EVOLUCIÓN DE LA INTELIGENCIA ARTIFICIAL EN LA PREVENCIÓN DE FRAUDES BANCARIOS EN COLPATRIA

UNIVERSIDAD EAN

FACULTAD DE INGENIERÍA

ESPECIALIZACIÓN EN GERENCIA DE TECNOLOGÍA

SEMINARIO DE INVESTIGACIÓN

AUTORES

EDNA GERALDYN URICOECHEA SALAZAR
JENNY LORENA MONROY GOMEZ
JESSICA ANDREA URRUTIA BONILLA

TUTOR

LINA MARÍA CHACÓN RIVERA

BOGOTÁ, NOVIEMBRE 2024

TABLA DE CONTENIDO

Resumen

La inteligencia artificial ha transformado las empresas en muchos ámbitos, sin embargo, con el nacimiento de nuevas herramientas tecnológicas, surgen nuevas formas de ciberataque, el sector financiero es uno de los más afectados por los ciberdelincuentes y el banco Colpatria no es la excepción. Esta investigación busca explorar la evolución del uso de la Inteligencia Artificial en la detección y prevención de fraudes en el banco, para así conocer su nivel de madurez, beneficios y oportunidades de mejora. El presente estudio tiene un alcance cuantitativo y cualitativo, empleando una encuesta estructurada dirigida al área de fraude, la cual busca obtener una perspectiva desde el conocimiento de quienes cuidan el banco y su experiencia en la implementación de esta tecnología emergente en la organización.

Los resultados de esta investigación tienen un impacto relevante, que pueden ayudar a encaminar a la organización al alcance de sus objetivos estratégicos enfocados en ser un banco 100% digital.

Palabras clave: Inteligencia artificial, fraude bancario, prevención, riesgo, aprendizaje automático.

Planteamiento del problema

Antecedentes

Al pasar de los años se ha afrontado una evolución en el mundo financiero y empresarial pasando del papel, oficinas y escritorios a la inteligencia artificial, virtualidad, internet de las cosas, vehículos autónomos, robótica, nanotecnología, entre otras.

El mundo está impulsado en la cuarta revolución industrial y los más importante es saber cómo hacer buen uso de esta tecnología, las entidades bancarias se han obligado a buscar las mejores estrategias de innovación tecnológica para velar por la protección de sus datos y evitar los fraudes informáticos a los que día a día están expuestos.

En Colombia no es favorable el horizonte de la seguridad informática con relación a los fraudes, cada año América Latina pierde 90 millones de dólares para afrontar los daños causados por los ciberdelitos, según datos brindados por el Registro de Direcciones de Internet de América Latina y Caribe, los países más afectados son Brasil y México, seguidos por Colombia, Argentina, Perú y Ecuador (Equipo de Contenido, 2023, párr. 1). Ahora bien, ¿Cuáles son los fraudes más frecuentes?

El cambiazo. "según el informe de Asobancaria el cambiazo representa un 46,2 % de los casos reportados" (Lesmes, 2024, párr. 2), el cual consiste en el cambio de su tarjeta débito o crédito por otra falsa, la estrategia de los delincuentes está basada en el poder del engaño, ofreciendo ayuda a la víctima, lo confunden logrando cambiar rápidamente su tarjeta y luego cuando la persona intenta continuar con su transacción, el delincuente en colaboración de su cómplice observa la clave secreta. Seguidamente ya con su tarjeta y clave proceden a retirar su dinero.

Por esta razón, es importante tener en cuenta las siguientes sugerencias expuestas por, DataCrédito Experian (2024) al momento de realizar retiros un cajero automático:

- Cubrir teclado al momento de digitar tu clave en cajeros automáticos y/o establecimientos de comercio.
- No aceptar ayuda o sugerencias de extraños cuando se esté retirando efectivo.

- Cambiar la clave con regularidad.

El phishing, es la segunda modalidad más común con 20% de los casos. Consiste en hacer el diseño páginas web, correos electrónicos, perfiles de redes sociales falsos, para suplantar a entidades de confianza y así solicitar datos financieros a los clientes**.** Los ataques de phishing se dividen en diferentes tipos: el correo de phishing, el spear phishing, el smishing, el vishing y el whaling (Trend Micro Incorporated, 2024).

"El término phishing en inglés se pronuncia igual que la palabra fishing, literalmente pescar. Un ataque de phishing tiene como objetivo engañar al destinatario para que haga clic y descargue e instale archivos malintencionados que logran revelar información privada (proofpoint, 2024, párr. 1).

Unas de las estrategias más empleada de los ciberdelincuentes es suplantar marcas conocidas, ya que, trasmiten confianza a sus víctimas según la publicación de, Forbes Staff (2024) están: Microsoft (57%), Apple (10%), LinkedIn (7%), Google (6%), Facebook (1.8%), Amazon (1.6%), WhatsApp (0,8%), Instagram (0,7%) (proofpoint, 2024, párra. 8).

Es importante que, para la prevención de los ataques de phishing, se requiere una fuerte formación y entrenamiento de los empleados de la empresa para reconocer las señales de advertencia y sistemas de ciberseguridad robustos, es tarea de cada persona hacer uso correcto de la información.

La suplantación, en el tercer lugar con un 9,2%, se usa para apoderarse de la identidad de un usuario financiero con el propósito de obtener productos financieros en cualquier ciudad del país (Héctor José García Santiago, 2021, párr. 1), retirar dinero de las cuentas, adquirir servicios como por ejemplo planes de Telefonía Móvil o fija, solicitar tarjetas de crédito en su nombre.

El hurto por celular representa el 4,7 %, el menos frecuente de fraudes. Esta modalidad consiste en usar la información financiera disponible en los teléfonos hurtados (Barrera Perico, 2024, párr. 1). Una vez que accedan a las APP bancarias, los delincuentes cambian contraseñas en las cuentas, autorizan retiros de dinero, de compras en línea y realizan adelantos de nómina

Es así, como surge la necesidad del uso de la inteligencia artificial por parte de las entidades bancarias al rededor del mundo, un 83% de los bancos europeos la usan con diferentes finalidades y se estima que en 2025 todos implementarán soluciones basadas en esa tecnología (Carbó Valverde et al., 2023, párr. 1). Un ejemplo es el Proyecto Aurora del Centro de Innovación del Banco de Pagos Internacionales de suiza, que demostró que las redes neuronales, pueden contribuir a detectar el lavado de dinero identificando patrones y anomalías en las transacciones que los métodos tradicionales no pueden identificar (Kearns Jeff, 2023, párr. 20).

En Colombia el panorama es similar, según el Informe de Gestión Gremial de Asobancaria 73% de las entidades financieras, ha implementado nuevas tecnologías en sus operaciones, destacando la inteligencia artificial y el big data como las más populares en el sector (Moreno, 2024, párr. 12).

Descripción del problema

La tecnología ha revolucionado el sector financiero, ofreciendo un sinfín de oportunidades para la optimización de procesos y mejoras en el servicio, pero también ha dado pie para que surjan nuevas formas de fraude, lo cual ha puesto en un riesgo latente a las entidades financieras; Según indica Asobancaria “se ha registrado 50 entidades financieras afectadas por ciberataques y más de 240.000 quejas por fraudes tecnológicos” (La Nota

Económica, 2024, párr. 2). A nivel nacional en el sector financiero se detectan más de 40 ataques informáticos por segundo.

Ahora bien, si la tecnología enfrenta a todo tipo de riesgo, también brinda soluciones amplias que provienen del mismo avance al que se enfrenta, la inteligencia artificial ha marcado un antes y un después en el mundo y precisamente es una de las que ha permitido a los bancos fortalecer la prevención de fraudes. Su implementación y operación presentan desafíos significativos, ya que la integración entre tecnología avanzada y los sistemas actuales bancarios, pueden generar un cierto vacío donde se puede abrir más las puertas para los delincuentes que buscan ingeniosamente espacio para realizar sus actos fraudulentos.

Actualmente, el sector bancario está expuesto a grandes retos en detectar fraudes, con el aumento de la tecnología se acrecientan los riesgos y aún más cuando los bancos dependen de herramientas obsoletas y poco eficientes para analizar datos y tomar decisiones.

El uso de la inteligencia artificial como apoyo para detección de riesgos, es cada vez más frecuente en bancos del exterior, sin embargo, su adopción en Colombia no es la esperada, lo que genera inquietudes en cuanto a la eficiencia, seguridad y beneficios en su implementación en el Banco Colpatria.

Pregunta de investigación

Teniendo en cuenta el creciente auge del uso de la inteligencia artificial en las entidades bancarias del mundo, se debe asegurar una automatización responsable de los procesos y que sirvan de guía para implementar este tipo de soluciones de una forma adecuada (Rodríguez de las Heras Ballell, 2022, p. 93), así mismo determinar su nivel de madurez y confianza, con el fin de identificar oportunidades de mejora e implementación en otras áreas no exploradas del sector financiero.

Dado lo anterior, con esta investigación buscamos resolver ¿Cuál ha sido la evolución del uso de la inteligencia artificial en la detección y prevención de fraudes en Colpatria?

Objetivos

Objetivo general

Identificar la evolución del uso de la Inteligencia Artificial en la detección de fraudes bancarios en Colpatria.

Objetivos específicos

- Conocer el nivel de madurez con el que cuentan las diferentes implementaciones realizadas de IA en la organización.
- Explorar los diferentes beneficios del uso de la IA en las aplicaciones del banco.
- Identificar el nivel de confianza que ofrecen la solución de IA para la detección de fraudes bancarios.
- Evaluar las ventajas y desventajas de la utilización de soluciones con IA en el banco.

Viabilidad del problema

Justificación

La detección de fraudes bancarios se ha convertido en un reto para las entidades financieras; según informes, las pérdidas económicas por estafas bancarias ascendieron a 500.000 millones de dólares el año pasado, lo que pone en riesgo la estabilidad financiera de las organizaciones y por ende la economía del país (Forero, 2024, p. 1).

La Inteligencia Artificial (IA) ha surgido como una herramienta novedosa para poder afrontar esta problemática, ya que permite analizar cantidades de datos ilimitados e identificar patrones complejos. “El gran impacto de la inteligencia artificial en el sector bancario es

evidente porque ya está comprobado que facilita el proceso de automatización, mejora la experiencia al cliente y mitiga un sin número de riesgos" (Pragma, 2024, p. 1). Sin embargo, las tecnologías emergentes se encuentran en constante en evolución, por lo cual, es importante investigar cómo se utiliza actualmente para minimizar el riesgo bancario, su eficiencia y posibles mejoras, facilitando su implementación dentro del Banco.

El diseño de esta investigación está basado en la recopilación de datos mixtos, con un análisis de datos cuantitativos y cualitativos, con el fin de brindar la información necesaria para que Colpatria mejore la forma en la que ofrece sus servicios, esto desde la perspectiva operacional hasta la experiencia del cliente, por esta razón la justificación de la investigación se divide en 4 partes:

Eficiencia Operacional: A partir de la investigación se tendrá la información suficiente para la implementación de nuevas soluciones que permitan al equipo de trabajo contar con todos los insumos necesarios para generar estrategias y tomar decisiones de alta complejidad, optimizando la ejecución de procesos manuales.

Competitividad: La organización contará con una recopilación de mejores prácticas en la adopción de la Inteligencia Artificial en los procesos de detección de fraudes, lo que permitirá ofrecer soluciones más sofisticadas y eficientes, así alcanzando posiciones competitivas en el mercado.

Manejo del riesgo: Al conocer los fraudes que han surgido a través de los años y los delitos cibernéticos a los que las organizaciones están expuestas, el Banco pueden anticiparse con las nuevas tecnologías, para fortalecer su seguridad y así brindar tranquilidad a los clientes al usar la banca digital.

Contribución a las teorías de la IA: La investigación espera aportar al avance del conocimiento sobre la detección de fraudes con el uso de la IA en la banca, proporcionando información real sobre su efectividad, beneficios, ventajas y desventajas y a su vez brindando datos concretos que puedan soportar la teoría de la IA, la teoría de la detección de anomalías y la teoría de toma de decisiones.

Los resultados de la investigación permitirán a Colpatria crear oportunidades de innovación en su oferta de productos y servicios, generando confianza y seguridad a sus clientes y favoreciendo la percepción de estabilidad en el entorno financiero, lo cual es fundamental para mantener los procesos operativos a la vanguardia, seguros, transparentes y aumentar la satisfacción de los clientes, pieza clave para que puedan ser competitivos en un mercado en constante evolución.

1. Marco teórico

¿Qué es la detección de fraude?

La detección de fraude es el sistema para identificar y bloquear actividades sospechosas para evitar poner en riesgo el negocio, involucra varias industrias, incluidos servicios bancarios, financieros, seguros, atención médica, agencias gubernamentales, entre otras. Antes de que las computadoras y las tecnologías de la información fueran inteligentes, el método tradicional de detectar fraude era analizar datos estructurados contra reglas capaces de detectar escenarios fraudulentos obvios, requerían investigaciones exhaustivas, lo que

implicaba un considerable esfuerzo manual y demandaba una gran cantidad de tiempo (uFlow LLC, 2024).

Evolución de los sistemas en detección de fraudes bancarios

La evolución de la Inteligencia Artificial ha dado grandes pasos en los últimos años, incorporando algoritmos de aprendizaje automático, el procesamiento de grandes volúmenes de datos, análisis predictivos y detección de anomalías, ya que, con los años, los delitos financieros se vuelven más sofisticados, robustos y complejos de detectar.

Aunque la implementación de estas tecnologías no está exenta de desafíos, los beneficios superan las mayores dificultades. A medida que la IA continúa evolucionando, su función en la guerra para combatir el fraude financiero será cada vez más crucial, proporcionando a las instituciones la capacidad de proteger mejor sus activos y a sus clientes (IT-NOVA, 2024, párr. 5)

A continuación, se describe una línea cronológica de los diferentes sistemas de detección de fraudes bancarios más relevantes:

Década de 1990 – 2000. **Sistemas basados en reglas**, es el tipo de sistemas más tradicional, su uso estaba basado en reglas predefinidas con críticos humanos de experiencias pasadas y en la lógica, por lo cual únicamente eran útiles para identificar patrones conocidos, no para detectar nuevos tipos de patrones de fraude (FasterCapital, 2024).

Década de 2000. Sistemas estadísticos tradicionales, surge de la necesidad y dificultad de manejar alto volumen de datos, por esta razón los bancos implementaron sistemas estadísticos como análisis de correlación, para identificar comportamientos atípicos, por lo tanto, estos sistemas tenían ventajas para encontrar relaciones complejas con diferentes variables, como limitante estos sistemas aún no aprendían de manera autónoma por lo tanto

siempre se necesitaba la intervención humana para alimentar las bases de datos con nuevos patrones de fraudes (Grapheverywhere, 2024).

Década de 2010. Sistemas de aprendizaje automático, las ventajas de estos sistemas es que integran algoritmos de aprendizaje automático, los cuales aprenden de datos históricos entrenando el motor del machine learning con casos de fraude y no fraude anteriores para evitar falsos positivos y mejorar la precisión de las reglas de riesgo, como indica (Florian Tanant, 2024, párr. 2). Se pueden implementar reglas para bloquear o permitir acciones de usuario, como accesos sospechosos, robos de identidad o movimientos inusuales.

Acorde a un estudio realizado por científicos en computación de la Universidad de Yakarta, los algoritmos de machine learning alcanzaron una exactitud por encima del 96% en la reducción del fraude en los negocios de comercio electrónico (Florian Tanant, 2024, párr.12).

Década de 2010. Sistemas de redes neuronales profundas y aprendizaje profundo, es el campo de la inteligencia artificial que enseña a las computadoras a procesar datos de una manera que simulan el cerebro humano, pueden reconocer patrones de datos, como imágenes, textos, sonidos complejos, para generar información y predicciones precisas (Amazon Web Services, 2023, párr. 1).

Herramientas Innovadoras

“De acuerdo con el más reciente informe de Gestión Gremial de Asobancaria, el 73% de las entidades financieras han implementado nuevas tecnologías en sus operaciones” (Equipo editorial Capital Inteligente Grupo Bancolombia, 2024, párr. 6), para maximizar la prevención de riesgos. Según estudios realizados en conjunto con Finnovista , Colombia Fintech las herramientas más innovadoras que lideran los sistemas de pago y transacciones en Colombia son las siguientes:

API, (Interfaz de programación de aplicaciones) “es un conjunto de reglas o protocolos que permiten que las aplicaciones de software se comuniquen entre sí para intercambiar datos, características y funcionalidades” (Michael Goodwin, 2024, párr. 1), permiten compartir solo la información necesaria, ocultando otros detalles internos del sistema. Su implementación en el sector financiero es usada para sincronizar la base de datos del banco con cualquier aplicación o programa y así garantiza el tráfico de información segura sin involucrar terceros.

Cuando un banco desarrolla sus propias APIs puede enlazarlas con otras y así tener un crecimiento en el sistema, adicional son un canal excelente para llevar a cabo todo tipo de estrategias comerciales.

Biometría, hace parte de las tecnologías de identificación automática de individuos a partir de características físicas y de comportamiento como el reconocimiento facial, de voz, lectura huellas dactilares o del iris, para verificar la identidad de los usuarios, reduciendo el riesgo de accesos no autorizados (iuvity, 2020).

Actualmente la más usada por los bancos es la biometría 3D, puede detectar identidades falsas con mayor efectividad y realizar pruebas de vida de manera rápida, sencilla, sin afectar negativamente la experiencia del usuario (Digital360 Iberia, 2023, párr. 1).

Así, la integración de la biometría asegura la protección de los datos en las transacciones, fortaleciendo la confianza para que las personas realicen actividades como compras en línea o pagos digitales sin preocuparse por la posible suplantación o robo de identidad.

Billeteras digitales, se han convertido en un recurso cotidiano para agilizar la gestión financiera y usar menos el dinero en efectivo al facilitar las transacciones desde los teléfonos

móviles, para realizar pagos, transferencias y consultas financieras en cualquier momento y lugar.

En Colombia, estos servicios han impulsado la inclusión financiera de miles de personas que no contaban con acceso a la banca tradicional. En la actualidad, existen más de 12 billeteras digitales, impulsadas por instituciones tradicionales, bancos y por startups que lideran en el mercado según (Startups Latam, 2023) las más usadas son:

- ***Nequi**,* pertenece al grupo Bancolombia, los usuarios crean la cuenta desde su celular y pueden enviar pagos directos a otro móvil, realizar pagos por lectura de QR, recargar nuevo saldo desde PSE, creación de bolsillos, colchones y hasta solicitar créditos sin costos adicionales.
- ***Daviplata,*** es del Banco Davivienda y está en uso cuatro años antes que la aplicación de Nequi. Su funcionalidad es muy similar en cuanto a los servicios prestados a los usuarios y no es necesario tener una tarjeta o cuenta con la entidad financiera, solo es necesario crear la cuenta desde el dispositivo móvil.
- ***Dale*****,** pertenece al portafolio del Grupo Aval, el beneficio para los usuarios es que pueden tener privilegio a las preventas de los conciertos y espectáculos.
- **Tap to Phone**, también llamado toque al teléfono o pago sin contacto, como solución facilita la experiencia del usuario y la del comerciante al aceptar pagos con tarjetas de crédito, débito, billeteras digitales, tabletas, relojes inteligentes, códigos QR, links de pago, entre otros. (Banco Davivienda S.A., 2024). ¿Cómo funciona? Al realizar una compra, los clientes deben acercar el medio de pago de su preferencia al celular para realizar el pago, dando por hecho que el celular tiene “tecnología (NFC) Near Field Communications, “tecnológica de comunicación inalámbrica que

permite intercambiar información a corta distancia entre varios dispositivos electrónicos” (Dipole RFID, 2024, párr. 1).

Tokenización y claves dinámicas, “es un proceso a través del cual se sustituyen datos sensibles por símbolos de identificación únicos que conservan la información original, pero no comprometen la seguridad de los datos primarios” (Universidad Europea, 2023, párr. 2).

Con esta tecnología, los usuarios pueden confiar en que sus credenciales bancarias y datos personales están protegidos, mediante la generación de un código único que se habilita por un determinado tiempo y es aleatorio para realizarla cada transacción, o confirmación de un pago.

Uso de la inteligencia artificial en el sector bancario

Automatización de procesos, la implementación de la inteligencia artificial en la automatización, es utilizada para facilitar la toma de decisiones en las empresas, generalmente es usada para recopilar, procesar y analizar datos de forma continua, lo que permite mejorar la eficiencia operativa, eliminando la ejecución manual de tareas repetitivas y minimizando el riesgo de errores, “Al integrar la IA en la automatización, los sistemas pueden aprender y tomar decisiones basadas en datos, contexto y patrones” (McClintock, 2023, párr. 18).

En las entidades financieras se utilizan principalmente en procesos de ventas digitales, en el área de atención al cliente con chatbots y análisis de datos para ofertas personalizadas. Según Ruíz ((2020) los principales beneficios del uso de procesos automatizados son la reducción de costos, optimización de tiempos de ejecución en los procesos, aumento de la productividad y mejora de la experiencial al cliente.

Análisis predictivo, De acuerdo con SafetyCulture (2024) el uso del aprendizaje automático, análisis de datos, estadística y modelado de datos, busca obtener resultados combinando información actual e histórica, es utilizado principalmente para identificar riesgos y con toda la información a su disposición encontrar la forma más adecuada de mitigarlos. “La inteligencia artificial está transformando el panorama del marketing” (Benavidez et al., 2024, p. 13).

Seguridad y prevención del fraude, el uso de algoritmos de aprendizaje automático permite analizar grandes cantidades de información, con el fin de identificar anomalías y patrones, utilizados para cometer actos fraudulentos, para las entidades financieras es indispensable disminuir el riesgo por lo que se utilizan técnicas como las redes neuronales, árboles de decisión y máquinas de soporte vectorial (Borrero-Tigreros & Bedoya-Leiva, 2020, p. 39). En los bancos se utiliza principalmente para detectar la solvencia del cliente, el comportamiento de pago de los clientes, detección de fraude en solicitudes de crédito bancario, procesos de autenticación a canales, en la apertura de productos financieros en línea y en el análisis de transacciones sospechas en tiempo real, que según Fintech Américas (2023) permitirá no solo proteger los activos financieros de las entidades sino aumentar la confianza de los clientes.

Inteligencia Artificial en la banca colombiana

Implementación de la IA en el Banco de Bogotá, en el año 2017 el Banco de Bogotá pone a disposición de sus clientes, un modelo digital basado en el uso de inteligencia artificial para los procesos de apertura en línea de productos como cuentas de ahorro, solicitud de tarjetas de crédito, créditos hipotecarios e inversión, “Actualmente, en el Banco de Bogotá el 80% de la apertura de nuevas cuentas de ahorro y el 88% de las ventas de productos de crédito, se realizan de manera digital”(Inteligencia Artificial Colombia, 2022, párr. 4).

Centro de Competencias en IA de Bancolombia, se estableció en colaboración con IBM, cognitiva y Bancolombia para realizar investigación y desarrollo de soluciones con Inteligencia Artificial para la mejora de los procesos financieros, con el fin de aumentar la satisfacción de sus clientes y agilizar los servicios que ofrecen de forma digital. Uno de los resultados más significativos de este centro es Tabot, un asistente virtual entrenado con 70 habilidades basados en inteligencia artificial, que le permite interactuar con los clientes haciendo uso de un lenguaje natural, ofreciendo información sobre consultas de productos, ubicación de cajeros, guía en la apertura de productos, entre otras, impulsando soluciones novedosas que apalanquen el desarrollo de las personas y las empresas (Dirección Corporativa de Comunicaciones y Reputación, 2018).

Scotiabank Colpatria lanza plataforma global con IA, el banco ofrece a sus clientes consejos financieros personalizados de acuerdo con sus necesidades, haciendo uso de analítica de datos y patrones de operaciones de aprendizaje automático, para crear aplicaciones agiles e intuitivas, las cuales han sido implementadas en varios modelos operacionales de la banca personal.

Con estas soluciones se busca impulsar la confianza de los clientes y la transparencia en la venta de productos, teniendo en cuenta el nicho de mercado y las capacidades económicas de los usuarios (Scotiabank Colpatria, 2020).

Daviplata con IA, la billetera digital del banco Davivienda hace uso de tecnologías con Inteligencia Artificial como ChatGPT y Gemini, para optimizar sus procesos financieros y la comunicación con los clientes, ya que les permite realizar sus transferencias, pagos, recargas y consultas de una forma ágil, simple y segura, también se implementaron comandos de voz y chat, ofreciendo una experiencia novedosa al momento de realizar cualquier tipo de pago, el

cliente puede guiar su transacción si lo desea a través de instrucciones por voz o escritas(Redacción Tecnología, 2024).

Detección de fraudes en Colombia a partir de la IA

Desde la llegada de la IA a Colombia, formalmente en el 2017, en la ciudad de Medellín se abrió el Centro para la Cuarta Revolución Industrial, en el cual impulsan proyectos manejados con Inteligencia Artificial, el país ha querido adoptar esta tecnología en pro de su beneficio (Nuva, 2022)

A continuación, se listan algunos ejemplos de las campañas que promueve el gobierno para fomentar el uso de la inteligencia artificial en distintos ámbitos:

Women Training Series: programa realizado por el gobierno para todas las mujeres colombianas en donde son capacitadas en ciberseguridad e inteligencia artificial. (Gobierno digital, 2024)

ChatBot "Tavot": durante la campaña del candidato a la alcaldía de Bogotá Gustavo Bolívar implemento un chatbot, el cual ofrece diferente información de la campaña que permite a los usuarios sentirse parte de todo el programa de candidato. (IA Colombia, 2023)

Hoja de Ruta en Inteligencia Artificial: Documento estratégico que guiará el desarrollo todo el marco conceptual del uso de la IA en Colombia, promoviendo la tecnología, pero sobre una base ética y sostenible. (Miniciencias, 2024)

Siguiendo el contexto anterior a nivel de la banca colombiana, Bancolombia, Davivienda, BVBA, entre otros, usan las IA como mecanismo de defensa para la detección de fraudes, como las siguientes soluciones:

Análisis predictivo para identificación de patrones: Mediante la IA se realiza un análisis de gran cantidad de datos en tiempo real para así identificar patrones extraños en transacciones financieras. (Fintech Americas, 2023b)

Detección de anomalías con Machine Learning: Al usar esta solución en la vigilancia de transacciones, se pueden detectar de forma rápida actividades inusuales, lo que permite prever la amenaza y actuar de manera rápida.

Herramientas de procesamiento de lenguaje natural con IA generativa: La implementación de estas soluciones fortalece la seguridad en la interacción con clientes, ya uno de sus usos es el análisis de conversaciones para detectar posibles fraudes financieros.

Así mismo las siguientes entidades financieras aliadas usan la IA para la prevención y detección de fraudes financieros:

MasterCard utiliza una herramienta predictiva basada en la IA que permite escanear los datos transacciones de las tarjetas de crédito alertando nuevos y complejos patrones de fraude. (Mastercard, 2024)

Cencosud: Usan la verificación de identidad a través de la biometría protegiendo así la integridad de las transacciones y la privacidad de datos. (Fintech Americas, 2023)

Marco Institucional

Historia

En sus inicios, Colpatria fue un grupo que se focalizaban en la capitalización en Colombia, años después se integró con el mercado de inversiones y es hasta el año de 1969 cuando el grupo adquiere la mayoría de las acciones del Banco de la Costa y con esta operación surge el

banco Colpatria, en 1997 se da la constitución legal del Banco Multibanca Colpatria (Colpatria, 2024.)

Por último, en el 2017, Scotiabank se fusionó con el Banco Colpatria, integrándose para ofrecer soluciones financieras acordes a las necesidades y alcance global (Colpatria, 2024.)

Acerca de Colpatria

Su sede principal se encuentra en la ciudad de Bogotá D C, Colombia, en el icónico Edificio Colpatria, con una red a escala nacional de más de 178 oficinas y más de 316 Cajeros Automáticos (Colpatria, 2024.)

Misión

En la página de Colpatria se describe la misión de la siguiente manera: (Colpatria, 2024.)

> “Ser reconocido como un Banco claro y sencillo que brinda soluciones financieras flexibles, fáciles y rápidas a los colombianos trabajadores y a las medianas y pequeñas empresas para su continuo crecimiento” (párr 4).

Visión

Así mismo la misión la describe de la siguiente manera: (Colpatria, 2024.)

> “El Banco Scotiabank Colpatria S.A. tiene como visión el siguiente postulado:
> Cumpliremos con la obligación de satisfacer las expectativas de nuestros clientes con el concurso de un excelente equipo humano” (párr 5).

Objetivos estratégicos de la organización

Para (Colpatria, 2024.) los objetivos estratégicos son los siguientes:

- Ofrecer productos, servicios y experiencias que ayuden a los clientes a preparar su futuro, hacemos posible lo posible.
- Generar practicas sostenibles que ayuden a las comunidades mejorando la economía en su conjunto.
- Ayudar a nuestros empleados a construir sus futuros en un entorno de aprendizaje inclusivo.
- Generar ganancias para los accionistas, contribuyendo con la economía adoptando una perspectiva a largo plazo. (párr 6)

Metodología de investigación

El uso de una metodología mixta (cuantitativa y cualitativa) en el análisis de datos para estudiar la evolución de la IA en la detección de fraudes bancarios en Colpatria ofrece una perspectiva integral al combinar las fortalezas de ambos enfoques. Esta combinación permite obtener datos numéricos sólidos (cuantitativos) mientras se exploran las experiencias, percepciones (cualitativos) en la implementación y evolución de tecnologías de Inteligencia artificial del sector bancario. A continuación, algunas de las razones por las que se elige esta metodología:

Exploración de perspectivas y experiencias complejas: La evolución y adaptación de la IA implica una serie de factores complejos, como la adaptación al entorno digital, seguridad de datos, la continuidad del negocio y la gestión de recursos tecnológicos. Con la metodología mixta se pretende captar una visión detallada de las vivencias de los actores claves en el área evaluar.

Participación de los interesados: Es esencial la participación de los interesados para obtener una visión integral y completa sobre el tema. Son individuos o grupos que están directa

o indirectamente involucrados en el uso y la implementación de la tecnología de IA. Expresar sus opiniones, sus preocupaciones de manera abierta, detallada, saber si se ajusta o se enfrenta con la cultura existente y fomentar una mayor participación y compromiso en el proceso de toma de decisiones y los buenos usos para la detección de fraudes Bancarios en Colpatria.

Comunicación efectiva de resultados: Los resultados cualitativos y cuantitativos suelen ser más efectivos para la comunicación interna, asegurando que los hallazgos sean comprendidos, valorados y utilizados por todos los actores involucrados.

Alcance es descriptivo, ya que se especifica propiedades y características del proceso de la IA en Colpatria, se seleccionarán participantes del área de fraude, para garantizar diferentes puntos de vista.

El estudio se centrará en conocer como ha sido la evolución de la Inteligencia Artificial en la prevención de fraudes en la entidad y su proceso de adopción considerando la seguridad de datos y la continuidad de las operaciones. Se explorarán aspectos específicos de los beneficios que esta tecnología ha traído y traerá.

Diseño no experimental, debido a que se miden las variables en su contexto natural para analizarlas, por lo tanto, se diseñó una encuesta estructurada a expertos del área de fraude para comprender y explorar perspectivas, experiencias y desafíos con respecto a la adopción de la IA en la detección de fraude. Se realizará un análisis de contenido de las encuestas realizadas a los participantes claves.

Definición de Variables

Luego del análisis realizado para la identificación de los atributos que se medirán durante la investigación, a continuación en la tabla 1, se detallarán las variables seleccionadas, junto con su definición conceptual, definición operacional y dimensiones aplicables al uso de la inteligencia artificial en la detección y prevención de fraudes en el banco Colpatria.

Tabla 1

Definición de variables de Investigación

Variable	Definición Conceptual	Definición Operacional	Dimensiones
Uso de IA	Cantidad de aplicaciones de Colpatria que cuentan con Inteligencia Artificial	Encuesta área de Fraude. Pregunta abierta para determinar cantidad	Grado de utilización de la IA
Funcionamiento de la IA	Percepción del funcionamiento y estabilidad de las aplicaciones con IA en producción	Encuesta área de Fraude. Escala de 1 a 10, donde 1 indica "Muy Inestable" y 10 indica "Muy Estable"	Estabilidad de las aplicaciones
Fraudes detectados	Tasa de fraudes bancarios evitados con IA	Encuesta área de Fraude. Pregunta abierta para determinar cantidad	Beneficios uso de la IA
Fraudes materializados	Tasa de fraudes materializados según su tipo	Encuesta a Empleados área de Fraude. Pregunta abierta	Fraudes no cubiertos
Confianza	Percepción nivel de confianza con el uso de IA	Encuesta área de Fraude. Escala de 1 a 10, donde 1 indica "Poco confiable" y 10 indica " Muy confiable".	Confianza en el uso de la IA
Ventajas	Percepción de las ventajas del uso de la de la IA en la organización	Encuesta a Empleados área de Fraude. Selección de opciones múltiples	Eficiencia Productividad Innovación Seguridad
Desventajas	Percepción de las desventajas del uso de la de la IA en la organización	Encuesta a Empleados área de Fraude. Selección de opciones múltiples	Dificultades técnicas Seguridad Económicas

			Experiencia Usuario
Oportunidades	Percepción de las nuevas herramientas con IA que se pueden implementar en el banco	Encuesta a Empleados área de Fraude. Pregunta abierta	Oportunidades de implementación.

Nota: Elaboración propia

Población y muestras

Especificar las personas que serán medidas y analizadas es necesario para determinar la población y la muestra. Si bien Colpatria cuenta con más de cinco mil empleados, los cuales pertenecen a 2 sectores macro, operaciones y tecnología; La investigación se centrará en un área específica: Equipo Fraude perteneciente al sector tecnológico del banco.

El área de Fraude tecnológico cuenta con 11 empleados, los cuales están divididos entre seguridad, equipo de operaciones y equipo de desarrollo, por lo tanto, se utilizará el Censo trabajado con encuestas, con preguntas de selección múltiple y abiertas, al ser una población pequeña se recopilará información cualitativa y cuantitativa, con las encuestas estructuradas.

Las muestras utilizadas serán relevantes para las conclusiones y los datos que se requieren recopilar.

Selección de métodos o instrumentos para recolección de información

La recolección de información se realizará por medio de una encuesta que se llevará a cabo con los empleados del área de fraude del banco Colpatria, cada encuesta se compone de 13 preguntas, donde se recopilará información cuantitativa y cualitativa, con opciones de respuestas abiertas o de selección múltiple, permitiendo un mejor entendimiento y detalle acerca de la evolución de la IA en la detección de fraudes en el banco Colpatria.

Técnicas de análisis de datos

El análisis cuantitativo se centra en examinar volúmenes de datos relacionados con el número de aplicaciones empleadas, tasa de éxito de prevención, nivel de confianza, credibilidad del Banco al incorporar Inteligencia Artificial para detectar fraudes. Estos datos proporcionan patrones, tendencias y relaciones estadísticas que muestran cómo las nuevas técnicas han impactado en el Banco Colpatria.

En la metodología cuantitativa como técnica de análisis de datos se destaca estadísticas básicas como frecuencia de fraudes, promedios, medianas y tasas de éxito de las herramientas de IA. Estas estadísticas ayudan a identificar tendencias iniciales en el comportamiento fraudulento y cómo han evolucionado las tasas de detección a lo largo del tiempo.

Como complemento al estudio se incorpora el análisis cualitativo que explora el contexto, los desafíos y las experiencias humanas en la adopción y desarrollo de la IA. Es interpretativo y se enfoca en entender el "por qué" detrás de los secesos. Estos métodos proporcionaron una comprensión interna de las preocupaciones y percepciones centrando en el grupo de fraude.

La combinación de estas y técnicas de análisis proporcionó una comprensión integral del proceso, identificar posibles desafíos, maximizar oportunidades, mitigar riesgos y tomar decisiones estratégicas para una transición exitosa hacia las nuevas tecnologías emergentes en el Banco Colpatria.

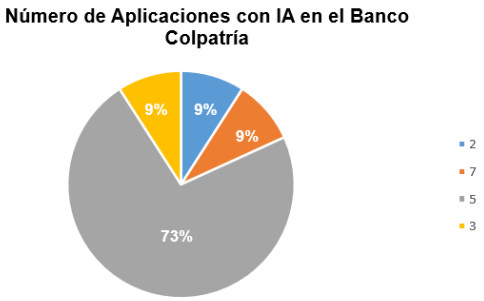
Análisis y discusión de los resultados

A continuación, se relacionan las respectivas preguntas realizadas junto con los resultados obtenidos:

1. **¿Relacione la cantidad de aplicaciones del banco Colpatria que cuentan con la tecnología de Inteligencia Artificial?**

Figura 1

Numero de aplicaciones con IA en el banco Colpatria



Nota: Elaboración propia

En el Banco Colpatria actualmente, como aprecia en la figura 1, según los resultados obtenidos el 73% de los funcionarios encuestados indicaron que 5 aplicaciones hacen uso de la inteligencia artificial para la detección de fraudes bancarios, las cuales representan tecnologías claves en la operación del banco. Igualmente se observó que el 27% de los encuestados pertenecen al frente operativo, los cuales desconocen las aplicaciones internas de tecnología que usan IA.

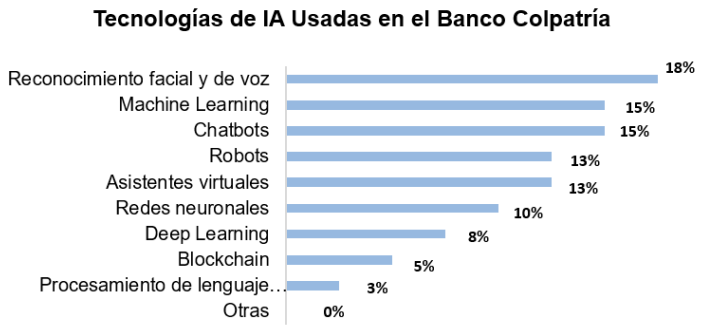
2. **¿Cuáles tecnologías de inteligencia artificial son usadas en el banco Colpatria?**

a. Chatbots
b. Asistentes virtuales
c. Machine Learning
d. Deep Learning
e. Robots
f. Reconocimiento facial y de voz
g. Procesamiento de lenguaje natural
h. Redes neuronales
i. Blockchain

j. Otra ¿Cuál?

Figura 2

Tecnologías de IA usadas en el banco Colpatria



Nota: Elaboración propia

El reconocimiento facial y de voz son las tecnologías de IA con el mayor uso en el Banco Colpatria, en la figura 2 se representa el 18% del total, igualmente se resalta con un 15% el manejo de machine learning y ChatBots, mientras que tecnologías como blockchain y procesamiento de lenguaje natural muestran un uso menor. Estás tecnologías son claves para incrementar la seguridad de los clientes y la entidad.

3. **Desde su perspectiva, ¿Cómo es la estabilidad de las aplicaciones con inteligencia artificial en producción? en una escala de 1 a 10, donde 1 indica "Muy Inestable" y 10 indica "Muy Estable".**

Figura 3

Estabilidad de aplicaciones con IA en el banco Colpatria

Nota: Elaboración propia

- Como indica la figura 3, el **NPS de 36** es considerado positivo. Esta puntuación muestra que la percepción de estabilidad de las aplicaciones de IA es en su mayoría favorable, pero aún hay margen para mejorar y optimizar la experiencia para los usuarios.

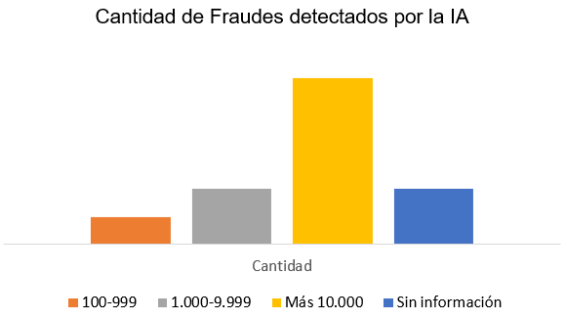
- También se realiza **Análisis de estabilidad**, calculado el promedio = **8,1**

La estabilidad de las aplicaciones con IA en el Banco Colpatria se evalúa en su mayoría como **alta** (promedio de 8.1) La percepción general es positiva, indicando que los sistemas están bien gestionados y que, en su mayoría, funcionan sin problemas significativos.

4. **¿Cuántos fraudes se han detectado por medio de la Inteligencia artificial a la fecha?**

Figura 4

Cantidad de fraudes detectados con IA en el banco Colpatria



Nota: Elaboración propia

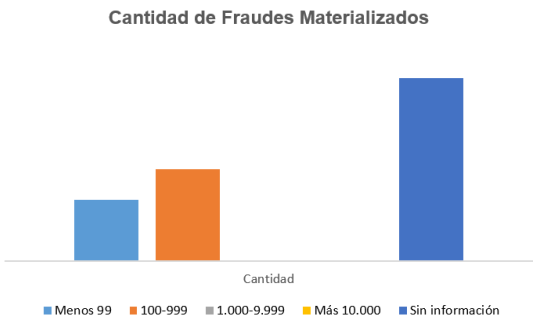
Este análisis muestra una percepción mixta, las respuestas muestran una diversidad de perspectivas y niveles de conocimiento sobre la detección de fraudes usando IA, los encuestados vistos en la figura 4, tienen una perspectiva positiva en cuanto al uso eficiente de la IA en la detección de fraudes bancarios en Colpatria con cifras relevantes de más de

10.0000, más sin embargo la fata de conocimiento es una alerta para evaluar internamente en el Banco.

5. **¿Cuántos fraudes se han materializado que no se hayan podido detectar con Inteligencia artificial a la fecha?**

Figura 5

Cantidad de fraudes materializados en el banco Colpatria



Nota: Elaboración propia

El análisis muestra, según la figura 5, una mezcla de percepciones cuantitativas y cualitativas sobre la cantidad de fraudes no detectados. La mayoría de las respuestas indican que no se cuentan con información, esto puede sugerir la necesidad de sistemas de seguimiento más integrados, que permitan una evaluación más precisa del rendimiento de la IA en la detección de fraudes.

Las cifras de la respuesta indican que por lo menos entre 100 y 999 fraudes no han sido detectados con la IA, lo cual requiere atención del área de fraude en implementar mejoras en las aplicaciones y en el monitoreo de fraudes materializados.

6. **¿Cuáles son los tipos de fraude que más se detectan?**

Figura 6

Tipos de fraudes evitados en el banco Colpatria

Nota: Elaboración propia

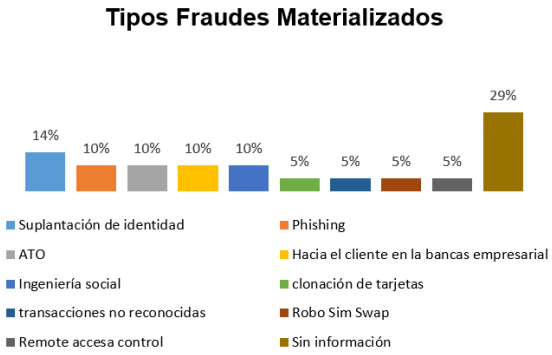
Como se observa en la figura 6, la mayoría de los encuestados representando el 70%, señalaron que el fraude más detectado es la suplantación de identidad, lo sigue el ATO (Account takeover), phishing y la Ingeniería social.

Los fraudes que menos ocurrencia tienen son duplicación de Sim-Card y la clonación de tarjetas.

7. ¿Cuáles son los tipos de fraude materializados más comunes?

Figura 7

Tipos de fraudes materializados en el banco Colpatria



Nota: Elaboración propia

Según el análisis, la figura 7 Tipos de fraudes materializados, la mayoría de las respuestas indican que no se cuentan con información de los tipos de fraude que se han

materializado, lo que confirma el análisis de las respuestas anteriores, sobre la necesidad de mejorar las políticas de monitoreo en el área de fraudes.

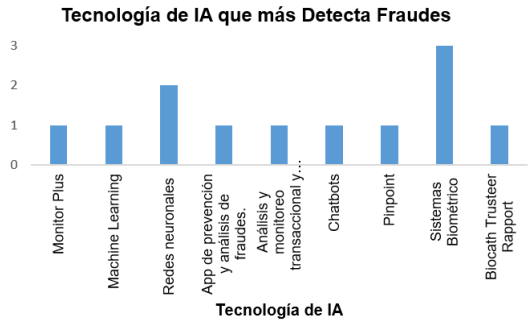
También algunos encuestados hacen énfasis en la ingeniería social que son diferentes técnicas de manipulación que usan los ciberdelincuentes para obtener información confidencial de los usuarios, usando la suplantación, robo de identidad, es decir los fraudes asociados a violentar la vulnerabilidad y poco conocimiento de las personas.

De igual manera relacionan el ATO (Account takeover), que es un ciberdelito que consiste en obtener acceso a las credenciales de inicio de sesión de una cuenta en línea para cometer fraude.

8. ¿Cuál es la tecnología que más detecta el fraude en la organización?

Figura 8

Tecnología que más detecta el fraude en el banco Colpatria



Nota: Elaboración propia

La tecnología de IA que más se emplea en el Banco Colpatria para detectar fraudes es la Biometría, esta variación se resalta en la figura 8, lo cual es fundamental en la verificación de

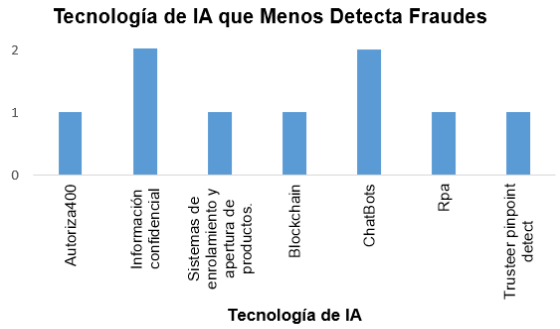
identidad de las personas al momento de abrir cuentas, retirar dinero, autorizaciones de movimiento financieros de grandes sumas de dinero; siendo este un servicio ligado al sistema de la Registraduría Nacional haciendo más confiable el sistema.

Otras de las tecnologías más utilizadas en la organización son las redes neuronales, machine learning, Trusteer Pinpoint Detect y la aplicación monitor plus para el análisis de transacciones en tiempo real.

9. ¿Cuál es la tecnología que menos detecta el fraude en la organización?

Figura 9

Tecnología que menos detecta el fraude en el banco Colpatria



Nota: Elaboración propia

Al validar los datos de la figura 9 las repuestas como "Información confidencial" se observa que los funcionarios consideran que al responder esta pregunta exponen la seguridad del banco, dando a conocer las aplicaciones que no blindan a la entidad de un ataque cibernético.

Respecto a las respuestas donde si se identifica las tecnologías, dos de los encuestados indicaron ChatBots como la que menos detecta fraudes bancarios, ya que están codificados para dar respuestas ya predefinidas y automáticas.

10. Desde su perspectiva, ¿Cuál es el nivel de confianza que existe en el uso de la Inteligencia Artificial para la detección de fraudes? en una escala de 1 a 10, donde 1 indica "Poco confiable" y 10 indica " Muy confiable".

Figura 10

Nivel de confianza en el uso de la IA para detección de fraudes en el banco Colpatria

Nota: Elaboración propia

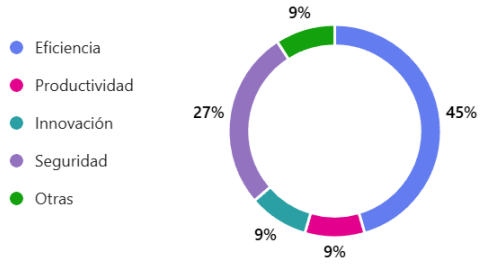
- En la figura 10, El NPS de 46 indica una percepción positiva general, con una buena proporción de promotores en comparación con detractores, sugiriendo que hay un apoyo considerable hacia el uso de la inteligencia artificial en la detección de fraudes.
- El nivel de confianza en la IA para la detección de fraudes es bueno con un promedio de **8,9.**

11. Seleccione la principal ventaja del uso de la inteligencia artificial para la detección de fraudes:

a. Eficiencia
b. Productividad
c. Innovación
d. Seguridad
e. Otra ¿Cuál?

Figura 11

Ventajas en el uso de la IA para detección de fraudes en el banco Colpatria



Nota: Elaboración propia

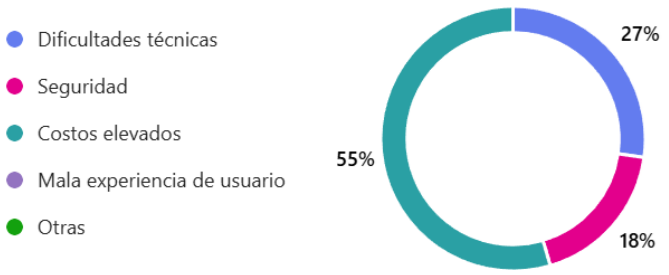
Como indica la figura 11, la eficiencia con un 45% es la principal ventaja que consideran las personas del área de fraude para el uso de la IA en Colpatria, lo que se ve reflejado en los objetivos del banco ofreciendo servicios y experiencias alineadas a las necesidades del cliente. La seguridad obtiene un segundo lugar con el 27% proporcionando confianza en la operatividad del banco.

12. Seleccione la principal desventaja del uso de la inteligencia artificial para la detección de fraudes:

a. Dificultades técnicas
b. Seguridad
c. Costos elevados
d. Mala experiencia de usuario
e. Otra ¿Cuál?

Figura 12

Desventajas en el uso de la IA para detección de fraudes en el banco Colpatria



Nota: Elaboración propia

Los costos elevados con un 55% sobresale en los resultados de la figura 12, como una desventaja para la implementación de la IA dificultando generar proyectos para la implementación de estas nuevas tecnologías. Otra desventaja son las dificultades técnicas, debido a que para estas implementaciones se requieren conocimientos especializados que pueden dilatar los tiempos de puesta en marcha.

13. Desde su perspectiva, ¿Qué nuevas herramientas con inteligencia artificial que no tengamos en el banco se pueden implementar para mejorar los procesos?

Figura 13

Herramientas de la IA para implementación en el banco Colpatria

Nota: Elaboración propia

Como recalca la figura 13 y finalizando con esta pregunta, el área de fraude hace un reconocimiento de la importancia de implementar soluciones avanzadas de análisis y detección

de fraude, que utilizan técnicas de machine learning y analítica de datos, de igual manera tiene interés en la automatización de proceso y tareas con eso poder lograr mayor eficiencia y reducción de errores humanos.

Lograr Implementar estas herramientas podría optimizar la eficiencia operativa y además también fortalecer la seguridad y la experiencia del cliente.

Conclusiones

Con la investigación se determina que en el banco Colpatria la implementación de la inteligencia artificial se encuentra en sus etapas iniciales, teniendo en cuenta que únicamente el 4% de sus aplicaciones cuentan con algunas de estas tecnologías, esto representa cinco aplicaciones que manejan biometría, machine learning y ChatBots, con una baja probabilidad de fallos en producción, teniendo en cuenta que se califican con un 81% en cuanto a estabilidad.

Entre los beneficios más importantes en el uso de la IA en la entidad se encuentran la detección de más de 10.000 fraudes, como suplantación de identidad, phishing, duplicación de tarjeta SIM y account takeover (ATO) que es “la culminación de una serie de ciberdelitos, que generalmente comienzan con un robo o una exposición de las credenciales del cliente” (F5, 2024, párr. 2).

Al no obtener información de la cantidad de fraudes que se materializaron en el banco, debido a que algunos funcionarios consideran que esta información es confidencial, se resalta el cumplimiento de las políticas de seguridad de la entidad, también se evidencia la falta de información de los tipos de fraudes materializados, puesto que estas métricas deberían ser conocidas por toda el área de fraude y de esta manera generar planes de acción, ya que según cifras a nivel mundial, los intentos de fraude digital han aumentado en un 80% en el último año (Transunion, 2023, párr. 1).

El nivel de confianza en el uso de la inteligencia artificial para la detección de fraudes en el banco es significativo, el equipo encuestado siente una confianza en su uso del 89%, resaltando que las tecnologías que más detectan el fraude son los sistemas biométricos, el análisis y monitoreo transaccional, machine learning y Trusteer Pinpoint Detect que es la detección de transacciones en tiempo real, tal como lo indica Alvarez (2020) en su artículo donde se menciona que con la gran cantidad de información que se debe procesar en una entidad bancaria es obligatorio el uso de herramientas automáticas; también se encontró que las tecnologías que menos lo detectan son los robots y ChatBots.

Con este estudio también se resalta que las principales ventajas en el uso de la IA son la eficiencia y seguridad, aumentando así la operatividad de la compañía y el nivel de confianza con los clientes, resultados similares del estudio realizado por ICADE (2020) que señala que al tener un buen servicio al cliente, se aumenta la productividad y se reducen costos de forma simultánea, de igual forma se determinaron las desventajas en cuanto a costos elevados y las dificultades técnicas en la implementación de estas tecnologías.

Por último, se determinó que el área de fraude está de acuerdo en que el banco requiere aumentar el uso de tecnologías de inteligencia artificial con la implementación de procesos de analítica de datos y sistemas automáticos, que permitan identificar comportamientos anormales, como lo considera Gutiérrez Portela et al (2023) quienes recalcan la amplia posibilidad de ocurrencia de fraudes y el alto riesgo operativo y económico por falta de nuevos controles, todo esto encaminado a alcanzar los objetivos estratégicos de tener un banco más seguro y competitivo.

Referencias

Alvarez, F. (2020). Machine Learning en la detección de fraudes de comercio electrónico aplicado a los servicios bancarios. https://www.palermo.edu/ingenieria/pdf2020/CyT_20_07.pdf

Amazon Web Services, Inc. (2023). ¿Cuál es la diferencia entre el aprendizaje profundo y las redes neuronales? https://aws.amazon.com/es/compare/the-difference-between-deep-learning-and-neural-networks/

Banco Davivienda S.A. (2024). “Tap to Phone”: la nueva opción de pago sin contacto. https://www.misfinanzasparaminegocio.com/tap-to-phone-o-toque-al-telefono-la-nueva-opcion-de-pago-sin-contacto/

Barrera, N. (2024, Julio). Los fraudes financieros más frecuentes que afectan el bolsillo de los colombianos. https://www.portafolio.co/economia/finanzas/conozca-algunos-de-los-fraudes-financieros-que-mas-estan-afectando-a-los-colombianos-608901

Benavidez, E., Martínez, Y., & Segura, N. (2024). Inteligencia Artificial y análisis predictivo: impulsores estratégicos para el sector bancario en Colombia. https://repositorio.unbosque.edu.co/server/api/core/bitstreams/750066e8-a612-43ab-a9fb-c5b1cbdbd1e0/content.

Borrero-Tigreros, D., & Bedoya-Leiva, O. (2020). Credit risk prediction in Colombia using artificial intelligence techniques. UIS INGENIERIAS, 19(4).

Bustos, J. (2024, April 18). *Estos son los bancos con mejor reputación en Colombia, según reconocido ranking financiero*. https://www.infobae.com/colombia/2024/04/19/estos-son-los-bancos-con-mejor-reputacion-en-colombia-segun-reconocido-ranking-financiero/

Carbó Valverde, S., Cuadros Solas, P. J., & Rodríguez Fernández, F. (2023). Algunas reflexiones sobre la inteligencia artificial en el sector bancario. Cuadernos de Información Económica, ISSN 1132-9386, No 295, 2023, Págs. 35-40, 295.

Colpatria - Cultura Organizacional. (n.d.). Cultura Organizacional. Retrieved October 9, 2024, from https://www.scotiabankcolpatria.com/acerca-de/inversionistas/gobierno/cultura-organizacional#:~:text=El%20prop%C3%B3sito%20fundamental%20del%20Banco,eficiente%20utilizaci%C3%B3n%20de%20los%20recursos.

Colpatria - Nuestra Historia en Colombia. (n.d.). Nuestra Historia en Colombia. https://www.scotiabankcolpatria.com/corporativo/quienes-somos/acerca-de/historia-en-colombia#:~:text=Con%20el%20fin%20de%20construir,y%20excelentes%20productos%20y%20servicios.

DataCrédito Experian. (2024). Tipos de fraudes con tarjetas de crédito más comunes en cajeros automáticos. https://www.datacredito.com.co/blogs/datablog/tipos-de-fraudes-con-tarjetas-de-credito-mas-comunes-en-cajeros-automaticos/

Digital360 Iberia. (2023). Biometría 3D, el único remedio fiable contra el deepfake. https://www.computing.es/noticias/biometria-3d-el-unico-remedio-fiable-contra-el-deepfake/

Dipole RFID. (2024). NFC: Qué es y cómo funciona. https://www.dipolerfid.es/blog-rfid/que-es-nfc

Dirección Corporativa de Comunicaciones y Reputación. (2018). El Centro de Competencias en Inteligencia artificial de Bancolombia, un acelerador de experiencias digitales. https://www.bancolombia.com/acerca-de/sala-prensa/noticias/innovacion/centro-de-competencias-inteligencia-artificial

Equipo de Contenido (2023) TOP TRES DE FRAUDES DIGITALES MÁS FRECUENTES EN EL SECTOR BANCARIO. https://blog.axur.com/es/top-tres-de-fraudes-digitales-m%C3%A1s-frecuentes-en-el-sector-bancario

Equipo editorial Capital Inteligente Grupo Bancolombia. (2024, June). Principales cambios tecnológicos en el sector financiero en Colombia. https://www.bancolombia.com/empresas/capital-inteligente/tendencias/innovacion/tecnologia-sector-financiero

F5. (2024). ¿Qué es el fraude por account takeover (ATO)?. https://www.f5.com/es_es/glossary/account-takeover-fraud#:~:text=El%20fraude%20por%20account%20takeover%20es%20la%20culminaci%C3%B3n%20de%20una,en%20l%C3%ADnea%20de%20un%20cliente.

FasterCapital. (2024, junio). Sistemas de deteccion de fraude en Regtech descubrir crimenes financieros. https://fastercapital.com/es/contenido/Sistemas-de-deteccion-de-fraude-en-Regtech--descubrir-crimenes-financieros.html

Fintech Americas. (2023, December 5). Cómo Cencosud Scotiabank redujo el fraude a cero gracias a la verificación de la identidad digital. https://blog.fintechamericas.co/como-cencosud-scotiabank-redujo-el-fraude-a-cero-gracias-a-la-verificacion-de-la-identidad-digital???utm_source=dutchit

Fintech Americas. (2023, November 15). 6 buenas prácticas para prevenir el fraude financiero utilizando Inteligencia Artificial. https://blog.fintechamericas.co/6-buenas-practicas-para-prevenir-el-fraude-financiero-utilizando-inteligencia-artificial

Florian Tanant. (2024). Machine learning para detectar fraude. https://seon.io/es/recursos/machine-learning-para-detectar-fraude/

Forbes Staff. (2024). Estas fueron las marcas más suplantadas por los ciberdelincuentes en el segundo trimestre. https://forbes.co/2024/07/29/tecnologia/las-marcas-mas-suplantadas-por-los-ciberdelincuentes

Forero, V. S. (2024). La República. Obtenido de https://amp.larepublica.co/finanzas-personales/estos-son-los-tipos-de-estafas-financieras-mas-comunes-3863361

Gobierno digital. (2024, July 23). Llega a Colombia “Women Training Series.” https://gobiernodigital.mintic.gov.co/portal/Noticias/383729:Llega-a-Colombia-Women-Training-Series

Grapheverywhere. (2024). Fraude Bancario | Métodos tradicionales de detección. https://www.grapheverywhere.com/fraude-bancario-metodos-tradicionales-de-deteccion/

Gutierrez Portela, F., Rodríguez Cárdenas, S., Patiño Ospina, L. P., & Hernandez Aros, L. (2023). Estudio de la prevención y detección de fraudes financieros a través de técnicas de aprendizaje automático. https://repositorio.uniremington.edu.co/server/api/core/bitstreams/5b6ba40d-20ba-4c18-b65e-0a2844a7558c/content

IA Colombia. (2023, October). La Inteligencia Artificial se abre camino en las campañas electorales. https://ia-colombia.co/la-inteligencia-artificial-se-abre-camino-en-las-campanas-electorales/

ICADE. (2020). Inteligencia artificial y el aprendizaje automatizado en la industria bancaria. https://repositorio.comillas.edu/rest/bitstreams/421811/retrieve

Inteligencia Artificial Colombia. (2022). Así utiliza la Inteligencia Artificial el Banco de Bogotá. https://ia-colombia.co/asi-utiliza-la-inteligencia-artificial-el-banco-de-bogota/

IT-NOVA. (2024). IA en la detección del fraude. https://it-nova.co/ia-en-la-deteccion-del-fraude/

iuvity. (2020). Biometría: la clave de la innovación en el sector financiero. https://www.iuvity.com/es/blog/biometria-la-clave-de-la-innovacion-en-el-sector-financiero

Kearns Jeff. (2023). LAS REPERCUSIONES DE LA INTELIGENCIA ARTIFICIAL EN LAS FINANZAS. https://www.imf.org/es/Publications/fandd/issues/2023/12/AI-reverberations-across-finance-Kearns

La Nota Económica. (2024). Top 5 de los fraudes financieros que hoy más afectan el bolsillo de los colombianos. https://lanotaeconomica.com.co/movidas-empresarial/top-5-de-los-fraudes-financieros-que-hoy-mas-afectan-el-bolsillo-de-los-colombianos/

Lesmes, L. (2024, February). Los cinco fraudes bancarios más comunes en Colombia. https://www.eltiempo.com/economia/finanzas-personales/los-cinco-fraudes-bancarios-mas-comunes-en-colombia-857858

Mastercard. (2024, May 22). Mastercard acelera la detección del fraude en tarjetas gracias a la tecnología IA Generativa. https://www.mastercard.com/news/latin-america/es/sala-de-prensa/comunicados-de-prensa/pr-es/2024/mayo/mastercard-acelera-la-deteccion-del-fraude-en-tarjetas-gracias-a-la-tecnologia-ia-generativa/

McClintock, M. (2023, septiembre 27). Cómo implantar la automatización de procesos y la IA: mejores prácticas y dificultades que hay que evitar. https://www.processmaker.com/es/blog/how-to-implement-process-automation-and-ai-best-practices-and-pitfalls-to-avoid/

Michael Goodwin. (2024). ¿Qué es una API (interfaz de programación de aplicaciones)? https://www.ibm.com/mx-es/topics/api

Miniciencias. (2024, February 12). Colombia ya cuenta con una Hoja de Ruta en Inteligencia Artificial. https://minciencias.gov.co/sala_de_prensa/colombia-ya-cuenta-con-una-hoja-ruta-en-inteligencia-artificial

Moreno Cristian. (2024). Prevenir fraudes y nuevos productos, algunos de los usos que los bancos le dan a la IA. https://www.larepublica.co/finanzas/asi-esta-utilizando-el-sector-bancario-la-inteligencia-artificial-3911903

Nuva. (2022, August 23). Inteligencia Artificial en Colombia: un escenario de innovación y Machine Learning. https://www.nuva.co/inteligencia-artificial-en-colombia-un-escenario-de-innovacion-y-machine-learning/

Pragma. (23 de 02 de 2024). Pragma. Obtenido de IA para el cumplimiento normativo de la banca: https://www.pragma.co/es/blog/como-ai-ayuda-a-los-bancos-a-reducir-el-fraude?hs_amp=true

proofpoint. (2024). ¿Qué es phishing? https://www.proofpoint.com/es/threat-reference/phishing

Redacción Tecnología. (2024). Daviplata anunció que integrará funciones de IA para realizar transacciones. https://www.elespectador.com/tecnologia/gadgets-y-apps/daviplata-anuncio-que-integrara-funciones-de-ia-para-realizar-transacciones/

Rodríguez de las Heras Ballell, T. (2022). Inteligencia Artificial en el sector bancario: reflexiones sobre su régimen jurídico en la Unión Europea. ICE, Revista de Economía, 926. https://doi.org/10.32796/ice.2022.926.7398

Ruiz, F. (2020). La inteligencia artificial ha llegado a los servicios financieros. https://blog.finerioconnect.com/la-inteligencia-artificial-ha-llegado-a-los-servicios-financieros/

SafetyCulture. (2024, enero 15). Análisis predictivo. https://safetyculture.com/es/temas/analisis-predictivo/

Scotiabank Colpatria. (2020). Scotiabank lanza plataforma global de Inteligencia Artificial para ofrecer a los clientes asesoría rápida y relevante. https://www.scotiabankcolpatria.com/sala-de-prensa/transformacion-digital/plataforma-ia

Startups Latam. (2023). Seis billeteras digitales que la están rompiendo en Colombia y tienes que conocer. https://startupslatam.com/seis-billeteras-digitales-que-la-estan-rompiendo-en-colombia-y-tienes-que-conocer/

Transunion. (2023). 859% aumentaron intentos de fraude digital en Colombia durante los últimos tres años. https://noticias.transunion.co/859-aumentaron-intentos-de-fraude-digital-en-colombia-durante-los-ultimos-tres-anos/

Trend Micro Incorporated. (2024). ¿Cuáles Son los Distintos Tipos de Phishing? https://www.trendmicro.com/es_mx/what-is/phishing/types-of-phishing.html uFlow LLC. (2024).

Fraud detection How to use machine learning (AI) in banks and fintechs? https://uflow.biz/en/blog/deteccion-de-fraude-usar-el-aprendizaje-automatico-ia-en-bancos-fintechs/

Universidad Europea. (2023). ¿Qué es la tokenización y cuál es su importancia? https://universidadeuropea.com/blog/tokenizacion/