin embargo, estas aplicaciones no deben distraernos del hecho de que la IA aun requiere de una supervisión humana constante de sus actuaciones que permita evitar la materialización de los escenarios desagradables, como bien lo resume el Congreso de los Estados Unidos (2024):

> Las entidades financieras deben evaluar constantemente la eficacia de la implementación de la IA y garantizar que estos añaden valor a sus planes de gestión de

> riesgos, especialmente a la luz del aumento de los ataques y el fraude posibilitados por la IA. (…)
>
> (p. 233. Traducido con deepl.com)

### *4.2.5 Conclusiones sobre normativa financiera internacional*

En este apartado analizamos tanto las tendencias en instrumentos de soft law como las tendencias regulatorias de jurisdicciones fuertes como los Estados Unidos y la Unión Europea. Encontramos entonces que la reglamentación europea representa el mayor intento realizado por cualquier jurisdicción de regular la IA, consagrando un gran número de definiciones y dejando claro que hay funciones que no podrán ser reemplazadas por la IA (Asobancaria, 2024c, p.199)

Por otro lado, regulaciones o propuestas más dirigidas al tema financiero y que pueden calificarse como "específicas al sector financiero" son los hallazgos del FMI en su Reporte y los hallazgos del Informe a la Cámara de Representantes de los Estados Unidos, que muy probablemente derivará en una nueva regulación en el país norteamericano y que nos permiten adecuar el lenguaje utilizado por todos los actores a la regulación financiera.

Finalmente, las propuestas de la OCDE y la reglamentación europea tienen un enfoque más humanístico y global de la IA, buscando más garantizar el respeto por los derechos humanos y de los consumidores que contar con una regulación enfocada en la estabilidad financiera.

## 5. Sección 4. Estándares mínimos que deben seguir las entidades financieras en la adopción de sistemas de IA. Una propuesta a la luz de las tendencias normativas nacionales e internacionales

En esta Sección, utilizaremos los insumos obtenidos y, con base en las tendencias regulatorias y en las características de la normativa financiera, elaboraremos una serie de propuestas que permitan a las entidades financieras identificar y mitigar los riesgos que genera la adopción de un sistema de IA.

Como ya se ha mencionado, la naturaleza misma tanto del sector financiero como de la materia a regular hacen que una regulación taxativa y rígida no sea deseable, puesto que la velocidad a la que se introducen los cambios en la tecnología no corresponde con la velocidad a la que se puede modificar la norma, en otras palabras, los procedimientos tradicionales no responden a las necesidades de seguridad jurídica que tienen las entidades financieras y, en una tecnología emergente que ha probado ser tan vital como la IA, las regulaciones taxativas pueden ser demasiado rígidas y terminar sofocando el avance tecnológico o la adopción de estos sistemas; es por ello que las propuestas que se elaborarán más adelante tienen vocación de soft law, es decir, buscan ser propuestas de buenas prácticas corporativas que preparen a las entidades financieras ante futuros cambios normativos mientras son lo suficientemente flexibles como para responder a los retos que presentan los avances tecnológicos.

## 5.1 Propuestas generales para la mitigación de riesgos por parte de las entidades financieras

Como se expresó en la Sección 3, la Circular Básica Jurídica de la Superintendencia Financiera de Colombia incluye una autorización general a la adopción de tecnologías por parte de las entidades financieras, siempre que se cumplan las condiciones del numeral 1.3 del Capítulo 1, Título 2, Parte 1, las cuales son:

- La existencia de un plan de gestión de riesgos

- La existencia de mecanismos de control y verificación de los riesgos
- El cumplimiento íntegro de las disposiciones sobre datos personales

Así, las siguientes propuestas intentan recoger estos mandatos de la SFC y condensarlos en forma de recomendaciones de fácil adopción y seguimiento por parte de las entidades financieras.

### *5.1.1 Manejo de datos personales y Propiedad Intelectual*

A manera de introducción, todas las acciones de protección de datos personales y de propiedad intelectual deben entenderse dentro de los principios de seguridad, confidencialidad y trazabilidad; entendiendo la seguridad en un sentido fáctico referente a la solidez de los sistemas informáticos, la confidencialidad como una garantía de no uso de datos innecesarios, y la trazabilidad como una adjudicación de la carga de la prueba en cabeza de las entidades financieras que adopten sistemas de IA.

Por esto, siguiendo las tendencias normativas, es recomendable contar con un marco de gobernanza de los datos que defina claramente las responsabilidades y funciones dentro de la organización, dicho marco debe contener también los criterios de depuración de datos y los objetivos que busca la organización con la gobernanza de los datos que recoge y utiliza.

Este marco es una parte importante del cumplimiento del principio de responsabilidad demostrada que han recogido varios pronunciamientos nacionales e internacionales; este principio exige la realización de (i) una identificación y clasificación de riesgos, (ii) una descripción detallada de las operaciones de datos (de sus fuentes, manejo y uso final) y (iii) un listado de las medidas de mitigación de riesgos.

Por lo tanto, el equipo de riesgos de la entidad financiera debe ocuparse de realizar un mapeo constante de las interdependencias entre datos, modelos, infraestructura y usos de la IA; aunque

no hay obligación de consignar esto en un documento, es recomendable que la entidad financiera lo custodie en virtud de los principios de trazabilidad y transparencia.

### *5.1.2 Ciberseguridad y rendimiento*

Por parte de la gestión de la ciberseguridad, para el caso concreto de las entidades financieras colombianas, estas deben asegurar que sus sistemas informáticos cumplan con los más elevados estándares de ciberseguridad y rendimiento, para ello, pueden hacer uso de herramientas como las pruebas de estrés y el hackeo ético; y es recomendable que atiendan a cualquier modificación que se realice al Modelo Nacional de Seguridad Digital.

Por otro lado, la entidad financiera debe realizar un análisis de los riesgos de sus proveedores de IA, sea que este le suministre el software, el hardware o ambos, la entidad financiera debe asegurarse un conocimiento integral de su proveedor y de los escenarios que podrían afectarlo y dejar a la entidad financiera expuesta a una situación perjudicial, como una falla en el servicio. Además, la entidad financiera debe tener claros los riesgos inherentes al uso de la IA para actividades financieras; para ello, se propone el insumo utilizado en el Gráfico 1 de este trabajo como esquema para la identificación y clasificación de los riesgos.

Así, es recomendable que la entidad financiera cuente con mecanismos que permitan la interrupción, corrección o desmantelamiento del sistema de IA sin afectar el giro ordinario de sus negocios, y la identificación y reparación de los daños causados por la IA. A continuación, se estudiará cómo se puede mitigar el riesgo de rendimiento, y más adelante se estudiará la responsabilidad por daños causados por la IA.

Por su parte, para mitigar el riesgo de rendimiento, las entidades financieras deben llevar un seguimiento constante a los riesgos de sus proveedores críticos de IA y a la infraestructura esencial

que soporta a la misma, haciendo un especial énfasis en los riesgos que pueden contagiarse a la propia entidad financiera, y la entidad financiera debe contar con la capacidad operativa, técnica y humana para garantizar la prestación de sus servicios sin hacer uso de la IA, es decir, que la IA debe ser una herramienta adicional de apoyo y soporte de la entidad, la cual no debe ser absolutamente dependiente de la misma.

Sin embargo, un estándar como el anterior puede llegar a producir un efecto escalofriante[6] y frenar la adopción de la IA, por lo cual, las entidades financieras deben poder elaborar algunos procesos completamente dependientes de la IA, para ello, las entidades financieras podrán determinar un monto máximo operable directamente por la IA sin intervención humana, dicho monto no podrá ser tal que ponga a la entidad en una situación de riesgo. Así, en principio no es reprochable que una entidad financiera automatice completamente algunas operaciones como el estudio de crédito de sus clientes, o incluso que delegue en una IA el desembolso de los recursos, siempre que se garantice que (i) la IA no adolece de sesgos y fue configurada con arreglo a las mejores prácticas, y (ii) que la operación, si bien no es intermediada, si está bajo supervisión humana, que sea directamente proporcional al nivel de riesgo de la operación, y que existe un profesional humano capaz de explicar los razonamientos realizados por la IA.

### *5.1.3 Gestión del sesgo algorítmico*

Finalmente, para gestionar de forma adecuada el riesgo de sesgo algorítmico, la entidad financiera, en su marco de gobernanza de datos o en algún otro documento, y como buena práctica corporativa,

[6] El efecto escalofriante de la responsabilidad civil puede entenderse como la demora o excesiva cautela por parte de los actores jurídicos en ejecutar determinada acción por el temor que les causa recibir una condena por responsabilidad civil y la publicidad negativa que esto conlleva. (Coral Díaz et al., 2018, p. 31)

establecerá un comité o equipo de depuración de datos; este equipo debe ser diverso y estar conformado por profesionales de varias disciplinas, no solo ingenieros de sistemas o analistas de datos, sino también por financieros, economistas, abogados y psicólogos, todo esto en aras de garantizar la diversidad de puntos de vista a la hora de depurar la información.

Este equipo se encargará de definir qué tipos de datos pueden formar parte del conjunto de datos de entrenamiento de la IA, y también definirá cuáles serán los datos de entrada que se entregarán a la IA en el futuro; su función será entonces la de evitar la inclusión de los datos sensibles definidos como tales por la Ley 1581 de 2012 y, de tal forma, evitar la generación de una IA sesgada por motivos de raza, sexo, orientación sexual, política o religiosa u origen geográfico, para ello, deberá trabajar de la mano con los equipos encargados del desarrollo informático de la IA.

El principal objetivo de este equipo será garantizar que, al momento de tomar una decisión financiera, la IA tenga en cuenta solo los datos e información financiera del individuo o de la inversión, evitando así la perpetuación de los sesgos, generando oportunidades para la entidad financiera y garantizando el mandato de democratización del crédito.

Sin embargo, la labor de este equipo no debe limitarse a la depuración inicial, adicional a ello debe realizar un monitoreo constante de la IA, extrayendo periódicamente estadísticas sobre el desempeño de esta y analizando las decisiones tomadas en busca de sesgos no detectados en las evaluaciones anteriores. Los resultados de estas evaluaciones y los criterios de depuración deberían estar custodiados y disponibles en todo momento en desarrollo de los principios de transparencia y trazabilidad, y corresponderá entonces a los órganos de administración de la entidad financiera definir su nivel de confidencialidad.

## 5.2 Propuesta de un nuevo régimen de responsabilidad de las entidades financieras por la adopción de sistemas de IA, basado en la teoría del guardián, del hecho de la cosa inanimada y del riesgo

Finalmente, para construir una propuesta de responsabilidad por daños causados por una IA, primero debemos tener claridad sobre una serie de conceptos que pueden ayudarnos a elaborar una propuesta viable de esquema de responsabilidad civil.

En primer lugar, debemos entender que la IA no puede ser considerada como una persona jurídica susceptible de ser titular de derechos y obligaciones; la IA es una herramienta, no un fin en sí misma, se compone de una red neuronal formada por algoritmos y carece de las características de la consciencia humana, es así como, en palabras de Coral Díaz et al. (2018):

> Los robots, en todo caso, carecen de consciencia moral, en el sentido castizo de la expresión. No disciernen ni discurren en abstracciones de corte ético, por lo cual los daños que causen procederán de la mera ejecución de directrices algorítmicas (e irreflexivas desde lo moral). Por tanto, no despliegan la libertad kantiana, la justicia correctiva les es inaplicable: mal se haría en imponer un deber primario, normativo, a un objeto, por autónomo que este sea, o en atribuirle el derecho a que no conculquen su libertad, si ni libertad tiene. (p.125)

Es así como, entendiendo a la IA como una cosa inanimada, debemos continuar con la clasificación del uso de la IA como una actividad segura o si por el contrario es una actividad riesgosa.

Si bien pueden existir voces a favor o en contra de considerar a la IA como una herramienta riesgosa, lo cierto es que, con base tanto en los riesgos analizados en la Sección 2 como en las disposiciones del Reglamento 2024/1689 de la Unión Europea que definió como riesgoso el uso de la IA en algunas actividades financieras, será entonces necesario considerar el uso de la IA en los servicios financieros como una actividad riesgosa, sumando a este razonamiento dos

argumentos: la especialidad y profesionalidad requerida para prestar servicios financieros se desprende de la importancia sistémica del sistema financiero en la economía; y, como se analizó previamente, las redes neuronales de la IA son, en muchos casos, demasiado complejas como para ser entendidas, incluso por sus propios desarrolladores, lo que crea un problema a la hora de explicar los razonamientos producidos por un sistema de IA.

Así, debemos comenzar nuestro análisis refiriéndonos a la teoría del guardián de la cosa; dicha teoría estipula que el responsable por el hecho de una cosa es quien tiene sobre la misma el control material (Coral Díaz et al., 2018), no necesariamente el propietario. Esta teoría representa un riesgo para las entidades financieras debido a que indudablemente se constituyen como guardianes materiales de sus sistemas de IA y, en principio, no pueden exonerarse alegando no ser los propietarios del software[7], ya que la definición de la guardia material cubre, en nuestro concepto, los escenarios de licenciamiento de software tan comunes en el ámbito de la innovación tecnológica. La guarda material se constituye entonces, en particular, por el uso continuado de la IA y por el lucro que le reporta a la entidad financiera. Ya la Corte Suprema de Justicia ha precisado, en sentencia de la Sala de Casación Civil del 18 de mayo de 1972, MP Ernesto Gamboa Álvarez, que:

> El responsable por el hecho de cosas inanimadas es su guardián, o sea quien tiene sobre ellas el poder de mando, dirección y control independiente.
>
> (…)

[7] Por supuesto, el nivel de responsabilidad y la exposición a este tipo particular de riesgo dependerá en gran medida de las condiciones contractuales pactadas con el proveedor de IA y de la forma en la que se resuelvan las cuestiones de propiedad industrial planteadas en la Sección 2. Para efectos prácticos en este trabajo, asumimos que las entidades financieras, por lo general, solo tienen el licenciamiento de uso de sus modelos de IA, no la propiedad industrial sobre los mismos.

> Y la presunción de ser guardián puede desvanecerla el propietario si demuestra que transfirió a otra persona la tenencia de la cosa en virtud de un título jurídico… (p.188)

Por lo tanto, en un principio la entidad financiera es la guardiana material de los sistemas de IA que utiliza; sin embargo, la Corte Suprema de Justicia utiliza los términos "poder de mando, dirección y control independiente", poderes que a todas luces las entidades financieras no tienen sobre los sistemas de IA, ya que, como se mencionó en la Sección 1, estos sistemas se caracterizan fundamentalmente por su carácter autónomo.

El tema fue extensamente tratado por Daniel Horacio Coral Díaz, María Alejandra Díaz Trujillo y Álvaro Enrique Macías Rodríguez en el libro *Robótica y responsabilidad civil: reflexiones en torno al fundamento del deber de reparar*, en el que plantean (Coral Díaz et al., 2018):

> La orfandad de control y dirección sobre los robots provistos con inteligencia artificial tiene hondas repercusiones dogmáticas y prácticas en cuanto a la adecuación de los eventos de daño hacia el régimen de responsabilidad por actividades peligrosas. En tanto que cualquier razonamiento jurídico y probatorio que se haga para determinar al responsable de los perjuicios ocasionados en ejercicio de una actividad peligrosa descansa sobre el criterio – aceptado por la jurisprudencia civil colombiana– del uso, control y dirección de las cosas a través de las cuales se desarrolla la actividad (…) (p. 101)

Así, para el caso de los sistemas de IA, debido a su autonomía y a la opacidad de sus algoritmos que, en muchas ocasiones, impiden a sus desarrolladores y a sus usuarios ejercer un adecuado entendimiento y control sobre los mismos, estos sistemas son entonces de carácter impredecible, lo cual dificulta en gran medida la determinación de la causalidad.

Por esto, es de vital importancia y alineado con los objetivos de esta investigación la construcción de una propuesta de responsabilidad por el uso de la IA que permita a las entidades financieras

prever y protegerse contra posibles casos futuros, en especial, por el uso creciente que está teniendo la IA.

Es así como la propuesta de esquema de responsabilidad civil que se propondrá a continuación se hará partiendo de la noción de responsabilidad por productos defectuosos que consagra nuestro ordenamiento jurídico, dicho esquema será híbrido pues, como se verá a continuación, la responsabilidad se predica tanto de la entidad financiera usuaria como del proveedor de la tecnología de IA.

Entonces, las entidades financieras serán responsables por los daños caudados por un sistema de IA que hayan adoptado, siempre que dicho daño sea causado por un error en la calidad de los datos de entrenamiento o de entrada, esto es así ya que es sobre este aspecto que la entidad financiera puede ejercer un mayor control a través de los mecanismos de depuración de datos estudiados. Por su parte, los proveedores de IA responderán por los daños causados por un sistema de IA desarrollado por ellos si la causa del daño subyace en la calidad del modelo informático, del código o de las redes neuronales que conforman los algoritmos.

Sin embargo, debemos también comprender que la IA conlleva un alto nivel de imprevisibilidad, y esta debe ser considerada como una posible causal de exoneración ya que, como menciona Coral Díaz et al. (2018):

> Esta causal deja una puerta abierta para los productores o fabricantes, consistente en la posibilidad de argüir que, en razón del carácter novedoso del robot y de las técnicas científicas en el momento de su fabricación en serie, las eventuales consecuencias dañinas del producto les eran totalmente desconocidas. (p. 106)

# 6. Conclusiones

En conclusión, podemos decir que la IA es una herramienta con un gran potencial para crear mejores oportunidades, incrementar la eficiencia y garantizar la equidad en el sistema financiero. Prueba de ello es el incremento de su valor en el mercado y en el porcentaje de su adopción por parte de las entidades financieras a nivel global; tiene el potencial de acelerar la cuarta revolución industrial a un ritmo sin precedentes.

Es así como la IA se ha convertido en una herramienta esencial para las entidades financieras, al punto que estas no pueden aspirar a competir en el mercado si no es de la mano de la adopción de uno o varios sistemas de IA. Es gracias a su gran potencial para realizar analítica de datos y manejar grandes cantidades de información lo que la convierte en una tecnología transformadora de gran importancia para el sector financiero.

Sin embargo, como nueva tecnología que impacta a un sector tan crítico para la economía y que promete causar cambios tan trascendentales en el comportamiento del sector financiero, no es de extrañar que tanto los estados como las organizaciones internacionales de todo tipo se estén dedicando a estudiar esta tecnología y el cómo regularla de mejor manera; si bien tienen buenas intenciones, es notorio como los estados son reacios a implementar regulaciones rígidas pues temen que normas de este tipo frenen el desarrollo de implementación de la IA dentro de sus fronteras y les deje rezagados en comparación con el resto del mundo, por ello, las tendencias regulatorias se decantan por instrumentos de soft law como estándares, guías, modelos, recomendaciones y buenas prácticas.

El progreso no obstante no puede cegarnos de una realidad, y es que la IA conlleva riesgos de consideración, riesgos que son especialmente relevantes en un sector tan sensible como el financiero, la regulación debe enfocarse entonces en la atención y cuidado de estos riesgos, sin

embargo, estos son manejables si se sigue una debida diligencia con responsabilidad corporativa que reconozca la importancia del compliance en esta materia.

Es así como la IA debe ser una herramienta de soporte para las entidades financieras, y estas no deben desarrollar una dependencia absoluta a la misma, de lo contrario, los riesgos de la IA pasan a ser riesgos sistémicos de la entidad financiera que además incurre en un comportamiento de delegación de la profesionalidad a una cosa inanimada, lo cual supone un riesgo innecesario para el sector financiero.

Por lo tanto, las entidades financieras tienen, con relación a la adopción de sistemas de IA, dos responsabilidades:

1. Tener una debida diligencia y cuidado, practicando una gestión integral de los riesgos asociados a la IA.
2. Actuar como garantes de la calidad de los datos utilizados para el entrenamiento de la IA.

Así, en el ámbito de la responsabilidad civil, será la entidad financiera la que responsa por los daños ocasionados por un sistema de IA cuya causa sea la mala calidad de los datos que la misma entidad financiera opera y que "entrega" a la IA y; por su parte, el tercero proveedor de la tecnología será responsable por los daños cuya causa sea la mala calidad o deficiencias previsibles en el software mismo.

Nuestro propósito con este trabajo no es causar pesimismo con respecto a la IA, sino dejar en claro los riesgos que esta conlleva y brindar a los actores del sistema financiero un insumo que facilite la identificación, medición, manejo y mitigación de los riesgos asociados, incluyendo el riesgo legal por responsabilidad civil, con esto, buscamos la protección de las entidades financieras, para

que puedan implementar de forma segura esta tecnología revolucionaria que tiene el potencial de cambiar de forma radical la manera en la que gestionamos las finanzas a nivel global.

## Bibliografía


1. Abbas, N., Cohen, C., & Jan Grolleman, D. (2024). *La inteligencia artificial puede mejorar la eficiencia de los mercados, y avivar su volatilidad*. imf.org. https://www.imf.org/es/Blogs/Articles/2024/10/15/artificial-intelligence-can-make-markets-more-efficient-and-more-volatile#:~:text=inteligencia%20artificial-,La%20inteligencia%20artificial%20puede%20mejorar%20la%20eficiencia%20de%20los%20mercados,volatilidad%20en%20%C3%A9pocas%20de%20tensi%C3%B3n.
2. Agarwal, R., Kremer, A., Kristensen, I., & Luget, A. (2024, 1 marzo). *Cómo la IA generativa puede ayudar a los bancos a gestionar el riesgo y el cumplimiento normativo*. McKinsey & Company. https://www.mckinsey.com/featured-insights/destacados/como-la-ia-generativa-puede-ayudar-a-los-bancos-a-gestionar-el-riesgo-y-el-cumplimiento-normativo/es
3. Asobancaria. (2023). *Inteligencia artificial en la banca* (1376.ª ed.) [Electrónico]. https://www.asobancaria.com/wp-content/uploads/2023/05/1376-BE-2.pdf
4. Asobancaria. (2024a). *Una banca personalizada por inteligencia artificial* (1437.ª ed.) [Electrónico]. https://www.asobancaria.com/wp-content/uploads/2024/08/1437-BE.pdf

5. Asobancaria. (2024b). *Visión actual del derecho financiero* (M. Valenzuela Gruesso, Ed.). Mauricio Valenzuela Gruesso. https://publicaciones.asobancaria.com/wp-content/uploads/Libros/2024/LIBRO-DERECHO-FINANCIERO-2024.pdf

6. Asobancaria. (2024c). *Visión actual del derecho financiero* [Electrónico]. Mauricio Valenzuela Gruesso. https://publicaciones.asobancaria.com/wp-content/uploads/Libros/2024/LIBRO-DERECHO-FINANCIERO-2024.pdf

7. Avance Jurídico Casa Editorial Ltda. (s. f.-a). *Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [CONSTITUCION_POLITICA_1991_PR006]*. Avance Jurídico Casa Editorial Ltda., Senado de la República de Colombia. http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991_pr006.html#189

8. Avance Jurídico Casa Editorial Ltda. (s. f.-b). *Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [DECRETO_4327_2005]*. Avance Jurídico Casa Editorial Ltda., Senado de la República de Colombia. http://www.secretariasenado.gov.co/senado/basedoc/decreto_4327_2005.html

9. Avance Jurídico Casa Editorial Ltda. (s. f.-c). *Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [DECRETO_4712_2008]*. Avance Jurídico Casa Editorial Ltda., Senado de la República de Colombia. http://www.secretariasenado.gov.co/senado/basedoc/decreto_4712_2008.html

10. Avance Jurídico Casa Editorial Ltda. (s. f.-d). *Leyes desde 1992 - Vigencia expresa y control de constitucionalidad*

*[ESTATUTO_ORGANICO_SISTEMA_FINANCIERO]*. Avance Jurídico Casa Editorial Ltda., Senado de la República de Colombia. http://www.secretariasenado.gov.co/senado/basedoc/estatuto_organico_sistema_financiero.html#1

11. Avance Jurídico Casa Editorial Ltda. (s. f.-e). *Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_0964_2005]*. Avance Jurídico Casa Editorial Ltda., Senado de la República de Colombia. http://www.secretariasenado.gov.co/senado/basedoc/ley_0964_2005.html
12. Avance Jurídico Casa Editorial Ltda. (s. f.-f). *Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_1266_2008]*. Avance Jurídico Casa Editorial Ltda., Senado de la República de Colombia. http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html
13. Avance Jurídico Casa Editorial Ltda. (s. f.-g). *Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_1581_2012]*. Avance Jurídico Casa Editorial Ltda., Senado de la República de Colombia. http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html
14. Avance Jurídico Casa Editorial Ltda. (s. f.-h). *Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_1915_2018]*. Avance Jurídico Casa Editorial Ltda., Senado de la República de Colombia. http://www.secretariasenado.gov.co/senado/basedoc/ley_1915_2018.html
15. Badman, A. (2024). *¿Qué es el manejo de riesgos de IA?* https://www.ibm.com/mx-es/think/insights/ai-risk-management

16. Baena Toro, D., Hoyos Walteros, H., & Ramírez Osorio, J. (2016). *Sistema financiero colombiano* (2.ª ed.) [Físico]. Ecoe ediciones.

17. Bancolombia. (2024, 24 abril). *Riesgos de la Inteligencia Artificial: fraudes y robo de identidad*. https://blog.bancolombia.com/tendencias/riesgos-inteligencia-artificial/

18. BBVA ESPAÑA & BBVA. (2024, 13 marzo). Ciberataques basados en Inteligencia Artificial. *BBVA*. https://www.bbva.es/finanzas-vistazo/ciberseguridad/ataques-informaticos/ciberataques-inteligencia-artificial.html

19. Cárdenas, M. (2020). *Introducción a la economía colombiana* (4.ª ed.) [Físico]. Fedesarrollo.

20. Comunidad Andina. (2000). *Decisión Andina 486 del 2000*. https://www.comunidadandina.org/StaticFiles/DocOf/DEC486.pdf

21. Congreso de los Estados Unidos. (2024). *BIPARTISAN TASK FORCE REPORT ON ARTIFICIAL INTELLIGENCE*. https://www.speaker.gov/wp-content/uploads/2024/12/AI-Task-Force-Report-FINAL.pdf

22. Consejo nacional de política económica y social, República de Colombia, & Departamento Nacional de Planeación. (2025). *Documento CONPES 4144 de 2025* (1.ªed.) [Electrónico]. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/4144.pdf

23. Coral Díaz, D. H., Díaz Trujillo, M. A., & Macías Rodríguez, Á. E. (2018). *Robótica y responsabilidad civil: reflexiones en torno al fundamento del deber de reparar* [Físico]. Universidad Externado de Colombia.

24. Corrales, M., Fenwick, M., & Forgó, N. (2018). *Robotics, AI and the Future of Law*. Springer.

25. Corte Suprema de Justicia. (1973). *Gaceta judicial de la Corte Suprema de Justicia* (Vol. 142) [Electrónico]. https://cortesuprema.gov.co/corte/wp-content/uploads/subpage/GJ/Gaceta%20Judicial/GJ%20CXLII%20n.%202352-2357%20(1972).pdf

26. Del Pozo, C., & Rojas, D. (2025). *The role of policies on technology and AI for innovation and increased competitiveness in North America*. https://www.brookings.edu/articles/the-role-of-policies-on-technology-and-ai-for-innovation-and-increased-competitiveness-in-north-america/#:~:text=The%20global%20artificial%20intelligence%20(AI,billion%20per%20year%20in%20revenues.

27. Departamento Administrativo de la Presidencia de la República. (2021). *MARCO ÉTICO PARA LA INTELIGENCIA ARTIFICIAL EN COLOMBIA*. https://dapre.presidencia.gov.co/TD/MARCO-ETICO-PARA-LA-INTELIGENCIA-ARTIFICIAL-EN-COLOMBIA-2021.pdf

28. El Tiempo. (2024, 24 septiembre). *El mercado de la IA duplicará su valor y alcanzará los 1,14 billones de euros para 2028*. eltiempo.com. https://www.eltiempo.com/tecnosfera/novedades-tecnologia/el-mercado-de-la-ia-duplicara-su-valor-y-alcanzara-los-1-14-billones-de-euros-para-2028-3384109

29. Fernando Capitani, J. (2022). *RIESGO INTELIGENTE: EL SESGO ALGORÍTMICO y LA TOMA DE DECISIONES EN UNA SOCIEDAD CADA VEZ*

*MÁS TECNOLÓGICA* [Tesis de grado, Pontificia universidad javeriana]. https://repository.javeriana.edu.co/handle/10554/62139

30. Fondo Monetario Internacional. (s. f.). *Global Financial Stability Report* [Electrónico]. 2024. https://www.imf.org/en/Publications/GFSR/Issues/2024/10/22/global-financial-stability-report-october-2024

31. Hunton Andrews Kurth LLP. (2023, 31 octubre). *Biden AI Order Enables Agencies to Address Key Risks*. https://www.hunton.com/privacy-and-information-security-law/biden-ai-order-empowers-agencies-to-hit-wide-ranging-risks

32. Hunton Andrews Kurth LLP. (2025, 29 enero). *The Impact of AI Executive Order's Revocation Remains Uncertain, but New Trump EO Points to Path Forward*. https://www.hunton.com/privacy-and-information-security-law/the-impact-of-ai-executive-orders-revocation-remains-uncertain-but-new-trump-eo-points-to-path-forward#:~:text=EO%2014110%2C%20issued%20by%20President,federal%20agencies%2C%20it%20also%20directed

33. IBM Corporation. (2025a). *Riesgo de intoxicación de datos para IA | IBM watsonx*. https://dataplatform.cloud.ibm.com/docs/content/wsj/ai-risk-atlas/data-poisoning.html?context=wx&locale=es

34. IBM Corporation. (2025b). *Riesgo de sesgo de decisión para IA | IBM watsonx*. https://dataplatform.cloud.ibm.com/docs/content/wsj/ai-risk-atlas/decision-bias.html?context=wx&locale=es

35. IBM Corporation. (2025c). *Riesgo de sesgo de los datos para la IA | IBM watsonx*. https://dataplatform.cloud.ibm.com/docs/content/wsj/ai-risk-atlas/data-bias.html?context=wx&locale=es

36. IBM Corporation. (2025d). *Riesgo de sesgo de salida para IA | IBM watsonx*. https://dataplatform.cloud.ibm.com/docs/content/wsj/ai-risk-atlas/output-bias.html?context=wx&locale=es

37. Kayser-Bril, N. (2020). *Google apologizes after its Vision AI produced racist results - AlgorithmWatch*. AlgorithmWatch. https://algorithmwatch.org/en/google-vision-racism/

38. Kearns, J. (2023, 14 diciembre). *Las repercusiones de la inteligencia artificial en las finanzas*. imf.org. https://www.imf.org/es/Publications/fandd/issues/2023/12/AI-reverberations-across-finance-Kearns

39. Kosinski, M. & IBM Corporation. (2024). ¿Qué es el phishing? *ibm.com*. https://www.ibm.com/es-es/topics/phishing

40. Kurzgesagt – In a Nutshell. (2015, 12 marzo). *Banking Explained – Money and Credit* [Vídeo]. YouTube. https://www.youtube.com/watch?v=fTTGALaRZoc

41. LISA Institute. (s. f.). *Deepfakes: Qué es, tipos, riesgos y amenazas*. Lisainstitute.com. https://www.lisainstitute.com/blogs/blog/deepfakes-tipos-consejos-riesgos-amenazas?srsltid=AfmBOoqm7JrnxN2FuyFtT7DLCw1nVK7J5S6FjoEjmoc2MRimIEXF9R4r

42. Ministerio de Hacienda y Crédito Público & Superintendencia Financiera de Colombia. (s. f.). *¿Qué es una actividad de intermediación de Valores?* [Electrónico]. https://www.superfinanciera.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=30546

43. OCDE. (2019). *OECD legal instruments 0449*. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

44. Partners, P. &. (2023, 29 junio). *Los desafíos de la Propiedad Intelectual (PI) en el contexto de la Inteligencia Artificial (IA)*. https://www.linkedin.com/pulse/los-desaf%C3%ADos-de-la-propiedad-intelectual-pi-en-el-contexto-inteligencia/

45. PricewaterhouseCoopers. (s. f.). *PwC's Global Artificial Intelligence Study: Sizing the prize*. PwC. https://www.pwc.com/gx/en/issues/artificial-intelligence/publications/artificial-intelligence-study.html

46. Real Academia Española. (s. f.). Inteligencia artificial. En *dle.rae.es*. https://dle.rae.es/inteligencia?m=form#2DxmhCT

47. Riobueno, H. J. U. (2024, 11 octubre). ¿Sabes cuáles son los desafíos y responsabilidades de la protección de datos en la era de la IA? *Grant Thornton Colombia*. https://www.grantthornton.com.co/Perspectivas/novedades/sabes-cuales-son-los-desafios-y-responsabilidades-de-la-proteccion-de-datos-en-la-era-de-la-ia/

48. *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*. (2023, 1 noviembre). Federal Register.

https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence

49. Sardanyés, E. (s. f.). *Ejemplos de ciberataques lanzados con inteligencia artificial*. esedsl.com. https://www.esedsl.com/blog/ejemplos-de-ciberataques-lanzados-con-inteligencia-artificial

50. Superintendencia de Industria y Comercio. (2024, 21 agosto). *Circular Externa 002 de 2024*. sedeelectronica.sic.gov.co. https://sedeelectronica.sic.gov.co/sites/default/files/normativa/Circular%20Externa%20No.%20002%20del%2021%20de%20agosto%20de%202024.pdf

51. Superintendencia Financiera de Colombia. (s. f.). *Glosario de innovación financiera* [Electrónico]. https://www.superfinanciera.gov.co/publicaciones/10113588/innovasfcglosario-de-innovacion-financierai-10113588/

52. Superintendencia Financiera de Colombia. (1995). *Circular Externa 100 de 1995: Circular Básica Contable y Financiera* [Electrónico]. https://www.superfinanciera.gov.co/publicaciones/15466/normativanormativa-generalcircular-basica-contable-y-financiera-circular-externa-de-15466/

53. Superintendencia Financiera de Colombia. (2014). *Circular Externa 029 de 2014: Circular Básica Jurídica* [Electrónico]. https://www.superfinanciera.gov.co/publicaciones/10083443/normativanormativa-generalcircular-basica-juridica-ce-10083443/

54. Superintendencia Financiera de Colombia. (2021a). *Circular Externa 002 de 2021* [Electrónico].

https://www.superfinanciera.gov.co/publicaciones/10102519/normativanormativa-generalcircular-basica-juridica-ce-parte-i-instrucciones-generales-aplicables-a-las-entidades-vigiladascapitulo-i-del-titulo-ii-de-la-parte-i-10102519/

55. Superintendencia Financiera de Colombia. (2021b). Sistema Integral de Administración de Riesgos «SIAR». En *Circular Básica Contable y Financiera*. https://www.superfinanciera.gov.co/publicaciones/15466/normativanormativa-generalcircular-basica-contable-y-financiera-circular-externa-de-15466/

56. Unión Europea. (2024). *REGLAMENTO (UE) 2024/1689 DEL PARLAMENTO EUROPEO Y DEL CONSEJO* [Electrónico]. https://www.boe.es/doue/2024/1689/L00001-00144.pdf

57. Webb, A. (2021). *Nueve gigantes*. Planeta Publishing.

58. Zapata Garrido, L. A., & Díaz Mojica, H. F. (2008). *Predicción del tipo de cambio peso-dólar utilizando Redes Neuronales Artificiales (rna)* [Electrónico]. http://www.scielo.org.co/pdf/pege/n24/n24a02.pdf