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: 2 Artículo no.:41 Período: 1 de enero al 30 de abril del 2025

TÍTULO: Impacto del ciberfraude en la banca digital y en la sociedad ecuatoriana.

AUTORES:

1. Máster. Carlos Wilman Maldonado Gudiño.
2. Est. Adrián Fernando Sánchez Puga.
3. Est. Alba Karina Vaca Morales.
4. Est. Daniela Marilin Núñez Taboada.

RESUMEN: El objetivo de este estudio fue analizar los niveles de conciencia y las medidas de prevención frente al fraude financiero por transacciones digitales en Ecuador; incluso, evaluar el rol de las instituciones financieras y la efectividad de las estrategias de seguridad implementadas para proteger a los usuarios. Se aplicaron encuestas y entrevistas en ciberseguridad sobre la percepción del riesgo y las medidas de seguridad actuales, incluyendo un análisis de las prácticas de seguridad adoptadas por las instituciones financieras. Se reveló una disparidad en el nivel de conciencia entre los usuarios, con una parte significativa aún desinformada sobre los riesgos asociados, identificándose áreas de mejora, particularmente en la necesidad de mayores inversiones en tecnología y capacitación continua para los usuarios.

PALABRAS CLAVES: seguridad en línea, transacciones online, protección de datos, educación en ciberseguridad, seguridad bancaria.

TITLE: Impact of cyberfraud on digital banking and in the Ecuadorian society.

AUTHORS:

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

3. Stud. Alba Karina Vaca Morales

4. Stud. Daniela Marilin Núñez Taboada

ABSTRACT: The objective of this study was to analyze the awareness levels and prevention measures against financial fraud through digital transactions in Ecuador; including to evaluate the role of financial institutions and the effectiveness of security strategies implemented to protect users. Cybersecurity surveys and interviews were applied on risk perception and current security measures, including an analysis of security practices adopted by financial institutions. A disparity in the level of awareness among users was revealed, with a significant portion still uninformed about the associated risks, identifying areas for improvement, particularly in the need for greater investments in technology and ongoing training for users.

KEY WORDS: online security, online transactions, data protection, cybersecurity education, banking security.

INTRODUCCIÓN.

La auditoría constituye una práctica que ha existido desde las primeras civilizaciones, estrechamente relacionada con el desarrollo de la contabilidad (Peñarreta-Angamarca et al., 2024). Ambas disciplinas han sido fundamentales para garantizar la transparencia en las transacciones económicas (Moya-Sánchez & Torres-Palacios, 2024).

A lo largo del tiempo, la auditoría ha evolucionado desde un mecanismo rudimentario de supervisión hasta convertirse en un proceso normativo y altamente estructurado (Castro Peñaloza & Narváez Zurita, 2024); sin embargo, persiste una distorsión en la comprensión de su origen y evolución, lo que ha llevado a que su aplicación se enfoque mayormente en un marco legalista. Esta situación conduce a la exploración de los elementos asociados para valorar adecuadamente la relevancia en las finanzas modernas y el papel en la prevención del fraude.

El fraude, entendido como un acto intencional de engaño o deshonestidad, tiene como objetivo perjudicar a una persona o entidad en beneficio propio. La intencionalidad es un elemento clave, ya que implica la búsqueda deliberada de una ventaja ilícita. Este fenómeno se presenta de diversas formas, al afectar

especialmente áreas sensibles como la información y los recursos financieros, que pueden ser manipulados, transferidos o robados (Ávila-Coello, 2024). En este sentido, es esencial comprender que el fraude, independientemente de su modalidad, se sitúa en la intersección entre la contabilidad y la ley, al ser ambas disciplinas afectadas por este tipo de conductas ilícitas.

Aunque el concepto de fraude es amplio, a menudo se asocia con acciones perpetradas por la gerencia o empleados de una empresa para obtener beneficios ilícitos, ya sea a nivel personal o grupal. Este tipo de acciones adquiere un impacto considerable en los estados financieros, al distorsionar la información crucial como el estado de resultados y el balance general; así no solo afecta la transparencia de los informes financieros, sino que también compromete la confianza en la gestión empresarial (Baroffio & Lara, 2024).

A nivel global, el fraude ha cobrado relevancia debido a su creciente interconexión con los sistemas contables y jurídicos (Bermeo-Giraldo et al., 2021). Las empresas que no implementan medidas de control interno adecuadas, se encuentran más expuestas a ser víctimas de fraudes financieros. Desafortunadamente, muchas organizaciones solo toman conciencia de estas deficiencias tras haber sufrido pérdidas significativas. Este tipo de lecciones gravosas insiste en la prioridad de contar con sistemas de control interno que prevengan el fraude antes de que cause daños irreversibles.

En el entorno digital actual, los fraudes financieros han adquirido una nueva dimensión, en conjunto con el desarrollo de las tecnologías (Córdova, 2024). Las transacciones en línea, que facilitan el comercio global, han aumentado los riesgos de fraude cibernético, al afectar tanto a individuos como a empresas. Esta situación ha llevado a que las preocupaciones en torno a la seguridad digital se sitúen en el centro de las estrategias organizacionales para proteger la información financiera y evitar pérdidas económicas (Guachún-Orellana & Andrade-Amoroso, 2024) (Lara et al., 2024) (Herrera et al., 2024) (Calle-Tenesaca & Andrade-Amoroso, 2024).

La falta de controles organizacionales sólidos no solo aumenta la vulnerabilidad frente al fraude, sino que también facilita el arraigo de prácticas corruptas (Ponce Tubay, 2024). Las empresas que no priorizan la implementación de sistemas de control efectivo se enfrentan a un mayor riesgo de sufrir desfalcos y otros

tipos de pérdidas financieras (López-Pincay et al., 2024). En muchos casos, la ausencia de estas medidas preventivas genera un entorno propicio para el fraude corporativo (Tubay, 2024), que conduce a consecuencias devastadoras para la viabilidad y la reputación de una empresa.

La creciente adopción de tecnologías financieras, como las criptomonedas, ha añadido una nueva capa de complejidad a la detección y regulación del fraude. Al operar fuera del control de las instituciones financieras tradicionales, estas tecnologías han facilitado en muchos casos actividades ilícitas como el lavado de dinero (Moreira-Basurto et al., 2024). Los esfuerzos para regular este tipo de operaciones aún están en desarrollo, pero enfrentan numerosos desafíos debido a la naturaleza descentralizada de las criptomonedas y la falta de supervisión por parte de entidades financieras convencionales (Astudillo-Romero & de las Mercedes Torres-Negrete, 2024).

El presente estudio se orienta en analizar los niveles de conciencia y las medidas de prevención frente al fraude financiero por transacciones digitales en Ecuador, además de evaluar el rol de las instituciones financieras y la efectividad de las estrategias de seguridad implementadas para proteger a los usuarios.

DESARROLLO.

Materiales y Métodos.

El estudio sobre el fraude financiero en transacciones digitales en Ecuador se realizó mediante una metodología integral que combinó múltiples enfoques y técnicas (Zhang et al., 2023). Inicialmente, se realizó una búsqueda de datos relevantes, al recopilar informes de instituciones financieras, estadísticas gubernamentales, estudios académicos y noticias relacionadas con casos de fraude digital en el país. Esta recopilación permitió establecer un contexto sólido, al facilitar la identificación de las áreas clave de interés para la investigación.

El marco teórico se construyó a partir de una revisión de la literatura existente sobre el fraude financiero, la auditoría financiera y la seguridad en transacciones digitales. Las teorías y conceptos analizados proporcionaron una base para comprender el fenómeno del fraude financiero en el contexto de las transacciones digitales en Ecuador.

En cuanto a las técnicas de recolección y análisis de datos, se optó por una metodología cualitativa (Tramullas, 2020). La técnica principal consistió en la realización de entrevistas en profundidad con una muestra diversa de usuarios del sistema financiero ecuatoriano; de modo, que se incluyó a clientes bancarios, tarjetahabientes, comerciantes en línea, y profesionales del sector financiero. Estas entrevistas, de manera semiestructurada, permitieron explorar las experiencias, percepciones y opiniones de los participantes sobre el fraude financiero por transacciones digitales.

Se diseñó una encuesta específica para el estudio, dirigida a una muestra de 40 participantes seleccionados mediante un muestreo por conveniencia. A través de esta encuesta, se recopiló información sobre los hábitos de transacciones en línea de los encuestados, su nivel de preocupación ante el fraude, así como sus experiencias previas y percepciones sobre las medidas de seguridad y la respuesta de las instituciones.

La elección de una metodología cualitativa, basada en entrevistas en profundidad, fue justificada por la naturaleza exploratoria del estudio. Esta aproximación permitió una comprensión y contextualizada de las vivencias de los participantes, al capturar una amplia variedad de perspectivas; a su vez, esta metodología facilitó la identificación de áreas críticas de preocupación, al sugerir posibles estrategias de prevención y mitigación del fraude financiero en las transacciones digitales en Ecuador.

Resultados.

Tipos de fraude financiero digital.

En Ecuador, los principales tipos de fraude financiero digital que afectan a los usuarios de servicios bancarios incluyen varias formas de ataque, entre las que destacan el phishing y el malware (ver tabla 1); incluso, se centra en engañar a los usuarios para obtener información confidencial, para acceder a los datos financieros de las víctimas.

Tabla 1. Tipos de fraude financiero digital en Ecuador.

Tipo	Descripción	Métodos comunes	Impacto
Phishing	Técnica para engañar a los usuarios y obtener información confidencial a través de correos electrónicos fraudulentos, mensajes de texto o sitios web imitados.	Correos electrónicos o mensajes fraudulentos que solicitan información personal o enlaces maliciosos.	Pérdida de fondos, robo de identidad, compromiso de cuentas bancarias.
Malware	Software malicioso como virus, troyanos y ransomware diseñado para infiltrarse en sistemas y obtener acceso a datos financieros.	Infección a través de descargas, enlaces en correos electrónicos o sitios web comprometidos.	Robo de información financiera, pérdida de acceso a datos, extorsión mediante ransomware.
Fraude de tarjeta de crédito	Uso no autorizado de datos de tarjetas de crédito para realizar transacciones fraudulentas.	Clonación de tarjetas o compras en línea sin autorización del titular.	Pérdidas económicas y afectación del historial crediticio.
Fraude de identidad	Obtención y uso no autorizado de la identidad de una persona para realizar transacciones financieras fraudulentas.	Uso de datos robados para abrir cuentas, solicitar créditos o realizar compras.	Problemas financieros y legales, así como la afectación de la reputación crediticia.
Fraude por redes sociales	Creación de perfiles falsos o suplantación de identidad en redes sociales para engañar a los usuarios.	Ofrecimiento de oportunidades de inversión falsas, venta de productos inexistentes, o recopilación de datos personales.	Pérdida de dinero y exposición de datos personales.

Fuente: Elaboración propia.

Percepción del fraude en transacciones digitales en Ecuador.

Los resultados de las encuestas y la revisión de los materiales consultado ofrecen un análisis sobre la percepción del fraude en transacciones digitales en Ecuador, al proporcionar una base para el desarrollo de estrategias preventivas tanto a nivel personal como institucional. Los hallazgos obtenidos contribuyen a la creación de un entorno digital más seguro y confiable para las transacciones financieras en el país. Entre ellos, se destacan:

- *Frecuencia de transacciones digitales.*

En la Figura 1, se detalla la frecuencia con que los participantes realizan transacciones en línea. Un 35,00% de los encuestados informó realizar transacciones diariamente, lo cual indica una confianza significativa en los servicios financieros digitales; además, un 40,00% afirmó llevar a cabo estas operaciones varias veces por semana, mientras que un 12,50% lo hace solo una vez a la semana; sin embargo, un 10,00% manifestó realizar transacciones con menor frecuencia, y solo un 2,50% indicó no utilizar estos servicios.

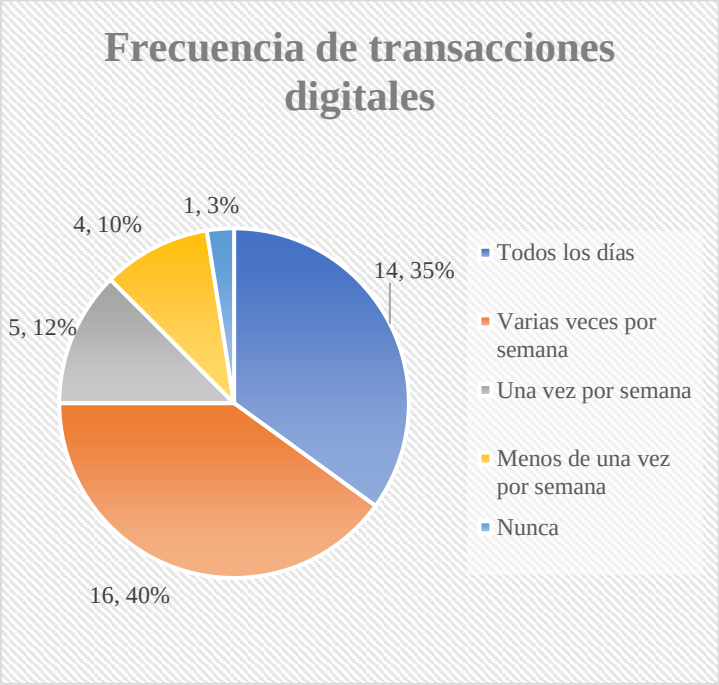

Figura 1. Frecuencia de transacciones digitales. Fuente: La investigación.

- *Preocupación sobre el fraude*.

Según la Figura 2, un 62,50% de los encuestados se mostró "muy preocupado" ante la posibilidad de ser víctima de fraude en transacciones digitales, y un 27,50% se declaró "preocupado". Apenas un 7,50% afirmó estar "poco preocupado", y un mínimo 2,50% expresó no tener inquietudes al respecto. Estos resultados evidencian la percepción generalizada del riesgo que conllevan las transacciones financieras en línea.

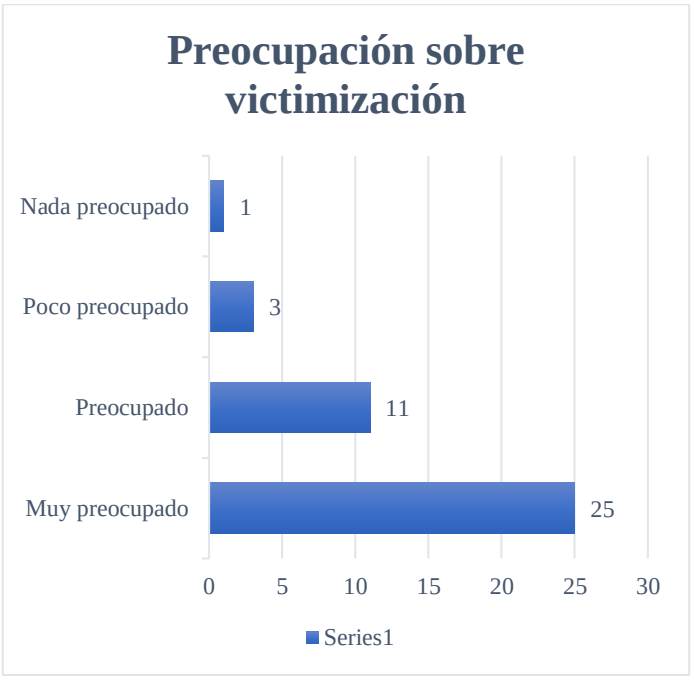

Figura 2. Preocupación sobre victimización. Fuente: La investigación.

- *Gravedad percibida del fraude*.

Como se observa en la Figura 3, un 55,00% de los participantes percibe el fraude en transacciones digitales como un problema "muy significativo" en Ecuador, y un 37,50% lo considera "significativo". Solo un 7,50% cree que el problema es "moderado", lo que acentúa la prioridad de implementar medidas preventivas y de seguridad más estrictas.

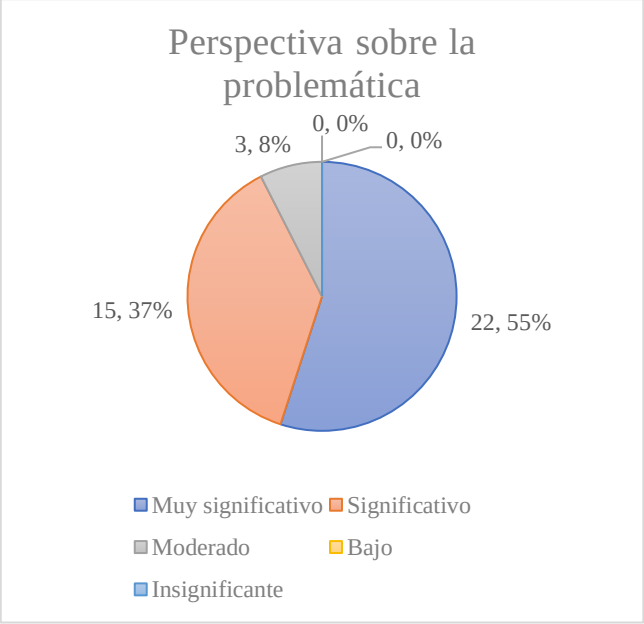

Figura 2. Perspectiva sobre la problemática. Fuente: La investigación.

- *Medidas de seguridad empleadas.*

En la Figura 4, se ilustra que un 57,50% de los encuestados emplea contraseñas seguras como principal medida de protección en transacciones digitales; además, un 20,00% ha adoptado la autenticación de dos factores, y un 7,50% utiliza software antivirus, mientras que un 15,00% ha incorporado tecnologías biométricas como el reconocimiento facial; por tanto, es notable que ningún participante dejó de implementar medidas de seguridad, lo que demuestra un alto nivel de concienciación sobre la prioridad de proteger las transacciones.

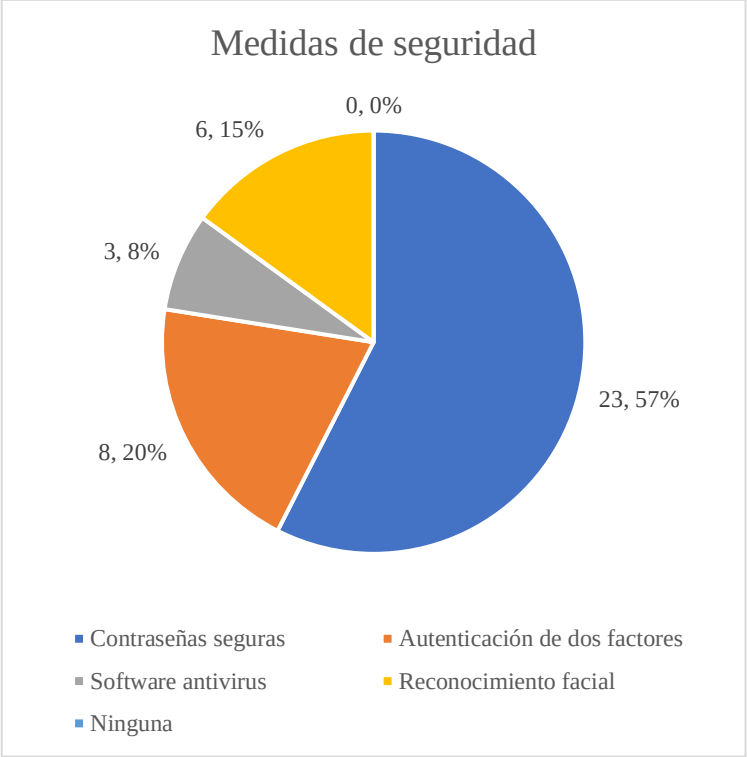

Figura 3. Medidas de seguridad. Fuente: La investigación.

- Educación en ciberseguridad.

La Figura 5 revela que un 57,50% de los encuestados recibe información regular sobre ciberseguridad por parte de sus instituciones financieras, mientras que un 20,00% la recibe con frecuencia. Un 17,50% informó recibir esta información ocasionalmente, y un 7,50% afirmó recibirla casi nunca. Solo un 2,50% no recibe ningún tipo de educación en ciberseguridad, lo que sugiere la necesidad de mejorar la difusión de este tipo de información.

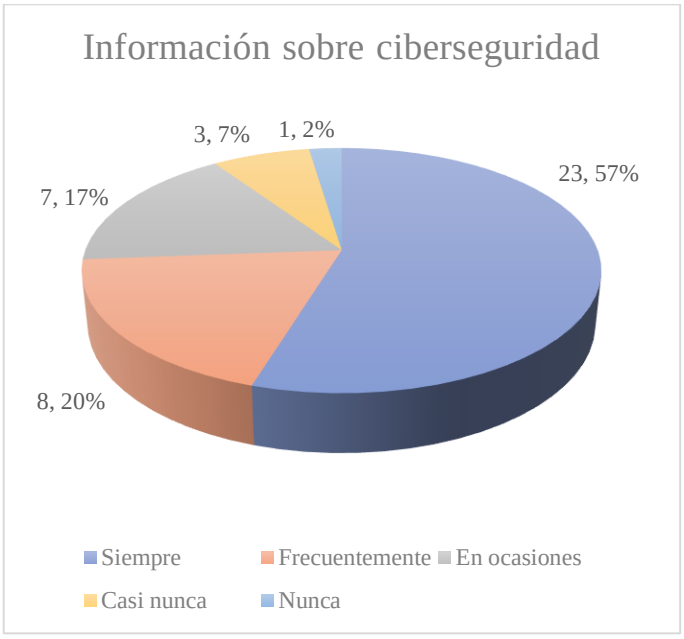

Figura 4. Información sobre ciberseguridad. Fuente: La investigación.

- Experiencia de victimización.

En la Figura 6, un 35,00% de los participantes afirmó haber sido víctima de fraude en transacciones digitales, mientras que un 60,00% indicó no haber sido afectado; sin embargo, un 5,00% expresó no estar seguro de haber sido víctima, lo que refleja una posible falta de conocimiento sobre los incidentes de fraude digital.

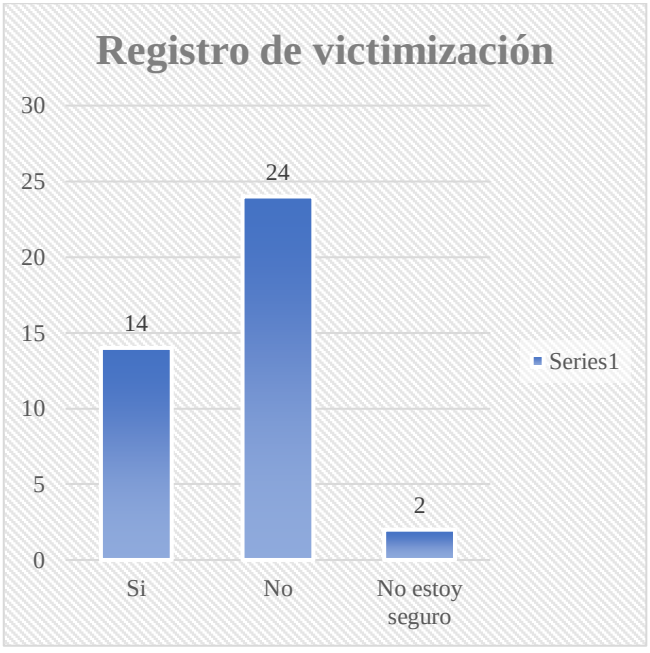

Figura 5. Registro de victimización. Fuente: La investigación.

- Intentos de fraude.

De acuerdo con la Figura 7, el 62,50% de los encuestados ha experimentado intentos de fraude en sus transacciones digitales. En contraste, un 32,50% no ha sido objeto de tales intentos, mientras que un 5,00% no estaba seguro, lo que sugiere que algunos usuarios no siempre logran identificar los intentos de fraude.

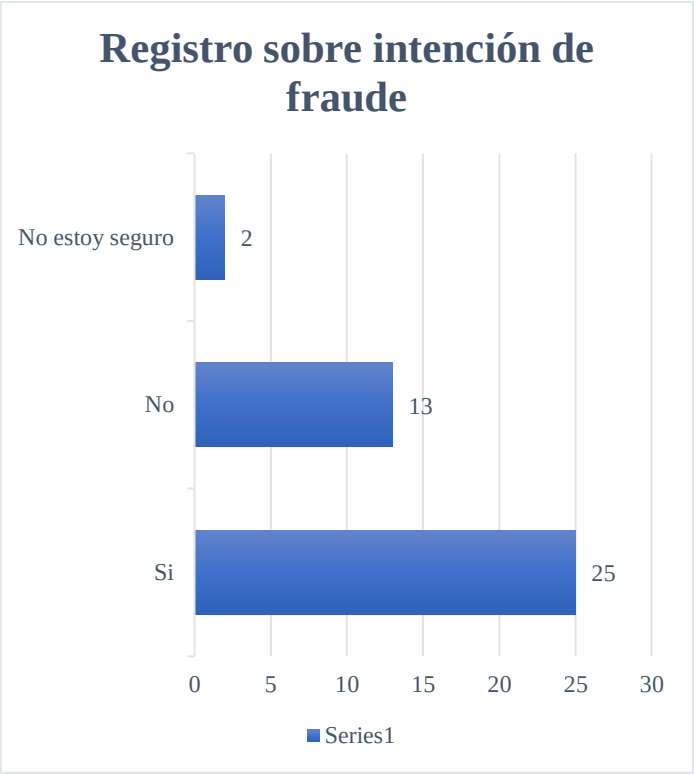

Figura 6. Registro sobre intención de fraude. Fuente: La investigación.

- Percepción sobre la protección institucional.

Finalmente, en la Figura 8, se evidencian percepciones divididas respecto a la protección ofrecida por las instituciones financieras frente al fraude digital. Un 27,50% consideró que las medidas actuales son adecuadas, mientras que un 40,00% opinó lo contrario. En cambio, un 32,50% no está seguro de la efectividad de dichas medidas, lo cual sugiere la necesidad de una mayor transparencia y efectividad en las estrategias de seguridad.

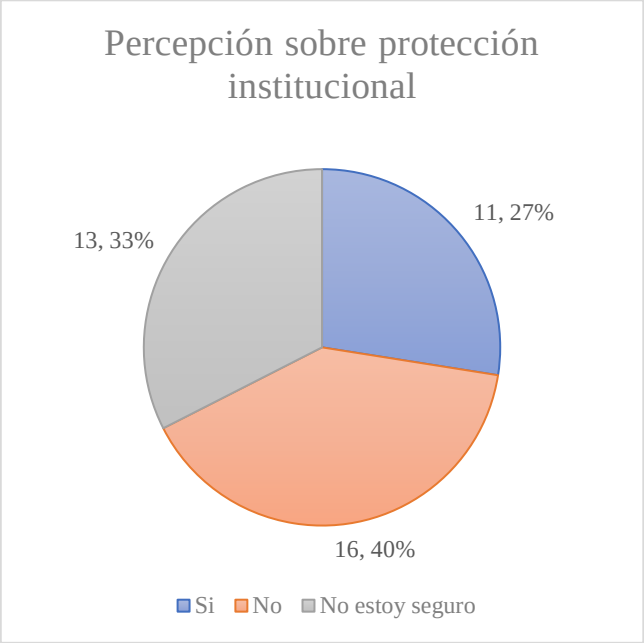

Figura 7. Percepción sobre protección institucional. Fuente: La investigación.

Los encuestados expresaron preocupaciones significativas sobre el fraude digital, especialmente en relación con el robo de identidad y el fraude con tarjetas de crédito. Si bien los usuarios aplican medidas de protección, existe una clara demanda por una mayor respuesta institucional ante la creciente amenaza del fraude en las transacciones digitales.

En cuanto al nivel de conocimiento y de percepción del riesgo entre los usuarios de transacciones digitales en Ecuador, se muestra una combinación de conciencia y desinformación. Mientras algunos usuarios están bien informados y toman precauciones adecuadas, existe una parte significativa de la población que aún no está completamente consciente de los riesgos o de las mejores prácticas de seguridad; por lo tanto, es esencial mejorar la educación sobre ciberseguridad y promover prácticas de seguridad entre todos los usuarios para mitigar los riesgos asociados con las amenazas cibernéticas.

Respuesta institucional de las entidades financieras frente al fraude digital.

El análisis de la respuesta institucional de las entidades financieras frente al fraude digital revela avances significativos en la implementación de medidas de seguridad. La autenticación de dos factores (2FA) ha demostrado ser altamente efectiva para prevenir accesos no autorizados, al añadir una capa adicional de verificación.

El monitoreo proactivo de actividades ha facilitado la identificación de patrones sospechosos en tiempo real, aunque su efectividad depende de la precisión del sistema de detección utilizado. En cuanto a la educación continua sobre seguridad, ha tenido un impacto moderado en la sensibilización de los clientes, al mejorar la capacidad para reconocer intentos de fraude. La protección contra malware y phishing ha sido altamente efectiva, al bloquear las amenazas antes de que afecten a los usuarios. Adicionalmente, el mantenimiento y actualización de sistemas ha prevenido la explotación de vulnerabilidades conocidas, al constituir una medida crucial en la protección digital.

Se identifican áreas de mejora; por ejemplo, la educación de los clientes continúa insuficiente, por lo que es necesario intensificar las campañas de concientización, enfocadas en una formación práctica y accesible; además, algunas instituciones no han adoptado las últimas tecnologías para la detección y prevención de fraudes, lo que hace imprescindible la inversión en inteligencia artificial y aprendizaje automático; incluso, la velocidad de respuesta ante incidentes debe optimizarse mediante protocolos más ágiles y mejor coordinación entre equipos, junto con una comunicación más transparente y efectiva con los clientes sobre los riesgos y medidas adoptadas; por último, se resaltó la necesidad de la colaboración entre el sector privado y las autoridades gubernamentales para compartir información sobre amenazas, establecer estándares de seguridad, y aumentar la conciencia pública.

Estrategias de concientización y formación en ciberseguridad.

Para reducir la vulnerabilidad ante el fraude, se deben implementar estrategias de concientización y formación en ciberseguridad tanto para usuarios de servicios financieros como para el personal de las instituciones financieras (ver tabla 2 y 3).

Estas estrategias deben ser adaptativas y actualizadas regularmente para enfrentar las amenazas emergentes y mejorar la seguridad general en el ámbito financiero.

Tabla 2. Estrategias para usuarios de servicios financieros.

Estrategia	Descripción	Objetivos	Implementación
Campañas de educación digital	Lanzar campañas de sensibilización mediante diversos canales, como redes sociales, correos electrónicos y medios de comunicación.	Informar a los usuarios sobre los riesgos cibernéticos y mejores prácticas de seguridad.	Crear contenido educativo atractivo y relevante para el público general.
Simulaciones de phishing	Realizar simulaciones de phishing para entrenar a los usuarios en la identificación de intentos fraudulentos.	Mejorar la capacidad de los usuarios para reconocer y responder a ataques de phishing.	Enviar correos simulados y proporcionar retroalimentación sobre las respuestas.
Tutoriales y Webinars interactivos	Ofrecer tutoriales y seminarios webs interactivos sobre seguridad cibernética y protección personal.	Proporcionar conocimientos prácticos sobre seguridad y herramientas de protección.	Organizar sesiones regulares con expertos en ciberseguridad.
Alertas de seguridad personalizadas	Enviar alertas personalizadas sobre las amenazas actuales y consejos de seguridad basados en el comportamiento del usuario.	Mantener a los usuarios informados sobre las amenazas emergentes y cómo mitigarlas.	Utilizar análisis de datos para enviar alertas relevantes y oportunas.

Fuente: Elaboración propia.

Tabla 3. Estrategias para el personal de instituciones financieras.

Estrategia	Descripción	Objetivos	Implementación
Capacitación continua en ciberseguridad	Desarrollar programas de capacitación continua sobre las últimas amenazas y prácticas de seguridad.	Mantener al personal actualizado sobre nuevas amenazas y técnicas de mitigación.	Implementar sesiones de formación periódicas y certificaciones.
Simulacros de respuesta a incidentes	Realizar simulacros de respuesta a incidentes cibernéticos para entrenar al personal en la gestión de crisis.	Mejorar la capacidad del personal para responder efectivamente a incidentes de seguridad.	Programar ejercicios de simulación que imiten escenarios de ataques reales.
Evaluaciones y pruebas de conocimiento	Aplicar evaluaciones regulares para medir el conocimiento del personal	Identificar áreas de mejora y garantizar la competencia en seguridad cibernética.	Realizar exámenes y pruebas de simulación sobre situaciones de ciberseguridad.

	sobre ciberseguridad y políticas internas.		
Desarrollo de políticas de seguridad internas	Crear y actualizar políticas de seguridad claras que definan las responsabilidades y procedimientos en caso de incidentes.	Establecer directrices claras para la gestión de riesgos y la respuesta a incidentes.	Revisar y comunicar políticas de seguridad regularmente al personal.

Fuente: Elaboración propia.

Colaboración público-privada en la lucha contra el fraude digital.

La colaboración entre el sector privado y las autoridades gubernamentales es fundamental para combatir el fraude digital de manera efectiva. El intercambio de información y la creación de estándares de seguridad comunes son dos pilares esenciales que fortalecen la defensa contra las amenazas cibernéticas. Esta asociación no solo mejora la capacidad de respuesta a incidentes y la protección de datos, sino que también fomenta una mayor seguridad y confianza en el entorno digital.

Prioridad del intercambio de información. La colaboración entre el sector privado y las autoridades gubernamentales fortalece la lucha contra el fraude digital, dado que la naturaleza transnacional y sofisticada de estos delitos requiere una respuesta coordinada y dirigida.

- *Intercambio de información*: La compartición de datos y alertas sobre amenazas emergentes entre empresas y entidades gubernamentales permite una detección y respuesta más rápida y eficaz. Las empresas privadas, especialmente las del sector financiero y tecnológico, suelen ser las primeras en identificar patrones de fraude y ataques cibernéticos. Al compartir esta información con las autoridades gubernamentales, se facilita una comprensión amplia y oportuna de las amenazas.
- *Cooperación en investigaciones*: Las investigaciones sobre fraudes digitales benefician la cooperación entre el sector privado y las agencias gubernamentales. Las empresas proporcionan datos técnicos y análisis, mientras que las autoridades ofrecen recursos investigativos y legales. Esta colaboración acelera la identificación de los delincuentes y la recuperación de fondos robados.

Creación de estándares de seguridad. El desarrollo y la implementación de estándares de seguridad comunes son esenciales para fortalecer la defensa contra el fraude digital. Estos estándares garantizan que todos los actores del ecosistema digital adopten prácticas de seguridad adecuadas y coherentes.

- *Desarrollo de normas:* Las entidades privadas y gubernamentales deben trabajar juntas para crear y mantener normas de seguridad que aborden las vulnerabilidades conocidas y las amenazas emergentes. Estas normas deben incluir requisitos para la autenticación de múltiples factores, cifrado de datos y protocolos de seguridad en las comunicaciones.
- *Certificaciones de seguridad:* La certificación de seguridad de productos y servicios financieros por parte de entidades independientes proporciona una garantía adicional de que se siguen las mejores prácticas. La colaboración en la creación de estos programas de certificación asegura que las evaluaciones sean rigurosas y relevantes.

Beneficios de la colaboración.

- *Resiliencia mejorada:* Una colaboración eficaz entre el sector privado y las autoridades gubernamentales mejora la resiliencia general contra el fraude digital, al alinear esfuerzos y recursos en una dirección común.
- *Innovación en seguridad:* La cooperación fomenta la innovación en tecnología de seguridad y en estrategias de protección, al combinar el conocimiento especializado y los recursos de ambos sectores.
- *Educación y concientización:* Trabajar juntos también facilita la implementación de programas educativos y de concientización que informan a los usuarios sobre prácticas seguras y riesgos asociados con las transacciones digitales.

Discusión.

El análisis del estudio mostró, que aunque la mayoría de los encuestados han sido conscientes de los riesgos asociados al fraude financiero en transacciones digitales, un grupo significativo aún no ha estado informado sobre estos peligros. Los avances tecnológicos transformaron profundamente el sector financiero, al permitir la aparición de nuevos modelos de negocio que ofrecieron productos innovadores y competitivos;

por tanto, este escenario destacó la necesidad de que los usuarios tomaran mayores precauciones para evitar ser víctimas de estafas.

La evolución de la banca digital, que combinó los servicios tradicionales con el acceso por internet, facilitó el acceso a servicios financieros; sin embargo, esta comodidad incrementó también la vulnerabilidad de los usuarios frente al fraude. En este sentido, se analizaron los factores que influyeron en los diferentes tipos de fraude, así como los efectos económicos y psicológicos que experimentaron las víctimas. Se observó, que a pesar de una percepción general de riesgo, existe una brecha significativa en el conocimiento específico sobre las amenazas digitales.

Los resultados revelaron, que aunque las transacciones en línea ofrecieron muchas ventajas, es esencial que los usuarios implementen medidas de seguridad adecuadas, como contraseñas fuertes, para protegerse de los delincuentes cibernéticos. Esto coincidió con estudios previos que señalaron la necesidad de una educación continua para mejorar la comprensión de los riesgos cibernéticos. Adicionalmente, la prevalencia del phishing y malware como técnicas de fraude predominantes en Ecuador no difirió de las tendencias globales. De modo que acentuó la necesidad de reforzar las medidas de seguridad en las instituciones financieras.

Finalmente, la respuesta institucional, con la implementación de la autenticación de dos factores y el monitoreo proactivo, representó un avance positivo en la protección contra el fraude digital; no obstante, la necesidad de mejorar la inversión en tecnología y la capacitación continua se alineó con recomendaciones de estudios anteriores. En consecuencia, se determinó que la integración de tecnologías avanzadas y la formación constante son esenciales para fortalecer la defensa contra el fraude, mientras que la colaboración entre el sector privado y las autoridades gubernamentales potencian significativamente la eficacia de las medidas de seguridad implementadas.

CONCLUSIONES.

La investigación ha evidenciado una notable disparidad en el nivel de conocimiento sobre los riesgos del fraude digital entre los usuarios de servicios bancarios en Ecuador. Aunque algunos usuarios están bien informados, una parte significativa de la población aún carece de una comprensión adecuada sobre amenazas como el phishing y el malware.

Esa situación refuerza la prioridad de implementar programas educativos más efectivos y accesibles, destinados a aumentar la conciencia y preparación de los usuarios frente a fraudes digitales. Estas iniciativas educativas deben ser promovidas tanto por las instituciones financieras como por entidades gubernamentales para garantizar una protección integral.

Los hallazgos indican, que aunque las instituciones financieras han adoptado medidas de seguridad como la autenticación de dos factores y el monitoreo proactivo, existen áreas de mejora significativa; incluso, la inversión insuficiente en tecnología de seguridad y la falta de capacitación continua para el personal son aspectos críticos que requieren atención; por tanto, se requiere de fortalecer estas áreas para mejorar considerablemente la capacidad de las instituciones para prevenir y responder a incidentes del denominado fraude digital.

El estudio ha destacado la prioridad de la colaboración entre el sector privado y las autoridades gubernamentales en la lucha contra el fraude digital. La cooperación en el intercambio de información sobre amenazas y el establecimiento de estándares de seguridad fomenta significativamente las estrategias de prevención y respuesta al fraude; inclusive, la creación de un marco colaborativo que incluya compartir información y desarrollar políticas comunes para mitigar el impacto del fraude digital; por tanto, se debe trabajar en explorar los resultados de la colaboración interinstitucional para reducir el fraude en el ecosistema digital.

REFERENCIAS BIBLIOGRÁFICAS.

1. Astudillo-Romero, A. E., & de las Mercedes Torres-Negrete, A. (2024). Auditoría digital un mundo interconectado: seguridad financiera y fiscal en empresas de construcción [Digital auditing in an interconnected world: financial and tax security in construction companies]. Revista Multidisciplinaria Perspectivas Investigativas, 4(especial), 152-163. https://www.rperspectivasinvestigativas.org/index.php/multidiscipinaria/article/view/178
2. Ávila-Coello, A. A. (2024). Seguridad de la información en instituciones públicas: desafíos y buenas prácticas en el contexto ecuatoriano. Journal of Economic and Social Science Research, 4(2), 140-156. https://economicsocialresearch.com/index.php/home/article/view/96
3. Baroffio, V. V., & Lara, R. G. (2024). Educación financiera como estrategia para fortalecer la protección de los usuarios financieros en entornos digitales. Cuadernos del CLAEH, 43(119), 215-232. https://ojs.claeh.edu.uy/publicaciones/index.php/cclaeh/article/view/618
4. Bermeo-Giraldo, M. C., Grajales-Gaviria, D., Valencia-Arias, A., & Palacios-Moya, L. (2021). Evolución de la producción científica sobre el fraude contable en las organizaciones: análisis bibliométrico. Estudios Gerenciales, 37(160), 492-505. http://www.scielo.org.co/scielo.php?pid=S0123-59232021000300492&script=sci_arttext
5. Calle-Tenesaca, M. E., & Andrade-Amoroso, R. P. (2024). Ciberseguridad en contabilidad: protegiendo la integridad de los datos financieros en empresas comerciales. Revista Metropolitana de Ciencias Aplicadas, 7(S2), 87-98. https://remca.umet.edu.ec/index.php/REMCA/article/view/734
6. Castro Peñaloza, D. A., & Narváez Zurita, X. E. (2024). Educación tributaria y reducción de la economía informal en América Latina. Conrado, 20(96), 77-91. http://scielo.sld.cu/scielo.php?pid=S1990-86442024000100077&script=sci_arttext&tlng=en
7. Córdova, L. A. O. (2024). El Marco Legal de los Delitos Cibernéticos en Ecuador. Reincisol., 3(5), 1447-1469. https://www.reincisol.com/ojs/index.php/reincisol/article/view/158

8. Guachún-Orellana, P. V., & Andrade-Amoroso, R. P. (2024). Medidas de ciberseguridad aplicadas a los softwares contables en las PYMES de Cuenca, Ecuador. CIENCIAMATRIA, 10(2), 168-187. https://cienciamatriarevista.org.ve/index.php/cm/article/view/1324
9. Herrera, G. C. H., Lojan, M. A. R., & Castro, S. M. (2024). Seguridad jurídica y protección de datos en Ecuador: validez legal de los Smart contract. Revista Lex, 7(25), 690-704. https://www.revistalex.org/index.php/revistalex/article/view/287
10. Lara, R. A. M., Benavides, J. O. B., Orbea, J. C. M., Vivero, G. N., & Angulo, R. M. M. (2024). Estrategias innovadoras para mitigar la suplantación de identidad en redes sociales.: Innovative strategies to mitigate identity theft on social networks. Revista Científica Multidisciplinar G-nerando, 5(1), 544-561. https://revista.gnerando.org/revista/index.php/RCMG/article/view/212
11. López-Pincay, P. R., Mendoza-Lino, K. M., Yagual-Tomalá, E. M., & Blum-Alcívar, H. M. (2024). Mecanismos de control para evitar el aumento del cibercrimen financiero. MQRInvestigar, 8(3), 1802-1818. https://www.investigarmqr.com/ojs/index.php/mqr/article/view/1554
12. Moreira-Basurto, C. A., Rivadeneira-Pacheco, J. L., Quintanilla-Gavilanes, J. A., & Moreira-Cañizares, A. C. (2024). El lavado de activos en el Ecuador y su incidencia en la normativa tributaria, societaria y mercantil. Revista Científica Arbitrada de Investigación en Comunicación, Marketing y Empresa REICOMUNICAR. ISSN 2737-6354., 7(13 Ed. esp.), 130-155. https://www.reicomunicar.org/index.php/reicomunicar/article/view/229
13. Moya-Sánchez, M. F., & Torres-Palacios, M. M. (2024). Optimización de recursos públicos mediante la auditoría continua: Análisis de beneficios y desafíos [Optimization of Public Resources through continuous auditing: Analysis of benefits and challenges]. Revista Multidisciplinaria Perspectivas Investigativas, 4(especial), 1-12. https://www.rperspectivasinvestigativas.org/index.php/multidiscipinaria/article/view/104
14. Peñarreta-Angamarca, M. T., Torres-Palacios, M. M., & Moreno-Narváez, V. P. (2024). Efectividad de la auditoría financiera en la prevención del fraude en pequeñas y medianas empresas [Analysis of

the Effectiveness of financial and tax auditing in fraud prevention]. Revista Multidisciplinaria Perspectivas Investigativas, 4(especial), 26-35. https://www.rperspectivasinvestigativas.org/index.php/multidiscipinaria/article/view/106

15. Ponce Tubay, M. A. (2024). Desafíos y respuestas legales ante los delitos informáticos en Ecuador. Revista San Gregorio, 1(58), 111-118. http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S2528-79072024000200111
16. Tramullas, J. (2020). Temas y métodos de investigación en Ciencia de la Información, 2000-2019. Revisión bibliográfica. El profesional de la información, 29(4), 2-6. https://revista.profesionaldelainformacion.com/index.php/EPI/article/view/77328
17. Tubay, M. A. P. (2024). Delitos informáticos: Caso Ecuador. Revista San Gregorio, 1(58), 119-123. https://revista.sangregorio.edu.ec/index.php/REVISTASANGREGORIO/article/view/2667
18. Zhang, C., Tian, L., & Chu, H. (2023). Usage frequency and application variety of research methods in library and information science: Continuous investigation from 1991 to 2021. Information Processing and Management, 60(6), 4-8. https://www.sciencedirect.com/science/article/abs/pii/S0306457323002443

DATOS DE LOS AUTORES.

1. **Carlos Wilman Maldonado Gudiño.** Magister 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. **Alba Karina Vaca Morales.** Estudiante de la Universidad regional Autónoma de Los Andes, Matriz Ambato, Ecuador. E-mail: albavm31@uniandes.edu.ec
4. **Daniela Marilin Núñez Taboada.** Estudiante de la Universidad regional Autónoma de Los Andes, Matriz Ambato, Ecuador. E-mail: ca.danielamnt58@uniandes.edu.ec

RECIBIDO: 5 de septiembre del 2024. **APROBADO:** 27 de septiembre del 2024.