

Uso de la inteligencia artificial en la gestión
del riesgo de una entidad financiera¹
Use of Artificial Intelligence in Risk Management
of a Financial Institution

CRISTINA ESCOBAR MONTALVO

Investigadora independiente, Quito, Ecuador

Correo electrónico: ciescobarmontalvo@gmail.com

ORCID: <https://orcid.org/0000-0001-5970-9127>

STEPHAN MORA VALDEZ

Investigador independiente, Quito, Ecuador

Correo electrónico: simvmora@gmail.com

ORCID: <https://orcid.org/0009-0005-4710-8339>

Resumen

El avance de la tecnología incluyendo el uso de la inteligencia artificial (IA) en la vida cotidiana ha traído consigo cambios significativos e impactos sustanciales; de igual manera ha sucedido con las transacciones electrónicas y sistemas de toma de decisiones. En este contexto, las diversas aplicaciones de la IA prometen varios beneficios en la gestión del riesgo de una entidad financiera, con miras a un control efectivo y a una posible mitigación. Las conclusiones de la investigación indican que la IA es un sistema que puede resultar efectivo en la gestión del riesgo de las entidades financieras. Sin embargo, previo a su implementación como sistema informático, se debe considerar los aspectos negativos y positivos que conlleva su aplicación, como el uso de datos personales, la actual inexistencia de un marco normativo, entre otros.

Palabras clave

Riesgo financiero, Inteligencia artificial, Regulación, Gestión del riesgo.

Abstract

The advancement of technology, including the use of Artificial Intelligence (AI) in everyday life, has brought about significant changes and substantial impacts; the same has occurred with electronic transactions and decision-making systems. In this context, the various applications of AI promise several benefits for risk management within financial institutions, aiming for effective control and potential mitigation. The research findings indicate that AI can be an effective system for managing risk in financial entities. However, before implementing it as an information system, it is essential to consider both the positive and negative aspects associated with this technology, such as the use of personal data, the current absence of a regulatory framework, among others.

Keywords

Risk, Financial, Artificial Intelligence, Regulation, Model.

¹ Los autores de este artículo han contribuido en partes iguales.



1. Introducción

Al entrar en el primer cuarto del siglo XXI, la tecnología se ha desarrollado de manera rápida. Recientemente, el mundo ha presenciado el surgimiento de la cuarta revolución industrial, en la cual dentro de sus avances se encuentra el desarrollo de tecnologías que sirven como catalizadores para esta era, en particular la IA.

En un contexto más restringido, el desarrollo de la tecnología de la información ha dejado al mundo sin fronteras y ha influido en cambios sociales significativos y rápidos (Ramli, 2004). El rápido ritmo del avance tecnológico ha impactado profundamente en la vida humana y ha traído efectos tanto positivos como negativos. La tecnología juega un papel crucial en la simplificación de tareas y actividades; es decir, si una tarea supone un reto para los humanos, la tecnología puede facilitar su ejecución (Haq & Yunanto, 2024).

En términos generales se define a la IA como “el conjunto de sistemas que muestran un comportamiento inteligente analizando su entorno y tomando medidas, con cierto grado de autonomía, para lograr objetivos específicos” (Sheikh, 2023, p. 19). Por lo tanto, la IA puede ser y es usada en diferentes procesos. El objetivo a través de esta investigación es analizar el rol de la IA en la gestión del riesgo de una entidad financiera, a través de un método análisis cualitativo que abarca la revisión bibliográfica y normativa.

Para el desarrollo de este artículo, se adoptó un enfoque metodológico de carácter cualitativo, basado principalmente en la revisión bibliográfica y normativa, tanto nacional como internacional. La revisión bibliográfica permitió identificar los principales aportes teóricos y empíricos relacionados con la aplicación de herramientas de IA en el ámbito financiero, mientras que el análisis de la normativa vigente facilitó comprender el marco legal y regulatorio aplicable a la gestión del riesgo en instituciones financieras, con un enfoque principal en el Ecuador. Este tipo de metodología resulta pertinente cuando se busca analizar fenómenos complejos desde una perspectiva descriptiva y analítica, sin recurrir a la recolección de datos empíricos directos (Hernández-Sampieri & Mendoza, 2018).

El trabajo abarca la definición de IA, la regulación internacional que existe en la materia y los proyectos de normativa presentados en Ecuador. Posteriormente, se definen los riesgos de las entidades financieras, sus clases y cómo se implementa la gestión del riesgo en las instituciones financieras ecuatorianas. Una vez obtenido el marco general, se analizaron las cuestiones negativas y positivas de la implementación de la IA como sistema informático en la gestión del riesgo en las entidades financieras. La conclusión a la que se llegó, producto de este estudio, fue que se puede utilizar la IA como sistema informático dentro de la gestión del riesgo en las entidades financieras; no obstante, existen problemáticas que aún deben ser superadas, como el costo de implementación y la falta de un marco normativo nacional en esta materia.

2. Breves consideraciones sobre la inteligencia artificial

2.1. Definición de inteligencia artificial

Es necesario, en primer lugar, definir y conceptualizar lo que es la IA. En principio, hay que tener en cuenta que esta se ha convertido en una de las innovaciones más relevantes de nuestro tiempo, transformando la manera en que trabajamos, nos comunicamos y tomamos decisiones.

Al igual que cualquier otro concepto de naturaleza informática, el definir la IA no es una tarea sencilla. En realidad, a pesar del desarrollo de esta, no existe una definición unívoca de lo que es. En la actualidad se utilizan numerosas definiciones, lo que puede generar confusión (Russell & Norvig, 2020).

Por ello, se partirá del concepto presentado por la Organización para la Cooperación y el Desarrollo Económicos (OCDE), la cual establece que un sistema de IA es “un sistema

basado en máquinas que, para objetivos explícitos o implícitos, infiere, a partir de la información que recibe, cómo generar resultados, predicciones, contenido, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales” (OCDE, 2024, 4).

De igual manera, se entiende que es un sistema que analiza el entorno y las medidas con las que se desarrolla, con un comportamiento inteligente, y con un determinado grado de autonomía, para cumplir objetivos específicos.

Ambas definiciones ayudan a entender cómo la IA puede ser utilizada para identificar, medir, controlar, mitigar y monitorear los diferentes riesgos que enfrentan las entidades financieras, así como asistir en la toma de decisiones oportunas y adecuadas.

2.2. Clases de inteligencia artificial

Una vez definida, es importante describir brevemente las clases de IA que existen actualmente. En términos generales la IA se clasifica según su capacidad de razonamiento y autonomía en tres niveles: (i) inteligencia artificial débil o estrecha (ANI), (ii) inteligencia artificial general (AGI) e (iii) inteligencia artificial superinteligente (ASI). Cada nivel representa una etapa distinta en el desarrollo de esta tecnología, desde los sistemas que ya usamos a diario hasta los que todavía pertenecen al terreno de la investigación y la teoría (Russell & Norvig, 2021).

La ANI o IA estrecha es la que más se utiliza en la actualidad. Se trata de sistemas diseñados para realizar tareas específicas, como reconocer rostros, recomendar productos o analizar datos financieros. Aunque su alcance es limitado, su impacto ha sido enorme, ya que facilita la automatización de procesos y mejora la precisión en distintos ámbitos. Este tipo de IA no “piensa” por sí misma, ni comprende el contexto, sino que aprende a partir de grandes volúmenes de datos para optimizar sus resultados (Kaplan & Haenlein, 2019).

En un nivel más avanzado, se encuentra la AGI, que sirve para desarrollar máquinas con capacidades similares a las del ser humano, tales como razonar, aprender y adaptarse a distintas situaciones. Este tipo de IA todavía no existe, pero numerosos investigadores trabajan en su desarrollo. El objetivo de esta clase de IA es lograr que los sistemas comprendan y resuelvan problemas complejos en cualquier campo, de forma autónoma y flexible (Goertzel, 2020).

La tercera clase corresponde a la ASI, la cual representa un escenario hipotético en el que las máquinas superarían la inteligencia humana en, prácticamente, todas las áreas. Aunque esta idea puede parecer lejana, es importante reflexionar desde ahora sobre las implicaciones éticas y los riesgos que podría conllevar su aplicación, por ello, la posibilidad de que una IA supere el control humano plantea preguntas profundas sobre la seguridad, la autonomía y la responsabilidad tecnológica (Bostrom, 2016).

2.3. Regulación en materia de inteligencia artificial

2.3.1. Internacional

Si bien la aplicación y utilización de la IA en varios aspectos de la vida cotidiana es relativamente reciente, no es menos cierto que su incorporación en el campo jurídico poco a poco está siendo regulada, mucho más si se tiene en cuenta el desarrollo y avance tecnológico de un país o región.

Acorde con lo mencionado, un ejemplo de normativa expedida para tal efecto, en materia de este artículo, es el Reglamento (UE) 2024/1689 (2024), expedido por el Parlamento Europeo. En este documento se establecieron normas armonizadas en materia de IA y se derogaron una serie de reglamentos que se contraponen al mismo. Este cuerpo legal prevé aspectos generales, definiciones, prácticas prohibidas a través de la IA, la clasificación de los sistemas de IA como sistemas de alto riesgo, las obligaciones de transparencia de los proveedores de estos sistemas, los modelos de uso, el código de conducta y directrices, entre otros.

En el Reglamento 2024/1689 no se estableció como una actividad prohibida aplicar la IA en los sistemas financieros. Al respecto, esta normativa sí prevé cuáles implementaciones de la IA están prohibidas, entre ellas que constan las siguientes:

- Para aplicar técnicas subliminales que trascienden la conciencia de una persona o de técnicas deliberadamente manipuladoras o engañosas con el objetivo o el efecto de alterar de manera sustancial el comportamiento de una persona o un colectivo.
- Para introducir en el mercado, poner en servicio o utilizar un sistema que explote alguna de las vulnerabilidades de las personas con la finalidad o el efecto de alterar de manera sustancial el comportamiento de dicha persona.
- Para evaluar o clasificar a personas naturales o a colectivos de personas durante un periodo determinado de tiempo con base en su comportamiento social o en sus características.
- Para realizar evaluaciones de riesgos de personas naturales con el fin de valorar o predecir el riesgo cuando una persona natural cometa un delito.
- Para crear o ampliar bases de datos de reconocimiento facial mediante la extracción no selectiva de imágenes faciales de internet o de circuitos cerrados de televisión.
- Para inferir las emociones de una persona natural en los lugares de trabajo y en los centros educativos.
- Para clasificar individualmente a las personas naturales sobre la base de sus datos biométricos con el fin de deducir o inferir su raza, opiniones políticas, afiliación sindical, convicciones religiosas o filosóficas, vida u orientación sexuales.
- Para usar sistemas de identificación biométrica remota “en tiempo real” en espacios de acceso público con fines de garantía del cumplimiento del derecho. (Reglamento UE 2024/1689, 2024, art. 5).

Asimismo, se establecieron regulaciones especiales para los sistemas de IA en los casos en los que estos puedan utilizar datos personales, señalando que estos pueden operar “siempre que ofrezcan las garantías adecuadas en relación con los derechos y las libertades fundamentales de las personas físicas” (Reglamento UE 2024/1689, 2024, art. 10).

En el caso que nos ocupa, bajo el régimen legal de la Unión Europea, se podría utilizar la IA para una serie de aspectos entre los que consta el manejo de control del riesgo en entidades financieras, en vista de que esto no es una actividad prohibida². Sin embargo, se debe tomar en cuenta que, igualmente, esta norma ya regula aspectos como las obligaciones de las entidades que proveen sistemas de IA y, también, establece los límites de cómo estos sistemas deben funcionar.

2.3.2. Nacional

En la legislación ecuatoriana, actualmente, no existe una normativa expedida en materia de IA; sin embargo, en la Asamblea Nacional se están tramitando tres proyectos de ley al respecto:

- Proyecto de Ley Orgánica de Regulación y Promoción de la Inteligencia Artificial en Ecuador.
- Proyecto de Ley de Fomento y Desarrollo de la Inteligencia Artificial.
- Ley Orgánica de Aprovechamiento Digital e Inteligencia Artificial para Niñas, Niños y Adolescentes.

² Esta aseveración parte de la naturaleza misma del derecho privado en la que todo lo que no está prohibido está permitido, siendo que los sistemas que utilicen los diferentes actores económicos y comerciales son de su entera responsabilidad y decisión.

El primer proyecto es la propuesta más extensa en su contenido y toma como ejemplo la regulación europea. En el proyecto se clasifica los sistemas de IA en diversos niveles del riesgo, se propone crear una autoridad nacional de control de la IA y se señala cuáles son los principios que deben regir a esta tecnología; pero, si no se ha cumplido con el respectivo trámite legislativo hasta su publicación en el Registro Oficial, dichos conceptos, definiciones y estructuras cuentan, únicamente, como enunciados y sirven para un análisis temporal (CECO, 2025).

3. Riesgos financieros

El riesgo es uno de los fenómenos más importantes en las ciencias económicas, y es inherente a la actividad financiera. Está también presente en la vida cotidiana de las personas y de las empresas, las cuales reconocen la necesidad de comprenderlo para gestionarlo y protegerse, reducir su nivel de impacto o aceptarlo en una magnitud que, en circunstancias normales, permita obtener ingresos satisfactorios (Brown, 2016, 85). Esta última observación se refiere principalmente a las instituciones financieras cuya actividad se basa, en gran medida, en asumir riesgos financieros (Adamowicz, 2018, p. 39).

El riesgo económico también podría considerarse, desde un enfoque proactivo, para administrar entidades económicas, lo que conduce al desarrollo de una construcción léxica estable denominada *gestión del riesgo*. La identificación, el modelado, la evaluación de los riesgos, las pruebas de estrés, la determinación del riesgo y el establecimiento de límites del riesgo deben utilizarse como herramientas de gestión del riesgo.

Es justamente por lo expuesto que las entidades de control tienden a normativizar los aspectos relacionados con los riesgos financieros. En el caso ecuatoriano, la Superintendencia de Bancos (SB) en su rol de control tiene la facultad normativa de emitir resoluciones de obligatorio cumplimiento. Dentro de la amplia normativa que ha emitido, la SB definió al riesgo como la posibilidad de que se produzca un hecho generador de pérdidas que afecte el valor económico de las instituciones (Codificación de Resoluciones de la Superintendencia de Bancos, 2017, cap. I, sección I, art. 2, núm. 2.1).

En resumen, la gestión del riesgo se considera como un método, sistema o enfoque numérico, mediante el cual los datos de entrada se convierten en estimaciones cuantitativas basadas en la aplicación de herramientas matemáticas, estadísticas y económicas (Kosova et al., 2021, p. 412).

3.1. Clases de riesgo

Para cumplir con el objetivo de este artículo, es necesario definir los tipos de riesgos a los que están expuestas las entidades financieras en el Ecuador y que, la SB, en su rol de ente de control, acertadamente ha regulado a través de su normativa interna denominada Codificación de Resoluciones de la Superintendencia de Bancos (CRSB), con el fin de lograr un mejor control y seguimiento de las entidades financieras.

Los tipos de riesgos son los siguientes:

3.1.1. Riesgo de crédito

Es la posibilidad de pérdida debido al incumplimiento del prestatario o la contraparte en operaciones directas, indirectas o de derivados, conlleva el no pago, el pago parcial o la falta de oportunidad en el pago de las obligaciones pactadas (CRSB, 2025, cap. II, sección I, art. 2, literal a).

3.1.2. Riesgo de mercado

Se entiende por riesgos de mercado a la contingencia que una entidad controlada incurra en pérdidas por movimientos de los precios del mercado como resultado de las posiciones que mantenga dentro y fuera del balance.

Los riesgos de mercado más comunes son los relacionados con actividades de negociación de valores, operaciones con derivados, variaciones en la tasa de interés y el riesgo de tipo de cambio, así como del precio de los *commodities* (cap. III, sección I, art. 2).

3.1.3. Riesgo de liquidez

Se entiende por riesgo de liquidez cuando la entidad enfrenta una escasez de fondos para cumplir sus obligaciones y que, por ello, tiene la necesidad de conseguir recursos alternativos o vender activos en condiciones desfavorables, esto es, asumiendo un alto costo financiero o una elevada tasa de descuento, lo que hace que incurra en pérdidas de valorización (cap. II, sección I, art. 2, literal a).

3.1.4. Riesgo operativo

El riesgo operativo se entenderá como la posibilidad de que se ocasionen pérdidas por eventos derivados de fallas o insuficiencias en los factores de procesos, personas, tecnología de la información y por eventos externos. El riesgo operativo incluye el riesgo legal, pero excluye los riesgos sistémico, estratégico y de reputación (cap. V, sección I, art. 3).

3.1.5. Riesgo legal

El riesgo legal es la probabilidad de que las entidades controladas sufran pérdidas debido a que los activos y contingentes se encuentren de la siguiente forma: (i) expuestos a situaciones de mayor vulnerabilidad, (ii) que sus pasivos puedan verse incrementados más allá de los niveles esperados o, (iii), que el desarrollo de sus operaciones enfrente la eventualidad de ser afectado negativamente, producto de error, negligencia, impericia, imprudencia o dolo que deriven de:

- la inobservancia, incorrecta o inoportuna aplicación de disposiciones legales o normativas;
- instrucciones de carácter general o particular emanadas de los organismos de control, dentro de sus respectivas competencias;
- sentencias o resoluciones jurisdiccionales o administrativas adversas;
- la deficiente redacción de los textos, formalización o ejecución de actos, contratos o transacciones, inclusive distintos a los de su giro ordinario de negocio, o
- porque los derechos de las partes contratantes no han sido claramente estipulados. (cap. V, sección I, art. 5).

3.1.6. Riesgo de lavado de activos

Es la posibilidad de pérdida o daño que puede sufrir una entidad controlada por su exposición a ser utilizada directamente o a través de sus operaciones como instrumento para el lavado de activos y/o canalización de recursos hacia actividades delictivas, entre ellas, el terrorismo y la proliferación de armas de destrucción masiva. Este riesgo se materializa a través de los riesgos asociados, tales como legal, reputacional, operativo y de contagio (cap. VI, sección I, art. 3, núm. 3.47).

3.2. La implementación de la gestión del riesgo en las entidades financieras

Por ser la gestión del riesgo un método o sistema para controlar y mitigar los diferentes tipos de riesgo que enfrentan las entidades financieras en el desenvolvimiento de su trabajo, es necesario que ese control no provenga únicamente de un organismo estatal como la SB, sino que, también, cada entidad financiera pueda previamente hacer un control y mitigación de manera interna.

Es por ello que la normativa ecuatoriana emitida por el ente de control prevé un marco normativo y una estructura interna que deben seguir las entidades financieras para llevar a cabo un efectivo control y mitigación del riesgo. Se expone dicha estructura a continuación.

3.2.1. Directorio

Es el órgano encargado de conocer y resolver sobre el contenido y cumplimiento de las comunicaciones de la SB referentes a disposiciones, observaciones, recomendaciones e iniciativas sobre la marcha de la entidad financiera, así como de analizar y aprobar sus políticas, controlar su ejecución y los informes de riesgo (Código Orgánico Monetario y Financiero, art. 410, núms. 1 y 2). Respecto de la gestión del riesgo, el directorio se encarga de conocer y aprobar las estrategias, políticas, procesos, procedimientos y metodologías que permitan una eficiente administración integral de los riesgos, que sean propuestas por el comité de administración integral de riesgos y la unidad de riesgos.

3.2.2. Comité de administración integral de riesgos

Es el órgano encargado de evaluar y, a su vez, de proponer al directorio la aprobación de estrategias, políticas, procesos, procedimientos y metodologías que permitan una eficiente administración del riesgo, así como su aplicación.

3.2.3. Unidad de riesgos

Es la unidad encargada de elaborar y remitir al comité de administración integral de riesgos estrategias, políticas, procesos, procedimientos y metodologías para la gestión integral de los riesgos e implementar mecanismos que aseguren su permanente actualización.

3.2.4. Sistema informático

La Superintendencia de Bancos, mediante su normativa, exige a las entidades bancarias contar con un sistema informático capaz de proveer al comité y a la unidad de riesgo toda la información necesaria para identificar, medir, controlar, mitigar y monitorear las exposiciones de riesgo que están asumiendo y apoyar en la toma de decisiones oportunas y adecuadas.

Estos sistemas incorporarán los procesos definidos para elaborar los informes que involucren todas las variables relacionadas con la medición de los riesgos y la vulnerabilidad institucional, bajo las condiciones del entorno. (CRSB, 2025, cap. I, sección II, segunda disposición general).

Es justamente dentro de esta parte de la estructura en la que cabría la utilización de la IA como sistema informático, con el objetivo de que desempeñe las funciones que se establecen en la normativa nacional. Dicha implementación sería efectiva en su rendimiento como herramienta informática y tendría la capacidad lógica de aprender políticas, estrategias, procesos, procedimientos y metodologías para gestionar el riesgo y, de igual manera, implementar mecanismos que aseguren un verdadero control para, probablemente, mitigar dicho riesgo.

4. Cuestiones alrededor de la implementación de la IA como sistema informático en la gestión del riesgo

Acorde con lo expuesto, es viable el uso de la IA en la gestión del riesgo en entidades financieras, siempre y cuando se la utilice como un sistema informático capaz de proveer al comité y a la unidad de riesgo toda la información necesaria para identificar, medir, controlar, mitigar y monitorear las diferentes exposiciones de riesgo. No obstante, se examinarán los aspectos negativos y positivos asociados a esta alternativa.

4.1. Aspectos negativos de la implementación de la IA como sistema informático en la gestión del riesgo

4.1.1. Protección de datos personales

La confidencialidad constituye uno de los pilares fundamentales en la gestión de los riesgos financieros, especialmente cuando se incorporan sistemas basados en IA. Estos sistemas procesan

grandes volúmenes de información sensible, como datos personales, historiales crediticios y patrones transaccionales.

En esta materia, la Ley Orgánica de Protección de Datos Personales ([LOPDP], 2021) es el marco normativo bajo el cual está regulado el uso de datos personales en el territorio ecuatoriano. Si bien esta ley no regula ningún aspecto relacionado con la IA, no es menos cierto que, en caso de implementar esta tecnología bajo la denominación de *sistema informático* para gestionar riesgos en el sistema financiero, se deberá cumplir con el objeto y finalidad de esta ley.³

Cualquier sistema de IA que se implemente deberá cumplir con al menos cuatro aspectos conforme lo establecido en la LOPDP:

- Principio de licitud, proporcionalidad y finalidad.
- Consentimiento expreso del titular para el tratamiento de datos a través de este sistema.
- Seguridad y confidencialidad de los datos.
- Finalidad específica de que los datos se utilicen para el propósito que se consiste. (LOPDP, 2021, arts. 4, 7, 8, 42 y 47).

Como se ve, al implementar una IA como sistema informático para la gestión del riesgo, se deberá acatar lo que la LOPDP está protegiendo y regulando. La IA utiliza la información que recibe para influir en entornos físicos o virtuales, y dicha información, actualmente, no puede ser filtrada o discriminada por la IA que es de uso libre u *open*. Sin embargo, las IA que sean creadas para un uso específico, como para la gestión del riesgo en entidades financieras, deberán ser diseñadas, configuradas y supervisadas para que puedan filtrar, identificar y manejar información sensible o protegida, tal y como rige la norma que regula los datos personales.

Por ello, aunque los sistemas de IA que se implementen para la gestión del riesgo financiero no utilizarían los datos *per se*, esta sí se alimentaría de ellos para estar en un constante aprendizaje, con el fin de controlar y mitigar el riesgo. Por lo que, en materia de consentimiento, forma de uso y finalidad de la recolección de datos personales, las entidades financieras deberán utilizar, únicamente, los sistemas de IA que cuenten con esas características para la gestión del riesgo.

A pesar de lo expuesto y de que existe la percepción de que la automatización aumenta el riesgo de filtraciones, lo cierto es que, cuando se desarrollan y se configuran de manera personalizada, los sistemas de IA pueden garantizar altos niveles de protección y confidencialidad de la información (European Union Agency for Cybersecurity [ENISA], 2023). La clave radica, según la ENISA, en integrar mecanismos de seguridad desde la fase de diseño, siguiendo principios de *privacidad por diseño* y *privacidad por defecto*.

Los algoritmos de IA personalizados permiten implementar capas de seguridad adaptadas a las necesidades específicas de cada entidad financiera, en las que se incluye técnicas de cifrado avanzado, anonimización de datos y control de acceso basado en roles. Estas herramientas limitan la exposición de información sensible y reducen significativamente la posibilidad de enfrentarse a accesos no autorizados o a fugas internas. Según el Fondo Monetario Internacional (2025), las instituciones financieras que aplican IA con base en arquitecturas seguras y supervisadas han logrado fortalecer sus mecanismos de gestión del riesgo sin comprometer la integridad de los datos.

³ Para efectos de comprensión se señala que el objeto y finalidad de la Ley Orgánica de Protección de Datos Personales, es “garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección. Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela.”

Sin embargo, la capacidad de mantener la confidencialidad depende también de la trazabilidad y transparencia del modelo. Un sistema de IA diseñado de manera opaca puede generar vulnerabilidades difíciles de detectar. La implementación responsable de la IA requiere auditorías constantes y marcos normativos que garanticen la rendición de cuentas (Fondo Monetario Internacional, 2023). Por ello, los modelos personalizados deben acompañarse de políticas internas que regulen la recolección, uso y almacenamiento de los datos, para garantizar que la automatización no sustituya el control humano sobre la información crítica.

En este contexto, la IA puede convertirse en una aliada estratégica para reforzar la confidencialidad en la gestión del riesgo financiero, siempre que su desarrollo responda a estándares éticos y regulatorios claros (Fondo Monetario Internacional, 2023). La adopción de protocolos internacionales, como el Reglamento General de Protección de Datos (GDPR) y las guías del Comité de Supervisión Bancaria de Basilea, contribuyen a que las entidades financieras mantengan la confianza de sus usuarios. En suma, la personalización de los sistemas de IA, acompañada de una gobernanza sólida de datos, permite equilibrar la innovación tecnológica con la protección efectiva de la información (Basel Committee on Banking Supervision, 2021).

Por lo expuesto, para aplicar la IA como sistema informático para la gestión del riesgo en una entidad financiera, previamente, se debe cumplir y aplicar la LOPDP.

4.1.2. Falta de marco regulatorio

El segundo aspecto negativo por considerar es la falta de un marco normativo especial en la materia. Si bien una implementación de esta naturaleza debe estar sujeta a la normativa vigente en diferentes aspectos, como la gestión del riesgo financiero y la protección de datos personales; el que no se tenga una normativa que regule la IA, como materia particular, puede generar inseguridad jurídica. Por ejemplo, no hay una certeza, mucho menos un control o protección en lo relacionado a qué plataformas de IA se pueden contratar o diseñar, qué ente será el encargado de vigilar la aplicación de esta normativa o, incluso en temas de responsabilidad, quién responderá por las decisiones automatizadas que tome la IA.

En resumen, para la aplicación de la IA en la gestión de los riesgos, que es un fenómeno relativamente nuevo, se necesita de regulaciones y leyes adecuadas para garantizar que sea utilizada de manera responsable y en conjunto con la normativa nacional vigente, con el fin de evitar usos con objetivos delictivos que vulneren derechos o que resulten en abusos en contra de las personas.

4.1.3. Responsabilidad por decisiones automatizadas

El uso de sistemas de IA en procesos de gestión del riesgo financiero implica que la toma de decisiones se hace sobre la base de algoritmos e información que, a criterio de la IA, se recopila para cumplir tareas asignadas; es decir, a pesar de que la persona natural es quien le asigna las tareas u objetivos, eso no quiere decir que sea siempre la responsable por las actuaciones que vaya tomando la IA, mucho más si esta no ha sido diseñada o configurada dentro de los parámetros de la legalidad.

De allí surge la pregunta, ¿qué pasa si una decisión tomada por la IA fue hecha con base en información errada?, por ejemplo, se niega un crédito o se detecta un fraude con base en criterios discriminatorios o que no puedan ser justificados. Estos aspectos necesitan ser más estudiados y estar regulados en términos de las especificaciones técnicas que deben tener los sistemas de IA que se van a implementar. Dicha regulación permitiría tener el marco de las responsabilidades –civiles, administrativas y penales– claras, para que en caso de errores se sepa a quien controlar o incluso demandar. En el mismo sentido, para evitar estos problemas, en la normativa se debería considerar aspectos mínimos que se deben tener en cuenta en los contratos de provisión de servicios de IA.

4.1.4. Costo de implementación

Para utilizar una IA como sistema informático para la gestión del riesgo en entidades financieras, no basta únicamente con su implementación, sino que se debe cumplir con el marco normativo de cada país. En el caso de Ecuador, pese a que no cuenta con una normativa propia que regule a las IA, estas si deben, al menos, cumplir con la protección de datos personales, lo que nos lleva a concluir que no se puede recurrir a las IA que son públicas u *open*, porque no cumplen con la normativa nacional, mucho menos pensar que se las pueda utilizar para manejar información o datos de carácter financiero.

Para la implementación real de la IA como sistema financiero es fundamental que sea creada a partir de los parámetros legales que constan en la normativa nacional. Esto sin duda hará que adquirir esta herramienta incremente sus costos, mucho más si se tiene en cuenta que se requeriría de una serie de consideraciones, por ejemplo, infraestructura tecnológica, personal capacitado, mantenimiento, monitoreo u actualización y escenarios de prueba.

Si las entidades financieras deciden recurrir a la IA para este fin, deberán tener en cuenta que solo pueden utilizar una IA que sea creada o monitoreada en el territorio nacional y, a su vez, el alto costo que demandará implementar una IA para la gestión del riesgo. Todo esto sin tener en cuenta que el país tiene una limitada capacidad tecnológica, ya sea para su creación o implementación.

En resumen, a pesar de no ser un tema de cuidado, como la protección de datos, el costo de la implementación es de gran importancia para las finanzas de las entidades financieras, principalmente si en algún momento en la legislación nacional se ordenara que esta sea implementada con carácter obligatorio; hay que tener en cuenta que, en el sistema financiero nacional, un solo banco es el que podría permitirse dicha inversión.

4.2. Aspectos positivos de la aplicación de la IA como sistema de control del riesgo, superados los aspectos negativos

La IA puede ser una herramienta informática muy útil, siempre y cuando se la pueda catalogar como tal y se pueda tener control sobre ella, mucho más si se la diseña o configura para que obedezca el marco regulatorio del territorio en donde se va a utilizar.

Si bien es prematuro pensar en una implementación de IA como sistema informático para la gestión del riesgo en las entidades financieras, en vista de los aspectos negativos mencionados, existen aspectos positivos para hacerlo.

Para ilustrar de mejor manera los aspectos positivos que implican la implementación de la IA como sistema informático, se presenta un ejercicio teórico en el que se aplica y explica el funcionamiento de la IA de IBM WATSON, la cual ha sido usada ampliamente en el sector bancario a nivel extranjero, a través de varias funciones clave para controlar y mitigar el riesgo, conforme la siguiente matriz de la tabla 1.

Tabla 1: Beneficios de la IA de IBM WATSON

Área de actuación	Ejemplo de implementación	Beneficios
Gestión del riesgo crediticio	Detectar que un segmento de clientes presenta caída en sus ingresos o un cambio en el comportamiento de gasto, y así ajustar información crediticia para disminuir existencia de impagos.	Evaluar la probabilidad de incumplimiento de clientes, mejorar modelos de puntuación crediticia, anticipar señales tempranas de riesgo de morosidad y tomar acciones que la prevengan.

Prevención del fraude y lavado de dinero	Revisar millones de transacciones y detectar conexiones ocultas, entre clientes o empresas, que pueden sugerir redes de lavado.	Detectar patrones anómalos o transacciones inusuales, analizar reportes para identificar riesgos de cumplimiento, priorizar alertas relevantes para reducir falsos positivos.
Cumplimiento normativo	Ayudar, mediante su configuración, a las instituciones a cumplir con regulaciones internas y externas.	Analizar normativa, detectar cambios regulatorios, generar informes de cumplimiento y monitorear constantemente los riesgos operacionales.
Riesgo operacional	Identificar riesgos de fallas humanas o de procesamientos internos.	Analizar reportes internos, datos de incidentes y auditorías para detectar vulnerabilidades operativas, y predecir qué áreas o procesos tienen mayor probabilidad de fraudes internos.
Riesgo de mercado	Procesar información pública como noticias, redes sociales e informes económicos.	Mediar la aprobación del mercado sobre el banco y sus actuaciones, anticipar riesgos reputacionales y detectar riesgos geopolíticos que afecten su cartera.

Fuente: elaboración propia a partir de Artikis, et al. (2017).

Si bien el IBM WATSON es un sistema que partió de ser un *machine learning*, actualmente es una IA que puede aplicarse a los riesgos financieros que existen, incluso conforme la normativa ecuatoriana, ya que se va desarrollando y evolucionando con toda la información que adquiere.

La propuesta de utilizar la IA como sistema informático para gestionar el riesgo en las entidades financieras, siempre y cuando se adecue a la normativa nacional, implica un avance significativo para su control y mitigación, principalmente, en las siguientes consideraciones:

- Gestionar, de forma rápida y de mejor manera, la información que se le proporcione y la que pueda obtener de manera autónoma, respecto de los diferentes tipos de riesgo que enfrentan las entidades financieras.
- Una vez recopilada la información, puede de manera autónoma medir los escenarios del riesgo que pueden enfrentar las entidades financieras.
- Analizados los potenciales escenarios del riesgo, la IA puede automáticamente controlarlos y monitorearlos para prevenir una afectación a la entidad financiera.
- En caso de que se haya podido prevenir completamente los escenarios del riesgo, solo ahí se puede hacer una referencia a una mitigación del potencial riesgo que pudo ocasionar una afectación a la entidad financiera y, sobre todo, a la confianza que brinda a sus depositantes.

5. Conclusiones

Una vez analizada la posibilidad de implementar la IA como sistema informático para la gestión del riesgo en las entidades financieras, así como los aspectos negativos y positivos que eso conlleva, se concluye que:

- La IA es una herramienta tecnológica que analiza la información que recibe, así como la que de forma autónoma consigue, con el fin de cumplir con objetivos específicos e influir en entornos físicos o virtuales.

- La gestión del riesgo se puede considerar como un método o sistema mediante el cual se analiza la información obtenida (riesgo), con el fin de generar estimaciones que se puedan medir o expresarse en números.
- La aplicación de la IA para la gestión del riesgo en el sistema financiero en el contexto actual cabe, únicamente, bajo la figura de sistema informático, puesto que es la posibilidad el uso de esta conforme la normativa de la materia.
- Para implementar la IA como sistema informático para la gestión del riesgo, previamente, se deberá considerar los siguientes aspectos: protección de datos personales en todo momento conforme la LOPDP; necesidad de existencia de un marco normativo que regule su implementación; determinación de los niveles de responsabilidad y los contenidos de los contratos de prestación de esta clase de servicios, y costo de implementación.
- Si se logran superar los aspectos negativos, se puede concluir que la implementación de la IA como sistema informático en la gestión del riesgo de las entidades financieras –como los sistemas del IBM WATSON– es útil para detectar segmentos de clientes de manera masiva, revisar millones de transacciones con conexiones ocultas, identificar fallas de procedimientos e incluso información pública que afecte el funcionamiento de las instituciones, puesto que el procesamiento de esta información sería óptimo y se realizaría de manera eficaz y rápida por el sistema de manera directa.

Referencias bibliográficas

Libros

- Bostrom, N. (2016). *Superintelligence: Paths, dangers, strategies*. Oxford: Oxford University Press.
- Brown, A. (2016). *Financial risk management for Dummies*. California: For dummies. <https://archive.org/details/financialriskman0000brow/page/n4/mode/1up>
- European Union Agency for Cybersecurity. (2023). *AI cybersecurity challenges: Threat landscape for artificial intelligence*. Publications Office of the European Union.
- Hernández-Sampieri, R., & Mendoza, C. (2018). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta*. CDMX: McGraw-Hill Education.
- Ramli, Ahmad. 2004. *Cyber Law dan HAKI dalam Sistem Hukum Indonesia*. Bandung: Refika Aditama.
- Russell, S., & Norvig, P. (2021). *Artificial intelligence: A modern approach* (4th ed.). Pearson. California: College of Berkley.
- Russell, S., & Norvig, P. (2020). *Artificial Intelligence: A modern approach* (4th ed.). Pearson. California: College of Berkley.

Artículos de publicaciones periódicas

- Artikis, A, Katzouris, N., et al. (2017). A Prototype for Credit Card Fraud Management: Industry Paper. In Proceedings of the *11th ACM International Conference on Distributed and Event-based Systems (DEBS '17)*. Association for Computing Machinery, New York, NY, USA, 249-260. <https://doi.org/10.1145/3093742.3093912>
- Adamowicz, T. (2018). Types of Risk in Banking Operations – Categorization and Definitions. *Economic and Regional Studies / Studia Ekonomiczne i Regionalne*, 11(4), 37-56. 10.2478/ers-2018-0034
- Goertzel, B. (2020). Artificial general intelligence: Concept, state of the art, and future prospects. *Journal of Artificial General Intelligence*, 5(1), 1-46. https://www.researchgate.net/publication/271390398_Artificial_General_Intelligence_Concept_State_of_the_Art_and_Future_Prospects

- Haq, S., & Yunanto, Y. (2024) Legal Implications of Using Artificial Intelligence (AI) Technology in Electronic Transactions. *International Journal of Social Science and Human Research*, 7(5), 3365-3371. <https://ijsshr.in/v7i5/Doc/108.pdf>
- Kaplan, A., & Haenlein, M. (2019). Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. *Business Horizons*, 62(1), 15-25. <https://doi.org/10.1016/j.bushor.2018.08.004>
- Sheikh, H., Prins, C., et al. (2023). Artificial Intelligence: Definition and Background. En H. Sheikh, et al. *Mission AI, Research for Policy* (pp. 15-42). https://doi.org/10.1007/978-3-031-21448-6_2
- World Economic Forum. (2023). *Artificial intelligence in financial services: Opportunities and risks*. https://reports.weforum.org/docs/WEF_Artificial_Intelligence_in_Financial_Services_2025.pdf

Publicaciones web

- Basel Committee on Banking Supervision. (2022). *Principles for the effective management and supervision of climate-related financial risks*, junio. Bank for International Settlements. <https://www.bis.org/bcbs/publ/d532.pdf>
- Fondo Monetario Internacional. (2025). AI Projects in Financial Supervisory Authorities: A toolkit for successful implementation. *IMF Working Paper No. 2025/199* <https://www.imf.org/en/Publications/WP/Issues/2025/10/03/AI-Projects-in-Financial-Supervisory-Authorities-570625>
- OCDE. (2024). Explanatory memorandum on the updated OECD definition of an AI system. OECD Artificial Intelligence Papers No. 8, marzo. https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/03/explanatory-memorandum-on-the-updated-oecd-definition-of-an-ai-system_3c815e51/623da898-en.pdf

Fuentes normativas

- Codificación de Resoluciones de la Superintendencia de Bancos. (2017). Normas de Control para las Entidades de los Sectores Financieros Público y Privado. Título IX De la Gestión y Administración de Riesgos, Capítulo I, Sección II, Segunda Disposición General, 31 de agosto. <https://www.superbancos.gob.ec/bancos/codificacion-de-normas-de-la-sb-libro-uno-sistema-financiero/>
- Codificación de Resoluciones de la Superintendencia de Bancos. (2017). Normas Generales para las Instituciones del Sistema Financiero, Libro I, Título X De la Gestión y Administración de Riesgos, capítulo i, sección i, art. 2, número 2.1, 31 de agosto. Norma derogada. <https://www.superbancos.gob.ec/bancos/codificacion-de-normas-de-la-sb-libro-uno-sistema-financiero/>
- Código Orgánico Monetario y Financiero. (2014). Segundo Suplemento, R. O. n.º 332, 12 de septiembre. Última reforma: Suplemento R. O. 309, 21 de agosto de 2018.
- Ley Orgánica de Protección de Datos Personales. (2021). Suplemento del R. O. n.º 459, 26 de mayo.
- Reglamento (UE) 2024/1689. (2024). European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), 13 de junio. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng?eliuri=eli%3Areg%3A2024%3A1689%3Aoj&locale=es>