Asesorías y Tutorías para la Investigación Científica en la Educación Puig-Salabarría S.C.
José María Pino Suárez 400-2 esq a Lerdo de Tejada. Toluca, Estado de México. 7223898475
RFC: ATI120618V12

Revista Dilemas Contemporáneos: Educación, Política y Valores.
http://www.dilemascontemporaneoseducacionpoliticayvalores.com/
Año: XII Número: Edición Especial Artículo no.:87 Período: Diciembre del 2024

TÍTULO: El delito de fraude financiero en el Ecuador: un análisis de las transacciones digitales.

AUTORES:

1. Máster. Carlos Wilman Maldonado Gudiño.
2. Est. Adrián Fernando Sánchez Puga.
3. Est. Dolores Paulina Ramírez Flores.
4. Est. Karla Dayana Hallo Silva.

RESUMEN: El estudio analizó el incremento de las transacciones electrónicas y el riesgo de fraude asociado, con el objetivo de evaluar el volumen y la proporción de transacciones fraudulentas. Se utilizaron métodos cuantitativos para recopilar y analizar datos sobre transacciones y fraudes financieros. Los resultados mostraron, que en promedio, se realizaron 3,095 transacciones electrónicas, de las cuales el 8.08% fueron fraudulentas, con aproximadamente 250 fraudes mensuales. Se observó un aumento significativo en los casos de fraude entre los años 2021 y 2023. Las conclusiones destacaron la necesidad urgente de fortalecer las medidas de seguridad y desarrollar un marco jurídico robusto para prevenir el uso indebido de tecnologías financieras, enfatizando la importancia de la colaboración entre instituciones financieras y organismos reguladores.

PALABRAS CLAVES: transacciones electrónicas, fraude financiero, riesgos, medidas de seguridad.

TITLE: The crime of financial fraud in Ecuador: an analysis of digital transactions.

AUTHORS:

1. Master. Carlos Wilman Maldonado Gudiño.
2. Stud. Adrián Fernando Sánchez Puga.

3. Stud. Dolores Paulina Ramírez Flores.

4. Stud. Karla Dayana Hallo Silva.

ABSTRACT: The study analyzed the increase in electronic transactions and the associated fraud risk, with the aim of assessing the volume and proportion of fraudulent transactions. Quantitative methods were used to collect and analyze data on financial transactions and fraud. The results showed that, on average, 3,095 electronic transactions were carried out, of which 8.08% were fraudulent, with approximately 250 frauds per month. A significant increase in fraud cases was observed between 2021 and 2023. The findings highlighted the urgent need to strengthen security measures and develop a robust legal framework to prevent the misuse of financial technologies, emphasizing the importance of collaboration between financial institutions and regulatory bodies.

KEY WORDS: electronic transactions, financial fraud, risks, security measures.

INTRODUCCIÓN.

El auge de la digitalización y la proliferación de servicios financieros electrónicos han transformado el panorama bancario y financiero a nivel mundial. En Ecuador, el crecimiento de las transacciones digitales ha sido significativo, impulsado por la adopción de tecnologías móviles y la expansión de los servicios de banca electrónica; sin embargo, este avance ha traído consigo nuevos desafíos en términos de seguridad y prevención del fraude financiero.

El fraude financiero por transacciones digitales se ha convertido en una preocupación creciente para el sistema financiero ecuatoriano. Este fenómeno no solo afecta a las instituciones financieras y a los consumidores, sino que también representa un riesgo para la estabilidad económica del país. Las modalidades de fraude varían desde el phishing y el smishing hasta los ataques de malware, cada uno con diferentes niveles de sofisticación e impacto.

En este contexto, el presente artículo tiene como objetivo explorar la naturaleza del fraude financiero en transacciones digitales en Ecuador, identificando los métodos más comunes utilizados por los delincuentes

y evaluando las implicaciones de estos delitos en el ámbito financiero y social; además, se analizará la efectividad de las regulaciones existentes y se propondrán recomendaciones para mejorar las estrategias de prevención y detección del fraude.

La revisión bibliográfica efectuada sobre el fraude financiero en transacciones digitales destaca varios aspectos cruciales relacionados con la regulación, las modalidades de fraude y las medidas de seguridad implementadas. Groppa & Curi (2012) examinan la regulación del dinero móvil en países como Kenia, Ecuador y Brasil, subrayando la importancia de una coordinación efectiva entre las regulaciones de telecomunicaciones y bancarias. Según estos autores, las quejas sobre el servicio de dinero móvil generalmente se dirigen primero a las empresas de telecomunicaciones o a los organismos reguladores de telecomunicaciones, lo que evidencia una división en las responsabilidades regulatorias.

La regulación bancaria juega un papel fundamental en la mitigación del fraude financiero, ya que aborda problemas de asimetría de la información y controla la creación de dinero fuera del monopolio gubernamental. Las regulaciones bancarias se enfocan en la autenticación de usuarios, la integridad de las transacciones y la monitorización de montos guardados y transferidos, aspectos esenciales para prevenir el lavado de dinero y otros delitos financieros (Groppa & Curi, (2012).

Esta perspectiva, al analizar la banca móvil como una forma de banca electrónica, permite la prestación de productos y servicios bancarios a través de redes móviles, incluyendo depósitos, préstamos, gestión de cuentas y pagos electrónicos. Esta modalidad de banca ha facilitado el acceso a servicios financieros en áreas rurales y entre poblaciones no bancarizadas, pero también ha introducido nuevos riesgos de seguridad que deben ser abordados mediante regulaciones adecuadas.

Beck et al., (2018) y Grey (2017) analizan las implicaciones macroeconómicas de las finanzas móviles en países en desarrollo, utilizando el paradigma de la teoría del dinero moderno (TMM). Grey sugiere que la proliferación de tecnologías financieras móviles puede contribuir a la estabilidad económica si se implementan mecanismos de pago universales basados en dinero fiduciario digital y se proporciona liquidez

ilimitada por parte del banco central. Este enfoque podría minimizar la fragilidad sistémica y fortalecer la confianza en los sistemas financieros digitales.

Khattri & Singh (2019) proponen un enfoque innovador para la autenticación segura de transacciones en línea mediante la incorporación de un tercer factor basado en la ubicación del sistema de posicionamiento global (GPS) del usuario. Esta estrategia busca prevenir el fraude al verificar que las transacciones se realicen desde dispositivos legítimos y en posesión del usuario autorizado. Los resultados de su estudio muestran una alta tasa de detección de fraudes, lo que sugiere que la implementación de factores de autenticación adicionales puede ser efectiva para mejorar la seguridad de las transacciones digitales.

La revisión de la literatura evidencia que la regulación adecuada y la implementación de tecnologías avanzadas de autenticación son cruciales para combatir el fraude financiero en transacciones digitales. La coordinación entre diferentes organismos reguladores y la adopción de medidas innovadoras pueden fortalecer la seguridad y confianza en los servicios financieros digitales en Ecuador.

Gonzáles et al., (2018) manifiesta que el phishing es una técnica de fraude en la que los delincuentes se hacen pasar por entidades confiables para engañar a las personas y obtener información sensible, como contraseñas, números de tarjetas de crédito o detalles de cuentas bancarias. Este tipo de fraude se realiza comúnmente a través de correos electrónicos, mensajes de texto o llamadas telefónicas que parecen provenir de una fuente legítima, como un banco o una plataforma de servicios en línea. Los mensajes suelen incluir enlaces o archivos adjuntos maliciosos, que al ser abiertos, permiten a los delincuentes acceder a la información personal de la víctima.

Para Macías-Lara et al (2022), el robo de identidad ocurre cuando un delincuente obtiene y utiliza la información personal de otra persona sin su consentimiento, generalmente con fines de lucro. Los delincuentes pueden usar esta información para abrir cuentas bancarias, solicitar tarjetas de crédito, obtener préstamos o realizar compras en nombre de la víctima. Este tipo de fraude puede tener consecuencias graves

para las víctimas, incluyendo daños a su historial crediticio y la necesidad de invertir tiempo y recursos en resolver los problemas causados por el uso fraudulento de su identidad.

Las transacciones no autorizadas son aquellas que se realizan en una cuenta sin el conocimiento o el consentimiento del titular de la cuenta. Este tipo de fraude puede ocurrir de varias formas, como el uso fraudulento de tarjetas de crédito o débito, el hacking de cuentas en línea o mediante el uso de datos de pago robados. Las transacciones no autorizadas pueden resultar en pérdidas financieras significativas y requieren que las víctimas actúen rápidamente para informar a sus instituciones financieras y limitar el daño. Es crucial monitorear regularmente las cuentas bancarias y de crédito para detectar cualquier actividad inusual y tomar medidas de seguridad, como la autenticación de dos factores, para protegerse contra este tipo de fraude.

Según Utkina (2023), la importancia de implementar medidas de seguridad frente a los delitos financieros digitales radica en la creciente sofisticación y prevalencia de las amenazas cibernéticas en un mundo cada vez más interconectado. Con el aumento de transacciones en línea y el uso de plataformas digitales para la gestión de activos, los delincuentes han encontrado nuevas oportunidades para perpetrar fraudes, robo de identidad y otros delitos que pueden tener consecuencias devastadoras para individuos y organizaciones. Proteger la información financiera y personal mediante medidas de seguridad robustas, como la autenticación multifactorial, la encriptación de datos y el monitoreo constante, no solo ayuda a prevenir pérdidas económicas significativas, sino que también refuerza la confianza de los consumidores y usuarios en el uso de servicios digitales. Al adoptar una postura proactiva en la seguridad, las entidades pueden mitigar riesgos, proteger sus operaciones y garantizar un entorno más seguro para todos en el ecosistema financiero.

Arner et al., (2019) mencionan, que la implementación de autenticación multifactorial (MFA) es un método de seguridad que requiere que los usuarios proporcionen dos o más factores de autenticación para verificar su identidad. Este enfoque puede incluir elementos como algo que el usuario sabe (como una contraseña),

algo que posee (como un teléfono móvil o un token de seguridad), o algo que es (como una huella dactilar o reconocimiento facial). Al adoptar MFA, se reduce significativamente el riesgo de acceso no autorizado, ya que un atacante necesitaría más que solo la contraseña de un usuario para lograr acceso a información sensible.

Para Nicholls et al (2021), la encriptación avanzada de datos se refiere al proceso de transformar datos legibles en un formato codificado, de manera que solo las personas autorizadas puedan acceder a esta información. Este proceso implica el uso de algoritmos de encriptación robustos y técnicas complejas de gestión de claves, tanto para proteger datos en reposo (almacenados) como en tránsito (mientras se transfieren). La encriptación es fundamental para salvaguardar la confidencialidad de información sensible, como datos personales, financieros o de salud, asegurando que solo aquellos que tienen permiso puedan acceder a ella.

Menciona Sekgoka et al (2022), que el monitoreo en tiempo real de transacciones consiste en la supervisión constante de las actividades realizadas en un sistema o red para detectar y responder a comportamientos sospechosos o inusuales. Utilizando sistemas de análisis y alertas automáticas, esta práctica permite identificar fraudes, violaciones de seguridad o amenazas cibernéticas en el momento en que ocurren. La capacidad de actuar rápidamente ante incidentes de seguridad es crucial para mitigar el daño y proteger los activos de información.

Por último, las auditorías de seguridad periódicas son revisiones sistemáticas que evalúan el estado de seguridad de un sistema, red o aplicación. Estas auditorías se llevan a cabo de manera regular para identificar vulnerabilidades, evaluar la efectividad de las medidas de seguridad implementadas y garantizar el cumplimiento de políticas y regulaciones. Pueden incluir revisiones de acceso, pruebas de penetración, análisis de configuraciones y auditorías de políticas de seguridad, y son un componente esencial en la gestión de riesgos y la mejora continua de la seguridad.

En conjunto, estos elementos son fundamentales para fortalecer las defensas de un sistema y proteger la información sensible frente a diversas amenazas.

DESARROLLO.

Materiales y métodos.

Para abordar el estudio sobre el fraude financiero por transacciones digitales en Ecuador, se implementó una metodología integral que incluyó varias etapas clave. Primero, se realizó una búsqueda exhaustiva de datos relevantes, recopilando informes de instituciones financieras, estadísticas gubernamentales, estudios académicos y noticias sobre casos de fraude digital en el país. Esta recopilación de datos proporcionó un contexto sólido y permitió identificar áreas clave de interés para la investigación.

El marco teórico se basó en la literatura existente sobre fraude financiero, auditoría financiera y seguridad en transacciones digitales. Se revisaron y analizaron teorías y conceptos relevantes para comprender el fenómeno del fraude financiero en el contexto de las transacciones digitales en Ecuador. Esto proporcionó una base sólida para la formulación de hipótesis y la interpretación de los resultados del estudio.

La investigación utilizó una combinación de técnicas cualitativas para la recolección y análisis de datos. La técnica principal fue la realización de entrevistas en profundidad con una muestra diversa de usuarios financieros ecuatorianos, incluyendo clientes de bancos, tarjetahabientes, comerciantes en línea y profesionales del sector financiero. Estas entrevistas se llevaron a cabo de manera semiestructurada para permitir una exploración detallada de las experiencias, percepciones y opiniones de los participantes sobre el fraude financiero por transacciones digitales.

Se diseñó una encuesta específica para este propósito, recopilando datos de 40 participantes mediante un muestreo por conveniencia. Los participantes proporcionaron información valiosa sobre sus hábitos de transacciones en línea, su nivel de preocupación por el fraude, y sus experiencias y percepciones sobre las medidas de seguridad y la respuesta institucional.

La elección de una metodología cualitativa, centrada en entrevistas en profundidad, y se justifica por la naturaleza exploratoria y descriptiva del estudio. Esta metodología permitió una comprensión profunda y contextualizada de las experiencias y percepciones de los participantes sobre el fraude financiero en el entorno digital ecuatoriano. Al centrarse en las narrativas individuales de los participantes, se pudo capturar una amplia gama de perspectivas, enriqueciendo así la comprensión del fenómeno estudiado. Esta aproximación también permitió identificar áreas clave de preocupación y sugerir posibles estrategias de prevención y mitigación del fraude financiero por transacciones digitales en Ecuador.

Para complementar el estudio, se consultaron informes como el de la Asociación de Bancos del Ecuador, que proporciona estadísticas y análisis sobre el impacto del fraude digital en el sector financiero ecuatoriano, y reportes de empresas de seguridad cibernética que detallan tendencias y amenazas actuales en el fraude por transacciones digitales (TransUnion) (Asobanca). Estos informes ayudan a contextualizar los datos obtenidos y ofrecen una visión más amplia de la situación en Ecuador.

Resultados.

La creciente adopción de transacciones electrónicas ha transformado significativamente la manera en que se realizan los pagos y las transferencias de dinero en el ámbito financiero. Este aumento en la digitalización de los servicios financieros ha traído consigo numerosos beneficios como la rapidez, la conveniencia y la capacidad de realizar operaciones sin fronteras; no obstante, también ha generado nuevos desafíos y riesgos, especialmente en lo que respecta a la seguridad y la prevención de fraudes. En este contexto, presentamos los resultados de nuestra investigación sobre el promedio y el porcentaje de transacciones electrónicas y fraudulentas. Este análisis busca proporcionar una visión detallada de la magnitud de las transacciones electrónicas y la prevalencia de fraudes, destacando la necesidad urgente de fortalecer las medidas de seguridad y los marcos legales para mitigar estos riesgos; además, se discuten los hallazgos en relación con estudios previos que abordan la intersección entre la digitalización y los delitos financieros, subrayando la

importancia de una respuesta integral y coordinada para asegurar la integridad del sistema financiero en la era digital.

Tabla 1. Transacciones por tipo de canal.

Transacciones por tipo de canal					
Tipo	**Promedio anual**		**Porcentaje anual**		**Variación**
	2022	**2023**	**2022**	**2023**	
Electrónicas	2.939	3.095	73,59%	73,67%	5,30%
Físicas	1.055	1.106	26,41%	26,33%	4,80%
Suman	3.994	4.201	100,00%	100,00%	10,10%

Fuente: Superintendencia de Bancos.

La tabla de "Transacciones por tipo de canal" presenta datos sobre el promedio anual y el porcentaje anual de transacciones, diferenciando entre transacciones electrónicas y transacciones físicas, para los años 2022 y 2023; además, incluye la variación porcentual de un año a otro.

En cuanto a las transacciones electrónicas, el promedio anual fue de 2,939 en el año 2022, aumentando a 3,095 en el 2023. Este incremento representa una variación del 5.30%. En términos de porcentaje anual, las transacciones electrónicas constituyeron el 73.59% del total en el año 2022, incrementándose ligeramente a 73.67% en el 2023. Esto indica una tendencia positiva en el uso de canales electrónicos para realizar transacciones.

Las transacciones físicas también mostraron un incremento, aunque más modesto. El promedio anual de estas transacciones fue de 1,055 en el año 2022, aumentando a 1,106 en el 2023, lo que representa un incremento del 4.80%. En cuanto al porcentaje anual, las transacciones físicas representaron el 26.41% del total en el año 2022, disminuyendo ligeramente a 26.33% en el 2023.

Sumando ambos tipos de transacciones, el total de transacciones fue de 3,994 en el año 2022 y aumentó a 4,201 en el 2023, lo que representa una variación del 10.10%. Este crecimiento general en el número de transacciones sugiere una tendencia positiva en la actividad transaccional en el país.

Tabla 2. Fraudes determinados en transacciones digitales.

Fraudes determinados en transacciones digitales					
Año	**Casos de fraude**	**Pérdidas económicas (en millones de usd)**	**Phishing**	**Robo de identidad**	**Transacciones no autorizadas**
2021	2400	7	30%	20%	15%
2022	2500	8	32%	22%	18%
2023	3000	10	35%	25%	20%

Fuente: Superintendencia de Bancos.

La tabla muestra un análisis de los fraudes determinados en transacciones digitales durante los años 2021, 2022 y 2023. Se incluyen datos sobre el número de casos de fraude, las pérdidas económicas en millones de dólares, y el porcentaje de los diferentes tipos de fraude: phishing, robo de identidad y transacciones no autorizadas; además, se presenta el promedio mensual de casos de fraude y pérdidas económicas.

En el año 2021, se reportaron 2,400 casos de fraude con pérdidas económicas que ascendieron a 7 millones de dólares. Los tipos de fraude más comunes fueron el phishing, representando el 30% de los casos, seguido por el robo de identidad con un 20% y las transacciones no autorizadas con un 15%.

En el año 2022, el número de casos de fraude aumentó ligeramente a 2,500, con pérdidas económicas de 8 millones de dólares. El phishing continuó siendo el tipo de fraude más prevalente, incrementando su participación al 32%. El robo de identidad representó el 22% de los casos y las transacciones no autorizadas aumentaron al 18%.

El año 2023 mostró un incremento significativo en los casos de fraude, alcanzando los 3,000, y las pérdidas económicas subieron a 10 millones de dólares. El phishing representó el 35% de los fraudes, seguido por el robo de identidad con un 25% y las transacciones no autorizadas con un 20%.

El promedio mensual de casos de fraude durante estos tres años es de 250, y las pérdidas económicas promedio mensuales ascienden a aproximadamente 0.83 millones de dólares.

Tabla 3. Porcentaje de transacciones electrónicas y fraudes.

Transacciones electrónicas promedio	3.095,00	10.316.666,67
Promedio mensual transacciones fraudulentas	250,00	833.333,33
Porcentaje de transacciones fraudulentas	8,08%	8,08%

Fuente: Superintendencia de Bancos.

La tabla titulada "Porcentaje de transacciones electrónicas y fraudes" proporciona un análisis detallado de las transacciones electrónicas promedio y las transacciones fraudulentas mensuales, junto con el porcentaje de transacciones fraudulentas en relación con el total.

El promedio de transacciones electrónicas se sitúa en 3,095 con un valor total de 10,316,666.67. Este dato refleja la cantidad promedio de transacciones que se realizan electrónicamente, indicando una adopción significativa de métodos de pago y transacciones digitales. La adopción de estas tecnologías sugiere una tendencia hacia la conveniencia y la eficiencia que ofrecen las transacciones electrónicas.

El promedio mensual de transacciones fraudulentas es de 250, con un impacto económico mensual promedio de 833,333.33. Esto subraya el hecho, de que a pesar del crecimiento en el uso de transacciones electrónicas, las actividades fraudulentas siguen representando un desafío considerable. La cifra indica, que mensualmente una cantidad significativa de transacciones son identificadas como fraudulentas, lo que afecta tanto a los consumidores como a las instituciones financieras.

El porcentaje de transacciones fraudulentas se calcula en un 8.08% del total de transacciones electrónicas. Este dato es crucial para comprender el alcance del problema del fraude en el contexto de las transacciones digitales. Un porcentaje del 8.08% sugiere, que aunque la mayoría de las transacciones electrónicas son seguras y legítimas, una parte considerable sigue siendo vulnerable al fraude.

Tabla 4. Matriz integral sobre medidas tecnológicas, legales y de formación para el fortalecimiento de la seguridad y prevención de fraudes en transacciones digitales.

Área	Medidas/Actividades	Objetivo	Responsables	Plazo
Seguridad Tecnológica	Implementación de autenticación multifactorial (MFA)	Aumentar la seguridad de acceso a las cuentas de usuarios	Instituciones Financieras	Corto plazo
	Encriptación avanzada de datos	Proteger la información sensible de los usuarios	Instituciones Financieras	Corto plazo
	Monitoreo en tiempo real de transacciones	Detectar y responder rápidamente a actividades sospechosas	Instituciones Financieras	Mediano plazo
	Auditorías de seguridad periódicas	Identificar y corregir vulnerabilidades en los sistemas	Instituciones Financieras	Largo plazo
Marco Jurídico	Actualización de leyes para incluir delitos digitales específicos	Adaptar el marco legal a las nuevas formas de delitos financieros digitales	Ejecutivo y Legislativo	Mediano plazo
	Fortalecimiento de las sanciones por fraudes financieros	Disuadir a potenciales criminales mediante sanciones más severas	Ejecutivo y Legislativo	Mediano plazo
	Creación de un organismo regulador especializado en delitos financieros digitales	Coordinar y supervisar las acciones contra el fraude digital	Gobierno Nacional, Organismos Reguladores	Largo plazo
	Desarrollo de reglamentos específicos para la protección de datos personales según la Ley Orgánica De Protección De Datos Personales	Proteger la privacidad y los datos personales de los usuarios	Ejecutivo y Legislativo	Mediano plazo
Capacitación y Conciencia	Programas de capacitación continua para empleados sobre ciberseguridad y protección de datos personales	Mejorar la respuesta y prevención de fraudes mediante un personal capacitado	Instituciones Financieras	Corto plazo
	Campañas de concientización para los usuarios sobre las prácticas seguras en transacciones digitales	Empoderar a los usuarios para protegerse contra el fraude	Instituciones Financieras	Corto plazo

	Desarrollo de un protocolo de respuesta rápida ante incidentes de seguridad	Minimizar el impacto de los fraudes y ataques mediante una respuesta eficiente	Instituciones Financieras	Corto plazo
Colaboración y Coordinación	Establecimiento de alianzas con otras instituciones financieras y agencias gubernamentales para compartir información y mejores prácticas	Mejorar la eficacia de la prevención y respuesta a fraudes mediante la colaboración y el intercambio de información	Instituciones Financieras, Gobierno Nacional	Largo plazo
	Participación en iniciativas internacionales contra el fraude financiero	Fortalecer la capacidad de respuesta ante fraudes transnacionales	Instituciones Financieras, Gobierno Nacional	Largo plazo
	Creación de un centro de ciberseguridad nacional especializado en la protección de transacciones digitales	Centralizar y coordinar los esfuerzos de seguridad a nivel nacional	Gobierno Nacional, Organismos Reguladores	Largo plazo

Fuente: Investigación.

La matriz integral presentada se basa en los resultados obtenidos a través de una encuesta desarrollada y aplicada mediante entrevistas en profundidad con una muestra diversa de usuarios financieros ecuatorianos. Esta muestra incluyó clientes de bancos, tarjetahabientes, comerciantes en línea y profesionales del sector financiero, proporcionando una visión amplia y representativa de las necesidades y percepciones de seguridad en las transacciones digitales en Ecuador.

En el área de Seguridad Tecnológica, se destacan medidas como la implementación de autenticación multifactorial (MFA) y la encriptación avanzada de datos, que buscan aumentar significativamente la seguridad de acceso y protección de información sensible. Estas medidas son cruciales para proteger a los usuarios de posibles fraudes y ataques cibernéticos, permitiendo una respuesta rápida y efectiva a actividades sospechosas a través del monitoreo en tiempo real de transacciones y auditorías periódicas.

El Marco Jurídico requiere actualizaciones para incluir delitos digitales específicos y fortalecer las sanciones por fraudes financieros. La creación de un organismo regulador especializado y el desarrollo de

reglamentos específicos en línea con la Ley Orgánica de Protección de Datos Personales (Asamblea Nacional del Ecuador, 2021) son pasos fundamentales para garantizar un entorno legal robusto que proteja la integridad del sistema financiero y la privacidad de los usuarios.

En cuanto a Capacitación y Conciencia, se identificó la necesidad de programas continuos de capacitación para empleados y campañas de concientización para los usuarios. Estas actividades buscan mejorar las capacidades de prevención y respuesta ante fraudes, empoderando a los usuarios y asegurando que el personal esté bien preparado para enfrentar posibles amenazas.

Finalmente, en el ámbito de Colaboración y Coordinación, la matriz sugiere la formación de alianzas entre instituciones financieras y agencias gubernamentales, así como la participación en iniciativas internacionales contra el fraude financiero. Estas colaboraciones son esenciales para compartir información y mejores prácticas, fortaleciendo la capacidad de respuesta ante fraudes transnacionales y centralizando los esfuerzos de seguridad a nivel nacional.

Discusión.

Los resultados obtenidos en la tabla "Promedio y Porcentaje de Transacciones Electrónicas y Fraudes" indican, que aunque las transacciones electrónicas han aumentado significativamente, el porcentaje de fraudes en estas transacciones sigue siendo una preocupación importante. En promedio, se realizan 3,095 transacciones electrónicas, con un promedio mensual de 250 transacciones fraudulentas, lo que representa un 8.08% del total de transacciones.

En el contexto del artículo de Wiwoho et al (2022), se puede observar, que la proliferación de pagos digitales y la rápida transformación digital presentan riesgos inherentes de delitos financieros, incluidos el lavado de dinero y la financiación del terrorismo. La investigación destaca la necesidad de un marco jurídico integral para prevenir el uso indebido de las tecnologías financieras (FinTech). Los resultados de nuestra investigación confirman que las transacciones electrónicas están sujetas a fraudes significativos, lo que refuerza la urgencia de establecer leyes y regulaciones robustas que aborden estos riesgos.

La digitalización está fomentando nuevos métodos de delitos económicos y financieros, manteniendo al mismo tiempo los métodos clásicos. La digitalización aumenta la probabilidad de estos delitos debido a la conectividad y el uso de internet. Los datos de nuestra investigación muestran, que aunque el uso de transacciones electrónicas es alto, el porcentaje de fraudes sigue siendo alarmante, lo que sugiere que la digitalización, si bien es beneficiosa, también introduce nuevas vulnerabilidades que deben ser abordadas. El artículo de Nikkel (2020) enfatiza la necesidad de una subdisciplina emergente en la informática forense dedicada a las tecnologías financieras. La transformación digital está siendo explotada por criminales para cometer fraudes y otros delitos financieros. Los resultados de nuestra investigación indican que la comunidad de expertos en informática forense tiene un papel crucial en la identificación y prevención de fraudes en transacciones electrónicas. La existencia de un promedio mensual de 250 transacciones fraudulentas destaca la necesidad de mejorar las técnicas de investigación y las capacidades forenses para combatir estos delitos.

Finalmente, Armey et al (2014) sugieren, que el acceso a pagos electrónicos puede tener un impacto positivo al reducir ciertos tipos de delitos económicos; sin embargo, nuestros datos muestran, que aunque las transacciones electrónicas están ampliamente adoptadas, el porcentaje de fraudes sigue siendo un desafío significativo. Esto sugiere, que si bien las transacciones electrónicas pueden disuadir algunos delitos, también es crucial implementar medidas adicionales de seguridad y prevención de fraudes.

CONCLUSIONES.

Los datos muestran un crecimiento general en el número de transacciones, con un incremento total del 10.10% del año 2022 al 2023. Las transacciones electrónicas son predominantemente más comunes que las físicas, representando más del 73% del total en ambos años. Aunque ambos tipos de transacciones han aumentado, el incremento porcentual es ligeramente mayor en las transacciones electrónicas (5.30%) en comparación con las transacciones físicas (4.80%). Este análisis sugiere una tendencia creciente en el uso

de canales electrónicos para realizar transacciones, lo cual podría estar relacionado con una mayor adopción de tecnologías digitales y una preferencia creciente por métodos de pago más convenientes y rápidos.

Se puede verificar un aumento constante en el número de casos de fraude y las pérdidas económicas asociadas a las transacciones digitales. El phishing es el tipo de fraude más común y ha mostrado un incremento en su prevalencia a lo largo de los años. También se observa un aumento en los casos de robo de identidad y transacciones no autorizadas. Estos hallazgos subrayan la necesidad de implementar medidas de seguridad más robustas y de concienciar a los usuarios sobre los riesgos y métodos de prevención de fraudes en el ámbito digital.

El análisis revela, que mientras que las transacciones electrónicas continúan siendo una parte esencial del comercio y las finanzas modernas con un promedio significativo de 3,095 transacciones, existe una preocupación constante por el fraude, con un promedio mensual de 250 transacciones fraudulentas y un porcentaje de fraude del 8.08%. Estos datos resaltan la necesidad de seguir mejorando las medidas de seguridad y educar a los usuarios sobre cómo protegerse contra actividades fraudulentas en el ámbito digital.

Los resultados obtenidos subrayan la necesidad de un marco legal integral, mejoras en la investigación forense de las FinTech y una atención continua a las vulnerabilidades introducidas por la digitalización. Aunque las transacciones electrónicas presentan beneficios claros, es esencial abordar los riesgos de fraudes para asegurar la integridad y seguridad del sistema financiero. Las investigaciones futuras deberían centrarse en desarrollar tecnologías y políticas que mitiguen estos riesgos y fortalezcan las medidas de prevención de fraudes.

En resumen, la matriz integral ofrece un enfoque multifacético para abordar los desafíos de seguridad en las transacciones digitales, basándose en la percepción y necesidades reales de los usuarios financieros ecuatorianos. A través de medidas tecnológicas avanzadas, un marco jurídico actualizado, capacitación

continua y una estrecha colaboración, se busca crear un entorno financiero más seguro y confiable en la era digital.

REFERENCIAS BIBLIOGRÁFICAS.

1. Armey, L., Lipow, J., & Webb, N. (2014). The impact of electronic financial payments on crime. Information Economics and Policy, 29, 46-57. https://www.sciencedirect.com/science/article/abs/pii/S0167624514000432
2. Arner, D., Zetzsche, D., Buckley, R., & Barberis, J. (2019). The identity challenge in finance: from analogue identity to digitized identification to digital KYC utilities. European business organization law review, 20, 55-80. https://link.springer.com/article/10.1007/s40804-019-00135-1
3. Asamblea Nacional del Ecuador (2021). Ley Orgánica de Protección de Datos Personales. Registro Oficial Suplemento N. 459. https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf
4. Beck, T., Pamuk, H., Ramrattan, R., & Uras, B. R. (2018). Payment instruments, finance and development. Journal of Development Economics, 133, 162-186. https://www.sciencedirect.com/science/article/pii/S0304387818300075
5. Gonzáles, J., Bermeo, J., Villacreses, E., & Guerrero, J. (2018). Delitos informáticos: una revisión en Latinoamérica. In Conference Proceedings (Machala) (Vol. 2, No. 1, p. 6). https://dialnet.unirioja.es/servlet/articulo?codigo=9358671&orden=0&info=link
6. Grey, R. (2017). Mobile finance in developing countries: macroeconomic implications and potential. Global Institute for Sustainable Prosperity. https://www.global-isp.org/wp-content/uploads/WP-116.pdf
7. Grisanti, A. (2016). Los fraudes en las organizaciones y el papel de la auditoría forense en este contexto. Sapienza Organizacional, 3(6), 11-36.

8. Groppa, O., & Curi, F. (2012). Mobile Money Regulation: Kenya, Ecuador and Brazil Compared. Ecuador and Brazil Compared (September 20, 2012). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2298781

9. Khattri, V., & Singh, D. K. (2019). Implementation of an additional factor for secure authentication in online transactions. Journal of Organizational Computing and Electronic Commerce, 29(4), 258-273. https://www.tandfonline.com/doi/full/10.1080/10919392.2019.1633123?scroll=top&needAccess=true

10. Macías-Lara, R. A., Andrade, M. F. B., Angulo, F. Q., Loor, J. J. M., Estupiñan-Troya, G., & Vizuete, J. D. R. (2022). Casos frecuentes, penalización y prevención de los delitos informáticos en el Ecuador: una breve revisión sistemática. Sapienza: International Journal of Interdisciplinary Studies, 3(2), 231-243. https://www.journals.sapienzaeditorial.com/index.php/SIJIS/article/view/324/199

11. Nicholls, J., Kuppa, A., & Le-Khac, N. A. (2021). Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. Ieee Access, 9, 163965-163986. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9642993

12. Nikkel, B. (2020). Fintech forensics: Criminal investigation and digital evidence in financial technologies. Forensic Science International: Digital Investigation, 33, 200908. https://www.sciencedirect.com/science/article/abs/pii/S2666281720300287

13. Sekgoka, C. P., Yadavalli, V. S. S., & Adetunji, O. (2022). Privacy-preserving data mining of cross-border financial flows. Cogent Engineering, 9(1), 2046680. https://www.tandfonline.com/doi/full/10.1080/23311916.2022.2046680

14. Utkina, M. (2023). Digital Identification and Financial Monitoring: New Technologies in the Fight against Crime. Scientific Journal of Polonia University, 58(3), 303-308. http://pnap.ap.edu.pl/index.php/pnap/article/view/1155/1105

15. Wiwoho, J., Kharisma, D. B., & Wardhono, D. T. K. (2022). Financial crime in digital payments. Journal of Central Banking Law and Institutions, 1(1), 47-70. https://www.jcli-bi.org/index.php/jcli/article/view/7/10

DATOS DE LOS AUTORES.

1. **Carlos Wilman Maldonado Gudiño.** Magíster en Auditoría Integral. Docente de la Universidad Regional Autónoma de Los Andes, Matriz Ambato, Ecuador. E-mail: ui.carlosmaldonado@uniandes.edu.ec
2. **Adrián Fernando Sánchez Puga.** Estudiante de la Universidad Regional Autónoma de Los Andes, Matriz Ambato, Ecuador. E-mail: adriansp93@uniandes.edu.ec
3. **Dolores Paulina Ramírez Flores.** Estudiante de la Universidad Regional Autónoma de Los Andes, Matriz Ambato, Ecuador. E-mail: doloresrf69@uniandes.edu.ec
4. **Karla Dayana Hallo Silva.** Estudiante de la Universidad Regional Autónoma de Los Andes, Matriz Ambato, Ecuador. E-mail: karladhs48@uniandes.edu.ec

RECIBIDO: 20 de septiembre del 2024. **APROBADO:** 16 de octubre del 2024.