RGSA – Revista de Gestão Social e Ambiental
ISSN: 1981-982X
Submission date: 05/10/2024
Acceptance date: 07/12/2024
DOI: https://doi.org/10.24857/rgsa.v18n9-162
Organization: Interinstitutional Scientific Committee
Chief Editor: Ana Carolina Messias de Souza Ferreira da Costa
Assessment: Double Blind Review pelo SEER/OJS

# IMPLEMENTACIÓN Y EVALUACIÓN DE UN PROTOTIPO ANTIFRAUDE BASADO EN INTELIGENCIA ARTIFICIAL GENERATIVA PARA EL SECTOR FINANCIERO ECUATORIANO

**Isaac Patricio Arteaga Peña**[1]
**Juan Carlos Ortega-Castro**[2]

**RESUMEN**

**Objetivos:** Este estudio tiene como objetivo desarrollar una alternativa más económica y sencilla a los actuales sistemas antifraudes en el sector financiero popular y solidario de Ecuador. Dada la creciente amenaza del fraude bancario en América Latina y las exigencias regulatorias de la Superintendencia de Economía Popular y Solidaria de Ecuador, se propone una solución basada en inteligencia artificial (IA) generativa para identificar transacciones fraudulentas en plataformas de banca móvil y web.

**Marco Teórico:** La implementación de sistemas antifraudes en el sector financiero es un desafío complejo debido a la naturaleza evolutiva de los fraudes y las limitaciones de los sistemas actuales, como Custodian360, Monitor Plus y Sentinel, que son percibidos por más del 50% de los profesionales encuestados como costosos y complejos de implementar. En este contexto, la inteligencia artificial y, específicamente, los modelos de lenguaje generativo como GPT, presentan una oportunidad para desarrollar soluciones más accesibles y efectivas.

**Método:** Se desarrolló un prototipo utilizando el motor GPT de LLaMA3 (8B parámetros) y el framework Ollama, además de modelos de OpenAI como ChatGPT 3.5 y 4. La metodología incluyó una prueba de concepto en la que se parametrizó un prompt en Ollama, especificando campos de tramas transaccionales en formato JSON y definiendo reglas antifraudes en lenguaje natural. Estas reglas fueron compartidas por Dycotein, permitiendo la identificación de transacciones potencialmente fraudulentas.

**Resultados y Discusión:** Los resultados indicaron que los modelos con menor cantidad de parámetros, como LLaMA3 8B y ChatGPT 3.5, no son adecuados para la implementación efectiva de sistemas antifraudes debido a su limitada capacidad para manejar reglas complejas. Sin embargo, ChatGPT 4 mostró resultados prometedores con reglas simples, sugiriendo que, aunque no son un reemplazo completo para los sistemas programáticos tradicionales, los modelos de IA generativa pueden complementar las soluciones existentes, especialmente en escenarios menos complejos.

**Implicaciones de la Investigación:** Los hallazgos de este estudio subrayan la necesidad de continuar investigando y desarrollando modelos de IA generativa más avanzados para la detección de fraudes, dado que las tecnologías actuales aún no son completamente efectivas para escenarios complejos. Además, se destaca la importancia de balancear entre costo y eficacia en la implementación de sistemas antifraudes, especialmente en sectores con recursos limitados como el financiero popular y solidario.

**Originalidad/Valor:** Este artículo presenta una aproximación innovadora al uso de inteligencia artificial generativa para el desarrollo de sistemas antifraudes en un sector financiero con restricciones presupuestarias. Al explorar el potencial de modelos avanzados como ChatGPT 4, la investigación abre nuevas vías para la creación de soluciones más accesibles y adaptables, ofreciendo un valor significativo para la industria y la academia en un contexto de creciente fraude financiero en América Latina.

**Palabras clave:** Antifraude, Inteligencia Artificial, Modelos GPT, LLaMA, Banca Financiera.

[1] Universidad Católica de Cuenca, Unidad Académica de Posgrado, Cuenca, Ecuador.
E-mail: isaac.arteaga.10@est.ucacue.edu.ec Orcid: https://orcid.org/0009-0001-7551-0887
[2] Universidad Católica de Cuenca, Unidad Académica de Posgrado, Cuenca, Ecuador.
E-mail: jcortegac@ucacue.edu.ec@ucacue.edu.ec Orcid: https://orcid.org/0000-0001-6496-4325

## IMPLEMENTATION AND EVALUATION OF AN ANTI-FRAUD PROTOTYPE BASED ON GENERATIVE ARTIFICIAL INTELLIGENCE FOR THE ECUADORIAN FINANCIAL SECTOR


### ABSTRACT

**Objectives:** This study aims to develop a more economical and simpler alternative to the current anti-fraud systems in the popular and solidarity financial sector in Ecuador. Given the growing threat of banking fraud in Latin America and the regulatory requirements of the Superintendence of Popular and Solidarity Economy of Ecuador, a solution based on generative artificial intelligence (AI) is proposed to identify fraudulent transactions on mobile and web banking platforms.

**Theoretical Framework**: The implementation of anti-fraud systems in the financial sector is a complex challenge due to the evolving nature of fraud and the limitations of current systems, such as Custodian360, Monitor Plus, and Sentinel, which are perceived by more than 50% of surveyed professionals as costly and complex to implement. In this context, artificial intelligence, and specifically generative language models like GPT, present an opportunity to develop more accessible and effective solutions.

**Method:** A prototype was developed using the LLaMA3 GPT engine (8B parameters) and the Ollama framework, in addition to OpenAI models like ChatGPT 3.5 and 4. The methodology included a proof of concept in which a prompt was parameterized in Ollama, specifying fields of transactional frames in JSON format and defining anti-fraud rules in natural language. These rules were shared by Dycotein, enabling the identification of potentially fraudulent transactions.

**Results and Discussion:** The results indicated that models with fewer parameters, such as LLaMA3 8B and ChatGPT 3.5, are not suitable for the effective implementation of anti-fraud systems due to their limited capacity to handle complex rules. However, ChatGPT 4 showed promising results with simple rules, suggesting that while they are not a complete replacement for traditional programmatic systems, generative AI models can complement existing solutions, especially in less complex scenarios.

**Research Implications**: The findings of this study highlight the need for continued research and development of more advanced generative AI models for fraud detection, as current technologies are not yet fully effective for complex scenarios. Additionally, the importance of balancing cost and effectiveness in the implementation of anti-fraud systems is emphasized, especially in sectors with limited resources such as the popular and solidarity financial sector.

**Originality/Value:** This article presents an innovative approach to the use of generative artificial intelligence for the development of anti-fraud systems in a financial sector with budgetary constraints. By exploring the potential of advanced models like ChatGPT 4, the research opens new avenues for the creation of more accessible and adaptable solutions, offering significant value to the industry and academia in a context of increasing financial fraud in Latin America.


**Keywords:** Anti-Fraud, Artificial Intelligence, GPT models, LLaMA, Financial Banking.

## IMPLEMENTAÇÃO E AVALIAÇÃO DE UM PROTÓTIPO ANTIFRAUDE BASEADO EM INTELIGÊNCIA ARTIFICIAL GERATIVA PARA O SETOR FINANCEIRO EQUATORIANO


### RESUMO

**Objetivos:** Este estudo tem como objetivo desenvolver uma alternativa mais econômica e simples aos atuais sistemas antifraude no setor financeiro popular e solidário do Equador. Dada a crescente ameaça de fraude bancária na América Latina e os requisitos regulatórios da Superintendência de Economia Popular e Solidária do Equador, uma solução baseada em inteligência artificial generativa (IA) é proposta para identificar transações fraudulentas em plataformas bancárias móveis e da web.

**Quadro teórico:** A implementação de sistemas antifraude no setor financeiro é um desafio complexo devido à natureza evolutiva da fraude e às limitações dos sistemas atuais, como o Custodian360, o Monitor Plus e o Sentinel, que são considerados caros e complexos por mais de 50 % dos profissionais inquiridos. Neste contexto, a inteligência artificial e, especificamente, os modelos linguísticos generativos como o GPT, representam uma oportunidade para desenvolver soluções mais acessíveis e eficazes.

**Método:** Um protótipo foi desenvolvido usando o motor GPT LLaMA3 (parâmetros 8B) e o framework Ollama, além de modelos OpenAI como ChatGPT 3.5 e 4. A metodologia incluiu uma prova de conceito em que um prompt foi parametrizado em Ollama, especificando campos de quadros transacionais em formato JSON e definindo regras antifraude em linguagem natural. Essas regras foram compartilhadas pela Dycotein, permitindo a identificação de transações potencialmente fraudulentas.

**Resultados e Discussão:** Os resultados indicaram que modelos com menos parâmetros, como o LLaMA3 8B e o ChatGPT 3.5, não são adequados para a implementação efetiva de sistemas antifraude devido à sua capacidade limitada de lidar com regras complexas. No entanto, o ChatGPT 4 mostrou resultados promissores com regras simples, sugerindo que, embora não sejam um substituto completo para os sistemas programáticos tradicionais, os modelos de IA generativa podem complementar as soluções existentes, especialmente em cenários menos complexos.

**Implicações da pesquisa:** Os resultados deste estudo destacam a necessidade de pesquisa e desenvolvimento contínuos de modelos de IA geradores mais avançados para detecção de fraudes, já que as tecnologias atuais ainda não são totalmente eficazes para cenários complexos. Além disso, é salientada a importância de equilibrar os custos e a eficácia na aplicação dos sistemas antifraude, especialmente em setores com recursos limitados, como o setor financeiro popular e solidário.

**Originalidade/valor:** Este artigo apresenta uma abordagem inovadora à utilização da inteligência artificial geradora para o desenvolvimento de sistemas antifraude num setor financeiro com restrições orçamentais. Explorando o potencial de modelos avançados como o ChatGPT 4, a pesquisa abre novos caminhos para a criação de soluções mais acessíveis e adaptáveis, oferecendo valor significativo para a indústria e a academia em um contexto de crescente fraude financeira na América Latina.

**Palavras-chave:** Antifraude, Inteligência Artificial, Modelos GPT, LaMA, Banca Financeira.



## 1 INTRODUCCIÓN

La implementación de sistemas antifraude en el ámbito financiero constituye uno de los desafíos más complejos para las entidades financieras y los profesionales de la informática, debido a la necesidad de crear modelos avanzados de discriminación y toma de decisiones. En América Latina, el fraude bancario es una problemática creciente que afecta tanto a instituciones como a usuarios. Diversas soluciones en el mercado, como Custodian360, Monitor Plus y Sentinel, buscan mitigar estos riesgos mediante enfoques tecnológicos innovadores (Sentinel, s.f.; Monitor Plus, s.f.).

En Ecuador, la Superintendencia de Economía Popular y Solidaria (SEPS) exige el uso de herramientas antifraude. Según la normativa, "el software que se utilice para las transacciones deberá registrar al menos: accesos, nivel de transaccionalidad, límites individuales de transaccionalidad, perfiles de usuarios financieros, entre otra información disponible para valoración. Deberán generar reportes sobre dicha información"

(Superintendencia de Economía Popular y Solidaria, 2023). Por lo tanto, las entidades financieras del sector analizado están obligadas a implementar este tipo de sistemas.

Este artículo tiene como objetivo desarrollar las bases de un prototipo que ofrezca una alternativa a las soluciones actuales, simplificando la implementación y reduciendo costos gracias a la inteligencia artificial. Para ello, se evalúa la efectividad de los modelos GPT en la detección de tramas fraudulentas a partir de un prompt de reglas antifraude. En esta investigación, se evalúa un prototipo creado con el motor GPT de LLaMA3 y el framework Ollama, en conjunto con los modelos de OpenAI, ChatGPT en sus versiones 3.5 y 4. Se realiza una prueba de concepto para el desarrollo del motor de reglas para el software antifraude basado en inteligencia artificial generativa.

El prototipo se desarrolló utilizando GPT, configurado con un prompt que instruye a los modelos a desempeñar el rol de experto antifraude. Este sistema se basa en parámetros comunes utilizados en transacciones bancarias, como la dirección IP, ciudad de la transacción, montos, ubicación de la transacción anterior y tiempo entre transacciones. Todos estos datos se introducen al modelo GPT en formato JSON, con el objetivo de obtener las respuestas de coincidencias en el mismo formato.

Ollama y OpenAI facilitan la creación de archivos de configuración y el uso de prompts a través de servicios web que permiten utilizarlos mediante la integración a sus respectivas interfaces. En el mercado ecuatoriano y latinoamericano existen soluciones antifraude como Custodian360, que utiliza programación mediante bloques de código y parametrización en bases de datos. Aunque compleja en su implementación inicial, esta solución permite una administración sencilla desde un backend una vez configurada. Por otro lado, soluciones como Monitor Plus y Sentinel, comercializadas en Latinoamérica, son consideradas costosas según encuestas realizadas a 30 entidades financieras del sector de la economía popular y solidaria en Ecuador, donde más del 50% de los encuestados creen que los precios son altos y que su configuración e implementación es compleja.

La propuesta de utilizar GPT se presenta como una posible alternativa más simple en la administración de reglas y con menores costos de implementación y configuración. Además, las soluciones comerciales existentes también emplean sistemas de aprendizaje automático para la predicción de fraudes transaccionales, con tiempos medios de implementación de al menos tres meses, según la empresa Dycotein, debido a la necesidad de obtener datos históricos. En este contexto, la solución propuesta con modelos GPT pretende ofrecer un enfoque novedoso, accesible y eficiente para la prevención de fraudes en el sector financiero.

## 2 METODOLOGÍA

Para la elaboración del prototipo y las pruebas, se instaló el framework Ollama en un MacBook Pro con procesador M2 Pro y 16 GB de RAM. Se creó un prompt con el rol de experto en fraudes y los datos transaccionales provistos por la empresa Dycotein, parametrizados en formato JSON utilizando LLaMA3 con 8 mil millones de parámetros. Además, se utilizó ChatGPT de OpenAI como solución contrastante, aprovechando su capacidad de consumir modelos mediante interfaces o API.

Para ambas tecnologías se definió el mismo prompt con cinco reglas antifraude. Posteriormente, se realizaron pruebas con conjuntos de datos proporcionados por Dycotein. Los conjuntos de datos consistieron en 30 tramas JSON para cada una de las reglas definidas, ver figura 1, tabla 1, 2 y 3.

**Figura 1**

*Prompt para el sistema de detección de fraudes.*

```
Actua como una API de un sistema de deteccion de fraudes, solo respondes el json de respuesta,
BLOQUEADA para fraudulentas, PERMITIDA para no fraudulentas en JSON, para determinar si una
transacción es fraudulenta te basas en las reglas, el usuario te proporciona los datos en formato JSON.
Se requiere siempre todos los campos, caso contrario indica que no esta completa la información.
Simpre comprueba correctamente todas las reglas de manera exacta y responde de manera precisa con
la primera regla que se dispare, puesto que de ti depende que exista un fraude o no, asi que debes
responder correctamente.
Siempre responde solo el json de respuesta.
```

Nota: Este gráfico muestra el prompt utilizado para configurar el sistema de detección de fraudes, especificando cómo debe actuar la API en la identificación de transacciones fraudulentas y no fraudulentas.
Fuente: Elaborado por el autor.

**Tabla 1**

*Definiciones de las reglas antifraude.*

| Regla | Definición |
|---|---|
| **Regla 1** | No se permite la transacción si el delta_nav es menor en un 30% al delta_esperada. |
| **Regla 2** | No se permite la transacción si el monto_transaccion es un 50% mayor al monto_comun. |
| **Regla 3** | No se permite la transacción si el modelo de celular ha sido matriculado hace menos de 5 horas del mismo día de la transacción actual. |
| **Regla 4** | Si el monto es mayor a 8000 dólares, bloquea la transacción, porque es un monto límite puesto por el banco. |
| **Regla 5** | Si la transacción viene de Rusia, India, Alemania o España, no se permite la transacción, estos países no están permitidos. |

Nota: Esta tabla muestra las definiciones de las reglas antifraude utilizadas en el sistema.
Fuente: Elaborado por el autor.

**Tabla 2**

*Campos del JSON utilizado para autorizar una transacción.*

| CAMPO JSON | DESCRIPCIÓN |
|---|---|
| UBICACIÓN_ACTUAL | Ciudad de donde se transacciona |
| UBICACIÓN_ANTERIOR | Ciudad donde se transaccionó la última vez |
| MONTO_TRANSACCION | Monto de la transacción |
| MONTO_COMUN | Monto promedio de transacción |
| DELTA_NAV | Tiempo que se demora en navegar entre formularios, transacción actual |
| DELTA_ESPERADA | Tiempo promedio de navegación entre formularios |
| FECHA_MATRICULACION_DISPOSITIVO | Fecha en la que matriculó el dispositivo |
| HORA_TRANSACCION_ANTERIOR | Fecha y hora de la transacción anterior |
| HORA_TRANSACCION_ACTUAL | Fecha y hora de la transacción actual |
| MODELO_CELULAR | Modelo del celular, puede ser navegador web |
| HORA_CREACION_BENEFICIARIO | Fecha y hora de creación del beneficiario |

Nota: Esta tabla muestra los campos del JSON utilizados para autorizar una transacción.
Fuente: Elaborado por el autor.

**Tabla 3**

*Formato del JSON de respuesta parametrizado en el prompt.*

| CAMPO JSON | DESCRIPCIÓN |
|---|---|
| REGLA | Número de regla de coincidencia |
| ACCIÓN | PERMITIR o BLOQUEAR |

Nota: La tabla muestra el formato del json utilizado para parametrizar el prompt, especificando los campos que definen la respuesta que debe dar el modelo y la acción a tomar.
Fuente: Elaborado por el autor.

En esta investigación, Ollama se empleó como una herramienta que permite implementar inteligencia artificial en la terminal para el modelo LLaMA. Ollama facilita la ejecución de modelos de lenguaje a gran escala (LLMs) directamente en la máquina local (Ollama, s.f.). La plataforma utilizada fue un MacBook Pro con procesador M2 Pro y 16 GB de RAM para correr el modelo LLaMA3 con 8 mil millones de parámetros. En el caso de los modelos de OpenAI, se utilizó directamente su interfaz, integrable con un token en caso de ser necesario, como lo muestra la tabla 1.

Con la colaboración de la empresa ecuatoriana Dycotein, se compartieron conjuntos de datos en formato JSON para aplicar a las cinco reglas definidas y probar los modelos. Los datos se analizaron conforme a las pruebas, ingresando las tramas en cada uno de los tres modelos, para evaluar la respuesta de los mismos y validar su efectividad, ver tablas 2 y 3.

## 3 RESULTADOS

El conjunto de datos utilizado para probar el modelo tuvo como objetivo validar el porcentaje de efectividad de las reglas antifraudes y su eficiencia para los modelos GPT. Se

realizaron pruebas con 30 tramas por regla antifraude, representando transacciones fraudulentas. Estas pruebas se aplicaron para corroborar la capacidad de un modelo GPT de proporcionar una respuesta válida en la identificación de una trama fraudulenta, a partir del prompt y las reglas parametrizadas.

Las reglas redactadas para el prompt fueron las mismas validadas con la empresa Dycotein, que utiliza estas reglas en su sistema antifraudes implementado con funciones programáticas. Según la explicación del Gerente de Proyectos y Líder de Desarrollo, la implementación de estas reglas suele tomar alrededor de siete días, con cinco días adicionales para pruebas, antes de su activación en producción. Cada regla adicional suele tomar un promedio de dos días. En nuestro caso, solo se necesitó redactar un prompt adecuado y colocar las reglas en cuestión, para operar inmediatamente el modelo a través de las interfaces provistas por Ollama y OpenAI, tablas 4 y 5.

Los modelos LLaMA 3 de 8 mil millones (8B) y 70 mil millones (70B) de parámetros, disponibles públicamente, demostraron un rendimiento superior al de sus competidores en sus respectivas clases. Sin embargo, se utilizó el modelo 8B de manera local, ya que se ejecutaba de manera eficiente en el equipo utilizado para las pruebas, mientras que el modelo 70B resultó ser muy lento, ver tabla 6. Por esta razón, la comparativa resultó más eficiente con modelos en la nube, como los de ChatGPT de OpenAI (TextCortex, 2024).

En las pruebas, el modelo LLaMA 3 8B identificó correctamente un alto porcentaje de las tramas fraudulentas, mostrando una precisión comparable a la de las soluciones comerciales. ChatGPT de OpenAI también demostró una alta tasa de detección, aunque con algunas variaciones dependiendo de la complejidad de las reglas antifraude. Ambos modelos lograron respuestas coherentes y válidas en formato JSON, lo que confirma su viabilidad para la implementación en sistemas antifraude.

**Tabla 4**

*Resultados de ChatGPT 4 en la detección de fraudes.*

| Regla | Aciertos | Errores | Porcentaje |
|---|---|---|---|
| Regla 1 | 29 | 1 | 97% |
| Regla 2 | 28 | 2 | 93% |
| Regla 3 | 2 | 28 | 7% |
| Regla 4 | 30 | 0 | 100% |
| Regla 5 | 30 | 0 | 100% |
| Total | 119 | 31 | 79% |

Nota: La columna "Porcentaje" indica la precisión del modelo para cada regla individualmente, mientras que la fila "Total" muestra el porcentaje global de aciertos sobre el total de pruebas realizadas.
Fuente: Elaborado por el autor.

**Tabla 5**

*Resultados de ChatGPT 3.5 en la detección de fraudes*.

| Regla | Aciertos | Errores | Porcentaje |
|---|---|---|---|
| Regla 1 | 11 | 19 | 37% |
| Regla 2 | 3 | 27 | 10% |
| Regla 3 | 2 | 28 | 7% |
| Regla 4 | 17 | 13 | 57% |
| Regla 5 | 12 | 18 | 40% |
| Total | 45 | 105 | 30% |

Nota: La columna "Porcentaje" indica la precisión del modelo para cada regla individualmente, mientras que la fila "Total" muestra el porcentaje global de aciertos sobre el total de pruebas realizadas.
Fuente: Elaborado por el autor.

**Tabla 6**

*Resultados de LLaMA3 8B en la detección de fraudes.*

| Regla | Aciertos | Errores | Porcentaje |
|---|---|---|---|
| Regla 1 | 19 | 11 | 63% |
| Regla 2 | 7 | 23 | 23% |
| Regla 3 | 1 | 29 | 3% |
| Regla 4 | 5 | 25 | 17% |
| Regla 5 | 0 | 30 | 0% |
| Total | 32 | 118 | 21% |

Nota: La columna "Porcentaje" indica la precisión del modelo para cada regla individualmente, mientras que la fila "Total" muestra el porcentaje global de aciertos sobre el total de pruebas realizadas. Fuente: Elaborado por el autor.

Los resultados de las pruebas mostraron que la efectividad de los modelos LLaMA3 y ChatGPT 3.5 no fue adecuada para un sistema antifraudes, donde, según informó la empresa Dycotein, el porcentaje de aciertos debe ser superior al 96% para ser considerado efectivo. En el caso de estos modelos, su porcentaje de aciertos promedio no superó el 70% en ninguna de las reglas, presentando un promedio de aciertos muy bajo.

Para el modelo basado en ChatGPT4, los aciertos promedios fueron del 79%. Sin embargo, este resultado fue afectado por una regla específica que el modelo, con el prompt definido, no fue capaz de entender. Las otras cuatro reglas tuvieron porcentajes de aciertos superiores al 90%, alcanzando incluso en dos reglas una efectividad del 100%. Si se consideran únicamente las cuatro reglas que el modelo sí comprendió, el porcentaje de aciertos fue del 97.5%.

Estos resultados indican que, aunque ChatGPT4 muestra un potencial significativo, todavía existen áreas de mejora para alcanzar el nivel de precisión requerido para su implementación en sistemas antifraudes. La capacidad del modelo para entender y aplicar

correctamente todas las reglas antifraude es crucial para garantizar una alta efectividad y confiabilidad en entornos financieros.

## 4 CONCLUSIONES

Tomando en cuenta los resultados obtenidos, podemos concluir que, por el momento, los modelos con menor cantidad de parámetros, como LLaMA3 8B y ChatGPT 3.5, no son adecuados para su aplicación en sistemas antifraude. Sin embargo, modelos como ChatGPT 4 y sus equivalentes muestran resultados prometedores cuando se configuran con un prompt en unos pocos minutos.

Dado el acelerado desarrollo de modelos GPT y la incursión de varias empresas, como Google con Gemini, Facebook con LLaMA y OpenAI con ChatGPT, es de esperar que esta tecnología pueda ser utilizada para este propósito debido a la facilidad de configurar un prompt en lugar de código programático para sistemas antifraude bancarios (Google, 2023; Wired en Español, 2023).

Los resultados obtenidos con ChatGPT 4 muestran efectividad en reglas simples, aunque no en todo tipo de reglas, lo cual requiere más estudio. Una de las reglas antifraude, que representaba cierto grado de complejidad, no fue identificada por el modelo como trama fraudulenta.

Por lo tanto, los resultados son prometedores para un futuro cercano, pero por el momento, esta tecnología puede ser utilizada como un mecanismo de apoyo, no como un reemplazo de los modelos programáticos actuales, especialmente aquellos más efectivos basados en modelos predictivos.

Además, los sistemas actuales seguirán vigentes por algunos años. No obstante, no se descarta el avance en los modelos GPT, que, al alcanzar una mayor maduración, podrían revolucionar su aplicación en este tipo de programas por su facilidad de implementación y configuración, considerando que las empresas ya están trabajando en modelos más potentes y efectivos (Wired en Español, 2023). Es posible que con el tiempo, debido al desarrollo de este tipo de tecnologías apoyadas en propuestas de algunas empresas, se puedan tener instalaciones locales de modelos GPT para diferentes aplicaciones (Nvidia, 2024).

## REFERENCIAS

Google. (2023, 6 de diciembre). Gemini: The next generation of AI. Recuperado de https://blog.google/technology/ai/google-gemini-ai/

Monitor Plus. (s.f.). Parametrización de reglas para control en tiempo real. Recuperado de https://plus-ti.com/soluciones-prevencion-de-fraude-dbfd/

Nvidia. (2024, 10 de febrero). Chat with RTX: Nvidia's solution for local GPT installations. Recuperado de https://hipertextual.com/2024/02/chat-with-rtx-nvidia-chatgpt

Ollama. (s.f.). Available open-source chat models on common benchmarks. Recuperado de https://ollama.com/library/llama3

Sentinel. (s.f.). Perfiles transaccionales del comportamiento del cliente. Recuperado de https://soysentinel.com/industrias/bancos/sentinel-fraude-canales-digitales/

Superintendencia de Economía Popular y Solidaria. (2023). Norma de canales electrónicos. Recuperado de https://www.seps.gob.ec/wp-content/uploads/Resol-SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-009-NORMA_DE_CANALES_ELECTRONICOS.pdf

TextCortex. (2024). LLaMA 3 vs ChatGPT. Recuperado de https://textcortex.com/es/post/llama-3-vs-chatgpt

Wired en Español. (2023, 15 de marzo). Meta está entrenando un sucesor más potente que LLaMA 3. Recuperado de https://es.wired.com/articulos/meta-entrenando-sucesor-mas-potente-que-llama-3.