UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

MAESTRÍA EN
GESTIÓN DE PROYECTOS
RPC-SO-20-NO.313-2022

OPCIÓN DE TITULACIÓN:
PROYECTO DE TITULACIÓN CON COMPONENTES DE INVESTIGACIÓN APLICADA Y/O DE DESARROLLO

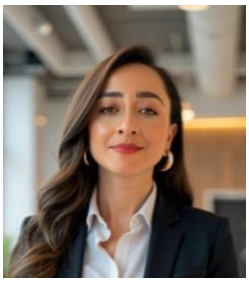
TEMA:
IMPACTO DE LA INTELIGENCIA ARTIFICIAL EN CANALES DIGITALES PARA EL PROCESO DE CONSUMO NO RECONOCIDO DE LA BANCA

AUTOR(ES)
MARÍA ANGÉLICA BERRONES GARCÉS
KELLY MICHELLE MACÍAS MENDOZA

DIRECTOR:
JUAN DIEGO JARA SALTOS

CUENCA – ECUADOR
2026

Autoras:



María Angélica Berrones Garcés
Ingeniería en Administración de Empresas.
Candidata a Magíster en Gestión de Proyectos por la Universidad Politécnica Salesiana – Sede Cuenca.
Maangelikb.77@gmail.com

Kelly Michelle Macías Mendoza
Ingeniería en Administración de Empresas.
Candidata a Magíster en Gestión de Proyectos por la Universidad Politécnica Salesiana – Sede Cuenca.
kelmich_2507@hotmail.com

Dirigido por:

Juan Diego Jara Saltos
Ingeniero Electrónico.
Abogado.
Magister en Telemática.
Magíster en Métodos Matemáticos y Simulación Numérica en Ingeniería.
jjaras@ups.edu.ec

DEDICATORIA

A mis docentes y tutor, quienes con su guía y sabiduría pude alcanzar la meta propuesta.
Y, en especial, a quienes creyeron en mí cuando las fuerzas parecían agotarse, pues gracias a ellos hoy este logro se convierte en realidad.

Kelly Michelle Macias Mendoza

A mis docentes y tutor el Ingeniero Juan Diego Jara por impartir sus conocimientos para alcanzar los propósitos definidos en el proyecto, a Dios por ser el inspirador para cada uno de mis pasos

María Angélica Berrones Garcés

AGRADECIMIENTO

A mis padres, por su amor, sacrificio y apoyo, que han sido el motor que me impulsó a seguir adelante aun en los momentos más difíciles.

A mi novio, por estar a mi lado en cada etapa de este proceso, por su apoyo incondicional. Gracias por creer en mí incluso en los momentos en que yo dudaba y me brindo esa motivación para alcanzar esta meta.

Y, finalmente, a mis compañeras de maestría que de una u otra manera contribuyeron con su apoyo, consejo o gesto de ánimo.

Kelly Michelle Macias Mendoza

A mi madre por brindarme esa fortaleza para seguir adelante pese a las adversidades que nos presenta el diario vivir.

A mis hermanos por ser esas personas vitamina en la vida y que no me suelten de la mano nunca.

A mis compañeras de trabajo y maestría por impulsarme a seguir mejorando y creciendo profesionalmente.

María Angélica Berrones Garcés

Tabla de Contenido

Impacto de la Inteligencia Artificial en canales digitales para el proceso de consumo no reconocido de la Banca

Autor(es):

María Angélica Berrones Garcés

Resumen

En el Ecuador, el incremento de los consumos no reconocidos realizados con tarjetas de crédito ha representado una problemática relevante para las entidades emisoras de dichas tarjetas y más aún para los clientes que los utilizan; En el presente proyecto se brinda una visión analítica documental respecto a la situación actual de las entidades bancarias frente a este problema, para buscar una solución a los reclamos por efecto de consumos no reconocidos en las instituciones bancarias a nivel nacional. Al revisar esta problemática se busca implementar soluciones utilizando metodologías con IA para lograr la prevención y optimización de requerimientos generados por fraudes.

Según un diagnóstico realizado en una de las instituciones bancarias se pudo observar que, al cierre del año 2024, se recibieron un total de 26.155 casos, generados como consulta por consumos no reconocidos, de los cuales 25.866 fueron ingresados para el siguiente proceso dentro de los tiempos establecidos y quedando 289 casos fuera de tiempo, esto puede deberse a que el recurso humano asignado no es el suficiente para solventar esta problemática.

Del análisis se desprenden algunos hallazgos de los sistemas de inteligencia artificial, donde podría generar un cambio significativo en la gestión de fraudes efectuados con tarjetas de crédito, en el cual el objetivo de esta propuesta es considerar el impacto IA en los canales digitales, con el fin de realizar una optimización en cuanto a los procesos respecto a los consumos no reconocidos.

Palabras clave:

Consumos no reconocidos, fraudes, tiempos, tarjetas de crédito, Inteligencia Artificial, Suplantación de identidad, Detección de phishing, proceso.

Abstract

In Ecuador, the increase in unauthorized credit card transactions has become a significant problem for card issuers and, even more so, for their customers. This project provides an analytical overview of the current situation of banks facing this issue, seeking solutions to claims related to unauthorized transactions at banking institutions nationwide. By examining this problem, the project aims to implement solutions using AI methodologies to optimize the handling of fraud-related requests.

According to a diagnostic study conducted at one of the banks, a total of 26,155 cases of unauthorized transactions were received by the end of 2024. Of these, 25,866 were processed within the established timeframes, while 289 cases remained unresolved. This delay may be due to insufficient human resources to address the problem.

The analysis reveals some findings regarding artificial intelligence systems, which could generate a significant change in the management of credit card fraud. The objective of this proposal is to consider the impact of AI on digital channels, in order to optimize processes related to unauthorized charges.

Palabras claves:

Unrecognized charges, fraud, timing, credit cards, Artificial Intelligence, Identity theft, Phishing detection, process.

Introducción

Los consumos no reconocidos se refieren a compras o cargos realizados con una tarjeta de crédito sin la autorización o consentimiento del titular. Estas situaciones pueden originarse debido a la clonación de la tarjeta, robo de identidad, por apropiación fraudulenta por medios magnéticos, o por descubrimiento indebido de bases de datos, etc., permitiendo que terceros utilicen la tarjeta de manera fraudulenta para efectuar pagos en diferentes establecimientos. En el siguiente proyecto se busca optimizar los procesos que actualmente se maneja en los call center para consumo no reconocido, debido que los tiempos de respuesta a un reclamo son muy elevados.

Se puede evidenciar también que con los sistemas de inteligencia artificial esta problemática puede disminuir significativamente, dado que los tiempos de gestión reducirían y cierta documentación se solicitaría mediante medios digitales.

Además, con la inteligencia artificial también se pueda prevenir los fraudes cibernéticos, y así evitar que se materialicen los consumos, ya que día a día esta problemática va incrementando, por lo que presentaremos opciones de IA para reducir este impacto.

La inteligencia artificial en la banca puede ayudar en algunas áreas cómo:
crear posibilidades, manejar riesgos y fraudes, personalizar servicios y productos, informatizar procesos y optimizar costos, facultar la transparencia y el cumplimiento.

1. Determinación del problema

Actualmente en las instituciones bancarias se ha venido evidenciando un incremento en requerimientos de consumos no reconocidos el cual ha impactado en tiempos de gestión y capacidad instalada principalmente en el área de call center, por ende, lo que se busca es disminuir dicha problemática mediante el uso de la Inteligencia Artificial en los canales digitales.

2. Objetivo

- ✓ Analizar el impacto de la inteligencia artificial en los canales digitales utilizados por la banca, para optimizar el proceso de gestión de consumos no reconocidos.

2.1 Objetivos Específicos

- ✓ Analizar la situación actual del proceso de gestión de consumos no reconocidos.
- ✓ Evaluar las tecnologías de IA utilizadas en canales digitales para la detección y prevención de consumos no reconocidos.
- ✓ Realizar una propuesta que permita mejorar los procesos de gestión de consumos no reconocidos mediante la integración de herramientas basadas en IA.

3. Marco Teórico

3.1 Inteligencia artificial aplicada a canales digitales

La inteligencia artificial tiene la capacidad de sustituir la inteligencia de los humanos, instruirse de información y mecanizar tareas complicadas, cambiando así otras entidades, incluso la banca. En este proyecto se busca ofrecer una visión integral del estado actual de la IA en la banca, la necesidad de su integración en bancos tradicionales con sistemas heredados y un vistazo a lo que nos depara el futuro. (Latina Real Experiences, 2024)

La IA son tecnologías que procesan datos y adaptan modelos que provocan una cabida que forman labores de aprendizajes, proporcionando resultados como la anticipación y la aceptación en entornos virtuales. (Unesco, 2021)

3.2 Opciones de IA:

De acuerdo con la búsqueda de herramientas de IA para la optimización de gestiones en la banca, se presentan recomendaciones, las cuales se detallan a continuación:

Device Intelligence: Es un sistema de IA que se emplea para establecer si una cuenta de aplicativo móvil está procesando un movimiento, es decir si es fidedigno en un tiempo optimo que puede ser de hasta milésimos de segundos, lo que ayuda a las entidades financieras a interrumpir los robos cibernéticos antes de que estos sucedan. Se logra coleccionar datos de aplicativos establecidos en reseñas y páginas web tan rápido que un usuario utilice la página web de un banco.

Tal sistema puede ser entrenado usando una lista de fraudes previos (tanto internos como externos) que han ocurrido y que han sido detectados por analistas de fraude. (Krishnan, 2021)

Detectar estas transacciones de consumos no reconocidos a tiempo permite a los bancos ahorrar recursos significativos, por ello el uso de herramientas que permitan mitigar la problemática mencionada es de gran importancia para las entidades involucradas, en este contexto existen algunas herramientas computacionales que permiten lograr una automatización en la detección de fraudes con el objetivo de optimizar la gestión de consumos no reconocidos.

Bio Catch: BioCatch aprovecha la conducta humana para identificar el fraude y notificar los delitos financieros. Nuestro procedimiento para enfrentar este reto es trabajar codo a codo con algunas de las mentes más radiantes del mundo: analistas de amenazas, asesores globales, ingenieros de soluciones y científicos de datos. Profesionales que adoptan una atención minuciosa al detalle con una curiosidad incansable por la perspectiva completa.

BioCatch analiza el comportamiento del usuario en línea. Así, ayuda a los bancos prevenir estos fraudes, como son el reemplazo de identidad, estafas sensibles, robo de compras por internet, etc.

A medida que los farsantes se vuelven más expertos, la prevención debe ir más adelantada. Con la herramienta de IA BioCatch, los bancos pueden detectar una gran cantidad de estafas en línea, con resoluciones agrupadas que detienen la estafa antes de que se efectúe el fraude.

El 67% disminución de las pérdidas por estafas de ingeniería social a los pocos meses de su implantación en uno de los principales bancos de Latinoamérica; con una reducción del 70% de las pérdidas por estafas, por un total de más de 4 millones de euros anuales En 2024, BioCatch evitó más de 100 millones de dólares en pagos fraudulentos de alto riesgo en un banco estadounidense de tamaño medio, deteniendo fraudes que se habrían escapado a los controles tradicionales. (BioCatch, 2025)

TABLA 1.

Opciones de IA para prevención y optimización de fraudes por consumos no reconocidos.

Opciones	BioCatch	Device Intelligence
Tecnología Base	Detección temprana y en tiempo real	Analisa los perfiles de los dispositivos y biometría de comportamiento del usuario en tiempo real
Características Clave	Análisis la intención e identidad del usuario	Identifica el perfil de un dispositivo en menos de un segundo
		Esta IA está entrenada con históricos de fraudes
	Reemplaza CAPTCHAs e IP blocking, es decir distingue quién interactua, si es una persona o un programa automático	Identificación de manera continua a lo largo de una sesión (comportamiento más factores cognitivos y/o fisiológicos)
	Actualización constante frente a riesgos cibernéticos	Medición del riesgo en tiempo real
Ventajas	Experiencia del usuario sin interrupciones	Alta nivel en detección de fraude
	Previene y/o bloquea amenazas 24/7	Monitoreo de identificación constante más allá del login
	Utiliza grandes volúmenes de datos	Identifica esquemas y patrones de phishing, malware, ingeniería social, etc.
		Tiene un enfoque más completo, es decir combina factores técnicos, fisiológicos y contextuales
Desventajas	Licencias costosas	Tiene una mayor complejidad técnica
		Depende de datos históricos de fraude para entrenamiento de modelos
		Riesgos asociados a la privacidad
		Alta capacidad de cómputo
Casos de Uso	Prevención de fraude transaccional	Pagos digitales, bancos, transacciones
	Perfil biométrico conductuel	Valida identidad en registros
	Protección de contraseñas	Identifica riesgos en apps críticas
		Reconocimiento avanzada de malware, phishing y RAT
Recomendación	Esta IA se recomienda para organizaciones que buscan nivelar seguridad y experiencia del cliente.	Se recomienda utilizar en sectores de alto riesgo como por ejemplo banca, salud, gobierno, donde se requiera máxima autenticación continua y detección sofisticada de ataques cibernéticos.

3.3 Estudios previos o casos similares de entidades que usan IA

El objetivo de los métodos digitales y la IA es prevalecer el desafío de la efectividad, y a pesar del beneficio que tiene las tecnologías digitales para las instituciones, existen varios elementos principales que establecen su adaptabilidad y que se relacionan con la tecnología, las sociedades y el entorno, en cambio en las instituciones más grandes están con mayor posición para aprovechar las economías de gran escala, las pequeñas empresas afrontan más limitaciones económicas y de recurso humano. En conclusión, el marco regulatorio desempeña un papel importante al establecer los beneficios necesarios para la implementación tecnológica.

Un objetivo importante es extender las tecnologías de innovación digital, que aportan apoyo técnico para facilitar la adaptación especializada entre las pequeñas empresas. Además, es crucial que la transformación digital se integre en políticas de desarrollo productivo más amplias que incluyan la digitalización de sectores estratégicos, el fortalecimiento de clústeres tecnológicos y el fomento de ecosistemas de emprendimiento digital. (Cepal, 2025)

Según casos de éxito, se detalla una comparación con otras instituciones financieras a nivel nacional e internacional:

- ✓ El Banco Guayaquil toma los requerimientos de reclamos de forma más ágil y rápida mediante app y WhatsApp.
- ✓ El estatus de los requerimientos o reclamos que ingresa el banco Guayaquil se puede visualizar mediante el aplicativo móvil del banco, para evitar un nuevo contacto a las líneas del call center.
- ✓ La Cooperativa JEP aplica campañas más agresivas y constantes sobre la importancia de No entregar los datos de la tarjeta.
- ✓ Los bancos Banorte y Scotiabank ambos de México utilizan herramientas de prevención, como es Bio Catch que les ayuda a fortalecer defensas contra ataques cibernéticos 24/7.

3.4 Cómo funciona la IA en la detección de fraudes

Los sistemas de detección de fraude con IA emplean diversas tecnologías para combatir el fraude:

Aprendizaje automático**:** Los sistemas de IA utilizan el aprendizaje automático para analizar datos históricos y aprender de ellos. Estos sistemas pueden reconocer patrones e identificar anomalías que podrían indicar un comportamiento fraudulento. Por ejemplo, si se utiliza una tarjeta de crédito en dos países diferentes en un corto período de tiempo, el sistema de IA podría marcarlo como sospechoso. (Distrito, 2024)

Redes neuronales**:** Son algoritmos complejos que imitan el funcionamiento del cerebro humano. Las redes neuronales pueden procesar y analizar grandes conjuntos de datos, lo que ayuda a detectar patrones sutiles que otros métodos podrían pasar por alto.

Análisis de datos: La inteligencia artificial utiliza datos avanzados para analizar los datos de transacciones, el comportamiento de los clientes y otra información relevante. De

esta forma, pueden identificar rápidamente actividades potencialmente fraudulentas. (The District Credit Union, 2024)

3.5 Inteligencia de decisiones también se puede utilizar para reducir los fraudes con tarjetas de crédito.

Cuando un beneficiario ejecuta una compra, se puede utilizar métodos de aprendizaje para establecer si el tipo de consumo, el tiempo, la dirección, el precio de compra y una diversidad de puntos de datos como la dirección IP, ID del aplicativo, dirección electrónica, contacto telefónico, etc. están en línea con las transacciones que ha procesado anteriormente el cliente. Esta aplicación también comprueba el sistema de los negocios para validar si el cliente o el sistema tiene aplicado un puntaje de riesgo. En ausencia de un patrón que sea consistente con el fraude, el sistema puede aprobar la transacción. (Krishnan, 2021)

Vía de Pagos: Los algoritmos de aprendizaje automático también pueden estudiar la actividad en línea reciente de un cliente, como el comportamiento de pago, las redes sociales, la seguridad social, la ubicación de IP, la actividad del dispositivo y la dirección de facturación. Cuando más sitios de información estén accesibles de un usuario, menor será el peligro para el usuario. En base en estas participaciones del sistema, los negocios y los bancos pueden corregir su seguridad para certificar o evaluar el riesgo. Por ejemplo, si el mismo estafador enumera diferentes variaciones de nombre al abrir una cuenta, digamos Kris Jefferson, Kris Jeff, Kris Jesse, etc., el algoritmo analizará los puntos de datos (direcciones IP, dispositivos, cuentas bancarias, comportamiento de pago, etc.) estos inicios de sesión para determinar un puntaje de riesgo asociado con tales transacciones. (Krishnan, 2021)

La evolución de la IA en la prevención del fraude: A medida que avanzamos hacia 2025, los sistemas de detección de fraude con IA se centran cada vez más en la intención, no en la identidad. La pregunta ya no es simplemente si una solicitud proviene de un humano o de un bot, sino si su comportamiento indica un uso legítimo o una intención fraudulenta. (Plataforma D. , 2025)

Monitorizar y actualizar continuamente: Implementar un enfoque sistemático para monitorear los patrones de fraude y actualizar los modelos de detección. Esto debe incluir:

- Análisis periódico de intentos de fraude e infracciones exitosas

- Evaluación continua del rendimiento y la precisión del modelo
- Reentrenamiento programado de modelos de IA con nuevos datos
- Capacidades de implementación rápida para actualizaciones de modelos
- Autenticación multifactor para acciones de alto riesgo
- Autenticación basada en riesgos que ajusta los requisitos de seguridad en función del riesgo de la transacción
- Huellas digitales de dispositivos para identificar dispositivos sospechosos
- Biometría del comportamiento para reconocer patrones individuales de usuarios.

Este mantenimiento continuo garantiza que los sistemas de detección de fraude sigan siendo eficaces frente a las amenazas cambiantes y puedan adaptarse al comportamiento cambiante de los clientes.
Este enfoque en capas crea múltiples barreras que los estafadores deben superar, lo que reduce significativamente la probabilidad de ataques exitosos. (Plataforma D. , 2025)

3.6 Las estafas más comunes con tarjetas de crédito

Vishing: Los estafadores llaman a las víctimas haciéndose pasar por empleados bancarios. Con excusas como verificar una transacción sospechosa o activar una tarjeta, logran que los usuarios revelen sus datos confidenciales. Un ejemplo de esto es Carla, una joven profesional, recibió una llamada de "su banco" alertándola sobre una compra sospechosa. Asustada, compartió los datos de su tarjeta y poco después descubrió cargos fraudulentos por $800.

Phishing: Se envían correos electrónicos o mensajes SMS falsos con enlaces a sitios web fraudulentos que imitan los de bancos reales. Al ingresar sus datos, las víctimas los entregan directamente a los delincuentes, por ejemplo, Luis recibió un correo supuestamente de su banco pidiéndole actualizar su clave. Sin sospechar, ingresó sus credenciales en un sitio falso y los estafadores vaciaron su cuenta. (Safi, 2023)

Skimming: Es el procedimiento más utilizado. Los defraudadores colocan aparatos llamados "skimmers" en redes de cajeros o dispositivos de pago en establecimientos. Estos aplicativos exploran y almacenan los datos de la banda magnética de la tarjeta sin que el cliente se dé cuenta.

Además, los defraudadores suelen utilizar este método con una diminuta cámara oculta para registrar la clave del cliente, cuando lo digitan en el teclado del cajero. De esta forma, no solo consiguen la información de la tarjeta, sino también la clave exacta para procesar retiros de efectivo, estos pueden encontrarse en:

- Redes de cajeros automáticos mal ubicados o poco transitados.
- Estaciones de servicios que permiten el pago con tarjeta directamente en la bomba de combustible.
- Establecimientos donde los empleados pueden pasar la tarjeta en un dispositivo escondido.

Terminales de pago falsas: Los delincuentes ubican terminales de pagos fraudulentas en varios establecimientos a nivel nacional. Los terminales recopilan los datos de las tarjetas cuando los usuarios las entregan para realizar el pago. Estos robos son dificultosos de detectar ya que en muchas ocasiones los colaboradores del comercio están implicados, deslizan la tarjeta del usuario en un aparato skimmer antes de hacer el cobro correcto en el post.

Ataques en redes públicas: Al conectarse a redes Wi-Fi públicas, los ciberdelincuentes pueden interceptar información financiera transmitida sin protección. (Seguridad, 2025)

3.7 Modalidades de delitos informáticos más comunes

En Ecuador, el fraude financiero mediante la clonación de tarjetas bancarias ha crecido exponencialmente en los últimos años.

Las entidades bancarias han efectuado múltiples mecanismos de seguridad para neutralizar esta amenaza. Sin embargo, la educación del usuario sigue siendo una de las principales barreras de protección contra estos delitos. (Seguridad, 2025)

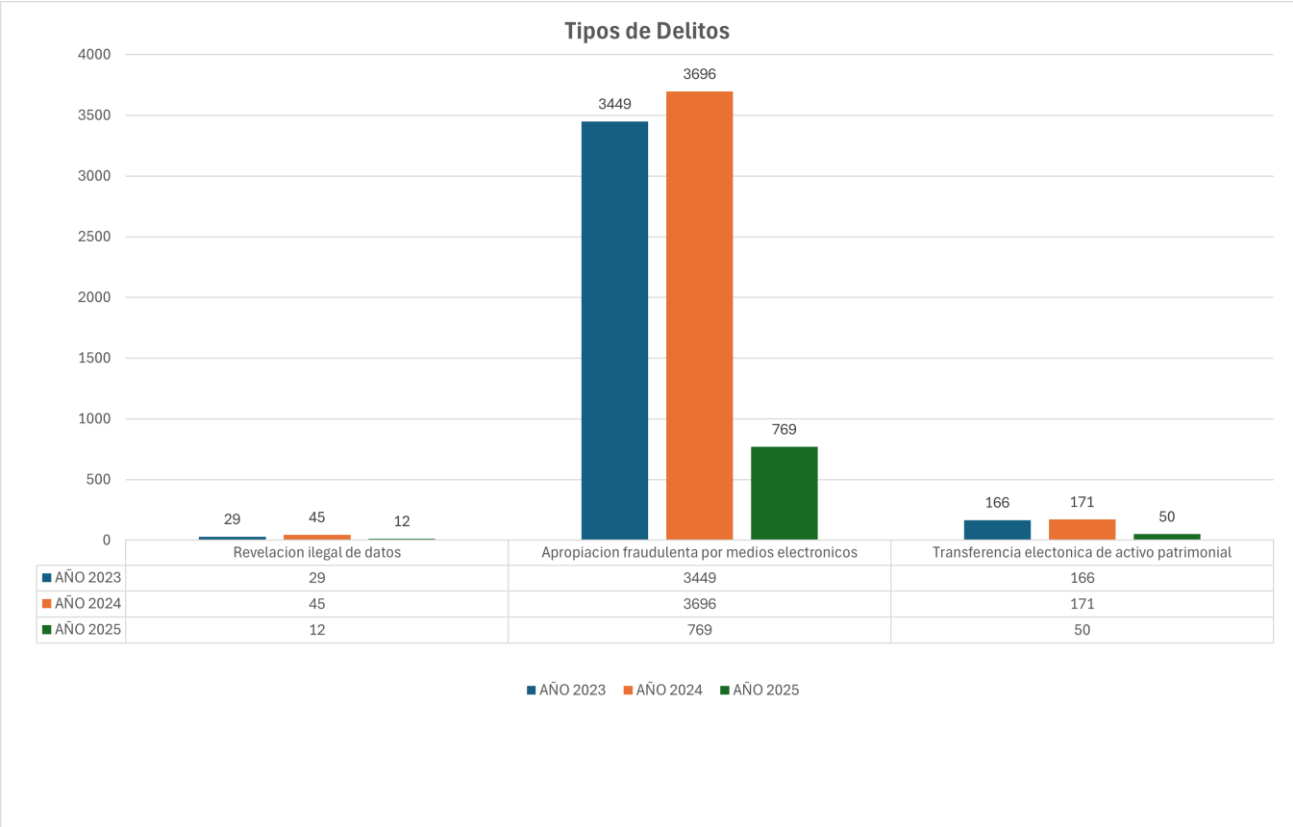
El COIP señala 4 formas de robos cibernéticos que afectan a las personas que usan tarjetas de crédito:

1. Apropiación fraudulenta por medios electrónicos, que se sanciona con una pena privativa de libertad de 1 a 3 años, previsto en el Art. 190 del COIP de Ecuador.
2. Interceptación ilegal de datos, que se sanciona con 3 a 5 años de prisión. Según Artículo 230 del COIP de Ecuador.
3. Revelación ilegal de base de datos, también con pena de 3 a 5 años de prisión. Según Artículo 229 del COIP de Ecuador.

4. Transferencia electrónica de activo patrimonial, que se sanciona con 3 a 5 años de prisión. Según Artículo 231 del Código Orgánico Integral Penal (COIP) de Ecuador. (Tapia, 2025)

Figura 1.

Tipos de delitos de consumos no reconocidos



Según la Figura 1 se visualiza un total de 3696 casos que han sido denunciados en el año 2024 a la Fiscalía y que corresponden al 94% del total; estos casos fueron por apropiación fraudulenta utilizando medios electrónicos.

Este delito se da cuando el defraudador utiliza un software y logra "hackear" al cliente sin que este se dé cuenta, para asociarse a sus cuentas en los aplicativos y efectuar consumos.

A continuación, se presentan varias opciones para no ser víctimas de ataques cibernéticos:

- ✓ Coloque programas de antivirus en sus dispositivos.
- ✓ Evitar utilizar puntos de Wifi públicas.
- ✓ No compartir información personal en redes sociales que puedan acceder los delincuentes y generen "inteligencia social" y

descubran sus claves.

- ✓ Comprobar la veracidad de los sitios web, por ejemplo, que en el navegador el sitio web comience con “https://”
- ✓ Es habitual que en las notificaciones de fraudes existan errores ortográficos. Si lo identifica, desconfíe del sitio web.
- ✓ Recuerde que las entidades bancarias no le solicitaran contraseñas, claves o datos de sus tarjetas.
- ✓ Active notificaciones bancarias para monitorear movimientos sospechosos en la aplicación móvil del banco y revise continuamente las cuentas.
- ✓ Descargue en su dispositivo móvil aplicaciones de identificador de llamadas. Estas suelen permitir a los clientes denunciar que una llamada es fraudulenta. Así que cuando reciba una llamada de un número denunciado, podrá estar alerta. (Tapia, 2025)

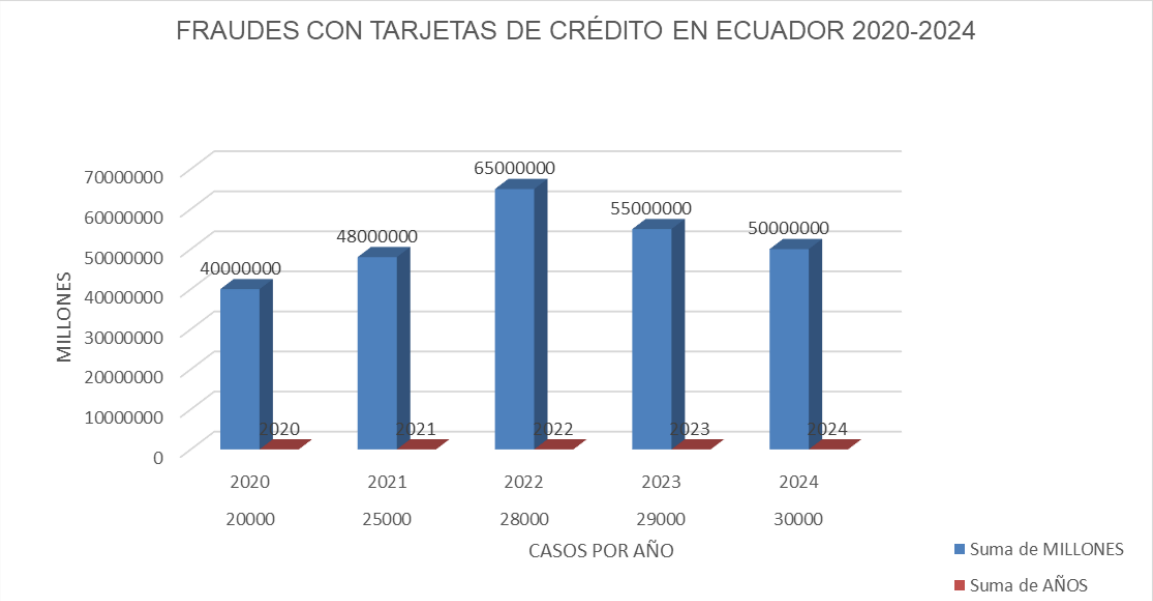
3.8 Problemas de fraude detectados en el Ecuador.

El uso de tarjetas de crédito sigue en aumento en Ecuador, pero con él también crecen las estafas. En 2024, se reportaron más de 30.000 casos de fraude con tarjetas de crédito en el país, representando pérdidas estimadas en más de $50 millones. La cifra más alta registrada de pérdidas por estafas con tarjetas de crédito en Ecuador fue de $65 millones en 2022.

Se estima que alrededor de 120.000 ecuatorianos son víctimas de estas estafas cada año, basándose en reportes bancarios y estudios sobre fraudes financieros en la región.

Figura 2.

Comparativo de fraudes con tarjetas de crédito en el Ecuador 2020-2024.



En promedio, cada víctima de fraude con tarjeta de crédito pierde $1.500. Para muchas familias, esto significa la diferencia entre pagar la renta, la educación de los hijos o quedar endeudados. Además, los procesos de reembolso pueden tomar meses, dejando a las personas en una situación financiera crítica.
Los delincuentes emplean cada vez métodos más sofisticados para robar datos bancarios y cometer fraudes que pueden afectar gravemente las finanzas personales y familiares. (Hora, 2025)

3.9 Estadístico anual de medios de pago electrónicos en el Ecuador.

Los medios de pagos son un conjunto de políticas, normas, materiales, operaciones y servicios por medio de los cuales se generan las transferencias de recursos a través de medios de pago, la compensación y cancelación de valores entre sus diferentes usuarios.

Sistema de Pagos en Línea, es el método que permite a las instituciones financieras y y entidades del sector público, la generación de órdenes de pago de alto valor entre entidades que disponen de una cuenta en el BCE, mediante una Liquidación Bruta en Tiempo Real.

El Documento Estadístico Anual de Medios de Pago Electrónicos, tiene como objetivo analizar e informar a la ciudadanía acerca del funcionamiento y el avance de los sistemas y medios de pago electrónicos en Ecuador hasta el año 2023.

En Ecuador, entre el 2013 y 2023, el Indicador de Grado de Desarrollo de Medios de Pago Electrónicos pasó de 64,1% a 187,2%, reflejando un aumento de casi tres (3) veces durante el periodo en mención. Es así que, para el 2023, los medios de pago electrónicos procesaron un valor equivalente a 1,9 veces del PIB del país.

El Sistema de Pagos Interbancarios, contribuyó en el Sistema Central de Pagos con un 48,0% del valor total, y el 81,6% de todas las operaciones. Por otra parte, la participación del Sistema de Cobros Interbancarios alcanzó un 3,3% y 7,1%, en valor y número de operaciones respectivamente. Asimismo, la participación del Sistema de Pagos en

Línea fue de 37,8% respecto al valor total transaccionado por medio del Sistema Central de Pago y 0,6% en el número de operaciones. (BCE, 2023)

Por lo expuesto, entre el 2013 y 2023, el Sistema de pagos interbancarios fue el sistema de mayor crecimiento en número de operaciones; mientras que, el Sistema de Cobros Interbancario también mostró un comportamiento positivo. Sin embargo, la CCC reportó un decrecimiento en la utilización de cheques como medio de pago. Las transferencias interbancarias de alto valor entre las entidades financieras canalizadas a través de Sistema de Pagos en Línea han movilizado un valor importante de operaciones, aunque su participación fue reducida en el total de la transaccionalidad generada por los diferentes sistemas. Por lo que, en el Ecuador se observa un incremento en el uso de los medios de pago electrónicos.

Datos del Banco Central del Ecuador, muestran una evolución en valor entre el 2013 y 2023, el valor de las operaciones canalizadas a través del Sistema de Pagos en Línea pasó de USD 67.256,7 millones a USD 130.447,8 millones. Entre el 2013 y 2015, estos valores crecieron a una tasa promedio de 16,3%. Posteriormente, desde el 2016 hasta el 2023, la tasa de promedio fue de 5,0%. Finalmente, es importante mencionar que, en el 2023, el valor canalizado aumentó en 2,2% con relación al año anterior. (BCE, 2023)

Figura 3.

Valor del sistema de pagos en línea consolidado 2010-2023.

Fuente: Banco Central del Ecuador
Elaboración: Subgerencia de Administración de Sistemas de Pago

De acuerdo a la Figura 3, podemos observar que a diferencia del año 2013 a la actualidad se ha visto un incremento de medio de pagos electrónicos, debido al avance de las tecnologías y por ende las instituciones financieras se están manejando de manera digital con sus propias aplicaciones mediante app y web; esto también facilita el uso y disminuye tiempos en los clientes, pero a la par se incrementan la cantidad de fraudes digitales con tarjetas de crédito ya que los delincuentes ven una oportunidad para cometer delitos cibernéticos.

3.10 Gestión de consumos no reconocidos en la banca

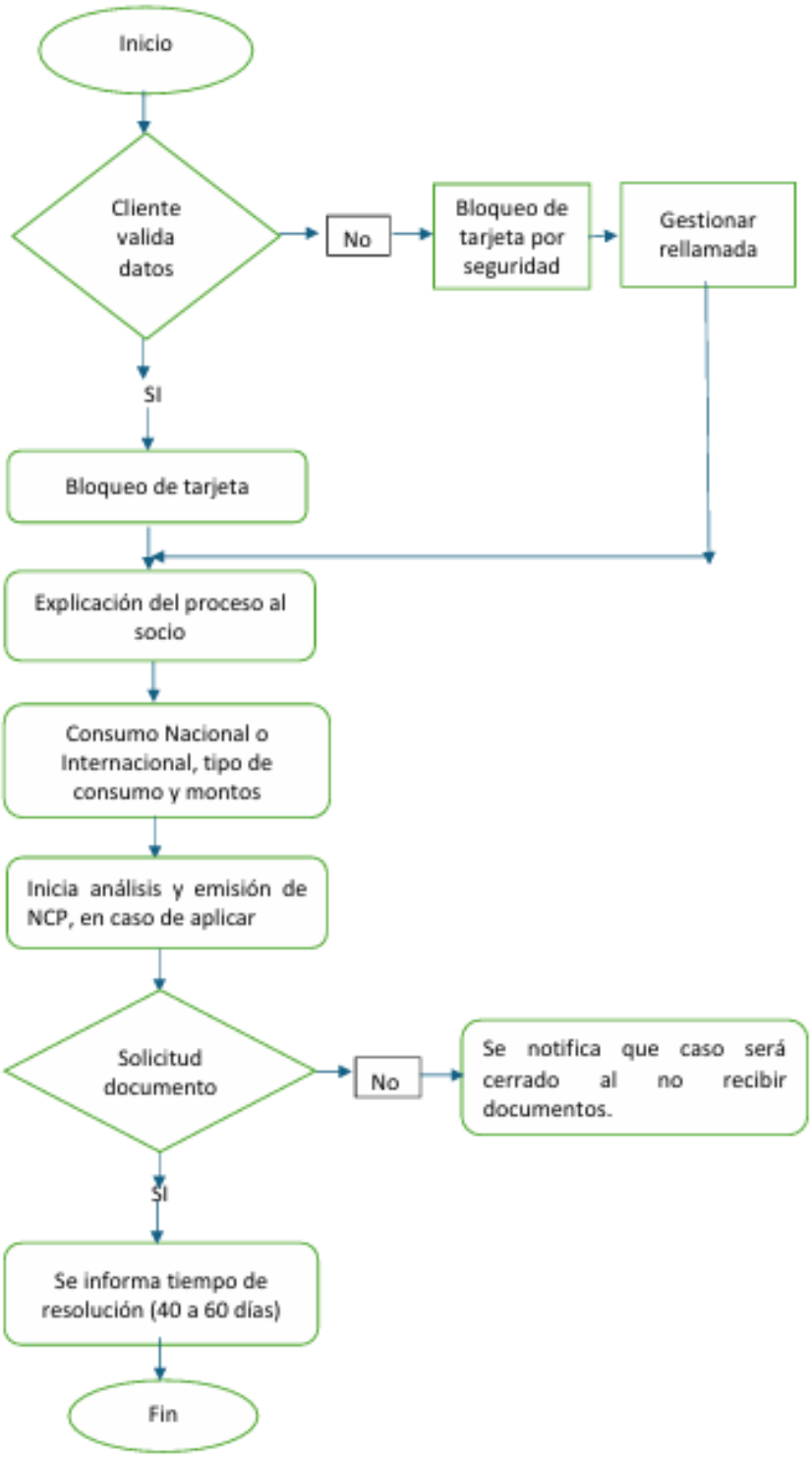
La gestión de consumos no reconocidos en la banca se refiere a un proceso de revisión de uno o varios fraudes cibernéticos presentados por el usuario en su entidad bancaria, en donde se inicia con un proceso de revisión y/o indagación con el cliente entregándole más información detallada sobre el consumo, es decir especialidad a la que corresponde, fecha exacta, hora en la que se procesó, si después de esta revisión el cliente se mantiene en que no reconoce o que no ha realizado dicha transacción, el requerimiento es tomado por el banco; En primera instancia se procede con el bloqueo de la tarjeta por seguridad para que no se generen más transacciones inusuales, posterior a ello se genera un caso para la revisión correspondiente y de ser necesario se solicitará documentos de respaldo como por ejemplo cédula de identidad, copia de la tarjeta para validar que mantiene en su poder y que no se trata de un robo o perdida de la misma y finalmente resolución del reclamo que toma alrededor de 45 hasta 60 días, siendo estos tiempos elevados la segunda problemática mas importante que tiene la banca en el Ecuador.

3.11 Proceso tradicional de gestión de reclamos

En el siguiente diagrama de flujo se puede observar cómo se realizaría el proceso de consumo no reconocido en una entidad financiera, que se lleva a cabo para colocar un reclamo.

Figura 4.

Diagrama de Flujo del proceso de consumo no reconocidos actualmente



3.12 Análisis de tiempos y demoras a los usuarios afectados

En el siguiente esquema se detalla el proceso que debe realizar el cliente para ingresar su reclamo por un consumo que no reconoce.

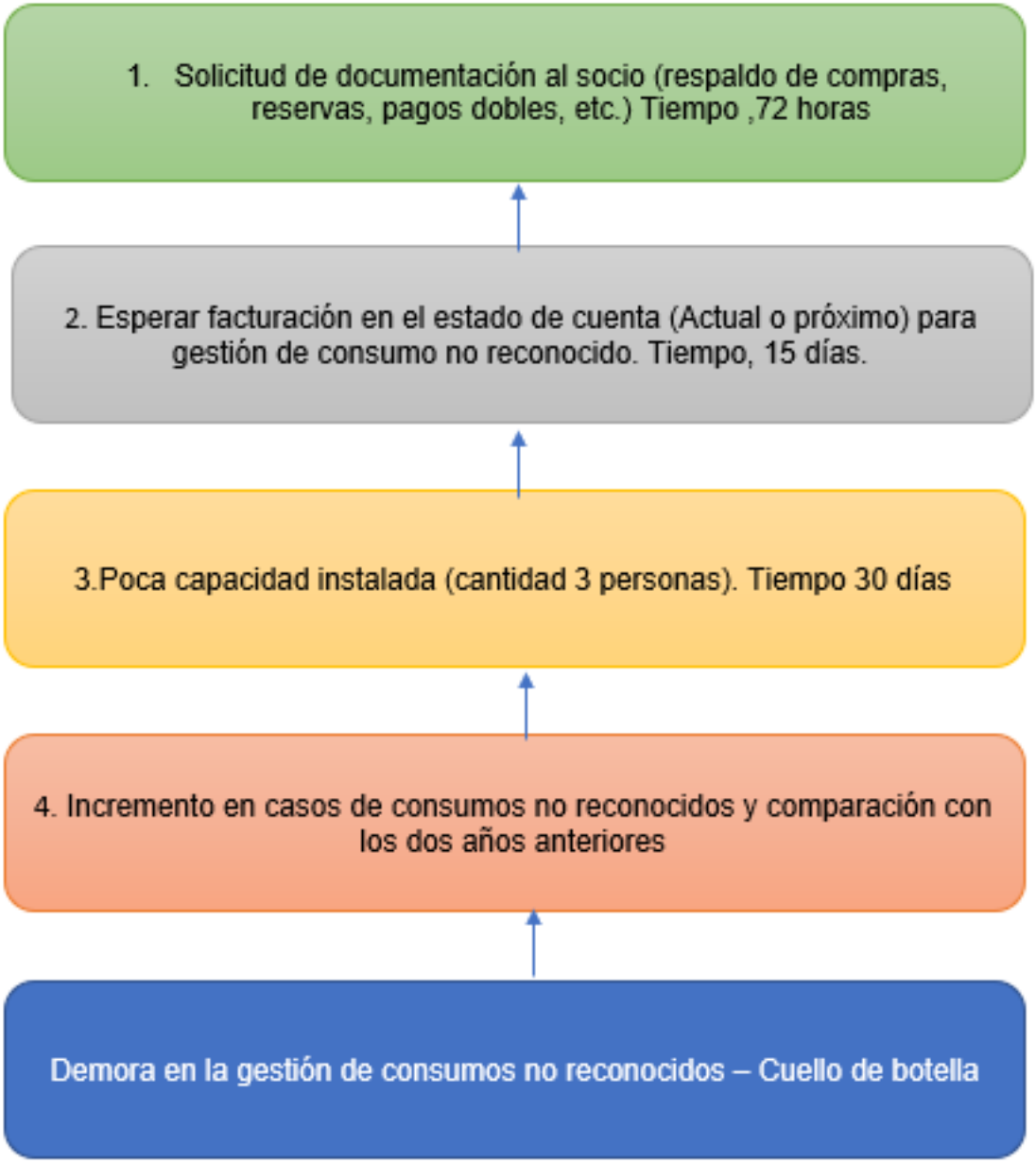
Tabla 2.

Esquema para registrar un reclamo de consumo no reconocido.

PASOS	DEMORAS PARA EL CLIENTE
LLAMADA INCIAL DEL CLIENTE	Tiempo de espera en la fila-canal fisico, tiempos altos de espera en el call center.
	No existen canales digitales eficientes para registrar el reclamo.
	No se puede colocar estos reclamos en 24/7 según la funcionalidad de los banco
REGISTRO DEL RECLAMO	Solicitud de información redundante, es decir piden la misma información varias veces, las instrucciones para el cliente no son claras, formularios obsoletos
SOLICITUD DE DOCUMENTOS	Canales de envio de documentación poco prácticos, es decir el uso del link para cargar la informacion es poco amigable con el usuario y en muchas ocasiones genera errores.
ANALISIS EN EL BANCO	La capacidad instalada para generar estos reclamos es minima, por lo que demanda tiempos de entre 30 hasta 60 días calendario.
RESOLUCIÓN TEMPORAL	No todos los bancos manejan un mismo criterio, es decir no aplican notas de crédito provisional hasta la resoluión definitva, lo que hace que el cliente se quede sin liquidez para asumir estos valores.
RESPUESTA FINAL	Según información otorgada por el cliente y el comercio se determinará si el reclamo es a favor o No del cliente, y esta se notificará vía telefónica y/o correo electrónico.

Figura 5.

Esquema de la problemática en la gestión de consumos no reconocidos.



4. Materiales y Metodologías

4.1 Materiales

Según la información obtenida de cierta institución financiera se pudo constatar algunas problemáticas como son tiempos de atención, cantidad de llamadas, capacidad instalada para atender los consumos no reconocidos y tiempos de resolución de reclamos, en las cuales se detalla la siguiente información:

Dentro de un análisis realizado se pudo evidenciar que al cierre del año 2024 se recibieron un total de 26.155 requerimientos, generados como consulta de los cuales 25.866 fueron ingresados para el siguiente proceso dentro del tiempo, quedando fuera de tiempo 289 casos, por ende, en el proceso de servicio y/o ejecución de reclamo se generó un total de 23.561 requerimientos, es decir la diferencia de 2.594 no continuaron con el análisis debido a varios factores como son:

- ✓ No llegaron a facturarse.
- ✓ Comercio los anulo.
- ✓ Socio asumió los consumos.
- ✓ Socio debe reclamar con comercio.
- ✓ Socio no envió respaldos (documentos)
- ✓ No salió a favor de socio.

4.2 Metodología

Para la elaboración del análisis de datos se ha explorado bibliotecas digitales mismos que se encuentran correlacionados con los objetivos del proyecto que consiste en las siguientes características:

- ✓ Para desarrollar el objetivo que relaciona a la optimización del proceso de consumos no reconocidos en tarjetas de crédito, se ha utilizado el método Analítico y cuantitativo buscando información de fuentes primarias como base de datos financieros, dentro de los principales artículos en el periodo no mayor a dos años.

- ✓ Para el objetivo relacionado a la situación actual se ha ejecutado el método analítico e histórico, mediante el levantamiento de información de bases de un tiempo no mayor a dos años.

- ✓ Para el objetivo relacionado a la propuesta del impacto financiero, se emplea el método hipotético mediante la revisión de la transaccionalidad histórica, relacionada entre requerimientos creados correctamente frente a requerimiento mal creados.

- ✓ Para el objetivo relacionado con la evaluación de tecnologías, se implementa el método analítico, descriptivo, donde se detalla las características principales con base a datos financieros.

4.3 Comparativo de consumos no reconocidos año 2023 – 2024

Según información del año 2023 y 2024 se pudo evidenciar que hubo un aumento de casos por consumos no reconocidos en el año 2024, los datos correspondientes a este incremento se muestran en la Tabla 3, en donde se presentan los casos ingresados por mes.

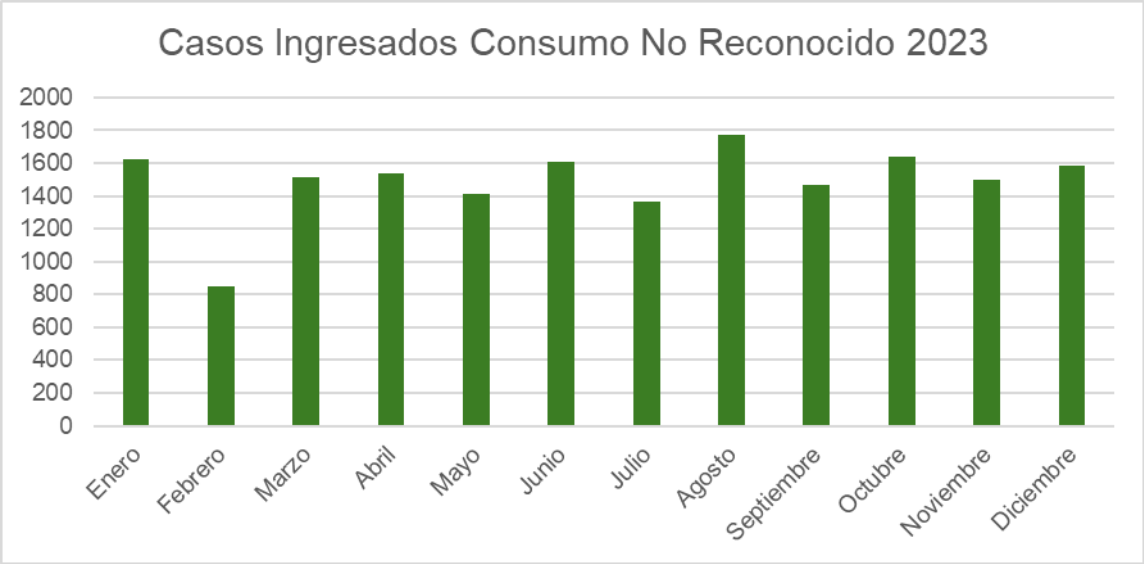
Tabla 3.

Análisis consumo no reconocido por mes año 2023

Consumos no Reconocido Año 2023	Casos Ingresados
Enero	1621
Febrero	850
Marzo	1516
Abril	1534
Mayo	1410
Junio	1611
Julio	1365
Agosto	1775
Septiembre	1470
Octubre	1640
Noviembre	1501
Diciembre	1586
Total reclamos ingresados	**17879**

Figura 6.

Gráfica de consumos no reconocidos mensual año 2023



Según la Figura 6, se puede evidenciar que, en el mes de agosto 2023, hubo un incremento de requerimientos a diferencia de otros meses, esto podría ser por varios factores, como, por ejemplo, período de vacaciones en el régimen sierra (consumos en línea/ tickets, reservas de hoteles, etc).

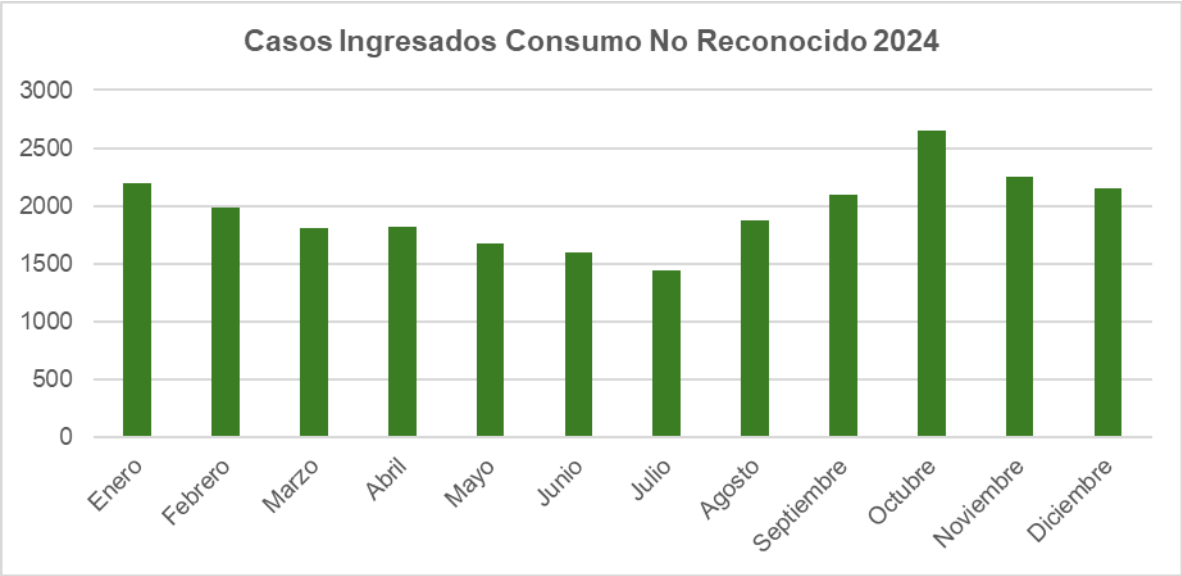
Tabla 4.

Análisis consumos no reconocidos año 2024

Consumos no Reconocido Año 2024	Casos Ingresados
Enero	2193
Febrero	1984
Marzo	1812
Abril	1823
Mayo	1679
Junio	1602
Julio	1440
Agosto	1874
Septiembre	2095
Octubre	2655
Noviembre	2250
Diciembre	2154
Total reclamos ingresados	**23561**

Figura 7.

Gráfica de consumos no reconocidos mensual año 2024



Según Figura 7, se puede evidenciar que, en el mes de octubre 2024, hubo un incremento de requerimientos a diferencia de otros meses, esto se pudo dar por inicios de festividades de fin de año (compras en línea/ black Friday).

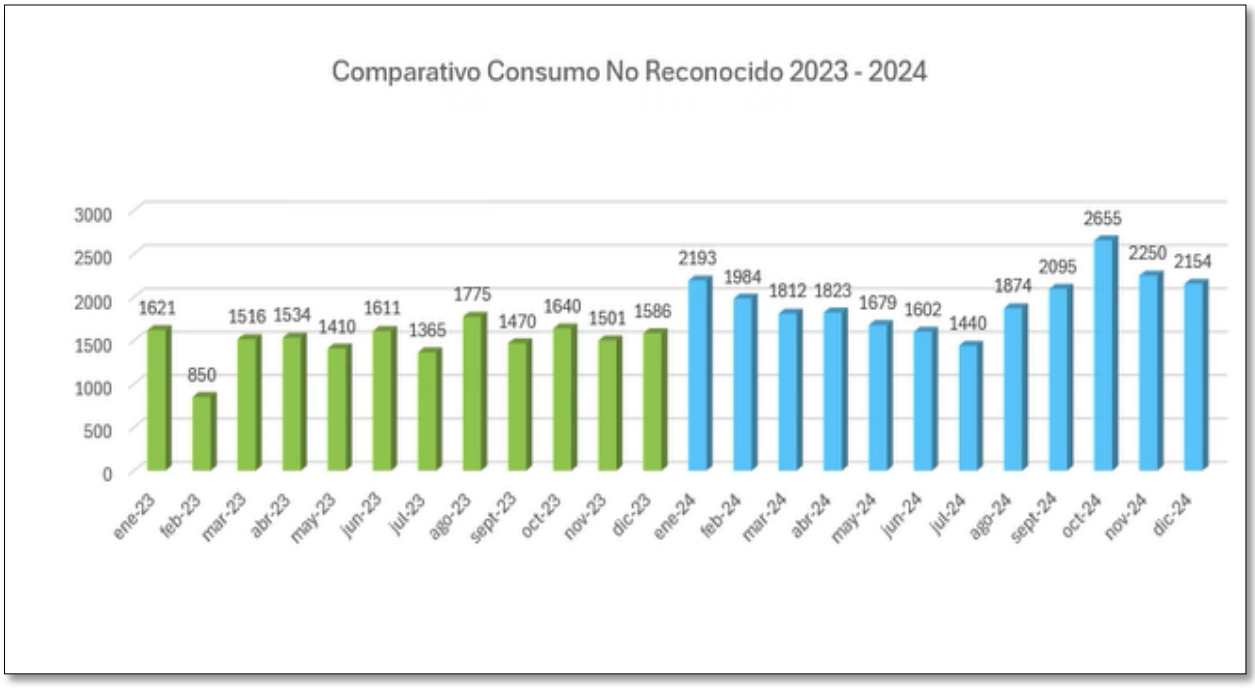
4.4 Análisis comparativo consumos no reconocidos años 2023-2024

De acuerdo con el análisis realizado podemos concluir que mientras más avanza el tiempo y las tecnologías, más frecuentes son los fraudes que presentan las entidades financieras sin que estas puedan frenar dichas incidencias, un ejemplo especifico es la cantidad de fraudes presentados en octubre 2024, en donde se registró el incremento mas relevante de consumos no reconocidos.

En 2023 se presentó una media mensual de reclamos por consumos no reconocidos de 1490, esta cantidad de llamadas son atendidas por aproximadamente 120 ejecutivos; A diferencia del año 2024 que registró un promedio mensual de 1963, atendidos por la misma capacidad instalada del año anterior.

Figura 8.

Comparativo consumos no reconocidos años 2023-2024



5. Resultados y discusión

Según los modelos de IA presentados en la Tabla 1 en cuanto a detección temprana de fraudes, respuestas automáticas, análisis y comportamiento, se recomienda el uso de IA Device Intelligence dado que segmenta sectores de alto riesgo como es la banca, y el costo de la aplicación no es tan elevado, entre sus principales características tenemos:

- ✓ Alto nivel en detención de fraudes
- ✓ Monitoreos de identificación o login constante
- ✓ Identifica esquemas y patrones de phishing
- ✓ Combina factores técnicos, fisiológicos y técnicos

Para integración o implementación de la IA en los canales digitales se puede aplicar mediante Chatbots o WhatsApp Business.

Tabla 5.

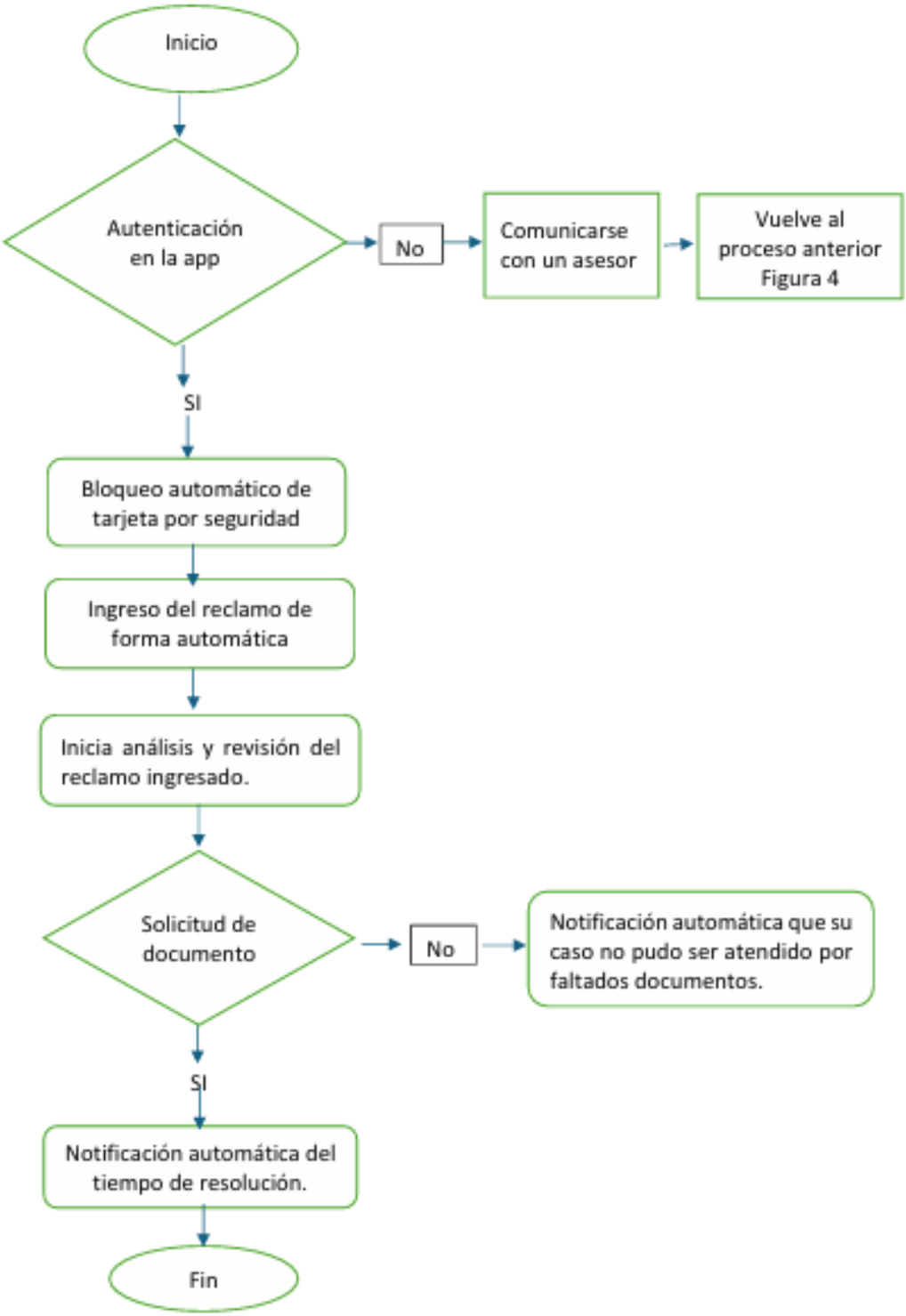
Cuadro comparativo del antes y después del uso de IA.

PROCESO ANTERIOR	DETALLE	TIEMPO	OPTIMIZACIÓN CON IA	TIEMPO
TIEMPO DE ESPERA EN SER ATENDIDO	Es el tiempo que el cliente tiene que esperar en la llamada para ser atendido por un ejecutivo que toma un tiempo aproximado de 1 minuto y dentro de este tiempo el cliente corre el riesgo de que le generan mas consumos en su tarjeta de crédito	1 minuto hasta ser atendido	Autenticación directamente desde la APP	No existe tiempo de espera, cliente ingresa directamente a autenticarse que le tomaría menos de 1 minuto
LLAMADA INCIAL E INGRESO DEL RECLAMO	La interacción inicial que realiza un cliente a un call center para colocar su reclamo de consumo no reconocido toma alrededor de 15 minutos promedio, en donde el agenete que toma el requerimiento debe indagar sobre el consumo reclamado ya que puede darse el caso de que sea un cargo recurrente que el socio si realizó o que efectivamente no realizó la transacción	15 minutos para registrar el reclamo	Bloqueo automático de la tarjeta por seguridad e ingreso del reclamo de consumo no reconocido desde la APP	Tomaría aproximadamente 5 minutos entre el bloqueo e ingreso del reclamo
SOLICITUD DE DOCUMENTOS	Se notifica al socio que debe remitir la documentación pernitente para el inicio del análisis del consumo no efectuado ejemplo cédula de identidad, firma en el formulario	72 horas hábiles	El mismo día que el cliente ingresa el reclamo en la APP	1 día
RECEPCION DE LOS DOCUMENTOS	Debido a la falta de capacidad instalada el tiempo de revisión de los documentos enviados por el cliente son elevados.	30 días calendario	Carga de docuemntos inmediata, dentro del mismo día que el cliente ingresa el reclamo	1 día
ANALISIS EN EL BANCO	Una vez validada toda la documentación se genera un nuevo requerimiento que se envia al área especializada en fraudes, frente a la marca y/o comercio según sea el caso; Dentro de esta revisión se genera un nota de crédito provisional de montos que superan los $25	30 días calendario	Validación frente a la marca y/o comercio se mantiene dado que requiere de análisis a profundidad	30 días calendario
RESPUESTA FINAL	La resolución final al cliente se le notifica dentro de los 60 días calendario detalladas en los dos items anteriores		RESPUESTA FINAL	
TOTAL TIEMPOS	65 días antes del uso de la IA		Optimización a 35 días con el uso de la IA	

Según Tabla 5, en el cuadro comparativo se puede evidenciar el tiempo estimado que un usuario tenía que esperar para la respuesta a su reclamo, a diferencia ya con el uso de la IA mediante la APP en donde se muestran optimizaciones significativas.

Figura 9.

Proceso de consumo no reconocidos optimizado con la IA



Según Figura 9, se puede evidenciar que al implementar la IA para el proceso de consumos no reconocidos disminuye la operativa en tiempos de resolución, ya que al ser de manera automatizado el proceso, el cliente ya no estaría esperando en la llamada para que un ejecutivo atienda su requerimiento.

Con este nuevo proceso se estaría generando una reducción del 50% aproximadamente en lo que se refiere a tiempos dado que en el proceso manual la resolución es de 65 días, a diferencia del proceso automatizado que tendría un tiempo de resolución de 35 días, evitando generar un caso de consulta e ingresaría directamente el caso de servicio, es decir ya no existirían los dos filtros que se maneja en el proceso manual, con esto se pretende aumentar la eficiencia del servicio.

5.1 Evaluación de IA a aplicar

Los intentos de las instituciones financieras por remediar la situación se ven limitados por una tecnología heredada y procesos manuales ineficientes que ya no pueden seguir el ritmo de los crecientes volúmenes de disputas actuales.

Muchas instituciones financieras aún no cuentan con un portal digital para presentar disputas; requieren que los clientes llamen, acudan a una sucursal, envíen sus disputas por correo postal o fax, lo cual contradice sus expectativas de una experiencia totalmente digital. Además, a falta de un sistema digital transparente, los clientes suelen tener una visión limitada del estado de su disputa. Como resultado, terminan llamando a sus instituciones financieras repetidamente, lo que aumenta el volumen de llamadas y aumenta la frustración del cliente.

Además, la ausencia de una manera sencilla para que los clientes carguen los documentos requeridos puede generar demoras más adelante en el proceso cuando los agentes se dan cuenta de que necesitan más información para procesar un caso.

Las decisiones sobre disputas suelen ser subjetivas, lo que genera una experiencia inconsistente para el cliente y un riesgo para la reputación de las instituciones financieras, ya que los clientes a menudo recurren a las redes sociales para expresar sus frustraciones. (Genpact, 2025)

6. Conclusiones

Una vez realizado el análisis de la problemática se detallan los puntos más importantes, en los que se debe tomar en cuenta para la mejora del proceso de consumos no reconocidos:

- ✓ Invertir en herramientas de detección de fraude con IA Device Intelligence o BioCatch que se adapten a las necesidades específicas y a los riesgos de fraude. Se considerará factores importantes como:
  Precisión de detección y tasas de falsos positivos

  Capacidades de respuesta en tiempo real

  Adaptabilidad para gestionar el volumen de transacciones

  Capacidades de integración con sistemas ya existentes

- ✓ Se sugiere el uso de herramienta Bio Catch ya que ayuda a la optimización de fraudes generados mediante ingeniera social, con una reducción de hasta un 70% de perdidas por estafas.

- ✓ Se recomienda el uso de la herramienta IA Device Intelligence dado que se pretende una disminución en los tiempos de ejecución de un reclamo por consumo no reconocido.

- ✓ Se optimizaría la entrega de la carta de consumo no reconocido de manera masiva utilizando herramientas macro, dado que anteriormente se lo generaba de manera manual e individual.

- ✓ La optimización con la IA ayuda a las instituciones financieras a disminuir a los ejecutivos de procesos recurrentes, permitiéndoles enfocarse en otras tareas que aportan más valor en la gestión de recamos por consumos no reconocidos.

- ✓ Con la implementación de la IA se espera obtener una reducción hasta un 50% menos de costos, mayor satisfacción del cliente y empleados más productivos.

7. Referencias

Blog Clip. (14 de 08 de 2024). Blog Clip. https://blog.clip.mx/articulo/que-hacer-si-tienes-cargos-no-reconocidos-en-tu-tarjeta-de-debito

La Hora. (26 de 09 de 2024). Crisis económica. https://www.lahora.com.ec/pais/crisis-economica-denuncias-diarias-estafas-financieras-ecuador-2024 Latina Real Experience. (2024). Inteligencia Artificial en la Banca.

Martínez Padilla, M. (2015). La Responsabilidad Bancaria frente a los delitos informáticos. Universidad Andina Simón Bolívar Sede Ecuador Área de Derecho, 7.

Minerva Sandoval, A. (2020). Consecuencias y efectos de los delitos financieros, económicos y bancarios. su impacto económico y social en las finanzas públicas y privadas, así como en la calidad de vida de la sociedad mexicana. derecho y opinión ciudadana, 167-189.

Santader, B. (28 de 04 de 2023). https://www.santander.com/es/stories/inteligencia-artificial#accordion-b291e2fa41-item-c9bd0a495d

¿Qué es la inteligencia artificial (IA) en finanzas? (s.f.).: https://cloud.google.com/discover/finance-ai?hl=es-419

bancario, L. I. (2024). *La IA en el sector bancario*. https://cloud.google.com/discover/ai-in-banking?hl=es

HAT, R. (3 de 1 de 2024). https://www.redhat.com/es/topics/ai/ai-in-banking

IBM. (01 de 05 de 2024). *IBM*. https://www.ibm.com/es-es/topics/ai-in-banking

Hora, L. (31 de Marzo de 2025). Caer en estafas con tarjetas de crédito representa pérdidas promedio de $1.500 en Ecuador. Ecuador.

Plataforma, D. (21 de 03 de 2025) https://datadome.co/learning-center/ai-fraud-detection/#:~:text=Los%20sistemas%20de%20detecci%C3%B3n%20de,dispositivos%20y%20se%C3%B1ales%20de%20red

The district credit union (01 de 08 de 2024). https://www.districtcreditunion.com/blog/ai-fraud-detection-in-banking/

Krishnan, K. (2021). Grupo Novatech. https://www.grupo-novatech.com/deteccion-de-fraude-utilizando-ia-en-servicios-financiero

Omisola, I. (4 de 11 de 2024). Zenrows. https://www.zenrows.com/blog/datadome-bypass#what-is-datadome

Krishnan, K. (2024). https://www.grupo-novatech.com/deteccion-de-fraude-utilizando-ia-en-servicios-financieros/

Tapia, E. (6 de 15 de 2025). https://www.primicias.ec/economia/tarjetas-credito-delitos-informaticos-estafas-cuentas-bancos-98471/

Unesco. (01 de 2021). Unesdoc Biblioteca Digital. https://unesdoc.unesco.org/ark:/48223/pf0000381137_spa

Seguridad, L. (21 de 03 de 2025). Laar Seguridad. https://www.laarseguridad.com/blog/como-los-delincuentes-clonan-tarjetas-bancarias-en-ecuador-la-tecnologia-detras-del-robo/b?utm_source=chatgpt.com

BCE. (2023). Documento estadístico anual de medios de pago electrónicos en Ecuador. Sistema de pagos en línea, 3-28.

Genpact. (2025). Genpact. Desafíos de la gestión de disputas: https://www.genpact.com/insight/transforming-dispute-resolution-with-ai?utm_source=chatgpt.com

Cepal. (2025). Superar las trampas del desarrollo de América Latina y el Caribe en la era Digital. El potencial transformador de las tecnologías digitales y la inteligencia artificial, 21.

Primicias. (15 de 06 de 2025) https://www.primicias.ec/economia/tarjetas-credito-delitos-informaticos-estafas-cuentas-bancos-98471/

BioCatch. (2025). *BioCatch*. Obtenido de BioCatch detecta las señales: https://www.biocatch.com/es/social-engineering-scam-detection.