Salud, Ciencia y Tecnología - Serie de Conferencias. 2025; 4:636
doi: 10.56294/sctconf2025636

ORIGINAL

Proposed legislative reform as a measure against non-consensual wire transfers in Ecuador

Propuesta de reforma legislativa como medida a transferencias electrónicas no consentidas en Ecuador

Madeline Vanessa López Bravo[1], Carmen Marina Méndez Cabrita[1], Marcelo Raúl Dávila Castillo[1], María Fernanda Gómez Ayala[1]

[1]Universidad Regional Autónoma de los Andes "Uniandes", Sede Tulcán, Ecuador.

Citar como: López Bravo MV, Méndez Cabrita CM, Dávila Castillo MR, Gómez Ayala MF. Proposed legislative reform as a measure against non-consensual wire transfers in Ecuador. Salud, Ciencia y Tecnología - Serie de Conferencias. 2025; 4:636. https://doi.org/10.56294/sctconf2025636

Recibido: 17-04-2024 **Revisado:** 07-09-2024 **Aceptado:** 10-02-2025 **Publicado:** 11-02-2025

Editor: Prof. Dr. William Castillo González

Autor para la correspondencia: Madeline Vanessa López Bravo

ABSTRACT

El presente estudio aborda la creciente problemática de las transferencias electrónicas no consentidas en Ecuador y la insuficiencia de las medidas actuales para proteger a las víctimas. Utilizando un enfoque mixto, se recopilaron datos mediante encuestas a expertos en derecho penal e informático y titulares de cuentas bancarias. Los resultados evidencian que el 60 % de los encuestados ha sido víctima de estos fraudes, destacando la ineficiencia del procedimiento legal vigente para la recuperación de activos. Como solución, se propone una reforma al artículo 231 del Código Orgánico Integral Penal que incluya el bloqueo temporal de activos ilícitos como medida de aseguramiento inmediato. El análisis multicriterio revela que esta alternativa es más efectiva y rápida frente a otras medidas como el embargo de cuentas bancarias o la intervención judicial, aunque enfrenta desafíos en costos administrativos y viabilidad legal.

Keywords: Non-Consensual Wire Transfers; Temporary Blocking of Illicit Assets; Legislative Reform; Comprehensive Organic Criminal Code.

RESUMEN

This study addresses the growing issue of unauthorized electronic fund transfers in Ecuador and the inadequacy of current measures to protect victims. Using a mixed-methods approach, data was collected through surveys with Criminal and IT Law experts and bank account holders. Results show that 60 % of respondents have fallen victim to such frauds, emphasizing the inefficiency of the current legal process in recovering assets. As a solution, a reform to Article 231 of the Comprehensive Organic Criminal Code is proposed to include the temporary blocking of illicit assets as an immediate safeguarding measure. Multi-criteria analysis reveals that this alternative is more effective and faster compared to other measures such as account freezing or judicial intervention, though challenges remain in administrative costs and legal feasibility.

Palabras clave: Transferencias Electrónicas no Consentidas; Bloqueo Temporal de Activos Ilícitos; Reforma Legislativa; Código Orgánico Integral Penal.

INTRODUCCIÓN

La historiografía de la humanidad ha hecho un importante esfuerzo por categorizar lógicamente los periodos

en los cuales ésta se ha venido desarrollando. En el marco de ese ejercicio de categorización, encontramos a la Era Digital, categoría que entiende una revolución en los medios de trabajo del hombre, pasando de la electricidad y los instrumentos análogos, a los puramente digitales. Esta era digital, resulta ser entonces un punto de inflexión en la vida humana, hasta tal punto que la historiografía la comprendió como el motivo de causación de lo que se entiende como la era de la información.[1]

La globalización, las nuevas tecnologías de la información y las comunicaciones, las redes sociales, el internet, son algunas de las expresiones más comunes que actualmente rigen el desarrollo económico, social y cultural de los países y organizaciones civiles en general.[2]

El impacto de las tecnologías, la informática y las comunicaciones en general, han permeado todos los aspectos de la vida posmoderna. Los usuarios prefieren la ubicuidad, la simultaneidad y sin darse cuenta se produce el rompimiento de los paradigmas del tiempo y el espacio, por lo que dichas tecnologías representan. Todo lo anterior no es ajeno a los sistemas de pago en general y a las Transferencias Electrónicas de Fondos.[3]

A finales del siglo XX empezaron a masificarse conceptos tales como Cashlees society, que consistió en una sociedad, en la cual los operadores económicos recurrieron a nuevos medios de transferencias de fondos, con la finalidad de no acudir al dinero en efectivo, también la ubicuidad de los pagos, debido a que un usuario deseaba poder enviar o recibir dinero a cualquier persona en cualquier parte del mundo de forma instantánea, y por último la electrificación de los sistemas de pagos, que respondiendo a una sociedad hiperconectada, con necesidad de realizar pagos ágiles, seguros y económicos, se vio en la obligación de diseñar nuevos instrumentos de pago o a redefinir los existentes.[4]

Las Transferencias Electrónicas de Fondos (TEF) se ubican en el sistema de pagos, específicamente en los instrumentos de pago inmateriales, esto no significa que cada vez que se realice una TEF se hace un pago, como por ejemplo, cuando se da el caso de una transferencia entre dos cuentas de un mismo sujeto jurídico, de la cuenta de ahorro se pasa dinero a la cuenta corriente bancaria o al encargo fiduciario, es decir, un mismo sujeto jurídico titular de diferentes cuentas en la misma o en distintas instituciones financieras, se transfiere dinero.[3]

El primer país del mundo en definir las TEF fueron los Estados Unidos, mediante la Electronic Funds Transfer Act (EFTA): "Es una transferencia de fondos, teléfono, computadora (incluyendo banca on-line) o cinta magnética con el propósito de ordenar, instruir o autorizar a una institución financiera a debitar o acreditar la cuenta de un consumidor".[3]

Es importante destacar que en sus inicios, estas transferencias fueron creadas para uso exclusivo de entidades financieras, como redes cerradas interbancarias que dotaron de seguridad y agilidad las comunicaciones en sistemas bancarios. Sin embargo, con el desarrollo de los cajeros automáticos en los años setenta 70, el sector financiero incluyó a los consumidores, masificando de esta forma el uso de las Transferencias Electrónicas de Fondos TEF, brindando una solución en tiempo real, rápida y sin necesidad de internet que en ese momento no era cotidiano, pero empezaban a emplearse las computadoras con fines financieros. En 1975 entró en servicio el primer sistema internacional de mensajes interbancarios de computadora a computadora. En 1978, Estados Unidos es pionero en establecer normatividad sancionando en este año la Electronic Funds Transfer Act -EFTA-, a nivel federal y en 1980 el reglamento Federal Reserve Board a nivel estadual. Desde este punto en adelante se han desarrollado diferentes mecanismos de operar las TEF, pero el concepto no cambia.[3]

El trabajo en todo este modo operativo cambiario económico ocasiona un profundo impacto a la ciencia jurídica ya que se observa que ésta, al ser una que pretende regular las relaciones humanas, sufre una transformación en un punto clave de su espacio de cobertura como son las manifestaciones de voluntad de las personas y los efectos que éstas ocasionen. Este impacto, permea todas las áreas de la disciplina jurídica a plenitud, siendo el derecho penal un ejemplo fehaciente de esta realidad. Tratando este último de adaptar sus principios doctrinales al cambio tecnológico, se concluye dentro del debate penalista que las nuevas tecnologías ponen de presente el desafío de estudiar, desarrollar y categorizar al delito informático como la transformación de la conducta criminal en los espacios generados por dicho cambio. Se entiende que las nuevas tecnologías han generado medios de actuación distintos, y de la mano de dicha realidad, el delito ha sufrido cambios sustanciales.[1]

No sólo resulta relevante comprender el delito informático y su estructura, si no también los efectos jurídicos que éste pueda generar acaecida su materialización. A nivel global, los delitos informáticos han incrementado significativamente afectando tanto a individuos como a organizaciones. Según María Paula Sempertegui Torres en su tesis de grado "dada la extensión del uso de los ordenadores y de las redes de transmisión de datos en la mayoría de los ámbitos de nuestra sociedad, prácticamente todos los delitos pueden cometerse a través de un sistema informático; en este sentido, las conductas ilícitas vinculadas con los sistemas informáticos son muchas y heterogéneas." Esto subraya que el uso generalizado de computadoras y redes permite la comisión de casi cualquier delito digitalmente, resultando en una variedad de crímenes cibernéticos. La velocidad y sofisticación con la que los delincuentes operan agravan la situación, aprovechando brechas en los sistemas de seguridad existentes.[4]

En América Latina, los fraudes electrónicos, particularmente las transferencias electrónicas no consentidas,

https://doi.org/10.56294/sctconf2025636

se han convertido en una problemática creciente. Las legislaciones a menudo no están actualizadas para enfrentar las rápidas evoluciones tecnológicas en este ámbito, lo que deja desprotegidos a los derechos de las víctimas, esto debido a que suelen enfrentar una burocracia lenta e ineficaz que no puede competir con la velocidad de las transferencias electrónicas no consentidas.

En una transferencia electrónica no consentida "se realiza la transferencia electrónica de dinero de una cuenta bancaria a otra sin intercambio de dinero físico y sin autorización expresa de la víctima (pueden estar involucradas una o varias instituciones financieras, pero, sin la intervención directa del personal del banco); estos fraudes se pueden ver reflejados en pagos de compras digitales o transferencia de fondos a unas o varias cuentas destino del delincuente". La ausencia de un intercambio físico de dinero facilita la ejecución rápida y discreta de las transferencias electrónicas no consentidas, complicando enormemente la tarea de rastrear y recuperar los fondos robados. Para las víctimas, esto no solo implica una pérdida económica inmediata, sino también la incertidumbre y el estrés asociados con la dificultad para resolver estos casos de manera oportuna.[5]

La ingeniería social es la práctica de obtener información a través de la manipulación de los usuarios. El principio básico detrás de esto es que «el usuario es el eslabón más débil» en las transacciones digitales. Es más fácil engañar a alguien para que facilite su contraseña que penetrar los complejos sistemas de seguridad de las empresas. Para ello los ciberdelincuentes recurren a diversos medios como correos electrónicos (phishing tradicional), SMS (smishing), llamadas telefónicas (vishing), páginas web falsas (web spoofing), etc.

El phishing es la estafa en la que se suplanta la identidad de un tercero, es este caso, mediante envío masivo de correos electrónicos fraudulentos empleando la identidad de organismos o empresas legítimas, como un banco. Es la primera fase de muchas con el objetivo final de obtener grandes sumas de dinero.[6]

Además ésta delincuencia especializada introduce malware y otros tipos de software malicioso que son frecuentemente empleados para alterar el funcionamiento de sistemas y robar información sensible. Malware es una combinación de dos palabras "malicioso" y "software". Este término describe cualquier forma de código malicioso independientemente de cómo afecte a las víctimas, cómo se comporte o el daño que cause.[7] El malware incluye todo tipo de software malicioso incluyendo todas las formas conocidas de troyanos, ransomware, viruses, gusanos y malware de banca. El denominador común de todo lo que se describe con este término es la intención maliciosa de sus autores u operadores.

Los creadores de malware actuales son muy creativos. Sus "creaciones" se difunden vía vulnerabilidades en sistemas no parcheados, pasan por alto medidas de seguridad, se esconden en la memoria o imitan aplicaciones legítimas para no ser detectadas.

En Ecuador, el Código Orgánico Integral Penal (COIP) en su artículo 231 tipifica el delito de transferencia electrónica de activo patrimonial, el cual se establece que:

Art. 231.- Transferencia electrónica de activo patrimonial. - La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona.[8]

No obstante, las medidas cautelares existentes son ineficaces debido a la burocracia y el tiempo requerido para su implementación.[9] destaca que "la consumación de estas transferencias no autorizadas se realiza mediante la intervención de cuentas bancarias propias, facilitando la desviación de fondos electrónicos con ánimo de lucro, frecuentemente sin que se conozca al autor original". La dispersión rápida de los fondos ilícitos suele superar la capacidad del sistema judicial para actuar eficazmente. El ingeniero Daniel Calderón dentro de su investigación establece que "la rápida dispersión de los activos a través de transferencias electrónicas complica la recuperación de los mismos y deja a las víctimas en una posición vulnerable".[10]

Es por esto que, Mariliana Rico Carrillo enfatiza la necesidad de reformas que permitan una respuesta más rápida y efectiva por parte de las autoridades, subrayando que "la implementación de medidas temporales es crucial para mitigar el impacto económico y psicológico en las víctimas de fraudes electrónicos".[11]

El objetivo de esta investigación incluye una propuesta de reforma legislativa que fortalezca el marco legal actual y ofrezca una solución efectiva para mitigar el impacto de las transferencias electrónicas no consentidas en Ecuador. Este estudio no solo busca proporcionar una respuesta legal más adecuada a los desafíos del fraude electrónico, sino también sentar las bases para futuras investigaciones y reformas en el ámbito de la protección de activos y derechos en el entorno digital.

MÉTODO

El estudio utiliza un enfoque mixto con un diseño metodológico no experimental y transversal, dado que los datos se recolectaron en un momento específico para su análisis. Se desarrolló con un alcance descriptivo, que permitió caracterizar la situación actual del problema.

Para el desarrollo de esta investigación se utilizaron los métodos hipotético-deductivo, analítico-sintético, análisis documental y método de análisis multicriterio para evaluar múltiples opciones o soluciones en base a varios criterios.

Se realizaron revisiones exhaustivas de legislaciones, estudios y casos relevantes sobre fraudes electrónicos y medidas de seguridad, y se consultó las opiniones y recomendaciones de expertos sobre la validez de la propuesta. La técnica utilizada para la recolección de datos es la encuesta mediante el instrumento del cuestionario, la cual se la realizó a 20 personas de la ciudad de Tulcán, quienes se dividían entre profesionales del Derecho Penal e Informático y personas titulares de cuentas bancarias. Los encuestados fueron seleccionadas bajo un criterio de inclusión que abarca los años de experiencia, el conocimiento sobre la normativa penal, o que han sido víctimas de este tipo de delitos informáticos.

Para la recolección de información de las encuestas se utilizó la herramienta Google Forms, la cual permitió realizarlas de manera digital obteniendo estadísticas más detalladas y precisas.

La investigación con métodos mixtos es un paradigma de investigación que implica la recopilación de datos cualitativos y cuantitativos sobre el mismo objeto de investigación. Los investigadores que emplean métodos mixtos sintetizan los resultados cualitativos con los cuantitativos para lograr una mejor comprensión.[12]

RESULTADOS

Para la presentación de los resultados obtenidos, se desarrollaron gráficas y tablas que exponen, analizan e interpretan los resultados recopilados a través de la encuesta.

¿Ha sido víctima alguna vez de una transferencia electrónica no consentida?

Figura 1. Resultados pregunta 1

El 60 % de los encuestados han sido víctimas de transferencias electrónicas no consentidas.

¿Confía en la capacidad de los bancos para prevenir transferencias electrónicas no consentidas?

Figura 2. Resultados pregunta 2

La confianza en las entidades bancarias para prevenir estos delitos es muy reducida según los encuestados.

¿Considera que la normativa penal actual en Ecuador es adecuada para proteger a las víctimas de fraudes electrónicos?

Figura 3. Resultados pregunta 3

https://doi.org/10.56294/sctconf2025636

La normativa penal ecuatoriana es insuficiente frente a la protección de fraudes electrónicos.

¿Cree que el procedimiento para la aplicación de medidas cautelares para delitos de transferencias electrónicas de activos patrimoniales retrasa tanto la protección de las víctimas como de sus activos?

Figura 4. Resultados pregunta 4

El 80 % coincide en que lo ineficiente no son las medidas en sí, sino el procedimiento para su aplicación.

¿Está de acuerdo en que el artículo 231 del COIP, que trata sobre las transferencias electrónicas de activos patrimoniales, está desprotegido debido a la rápida dispersión de los fondos dificultando tanto su recuperación como el seguimiento de los delincuentes?

Figura 5. Resultados pregunta 5

A pesar de que el Art. 231 sancione ese delito, la rápida dispersión de fondos impide su recuperación y seguimiento de quien lo comete.

¿Conoce el término «medida de aseguramiento» o tiene una idea de que puede referirse?

Figura 6. Resultados pregunta 6

El 70 % de las personas encuestadas se encuentra familiarizado con el término “medidas de aseguramiento”

¿Cree que la implementación de una medida de aseguramiento inmediato podría mejorar la protección de las víctimas y de sus activos?

Figura 7. Resultados pregunta 7

https://doi.org/10.56294/sctconf2025636

Todos los encuestados coinciden en que la protección de las víctimas y sus activos mejoraría con una medida de aseguramiento inmediato.

¿Estaría dispuesto a apoyar una propuesta de reforma al art. 231 que incluya como tercer inciso la medida de aseguramiento inmediato?

Figura 8. Resultados pregunta 8

El 100 % de los encuestados apoyarían la propuesta de reforma.

Uno de los métodos más eficaces que se plantea para enfrentar este desafío de las transferencias electrónicas no consentidas es el bloqueo temporal de activos ilícitos. Este bloqueo implica la suspensión temporal de los activos que han sido identificados como obtenidos o transferidos ilícitamente, lo que permite congelar los fondos y evitar su disposición mientras se lleva a cabo una investigación. La implementación de esta medida preventiva es especialmente relevante en el caso de fraudes electrónicos, ya que las transferencias pueden realizarse de manera extremadamente rápida, dificultando la recuperación de los fondos una vez que el delito ha sido cometido.

Se aplicó el Método AHP para evaluar la viabilidad y efectividad del bloqueo temporal de activos ilícitos en comparación con otras medidas de aseguramiento, como el embargo de cuentas bancarias y la intervención judicial. Los criterios considerados fueron:

- Tiempo de Respuesta: La rapidez con la que se puede implementar la medida tras la detección de una transferencia no consentida.
- Costos Administrativos: Los recursos financieros y humanos necesarios para ejecutar y supervisar la medida.
- Viabilidad Legal: La conformidad de la medida con el marco normativo vigente y el respeto a los derechos fundamentales.
- Efectividad en la Recuperación de Activos: El porcentaje de fondos recuperados y el tiempo requerido para su restitución a las víctimas.

El Método de Proceso Analítico Jerárquico es una técnica matemática utilizada para tomar decisiones en situaciones que involucran múltiples criterios, permitiendo comparar diversas alternativas y evaluarlas en función de los objetivos establecidos. Esta metodología se aplica comúnmente en problemas de toma de decisiones complejos donde es necesario considerar varios factores interrelacionados. El AHP ha demostrado ser eficaz en la resolución de problemas multidimensionales en áreas como la planificación estratégica, la gestión de proyectos y la ingeniería.[13]

Etapas del AHP

El AHP sigue un proceso estructurado que involucra varias fases que van desde la definición del problema hasta la toma de decisiones. Estas etapas incluyen:

- Definición del objetivo principal: Se definió el objetivo que se desea alcanzar. En este caso, el objetivo principal es evaluar la viabilidad y efectividad del bloqueo temporal de activos ilícitos como medida de aseguramiento inmediato ante transferencias electrónicas no consentidas.
- Estructuración de la jerarquía: El siguiente paso fue construir una jerarquía que organizara los elementos del problema. En el caso de esta investigación, la jerarquía se construye con un nivel superior, que es el objetivo de la toma de decisión (evaluar la medida de bloqueo temporal de activos ilícitos), un nivel intermedio, que está compuesto por los criterios de evaluación, y un nivel inferior, que está formado por las alternativas que se compararán.
- Comparación de criterios y alternativas: En esta etapa, se llevó a cabo la comparación de los criterios entre sí mediante una escala de prioridades (de 1 a 9, donde 1 significa igual importancia y 9 significa que un criterio es extremadamente más importante que otro). Se realizó lo mismo con las alternativas en relación con cada uno de los criterios.

https://doi.org/10.56294/sctconf2025636

- Cálculo de los pesos de los criterios y alternativas: A partir de las comparaciones realizadas, se calcularon los pesos relativos de cada criterio y alternativa. Esto se logró mediante el uso de matrices de comparación y la aplicación de métodos matemáticos para derivar un vector propio que represente la importancia relativa de cada factor.
- Evaluación y selección de la mejor alternativa: Finalmente, con los pesos de los criterios y las alternativas, se calculó el puntaje final de cada alternativa. La alternativa con el puntaje más alto se consideró la mejor opción para tomar la decisión.

Criterios de evaluación

- Tiempo de Respuesta: Qué tan rápido se puede implementar el bloqueo de activos tras la detección de una transferencia no consentida.
- Costos Administrativos: Los recursos financieros y humanos necesarios para ejecutar y monitorear la medida.
- Viabilidad Legal: La conformidad con el marco normativo y los derechos fundamentales involucrados.
- Efectividad en la Recuperación de Activos: Qué porcentaje de los fondos transferidos de manera ilícita pueden ser recuperados mediante el bloqueo temporal.
- Alternativas de aseguramiento de activos:
- Bloqueo temporal de activos ilícitos: Medida propuesta en esta investigación.
- Embargo de cuentas bancarias: Método tradicional utilizado en el aseguramiento de activos.
- Intervención judicial: Acciones tomadas por orden judicial para asegurar activos.
- Al proceder con las comparaciones, se construyó una matriz de comparación de criterios utilizando la escala estándar de 1 a 9 del AHP.

Tabla 1. Comparación de criterios

Criterio	Tiempo de respuesta	Costos Administrativos	Viabilidad Legal	Efectividad en Recuperación
Tiempo de respuesta	1	3	5	7
Costos Administrativos	1/3	1	3	5
Viabilidad Legal	1/5	1/3	1	3
Efectividad en Recuperación	1/7	1/5	1/3	1

En esta matriz, cada celda indica la importancia relativa de un criterio en comparación con otro. Por ejemplo, “Tiempo de Respuesta” es considerado más importante que Costos Administrativos, por lo que se asigna un valor de 3 en la celda correspondiente. Al inverso, la celda “Costos Administrativos vs Tiempo de Respuesta” se asigna como 1/3.

De forma similar, se realizó una comparación entre las tres alternativas utilizando una matriz de comparación para cada criterio. En este caso, los puntajes reflejan la preferencia de cada alternativa según cada uno de los criterios.

Una vez completadas las comparaciones de criterios y alternativas, se calculó el peso relativo de cada criterio y alternativa mediante la normalización de las matrices. El vector propio obtenido representó la importancia de cada alternativa para cada criterio. Posteriormente, se multiplicaron estos pesos por las puntuaciones de cada alternativa, y se sumaron los resultados para obtener un puntaje final para cada alternativa.

El puntaje final permitió determinar cuál de las alternativas es más adecuada para implementar como medida de aseguramiento inmediato ante las transferencias electrónicas no consentidas.

Los resultados mostraron que, aunque el bloqueo temporal de activos ilícitos tiene una alta efectividad en la recuperación de activos y una rápida implementación, sus costos administrativos pueden ser elevados, especialmente en jurisdicciones con sistemas legales y tecnológicos poco desarrollados. La viabilidad legal también representa un desafío, ya que la rapidez del proceso puede entrar en conflicto con los principios fundamentales de la ley.

Sin embargo, el análisis mostró que, en comparación con el embargo de cuentas y la intervención judicial, el bloqueo temporal de activos ilícitos es la alternativa que presenta un mayor balance en términos de efectividad y tiempo de respuesta.

DISCUSIÓN

En la pregunta 1 se estableció como análisis que el 60 % de los encuestados han sido víctimas de transferencias electrónicas no consentidas, esto porque como lo menciona Daniel Felipe Rey-Baracaldo el avance tecnológico ha permitido a las entidades financieras adoptar plataformas más innovadoras, pero también ha facilitado la proliferación de fraudes electrónicos, incluidas las transferencias no consentidas que dejan a los afectados sin

sus fondos bancarios. Con lo expuesto se entiende que el avance tecnológico ha facilitado el fraude electrónico, lo que respalda el alto porcentaje de encuestados que han sido víctimas de transferencias no consentidas, aumentando así la vulnerabilidad de sus usuarios.[14]

La pregunta 2 señala que la confianza en las entidades bancarias para prevenir los delitos de transferencia electrónica no consentida es muy reducida según los encuestados, esto porque una vez aprobada la transferencia por la entidad financiera, revertirla se vuelve extremadamente difícil debido a la naturaleza electrónica del dinero transferido; esto demuestra que lo que puede contribuir a la falta de confianza en las entidades bancarias es la dificultad para revertir transferencias electrónicas luego de que hayan sido aprobadas ya que así no podrán prevenirlas.

El análisis expresado en la pregunta 3 es que la normativa penal ecuatoriana es insuficiente frente a la protección de fraudes electrónicos, siendo ésta respaldada en el artículo Lagunas de ciberseguridad donde se manifiesta que la diversidad normativa genera conflicto al no estar acoplada a nuestra realidad actual, ya que, a pesar de contar con normativa vigente, los ciudadanos se encuentran en una situación de vulnerabilidad a diferencia de otros países de la región que cuentan con una normativa adecuada. Ante ello se puede entender que la normativa penal ecuatoriana no está bien adaptada como las normativas en otros países para combatir fraudes electrónicos como las transferencias electrónicas, dejando así a los ciudadanos en un estado de vulnerabilidad.[15]

La Pregunta 4 determina que el 80 % coincide en que lo ineficiente no son las medidas en sí, sino el procedimiento para su aplicación, ya que como lo resume María Eugenia Díaz Coral una vez que el juez conozca sobre la petición o solicitud de medidas cautelares y si verifica que se reúnen los requisitos previstos en la ley, las otorgará; entendiendo por esto que la normativa ecuatoriana cuenta con medidas cautelares que pueden ser aplicadas para esos delitos pero establecen un procedimiento para su aplicación que retrasan la efectividad de la medida, empezando por la presentación de la solicitud de la misma por parte del fiscal en la etapa de instrucción fiscal, para luego ser aprobada por el juez mediante audiencia, dejando en todo ese tiempo en desprotección no solo a la víctima, sino también a sus activos para que puedan ser dispersados junto con los transferidos ilícitamente.[16]

Lo mencionado anteriormente se complementa con la Pregunta 5 que determinó que, a pesar de que el Art. 231 sancione al delito de Transferencias Electrónicas de Activos Patrimoniales, la rápida dispersión de fondos impide su recuperación, coincidiendo con lo que dice Daniel Calderon que dicha dispersión a través de transferencias electrónicas complica la recuperación de los mismos dejando a las víctimas en una posición vulnerable; además, la Pregunta 6 muestra que los encuestados están de acuerdo con una medida que bloquee temporalmente solo los activos ilícitos al momento en el que se presenta la denuncia sin necesidad de la autorización judicial. Concluyendo de esta manera que una medida de bloqueo inmediato sin demora procedimental, podría acelerar el proceso de investigación y evitar la dispersión de fondos, mejorando así la protección de las víctimas y sus activos.

La Pregunta 7 ha establecido que el 70 % de las personas encuestadas se encuentra familiarizado con el término “medidas de aseguramiento”, esto concuerda con lo que menciona la Pregunta 8 de que la protección de las víctimas y sus activos mejoraría con una medida de aseguramiento inmediato, los resultados guardan estrecha relación con Mariliana Rico Carrillo quien a pesar de que no señala el dicho término, manifiesta que la implementación de medidas temporales es crucial para mitigar el impacto económico y psicológico en las víctimas de fraudes electrónicos. De acuerdo con lo mencionado, se desprende que la familiaridad con el término y el apoyo a las medidas inmediatas permiten una mayor comprensión de que estas medidas podrían aumentar la eficacia en la protección de las víctimas y en la reducción del impacto de los fraudes electrónicos como las transferencias electrónicas.[11]

Por último, la pregunta 8 expone como respuesta que el 100 % de los encuestados apoyarían la propuesta de reforma del artículo 231 del COIP que incluya como tercer inciso una medida de aseguramiento inmediato. El apoyo unánime para la reforma destaca la necesidad urgente de adaptar y fortalecer las medidas de aseguramiento en el contexto de los delitos informáticos.

Los resultados del análisis multicriterio indicaron que el bloqueo temporal de activos ilícitos obtuvo una puntuación superior en los criterios de Tiempo de Respuesta y Efectividad en la Recuperación de Activos, en comparación con las otras medidas evaluadas. Sin embargo, presentó desafíos en los criterios de Costos Administrativos y Viabilidad Legal, especialmente en jurisdicciones con marcos normativos menos desarrollados en materia de ciberseguridad y protección de datos.

Comparación con Otras Medidas de Aseguramiento

- Embargo de Cuentas Bancarias: Aunque efectivo en la retención de fondos, este método suele ser más lento debido a los procedimientos legales requeridos y puede ser menos eficiente en la recuperación de activos en casos de transferencias electrónicas rápidas.
- Intervención Judicial: Requiere una orden judicial, lo que puede demorar la acción y permitir que

los fondos sean movidos antes de la intervención.

- El bloqueo temporal de activos ilícitos se destacó por su capacidad para actuar de manera más inmediata, lo que es importante en el contexto de las transferencias electrónicas no consentidas, donde los fondos pueden ser transferidos a múltiples cuentas en cuestión de minutos.
- Desafíos y Consideraciones
- Viabilidad Legal: La implementación del bloqueo temporal de activos ilícitos requiere una base legal sólida que permita la acción inmediata sin vulnerar derechos fundamentales.
- Costos Administrativos: La necesidad de infraestructura tecnológica y personal capacitado para monitorear y ejecutar bloqueos de manera eficiente puede representar una carga significativa para las instituciones financieras y las autoridades competentes.
- Protección de Derechos: Es muy importante garantizar que el proceso de bloqueo temporal respete los derechos de los individuos, incluyendo el derecho a la defensa y a un juicio justo, evitando medidas arbitrarias o desproporcionadas.
- Recomendaciones:
- Desarrollo Normativo: Es fundamental que los marcos legales se actualicen para incluir disposiciones que permitan la implementación de medidas de aseguramiento inmediato, como el bloqueo temporal de activos ilícitos, adaptándose a la evolución de los delitos financieros en el entorno digital. Por ello se presenta la propuesta de reforma al artículo 231 del Código Orgánico Integral Penal en Ecuador para implementar como tercer inciso al bloqueo temporal de activos ilícitos como medida de aseguramiento inmediato ante transferencias electrónicas no consentidas.
- Capacitación y Recursos: Las instituciones financieras y las autoridades deben invertir en capacitación y en la adquisición de tecnologías adecuadas para detectar y responder rápidamente a las transferencias electrónicas no consentidas.
- Colaboración Internacional: Dado que los fraudes electrónicos a menudo trascienden fronteras, es esencial fomentar la cooperación internacional para la implementación de medidas de aseguramiento y la recuperación de activos a nivel global.

CONCLUSIONES

Al finalizar la investigación se puede expresar que las transferencias electrónicas no consentidas representan un desafío significativo para la legislación penal ecuatoriana, que carece de mecanismos ágiles y efectivos para proteger a las víctimas. Luego del análisis realizado se corrobora que el bloqueo temporal de activos ilícitos surge como una medida más efectiva y rápida en la recuperación de fondos frente a alternativas tradicionales como el embargo o la intervención judicial. La implementación de esta medida requiere reformas normativas que garanticen la viabilidad legal y respeten los derechos fundamentales de los involucrados.

Además, invertir en tecnologías avanzadas y capacitación para instituciones financieras y autoridades judiciales es muy importante para la eficacia de esta propuesta. La cooperación internacional es otro factor de gran importancia, dada la naturaleza transfronteriza de muchos fraudes electrónicos.

REFERENCIAS BIBLIOGRÁFICAS

1. Fayad Lemaitre AE, Peynado Villalba MP. Fraudes en línea: ¿hacia una responsabilidad civil objetiva de las entidades bancarias? [internet]. [bogotá]: universidad de los andes. Facultad de derecho; 2015. Disponible en: https://repositorio.uniandes.edu.co/server/api/core/bitstreams/29c1002a-7e13-4525-b8b4-fffeb4d189f1/content

2. Perlaza Guerrero CM, Rivera Vélez JM. Actuación del Estado en el delito de transferencia no consentida de activos en Colombia, periodo 2020-2023 [Internet] [bachelor thesis]. Derecho; 2024 [citado 26 de enero de 2025]. Disponible en: https://repositorio.uceva.edu.co/handle/20.500.12993/4600

3. Durán Vinazco R. Las Transferencias Electrónicas de Fondos –TEF- en Colombia: Análisis de la Responsabilidad contractual del establecimiento bancario según la jurisprudencia de la delegatura jurisdiccional de la Superintendencia Financiera de Colombia [Internet] [Trabajo de grado - Doctorado]. Universidad Nacional de Colombia; 2018 [citado 26 de enero de 2025]. Disponible en: https://repositorio.unal.edu.co/handle/unal/81592

4. Sempertegui Torres MP. DELITO DE APROPIACIÓN FRAUDULENTA POR MEDIOS ELECTRÓNICOS BAJO LA MODALIDAD DE PHISING DENTRO DEL MARCO JURÍDICO ECUATORIANO [Internet] [tesis de grado]. [Cuenca, Ecuador]: Univerisdad del Azuay; 2022. Disponible en: https://dspace.uazuay.edu.ec/bitstream/datos/12380/1/17907.pdf

5. Villamil Arcos CA. Selección de una Técnica de Aprendizaje de Máquina para la Detección de Fraude Financiero Digital Enfocado a Transacciones no Autorizadas o Consentidas [Internet] [Tesis de Magister en Ingeniería – Analítica, Profundización]. [Medellín, Colombia]: Universidad Nacional de Colombia. Facultad de Minas, Área curricular de Sistemas e Informática; 2022. Disponible en: https://repositorio.unal.edu.co/bitstream/handle/unal/84015/98626143.2023.pdf?sequence=4&isAllowed=y

6. ¿Qué es el phishing y cómo evitarlo? ¡No piques! - Cliente Bancario, Banco de España [Internet]. [citado 26 de enero de 2025]. Disponible en: https://clientebancario.bde.es/pcb/es/blog/que-es-el-phishing-y-como-evitarlo.html

7. Malware - Qué es y cómo funciona la protección antimalware | ESET [Internet]. [citado 25 de enero de 2025]. Disponible en: https://www.eset.com/es/caracteristicas/malware/

8. República del Ecuador Asamblea Nacional. Código Orgánico Integral Penal, COIP. 2014.Disponible en: https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

9. Bascur G, Sepúlveda RP. Los delitos informáticos en Chile: Tipos delictivos, sanciones y reglas procesales de la Ley 21.459, primera parte. Revista de Estudios de la Justicia [Internet]. 30 de diciembre de 2022 [citado 26 de enero de 2025];(37). Disponible en: https://rej.uchile.cl/index.php/RECEJ/article/view/67885

10. Yepez A. FEXLAW. 2021 [citado 26 de enero de 2025]. Recuperación de activos locales e internacionales. Disponible en: https://fexlaw.com/articulos/recuperacion-de-activos-locales-e-internacionales/

11. Rico Carrillo M. LA PROTECCIÓN DE LOS CONSUMIDORES EN LAS TRANSACCIONES ELECTRÓNICAS DE PAGO. Revista Electrónica de Estudios Telemáticos [Internet]. 2007;6. Disponible en: https://dialnet.unirioja.es/descarga/articulo/2961704.pdf

12. ATLAS.ti [Internet]. [citado 24 de enero de 2025]. ¿Qué es la investigación con métodos mixtos? Disponible en: https://atlasti.com/es/guias/guia-investigacion-cualitativa-parte-1/investigacion-con-metodos-mixtos

13. Pérez J. Some comments on Saaty's AHP. Management Science. 1995;41(6):1091-5. Disponible en https://pubsonline.informs.org/doi/abs/10.1287/mnsc.41.6.1091

14. Rey-Baracaldo DF. Responsabilidad civil en el sistema financiero frente a fraudes y/o transacciones electrónicas en Colombia [Trabajo de grado - Pregrado]. [Bogotá, Colombia]: Universidad Católica de Colombia; 2023. Disponible en: https://repository.ucatolica.edu.co/server/api/core/bitstreams/1aa4cb9d-fced-44d1-8d80-f8f03b02a611/content

15. FasterCapital [Internet]. [citado 26 de enero de 2025]. Lagunas de ciberseguridad al descubierto proteccion de sus activos digitales. Disponible en: https://fastercapital.com/es/contenido/Lagunas-de-ciberseguridad-al-descubierto--proteccion-de-sus-activos-digitales.html

16. Díaz Coral ME. Guía de jurisprudencia constitucional. Medidas cautelares onstitucionales. Centro de Estudios y Difusión del Derecho Constitucional (CEDEC); 2023. Disponible en: https://repositorio.dpe.gob.ec/bitstream/39000/3390/1/DEPE-DPE-005-2023.pdf

FINANCIACIÓN

Ninguna.

CONFLICTO DE INTERESES

Ninguno.

CONTRIBUCIÓN DE AUTORÍA

Conceptualización: Madeline Vanessa López Bravo, Carmen Marina Méndez Cabrita, Marcelo Raúl Dávila Castillo, María Fernanda Gómez Ayala.

Curación de datos: Madeline Vanessa López Bravo, Carmen Marina Méndez Cabrita, Marcelo Raúl Dávila Castillo, María Fernanda Gómez Ayala.

Análisis formal: Madeline Vanessa López Bravo, Carmen Marina Méndez Cabrita, Marcelo Raúl Dávila Castillo, María Fernanda Gómez Ayala.

Adquisición de fondos: Madeline Vanessa López Bravo, Carmen Marina Méndez Cabrita, Marcelo Raúl Dávila Castillo, María Fernanda Gómez Ayala.

Investigación: Madeline Vanessa López Bravo, Carmen Marina Méndez Cabrita, Marcelo Raúl Dávila Castillo, María Fernanda Gómez Ayala.

Metodología: Madeline Vanessa López Bravo, Carmen Marina Méndez Cabrita, Marcelo Raúl Dávila Castillo, María Fernanda Gómez Ayala.

Administración del proyecto: Madeline Vanessa López Bravo, Carmen Marina Méndez Cabrita, Marcelo Raúl Dávila Castillo, María Fernanda Gómez Ayala.

Recursos: Madeline Vanessa López Bravo, Carmen Marina Méndez Cabrita, Marcelo Raúl Dávila Castillo, María Fernanda Gómez Ayala.

Software: Madeline Vanessa López Bravo, Carmen Marina Méndez Cabrita, Marcelo Raúl Dávila Castillo, María Fernanda Gómez Ayala.

Supervisión: Madeline Vanessa López Bravo, Carmen Marina Méndez Cabrita, Marcelo Raúl Dávila Castillo, María Fernanda Gómez Ayala.

Validación: Madeline Vanessa López Bravo, Carmen Marina Méndez Cabrita, Marcelo Raúl Dávila Castillo, María Fernanda Gómez Ayala.

Visualización: Madeline Vanessa López Bravo, Carmen Marina Méndez Cabrita, Marcelo Raúl Dávila Castillo, María Fernanda Gómez Ayala.

Redacción – borrador original: Madeline Vanessa López Bravo, Carmen Marina Méndez Cabrita, Marcelo Raúl Dávila Castillo, María Fernanda Gómez Ayala.

Redacción – revisión y edición: Madeline Vanessa López Bravo, Carmen Marina Méndez Cabrita, Marcelo Raúl Dávila Castillo, María Fernanda Gómez Ayala.

https://doi.org/10.56294/sctconf2025636