Transferencia no consentida de activos como delito informático en el sector financiero

Monografía para optar al título de Abogados

Presentado por
Alexandra Pulgarín Pulgarín
Federico Augusto Muñoz Zapata

Programa de Derecho
Universidad Autónoma Latinoamericana
Medellín
2024

Tabla de contenido

Índice de Figuras

Resumen

El presente trabajo de investigación tuvo como finalidad analizar cómo afecta la transferencia no consentida de activos a la confianza de los usuarios y a la integridad del sistema financiero en Colombia. Metodológicamente se abordó un estudio de tipo cualitativo, de naturaleza normativa y con un método hermenéutico y como técnicas e instrumentos de recolección de información se implementó el análisis documental, la encuesta y la entrevista semiestructurada. Como resultado se pudo evidenciar que a pesar de los esfuerzos tecnológicos realizados por las entidades financieras la confianza en el sistema financiero en Colombia sigue generado incertidumbre, pues según el índice de confianza del consumidor registro un decrecimiento de (-7,8%) entre enero y agosto de 2024, y una desconfianza del (77%) de los clientes encuestados en este estudio, que solo cuentan con productos como cuenta de ahorro/corriente por la obligatoriedad para recibir pagos y/o bonificaciones.

Palabras Claves: Delitos Informáticos, Patrimonio Económico, Skimming y Transferencia no consentida de activos.

Abstract

The purpose of this research work was to analyze how the non-consensual transfer of assets affects user confidence and the integrity of the financial system in Colombia. Methodologically, a qualitative study of a normative nature and with a hermeneutic method was addressed and documentary analysis, survey and semi-structured interview were implemented as techniques and instruments for collecting information. As a result, it was possible to show that despite the technological efforts made by financial entities, confidence in the financial system in Colombia continues to generate uncertainty, since according to the consumer confidence index it registered a decrease of (-7.8%) between January and August 2024, and a distrust of (77%) of the clients surveyed in this study, who only have products such as savings/current accounts due to the obligation to receive payments and/or bonuses.

Keywords: Computer Crimes, Economic Assets, Skimming and Non-consensual Transfer of Assets.

Introducción

Con la evolución exponencial de las tecnologías de la información y las comunicaciones TIC, si bien es cierto ha permitido la generación de servicios más personalizados para brindar una mejor experiencia con los clientes, cabe señalar que para el sector financiero esto también trae consigo situaciones alarmantes como consecuencia de ataques cibernéticos que pueden constituir la manipulación de sistemas donde se administran activos y afectar corporativamente a las empresas y particularmente el patrimonio económico de sus clientes. En este sentido, la transferencia no consentida de activos se encuentra tipificado en el artículo 269 j de la ley 599 de 2000 o código penal en Colombia, que con relación a los avances tecnológicos ha generado altos riesgos en contra de la seguridad de los sistemas de entidades financieras que afectan la confianza comercial en el mercado.

Históricamente la sociedad ha considerado que el lugar más seguro para salvaguardar sus ingresos o activos es mediante la administración de bancos comerciales, cooperativas, brókeres, agencias de bolsa, entre otros, sin embargo, estas cosmovisiones han ido mutando a partir de la evolución sistemática de la tecnología que otorga herramientas en beneficio y en contra de dicha administración. En razón de lo anterior se ha propuesto el siguiente problema jurídico ¿Cómo afecta la transferencia no consentida de activos en el sector financiero a la confianza de los usuarios y la integridad del sistema financiero?

Para dar respuesta a la pregunta problema, el estudio propuso como objetivo general analizar las afectaciones que produce la transferencia no consentida de activos a la confianza de los usuarios y a la integridad del sistema financiero en Colombia, básicamente lo que se pretende es establecer la incidencia que tiene este delito en la relación empresa-cliente y las necesidades jurídicas que se producen a partir de este fenómeno. Bajo estos parámetros para dar cumplimiento a dicho objetivo general fueron desarrollados tres capítulos que reflejan lo siguiente:

La primera parte aborda las generalidades dogmáticas del delito de transferencia no consentida de activos, desde sus elementos objetivos, hasta los elementos subjetivos, su tipicidad, antijuridicidad y culpabilidad que permiten identificar las dificultades de los operadores judiciales al momento de la investigación judicial o administración de justicia, debido a la característica trasnacional del mismo. El segundo capítulo, analiza la percepción de los clientes con activos financieros en bancas comerciales o similares que han sido víctimas del delito de transferencia no consentida de activos sobre los efectos a la relación empresa-cliente que suponen estos ataques a sus recursos financieros. Finalmente se describe desde la experiencia corporativa la estructura del sistema financiero y las garantías actuales sobre los activos de los clientes cuando surgen estos delitos informáticos que generan incertidumbres a todo el sistema bursátil en el país.

En definitiva, este trabajo de investigación es importante porque crea la necesidad de realizar reflexiones legislativas y/o jurídicas sobre las acciones que debe considerar el Estado Colombiano para reducir las afectaciones que se presentan a la confianza entre los clientes y empresas del sistema financiero que realizan transacciones mediante dispositivos digitales y que de ello depende su mínimo vital hasta sus proyectos de vida individuales o familiares, cuando se presentan ataques a los sistemas como el que produce el delito de transferencia no consentida de activos, siendo necesario un fortalecimiento para salvaguardar los recursos administrados y disminuir las cargas a las bancas comerciales.

1. Descripción General del Problema

1.1.Planteamiento del problema

Los más recientes avances tecnológicos han transformado la operación financiera: a través de internet, han hecho que cada vez sea menos complicado realizar operaciones y que sean más rápidas y accesibles, proporcionando una comodidad total a los participantes. No obstante, estos logros han generado un incremento de las actividades delictivas, como la transacción sin permiso de activos. Su acumulación causa alarma debido a la transacción de bienes financieros por parte de clientes engañosos y a las multas exorbitantes de las bancas estadounidenses, que deben responder por la integridad de los referidos bienes (Ricaurte, 2022).

Esta situación problemática implica una variedad de retos y dilemas que debe enfrentar el Estado Colombiano a través de su ordenamiento jurídico y que deben ser abordados exhaustivamente desde diferentes disciplinas. Bajo estos parámetros se hace necesario que en los estamentos legislativos se incluyan al sector privado del ecosistema financiero para que describan la forma en que se presentan estas manipulaciones al sistema y por supuesto las cargas impositivas que distorsionan el mercado bursátil por la desfinanciación que dichos ataques producen.

De igual manera, las fintech y las innovaciones tecnológicas deben ser supervisadas cuidadosamente para aprovechar las oportunidades que ofrecen al mismo tiempo que se mitigan los riesgos inherentes, como el riesgo de ciberseguridad. Finalmente, las autoridades legales y los fiscales deben trabajar en el desarrollo de marcos normativos y jurisprudenciales que permitan una investigación efectiva de los ciberdelitos y contribuyan a enfrentar el ciberdelito, especialmente en el manejo de evidencia volátil y en la regulación de servicios financieros en dispositivos móviles (Asobancaria, 2019).

A medida que la digitalización financiera avanza, los sujetos activos del delito han encontrado nuevas oportunidades para llevar a cabo transferencias fraudulentas, aprovechando vulnerabilidades en sistemas, procesos y comportamientos humanos (Del Olmo & Fernández, 2021).

En cuanto al delito informático de transferencia no consentida de activos, ha habido un fuerte aumento en el número de denuncias realizadas en los últimos diez años. También se han observado varios métodos utilizados por los hackers, que van desde el phishing hasta los ataques de ingeniería social. El phishing se basa en correos electrónicos o sitios web falsos que parecen ser legítimos y confiables y que intentan engañar a la víctima en la entrega de información confidencial, como contraseñas o datos bancarios (Rueda, 2020).

Complementariamente, la falta de claridad y coherencia de los marcos legales a nivel internacional hace que la cooperación entre jurisdicciones sea difícil y, en última instancia, conduce a lagunas en la responsabilidad legal. Por lo tanto, los problemas arriba señalados resultan en la pérdida de confianza en el sistema y, sin confianza, no hay sistema, ya que, esta es clave para su actividad, lo que puede desencadenar un papel en la disminución en la adopción de servicios financieros digitales (Gamba, 2019).

Ante lo expuesto, es necesario la adopción y formulación de medidas preventivas y correctivas permitirá lograr lo anterior con respecto a la prevención y mitigación ya sea desde el conocimiento técnico o la perspectiva subsidia. Esto se puede lograr a través de protocolos de

violencia al ingreso avanzados sobre siniestros, un aumento en la alfabetización financiera, y la cooperación entre el gobierno y las instituciones financieras (Gamba, 2019).

A pesar de que todos los tipos de delitos cibernéticos son investigables y el seguimiento bajo la ley, muchos de estos delitos no llevan a la eliminación subyacente, se debe porque muchos ciberdelitos son transaccionales y bastante complejos, para las legislaciones actuales, especialmente la colombiana que es muy respetuosa del debido proceso y no puede saltarse los protocolos y tiempos en la búsqueda de material probatorio cuando depende de la política de seguridad de otros países, demostrando respeto hacia su soberanía (Gamba, 2019).

Habrá que establecer la cooperación por y entre las partes interesadas en la industria financiera enfocada en que sean las instituciones financieras, los legisladores, los reguladores y los expertos en ciberseguridad los que trabajarán juntos y cooperarán para abordar el problema. Todo lo anterior con el fin de mitigar y combatir el problema en conjunto, se necesitarán medidas de seguridad apropiadas, una legislación más dura, así como una mejor comprensión del problema relacionado con los ciberataques en el ámbito financiero (Gamba, 2019).

Desde una perspectiva crítica, se debe demostrar que la legislación y los sistemas de cooperación internacionales juegan un papel clave para abordar los agravios que representan una preocupación fundamental para la integridad y la privacidad a medida que el cambio se encuentra con la digitalización. Estos están enmarcados en la Ley 1273 de 2009 en Colombia donde se dictan disposiciones en materia de delitos informáticos también se crean e instituciones sujetas al herramienta y posibles violaciones (Sentencia de Casación, 2015).

Este delito de transferencia no consentida de activos ha traído consigo gran traumatismo en el sistema financiero en Colombia que no previo verse superado por los ataques de los sujetos activos de este hecho punible, lo que además de cooperación internacional que implique agilizar los tiempos para el proceso de investigación, se hace también conveniente que estas entidades que poseen la carga probatoria e investigativa como la Fiscalía General de la Nación, cuente con las capacidades instaladas (infraestructura tecnológica y formación académica) para identificar a los responsables e imputar sin duda alguna ante los administradores de justicia estos hechos como medida social de prohibición y por supuesto de prevención (Gamba, 2019).

La posibilidad de transferir activos sin permiso ha generado desconfianza y es probable que muchas personas eviten transacciones en línea precisamente a raíz del miedo, pues se produce incertidumbre por las perdidas adicionales en términos de inversión en seguridad y empleo de personal de TI adicional en el sector real de la economía. En general, debido a la naturaleza transnacional de los ciberdelitos, la cooperación internacional es esencial para luchar adecuadamente contra ellos, es por ello que la ratificación de convenios internacionales como el Convenio de Budapest sobre ciberdelito es una de las formas de abordar este problema.

1.2. Pregunta de Investigación

¿Cómo afecta la transferencia no consentida de activos a la confianza de los usuarios y a la integridad del sistema financiero en Colombia?

2. Justificación

Según un informe de Cybersecurity Ventures, el costo global del cibercrimen, que incluye transferencias no consentidas de activos, podría alcanzar los $10.5 billones anuales para 2025 (Diario las Americas, 2023). Asimismo, la Asociación de Examinadores de Fraude Certificados (ACFE) estimó en su Report to the Nations 2020 que las organizaciones pierden alrededor del 5% de sus ingresos anuales debido a fraudes internos y externos (FLAI, 2020). Por último, la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) estima que el monto de dinero lavado anualmente es de entre el 2% y el 5% del PIB mundial, lo que equivale a entre $800 mil millones y $2 billones (Naciones Unidas, 2011).

Por otro lado, desde la relevancia social, Montañez (2017) estudiar el delito de transferencia no consentida de activos es un delito complejo de investigar debido a su ejecución a través de la red y la naturaleza digital y volátil de las pruebas, lo que permite a los sujetos activos del delito obtener grandes ganancias económicas con mínimos riesgos de ser capturados, lo que incrementa el número de intrusiones ilícitas y las investigaciones relacionadas. Además, el bien jurídico protegido en estos delitos es principalmente el patrimonio económico, implica que la información privada y confidencial también está en riesgo, lo que subraya la necesidad de medidas de seguridad robustas y una legislación adecuada (Montañez, 2017).

En cuanto al aporte científico se evidencia que la impunidad en la comisión de este delito obedece a la falta de capacidad instalada que poseen las entidades de investigación y administración de justicia para determinar desde el análisis forense la manipulación de los sistemas corporativos y particulares hasta defraudar el patrimonio económico de estos. Bajo ese contexto este trabajo de investigación pretende dar a conocer las complejidades a las que se enfrentan los operadores judiciales en Colombia y las acciones administrativas y legislativas que deben realizarse por parte del Estado para generar una disminución en la comisión del delito o en su efecto aumentar las sanciones como mecanismo corrector. (Gonzalez, 2017).

Finalmente, como futuros profesionales del programa de derecho de la Universidad Latinoamericana de la ciudad de Medellín, consideramos conveniente que las normas creadas en los diferentes estamentos del orden jurídico colombiano sean de obligatorio cumplimiento, ya que, en su análisis legislativo se pudo inferir como afectaba a una parte importante de la población que confía en la seguridad jurídica de estos cuerpos normativos (Bechara, Mosquera, & Ledezma, 2020).

Objetivos

3.1.Objetivo General

- Analizar las afectaciones que produce la transferencia no consentida de activos a la confianza de los usuarios y a la integridad del sistema financiero en Colombia

3.2. Objetivos Específicos

- Identificar el alcance dogmático del delito de transferencia no consentida de activos en Colombia

- Determinar el impacto en la confianza de los usuarios a nivel económico y social respecto de la comisión del delito de transferencia no consentida de activos en el sector financiero en Colombia

- Explicar cómo se encuentra estructurada la integridad del sistema financiero en Colombia para la generación de respuesta a la comisión de delito de transferencia no consentida de activos

Marco de Referencia

4.1. Estado del Arte

Con la finalidad de identificar los aportes epistemológicos sobre el objeto de estudio, se hace necesario evaluar los resultados de investigaciones anteriores en los cuales se pueda establecer las necesidades actuales de investigaciones, la eficacia teórica y metodológica utilizada para llevar a cabo dichos estudios.

En primera instancia, Sánchez (2017), en su trabajo de investigación planteó como pregunta problema ¿Cuáles son las falencias y posibles mejoras en la legislación vigente para enfrentar eficazmente la delincuencia cibernética en Colombia? Para dar respuesta propuso como objetivo general identificar vacíos y proponer mejoras en la Ley 1273 de 2009 para fortalecer la protección contra delitos informáticos en Colombia. De esta manera, señalar que el estudio fue llevado con enfoque cualitativo, basado en la revisión de documentos bibliográficos y leyes de Argentina, Venezuela y Chile, además antecedentes de otras investigaciones sobre la materia. Por último, y a modo de cierre de la tabla, se puede expresar que, si bien la Ley 1273 es un importante paso, esta presenta fallas y ambigüedades por las cuales se pueden cometer delitos de forma impune. Evidencia de ello es cómo, por ejemplo, ciertos capítulos han sido modificados, o la inclusión de un artículo en el cual se definen las infracciones más comunes a través del uso de la tecnología. De esta manera, es necesario señalar que de esta tabla se desprende la necesidad urgente de regular y ajustar las leyes a las nuevas modalidades de crimen virtual en Colombia, de forma de proteger los datos personales y la seguridad de los sistemas de cómputo del país. (Sánchez, 2017).

El análisis de sentencias específicas y casos judiciales establece que la investigación señala no solo las dificultades en su empleo para los jueces y fiscales en los tribunales al momento de aplicar la Ley 1273, sino que también proporciona bases empíricas para las propuestas de cambio en la normativa e incluso subraya la necesaria ética de una normativa más clara y unificada. De la misma forma, señala cómo este avance se implementa a través de políticas de seguridad informática supervisadas por organizaciones de calidad internacional, lo que no solo ayuda a disminuir el impacto del delito informático realizado sino también a los problemas de rastreo, sino que también educa a las empresas y usuarios finales acerca de los riesgos de desconocer información.

De la misma forma, Guerrero & Castillo (2017), abordaron la cuestión del ciberdelito en el sector bancario colombiano, señalando las vulnerabilidades y amenazas que enfrentan las instituciones financieras y sus usuarios. El objetivo general fue analizar estas vulnerabilidades, amenazas y retos en el contexto colombiano. La metodología que utilizaron fue de tipo descriptiva, y el diseño de la investigación fue monográfica en el sentido de que los autores realizaron un riguroso proceso de adquisición, organización, sistematización y divulgación del conocimiento. Recopilaron en forma inductiva y deductiva información de bases de datos internacionales y relacionada con el marco jurídico y técnico acerca de ciberdelito financiero. Como resultado, se obtuvo que la globalización y el desarrollo de las TIC han aumentado los peligros de ciberdelito, afectando severamente al sector bancario, lo que hace necesario la implementación de protocolos de seguridad como IPSec, fortalecer el aparato jurídico para hacer frente a este delito. Como conclusión, los autores señalaron que es necesario un análisis más profundo de la colaboración internacional y de las tecnologías de seguridad en constante desarrollo para minimizar los riesgos y proteger a las instituciones y a los usuarios.

El estudio presenta recomendaciones y sugerencias en forma de estrategias integrales para la lucha contra el fenómeno y la implementación en la sociedad en su conjunto. Entre ellos se incluyen la formación y capacitación del personal judicial, la cooperación internacional y la actualización de la legislación, las campañas preventivas y la interacción con los representantes del sector privado. Así, el estudio ha logrado brindar un análisis multivariado sobre el delito de Transferencia no consentida de activos y, al mismo tiempo, sustentarse en algunas teorías que permiten identificar ciertas recomendaciones prácticas para la prevención y represión de este delito que implique proteger los bienes jurídicos en juego allí.

Por otra parte, Aránzazu & Delgado (2018) en su estudio, analizaron la eficacia normativa de la Ley respecto a los delitos informáticos en Colombia partiendo de la siguiente pregunta problemática. ¿Cuál es la eficacia normativa de la Ley 1273 de 2009 frente a los delitos informáticos en Colombia? El objetivo general fue establecer dicha eficacia normativa. La metodología utilizada es de tipo descriptivo con enfoque cualitativo, se emplea el método de análisis y síntesis, y se basa en fuentes de información secundarias. Las técnicas de recolección de información fueron: revisión de literatura y análisis de datos estadísticos proporcionados por el Centro Cibernético Policial. Los resultados, reflejaron que la Ley 1273 de 2009, cumple con los criterios de validez jurídica y ha sido correctamente promulgada; sin embargo, la eficacia sociológica de esta ley aun requiere ajustes. El número de denuncias por delitos informáticos en Colombia aumentó de un promedio anual de 5.926 en el periodo 2014-2016 a 11.618 en el año 2017. Los delitos más comunes son el hurto por medios informáticos, el acceso abusivo a sistemas informáticos y la violación de datos personales. Por tanto, se concluye que la ley es válida y aplicable desde el punto de vista jurídico; sin embargo, su eficacia es limitada.

Además, Castillo (2018), describe cómo los actores de las tecnologías de la información y la comunicación (TIC) promueven conductas delictivas dirigidas a lesionar el patrimonio económico de las personas en Colombia. El objetivo general del estudio es caracterizar el marco de la delincuencia del fraude informático y los actores y la afectación del hurto mediante TIC sobre el patrimonio económico y las consecuencias legales del delito en el país. Se utilizo una metodología meramente documental tomando como base los casos investigados por la Fiscalía. Este delito de transferencia no consentida de activos causa perjuicios al patrimonio ya que, a pesar de ser regulada por la ley como la Ley 1273 de 2009, el alto nivel de sofisticación de los actores delictivos y el poco conocimiento de los usuarios enfrenta aumentan el riesgo de ser vulnerados en sus sistemas y recursos económicos.

Basado en los resultados, el estudio ofrece recomendaciones prácticas para mejorar la eficacia de la legislación y la prevención de delitos informáticos, incluyendo la necesidad de fortalecer la educación y concienciación sobre los riesgos y deberes asociados con el uso de TICs, mejorar las capacidades de investigación y prevención, y avanzar en la cooperación internacional. Los resultados de este estudio no solo proporcionan una evaluación crítica de la Ley 1273 de 2009, sino que también ofrecen una comprensión más profunda de los delitos informáticos en Colombia y sugieren caminos para mejorar la respuesta legal y social a estos desafíos.

Nobles, Narváez & Rúgeles (2020), tuvieron como objetivo general examinar los criterios de validez actuales de la prueba electrónica en relación con los delitos cibernéticos, implementados a través de la Ley 1273 de 2009. Principalmente, el estudio se llevó a cabo en comparación con la prueba convencional con el fin de identificar los elementos objetivos que la

prueba electrónica debe cumplir y para definir el ámbito de los delitos cibernéticos en términos del derecho penal colombiano. La naturaleza cualitativa de la metodología fue implementada a través del enfoque dogmático-jurídico, y el marco de la revisión documental. Se prestará especial atención a la literatura jurídica, a la jurisprudencia y la doctrina relacionada, y permanecerá fundamental en la construcción de un marco interpretativo sólido que permita cumplir las disposiciones relacionadas con la prueba electrónica. Como resultados se obtuvo que los aspectos como la autenticidad y la veracidad en los sistemas deben crear un campo de defensa dentro del sistema corporativo de las bancas comerciales, esto es, que para disminuir la comisión de este delito se debe generar sinergia desde lo ejecutivo hasta lo operacional.

Cabe destacar que la contribución de esta investigación radica en el descubierto de los procedimientos y las características que deben ser cumplidos por las pruebas digitales para que sean válidas; es decir, la autenticación y la integridad aumentan significativamente la efectividad de la evidencia presentada en las pruebas digitales. Desde un punto de vista tecnológico cada transacción debería aprobarse desde los dispositivos de uso personal como estrategia de ciberseguridad.

Desde luego, en el mismo escenario Garzón & Quintero (2021) establecieron su objetivo general, para estudiar los riesgos legales asociados con el comercio electrónico en Colombia y su objetivo específico, para determinar si la legislación penal existente en el país es suficiente para combatir el ciberdelito. En cuanto a la metodología se abortó un estudio cualitativo con enfoque hermenéutico que supuso un análisis de contextos constitucionales, legales y jurisprudenciales. Como resultado se obtiene que las entidades gubernamentales para tener mayor precisión en sus funciones de control y vigilancia mediante la sofisticación de herramientas tecnológicas que faciliten a las bancas comerciales bloquear ataques, a los operadores judiciales mejorar procesos de investigación y mejorar capacidad de análisis probatoria para una correcta administración de justicia.

La protección del patrimonio económico es sin duda una prioridad en la postura de prevenir este delito de transferencia no consentida de activos, es de anotar que el sistema financiero se sostiene debido a que las bancas comerciales soportan las afectaciones de los ataques en la mayoría de los casos, como una forma de mantener la confianza en el sector, sin embargo, distorsiona la rigurosidad de la justicia que en dicha situación no concibe las acciones para repeler penalmente los ataques a la ciberseguridad de los clientes y de estas organizaciones que cada vez más pierden valor como consecuencia de la falta de resultado institucional.

En este mismo sentido, con relación al estudio desarrollado por Martínez (2023), quien estableció como objetivo general analizar el concepto dogmático y jurídico-penal del delito de hurto mediante el uso de dispositivos digitales en Colombia en comparación con los ordenamientos jurídicos de Alemania, Francia y España. La metodología utilizada se enfocó en un estudio comparado de legislaciones para establecer las formas de como enfrentan los delitos informáticos que afectan el patrimonio económico. Como resultado se estableció que si bien es cierto los avances normativos han sido significativos, aun presentan lagunas en relación a la transferencia no consentida de activos por la imposibilidad de ingresar a otros sistemas de rango internacional, en ese sentido, si existiera un convenio entre países afectados por este comportamiento las acciones restrictivas y de protección a dichos recursos podría ser mucho más eficiente. Es necesario enviar un mensaje sobre la capacidad sancionatoria que tienen los Estados para que los actores de delitos mediante la web puedan disminuir sistemáticamente.

Este estudio es importante porque permite comprender que países como Alemania, Francia y España mediante el endurecimiento de penas y la creación de nuevos hechos punibles por la alteración de estos sistemas han podido mitigar la comisión de este delito y similares, situación que debe analizarse bajo el contexto en el que Colombia se enfrenta para nadie es un secreto que las capacidades tecnológicas y técnicos que se forjan en Europa son mucho más avanzados que los de Sudamérica y Colombia, en este sentido se debe analizar los casos en concretos que se han presentado y tomar determinaciones tendientes a fortalecer los mismos.

Por último, Astaiza & Cuellar (2023), desarrollaron un análisis penal dogmático del sistema normativo que brinda regulación criminal a los delitos informáticos en el país. Su metodología fue descriptiva con enfoque cualitativo por medio de la recolección y revisión documental de aspecto jurídico. La falta de capacidad tecnológica y especialmente en temas de seguridad son algunos factores que han generado que este fenómeno punible se acrecenté y se afecten derechos fundamentales a particulares como el mínimo vital, demostrando las dificultades que deben enfrentar los operadores judiciales, para que pueda fortalecerse por lo menos desde el ámbito nacional y posteriormente desde la cooperación internacional. En conclusión, se evidencia que la normatividad actual no brinda las garantías necesarias para enfrentar de manera autónoma el delito de transferencia no consentida de activos.

4.2.Marco Contextual

Este estudio surge como consecuencia de los comportamientos deliberados de los sujetos activos del delito de transferencia no consentida de activos que ha colocado en vilo todo el sistema financiero, desde las bancas comerciales hasta los clientes particulares que ven afectada su confianza cada vez más en los esquemas de seguridad digital de estas bancas.

Lo anterior permite reconocer que la legislación colombiana requiere cambios inmediatos en relación a las leyes 1273 de 2009 y 1928 de 2018, porque si bien es cierto describen de manera adecuada los elementos subjetivos y objetivos del comportamiento punible, para efectos de los actos logísticos de investigación y actuación por parte de los entes facultados, pero que en materia tecnológica y formal se debe fortalecer para reducir la incertidumbre. También debe reconocerse que la inclusión de Colombia al Convenio de Budapest es un avance inherente a las necesidades mencionadas, pero dichas recomendaciones no se han podido imprimir debido a la ausencia de recursos técnicos y tecnológicos para que las entidades competentes hagan cumplir el ordenamiento jurídico, lo que entorpece la eficacia institucional (Suarez, 2019).

No obstante, desde el enfoque socioeconómico este delito desgasta el sistema financiero por la desconfianza que se produce en los sistemas tecnológicos de las organizaciones financieras, afectando la relación comercial organización – cliente, ocasionando una variación en la circulación del dinero y por supuesto en la adquisición de productos de inversión como CDT, compra de divisas, acciones, ahorros programados, entre otros. Este sector bursátil requiere de la transaccionalidad para su funcionamiento y sostenimiento en el tiempo, además, es una de las actividades económicas que genera un gran aporte al PIB, por la generación de empleos directos e indirectos y el impulso a la apertura de nuevos emprendimientos mediante productos de crédito, desde aquí la necesidad de aportarle a este delito informático la importancia que requiere en el ordenamiento jurídico colombiano (Salazar, 2011).

El delito de transferencia no consentida de activo debe enfrentarse a diferentes situaciones. En primer lugar, la tipificación del delito varía significativamente entre diferentes jurisdicciones,

lo que dificulta la comparación doctrinal y jurisprudencial. En algunos países, este delito se considera como estafa, apropiación ilícita o hurto, lo que complica la cooperación internacional y la extradición de los sujetos activos del delito. En Colombia, aunque el artículo 269J del Código Penal define claramente el delito, la aplicación de la ley enfrenta problemas debido a la falta de especialización y recursos en las fuerzas de seguridad y el sistema judicial, es de añorar que la naturaleza técnica y compleja de estos delitos requiere una formación especializada para los fiscales y jueces, lo cual no siempre está disponible (Posada M. , 2017).

4.3. Marco Teórico Conceptual

El presente acápite está fundamentado en (3) categorías de análisis principales que están directamente relacionados con los objetivos de investigación, entre estas se encuentran: (i) los efectos patrimoniales en el delito informático de transferencia no consentida de activos teniendo en cuenta dogmáticamente es el derecho esencial que se vulnera a la víctima siendo necesario analizar su alcance, características y los aspectos considerativos de culpabilidad, antijuridicidad y tipicidad; (ii) delitos informáticos y la complejidad de tipificación, los cuales permiten establecer una diferenciación en la metodología entre aquellos hechos punibles que se configuran mediante el uso de dispositivos digitales para obtener dinero y otros para obtener información personal o comercial y (iii) la Transferencia no consentida de Activos una enfermedad del sector financiero en relación al contexto actual que provoca afectaciones al sistema financiero en Colombia.

4.3.1. Los efectos patrimoniales en el delito informático de transferencia no consentida de activos

Los delitos contra el patrimonio económico se definen como aquellas conductas ilícitas que afectan la propiedad o los bienes de una persona o entidad, impidiendo que esta pueda disponer de ellos libremente o causando una disminución en su valor. Estos delitos están contemplados en el Código Penal Colombiano y abarcan una variedad de acciones ilícitas que perjudican el patrimonio de individuos, empresas o el Estado. Entre los delitos principales se encuentra el Hurto simple fundamentado en el artículo 239 de la Ley 599 de 2000, el Hurto Calificado, articulo 240, estafa, articulo 246, abuso de confianza, articulo 249, extorsión, articulo 244 y Daño a bien ajeno, artículo 265 del Código penal (Peréz, 2019).

Estos delitos tienen en común la conducta, básicamente está representada en una acción u omisión que tiene como finalidad afectar negativamente el patrimonio económico y el elemento de voluntariedad, pues generalmente en estos casos el dolo se entiende como el conocimiento previo, la intención consciente de hacer daño patrimonial (Peréz, 2019).

Históricamente, los productos bancarios han sido considerados seguros debido a la regulación estricta, la supervisión gubernamental y las medidas de seguridad física y lógicas implementadas por las instituciones financieras (Peréz, 2019).

Sin embargo, las tendencias actuales indican que mediante el uso de dispositivos digitales han surgido nuevas formas de defraudar el patrimonio económico de empresas y hogares que ven truncadas sus proyectos corporativos y personales por ausencia de estructura normativa que permita evitar este tipo de perjuicios, como el que causa la Transferencia No Consentida de Activos (art 269j ley 599 de 2000).

El delito informático de transferencia no consentida de activos tiene efectos patrimoniales significativos, ya que implica una afectación patrimonial efectiva del sujeto pasivo. Este delito se caracteriza por la transferencia automática y no autorizada de activos patrimoniales, como dinero escritural o contable, desde la cuenta del titular hacia otra cuenta, sin el consentimiento del titular legítimo, resultando como un perjuicio económico directo para el sujeto pasivo, quien pierde la capacidad de disponer de sus activos (Posada R. , 2012).

El resultado de este delito es un cambio en la adscripción de los activos, que pasan del patrimonio del sujeto pasivo al del beneficiario de la transferencia, generando un detrimento patrimonial para el primero. Este perjuicio puede manifestarse en diversas formas, como la disminución de fondos en cuentas bancarias, la pérdida de derechos de crédito, o la afectación de otros bienes y derechos con valor monetario (Posada R. , 2012).

4.3.2. La complejidad de tipificación de los delitos informáticos

Los delitos informáticos se conciben como aquellos actos que se cometen mediante el uso de dispositivos digitales con la intención de afectar el patrimonio económico de particulares, que, a su vez, pueden generar afectaciones a otros bienes jurídicos tutelados. Estos delitos pueden incluir una variedad de acciones como el acceso no autorizado a sistemas informáticos, el sabotaje de datos, la interceptación no autorizada de comunicaciones, el espionaje informático, y otros comportamientos que generan daño a personas, empresas o gobiernos. Los delitos informáticos se caracterizan por su ocurrencia en el ciberespacio y su capacidad de causar pérdidas económicas, desprestigio, chantaje y otros perjuicios a las víctimas (Acosta, Benavides, & García, 2020).

Entre los delitos informáticos se incluyen el acceso no autorizado, el daño a datos o programas, el sabotaje informático, la interceptación no autorizada y el espionaje informático. De aquí la importancia, de conocer las debilidades de las organizaciones en cuanto a seguridad informática y de implementar medidas como encriptaciones y políticas de seguridad para proteger la información (Acosta, Benavides, & García, 2020).

La impunidad en la administración de justicia con respecto a los delitos informáticos es un tema crítico, ya que, la falta de castigo adecuado y la existencia de vacíos legales permiten que muchos de estos delitos queden sin resolver, afectando gravemente a las víctimas, especialmente en los elementos claves para la tipificación del hecho punible, pues se requiere contar con una gran ingeniería digital por parte del ente acusador para poder crear medios probatorios que faciliten la imputación de cargos, como por ejemplo el delito de la transferencia no consentida de activos (Acosta, Benavides, & García, 2020).

Conforme a lo anterior, vale decir que la tipificación de delitos informáticos en Colombia es compleja debido a varios factores:

En primer lugar, por la rápida evolución de la tecnología y las técnicas utilizadas por los sujetos activos del delito supera con frecuencia la capacidad de las leyes existentes para abordar nuevas formas de criminalidad, lo que crea un desfase entre la legislación y la realidad tecnológica, dificultando la aplicación efectiva de la ley (Acosta, Benavides, & García, 2020).

En Segunda instancia, la naturaleza transnacional de los delitos informáticos complica la jurisdicción y la cooperación internacional, ya que, los sujetos activos del delito pueden operar

desde cualquier parte del mundo, lo que requiere una colaboración global y acuerdos internacionales para perseguir y sancionar estos delitos (Acosta, Benavides, & García, 2020).

Por último, las lagunas formales que impiden una adecuada diligencia en los procesos de investigación, análisis de elementos materiales probatorios, imputación de cargos, y por supuesto imposición de medidas, básicamente, implica afectar el proceso penal desde su inicio por falta de garantías, esto es, la capacidad de legalizar pruebas en escenarios trasnacionales, por ejemplo. Desde esta perspectiva debe establecerse mecanismos de autenticación de las IP, como medida obligatoria para que estas entidades financieras e institucionales puedan contar con registros en tiempo real de ingreso al sistema.

4.3.3. La Transferencia no consentida de Activos una enfermedad del sector financiero

La Corte Suprema de Justicia ha establecido que la creación del riesgo no implica automáticamente la responsabilidad del banco, ya que, las instituciones financieras pueden demostrar que el daño fue consecuencia de acciones u omisiones del consumidor, como en el caso de un cuentahabiente que pierde su tarjeta y deja el número de clave con el plástico. Esto introduce una complejidad adicional en la imputación de cargos, ya que se debe determinar la responsabilidad compartida entre el consumidor y la institución financiera (Asobancaria, 2022).

Las entidades vigiladas están obligadas a responder a pesar de haber obrado diligentemente, mientras que no hay normas ni precedentes que extiendan este criterio a las entidades de servicios similares no vigiladas, cabe señalar que la diferencia en la supervisión y jurisdicción crea regímenes y efectos diferenciales que complican la imputación de cargos (Asobancaria, 2022).

En el mismo sentido, la falta de una investigación adecuada o la aceptación de reclamos sin elementos de juicio puede llevar a decisiones judiciales desfavorables, lo que añade una capa de complejidad en la imputación de cargos, ya que se requiere una investigación exhaustiva y la presentación de pruebas concluyentes (Asobancaria, 2022).

También vale decir que desde las entidades financieras este delito (transferencia no consentida de activos), afectan considerablemente a dichas empresas y el sistema financiero en sentido general, ya que, implica una exposición a la seguridad de estos entes económicos, en donde los sujetos activos del delito obtienen acceso a las credenciales bancarias de los usuarios mediante engaños, como correos electrónicos o mensajes que aparentan ser de fuentes confiables (Calvo, 2023).

Las entidades financieras, al ser responsables de la seguridad de las transacciones, enfrentan la obligación de restituir los fondos sustraídos a los clientes, a menos que puedan demostrar negligencia grave por parte del usuario, esto no solo implica pérdidas económicas directas, sino también un impacto en la reputación de la entidad, ya que los clientes pueden perder confianza en la seguridad de sus servicios.

De igual manera, estas conductas implican desde todos los aspectos que las empresas deben invertir en mejorar sus sistemas de seguridad para prevenir futuros incidentes y complementariamente deben asumir costos legales asociados con la gestión de reclamaciones y posibles litigios, ya que las víctimas pueden optar por acciones civiles para recuperar sus fondos (Calvo, 2023).

Se ha precisado que estas inversiones para el fortalecimiento del sistema y procurar reducir los riesgos de vulneración de la plataforma de estas entidades financieras se debe optar por:

- **Autenticación Multifactor (MFA):** Implementar sistemas de autenticación Multifactor para acceder a cuentas bancarias. Esto añade una capa adicional de seguridad, ya que requiere que los usuarios proporcionen más de una forma de verificación, como un código enviado a su teléfono móvil, además de su contraseña.

- **Tecnología Antiphishing:** Desarrollar e implementar tecnologías avanzadas de detección de "phishing", como filtros de correo electrónico que identifiquen y bloqueen mensajes sospechosos, y sistemas que detecten y cierren sitios web fraudulentos que imitan a las páginas oficiales de las entidades financieras.

- **Monitoreo y Detección de Fraudes:** Establecer sistemas de monitoreo en tiempo real para detectar actividades inusuales o sospechosas en las cuentas de los clientes. Esto puede incluir alertas automáticas para transacciones que se desvíen de los patrones normales de comportamiento del usuario.

- **Actualización de Software y Sistemas de Seguridad:** Mantener todos los sistemas y software actualizados con los últimos parches de seguridad para proteger contra vulnerabilidades que los sujetos activos del delito podrían explotar.

- **Colaboración Interinstitucional:** Fomentar la colaboración entre entidades financieras, organismos reguladores y fuerzas del orden para compartir información sobre amenazas emergentes y mejores prácticas en ciberseguridad.

Por último, las empresas deben enfocarse en la estructuración de políticas de seguridad y confidencialidad sobre los empleados que tienen acceso a información corporativa de alto valor, lo cual permita reprimir la comercialización de información, ya que, puede ser uno de los móviles que facilitan la vulneración de los sistemas que en la mayoría de las ocasiones son susceptibles a los protocolos de defensa con los que cuentan estas empresas, posiblemente porque ya conocen su ingeniería tecnológica.

4.3.4. Nociones Generales sobre Skimming

El skimming es una metodologia de engaño que provoca la sustracción de datos confidenciales de tarjetas de créditos o débitos mediante el uso de dispositivos digitales que se apodan skimmers, que tienen como función principal escanear la información contenida en el chip de la tarjeta. Este tipo de acciones se sufren muchas generalmente en los cajeros automáticos muchas veces por los clientes que por desconocimiento no saben reconocer estos aparatos y por falta de vigilancia y control de las bancas comerciales que deben contar con los medios necesarios para evitar o alertar a los clientes sobre esta práctica en sus cajeros automáticos (Forero & Galeano, 2016). Esta técnica se hace imprevisible una vez la información es clonada en otras tarjetas realizando transacciones significativas que evidencian una lesión enorme en el patrimonio económico de los afectados y por supuesto la relación comercial banca-cliente.

4.4.Marco Jurídico

De acuerdo con las necesidades anteriormente esbozadas, se considera que el fortalecimiento del marco normativo y la implementación de medidas efectivas de seguridad son fundamentales para proteger al sector financiero colombiano y a los ciudadanos, al respecto.

4.4.1. Código Penal (Ley 599 de 2000)

El delito de Transferencia no consentida de activos se encuentra tipificada como delito en el Código Penal Ley 599 de 2000, específicamente en el artículo 269j, en la que se establece las características subjetivas y objetivas que deben tenerse en cuenta para su tipificación, ade-describe la penas y sanciones para los delitos informáticos, que incluye multas y prisión, dependiendo de la gravedad del delito y el daño causado. Busca fomentar la prevención de delitos informáticos y la formación de capacidades de investigación para enfrentar estos delitos.

4.4.2. Ley 1273 de 2009

En línea con lo anterior, se encuentra la Ley 1273 que modificó el Código Penal creando un nuevo bien jurídico "De la protección de la información y los datos". Esta ley establece disposiciones relacionadas con los delitos informáticos en Colombia. A partir de esta ley se aumenta el espectro en los procedimientos de investigación porque cuando se trata de uso de tecnologías de la información y la comunicación, exponencialmente aumentan los riesgos y las formas en que pueden afectarse los bienes jurídicos que se han comentado a lo largo del proceso de investigación. Básicamente pretende restringir los comportamientos que se desarrollan mediante el uso de dispositivos informáticos, realizando claras diferencias para evitar una mala praxis de los operadores judiciales cuando están en la ejecución de sus funciones.

Teniendo en cuenta que la transferencia no consentida de activos se desarrolla mediante el uso de dichos positivos es menester evaluar esta normatividad en razón de la afectación de la confianza hacia los actores más interesados en el sistema financiero en Colombia

4.4.3. Ley 1581 de 2012

La Ley de Protección de Datos Personales en Colombia, protege los derechos de las personas en relación con la recopilación, almacenamiento, uso y manejo de sus datos personales. Esta ley se caracteriza por proteger el derecho a la información, los titulares de los datos personales tienen el derecho a ser informados sobre la existencia de bases de datos que contengan sus datos, así como el propósito del tratamiento de sus datos personales (Ley 1581, 2012).

De igual manera, el proceso de acceso, los individuos tienen el derecho a acceder a sus datos personales que se encuentren en las bases de datos y sistemas de información, permitiéndoles conocer y revisar esta información. Asimismo, los titulares tienen el derecho de solicitar la actualización, rectificación y corrección de sus datos personales cuando estos sean inexactos, incompletos, fraccionados, erróneos o desactualizados (Ley 1581, 2012).

Por otro lado, los individuos pueden solicitar la eliminación de sus datos personales de las bases de datos cuando estos no sean necesarios para los fines para los cuales fueron recopilados, o cuando el titular haya retirado su consentimiento para el tratamiento de sus datos (Ley 1581, 2012).

Otro derecho que se relaciona en esta ley es la oposición, los titulares tienen el derecho a oponerse al tratamiento de sus datos personales en ciertos casos, como cuando el tratamiento se realice sin su consentimiento o cuando se utilicen sus datos para fines diferentes a los autorizados (Ley 1581, 2012).

Finalmente, la ley establece que los responsables y encargados del tratamiento de los datos personales deben garantizar la confidencialidad, seguridad e integridad de los datos, implementando medidas técnicas, humanas y administrativas necesarias para evitar su adulteración, pérdida, consulta, uso o acceso no autorizado (Ley 1581, 2012).

4.4.4. Ley 1298 de 2010 (Ley de Delitos Informáticos)

El marco normativo vigente en Colombia para la TNA se considera como suficiente en términos de tipificación del delito y establecimiento de sanciones. Sin embargo, existen algunos desafíos para su aplicación efectiva, como:

- Falta de especialización en la investigación y persecución de delitos informáticos: Las autoridades judiciales y policiales no cuentan con la capacitación y los recursos necesarios para investigar y perseguir de manera eficiente los delitos de TNA.

- Dificultades en la recolección de pruebas: La naturaleza digital de los delitos de TNA dificulta la recolección de pruebas suficientes para identificar y condenar a los sujetos activos del delito.

- Falta de coordinación entre las diferentes entidades involucradas: No existe una adecuada coordinación entre las entidades gubernamentales, las instituciones financieras y el sector privado para prevenir y combatir la TNA.

4.4.5. El Convenio de Budapest

De igual manera, en el marco internacional se encuentra el Convenio de Budapest (2001) Ciberdelincuencia. Serie de Tratados Europeos es un tratado internacional que tiene como objetivo combatir el cibercrimen mediante la armonización de leyes nacionales, la mejora de la cooperación internacional y la implementación de medidas de seguridad cibernética. Fue adoptado en Budapest, Hungría, en 2001, y es el primer tratado internacional que aborda específicamente los delitos informáticos y la ciberdelincuencia. Además, el convenio se basa en la cooperación y el intercambio de información entre los países miembros, lo que puede ser fundamental para abordar los desafíos globales de la ciberdelincuencia.

Es alentador que Colombia haya ratificado este convenio, ya que, demuestra el compromiso del país en enfrentar los desafíos de la ciberdelincuencia a nivel internacional y mejorar su capacidad para prevenir y perseguir delitos informáticos.

4.5. Marco Ético

Se establece que la presente investigación tendrá en cuenta la aplicación de la Ley 1581 de 2012, al momento de aplicar los instrumentos de recolección de información, aplicando los protocolos de ética, siempre respetando las diferencias y evitando la vulneración de derechos tendientes a la discriminación por temas de raza, condición económica o género. Cada uno de los instrumentos estarán acompañados de consentimiento informado y con el uso de un lenguaje respetuoso.

Se solicitará autorización a cada uno de los participantes para la publicación de los resultados de la investigación y el uso de sus nombres como participantes en el proceso de consolidación de la investigación.

Finalmente, en relación a la construcción del documento se respetará los derechos de autor, lo que implica que toda información secundaria será aplicada basado en la guía de normas APA séptima edición como lo exige la biblioteca de la Universidad Autónoma Latinoamericana de la ciudad de Medellín.

5. Diseño Metodológico

5.1.Tipo de investigación

El tipo de estudio propuesto es cualitativo teniendo en cuenta que se realizará una descripción dogmática del delito de transferencia no consentida de activos que evidencie las complejidades de configuración típica por la ausencia de normas que faciliten su control social, del mismo modo se estimará las afectaciones que se producen al sector financiero quienes oficiosamente asumen la carga económica por la comisión de estos hechos punibles.

5.2. Enfoque

El enfoque de investigación de acuerdo a la naturaleza es normativo, ya que, a partir de las dificultades de configuración típica y con el surgimiento de las nuevas modalidades que implica el uso de dispositivos digitales por hackers que son imposibles controlar por la falta de ingeniería tecnológica y que sean aplicables a los mecanismos probatorios actuales que permite el proceso penal acusatorio en Colombia.

5.3. Método

Por otro lado, el método que se pretende utilizar es hermenéutico, pues la interpretación normativa no solo del derecho en Colombia sino del derecho internacional frente a los esfuerzos para la aplicación integral de este delito en procesos penales que puedan probarse en el juicio oral posterior a la valoración probatoria y a su vez, como estas limitaciones normativas afectan sectores importantes en Colombia como el financiero.

En síntesis, el método de la presente investigación se cimentará desde la hermenéutica de Hans-Georg Gadamer, donde Gama (2021) plantea que el ser humano como individuo dotado de sentidos, comprende el mundo y su dinamismo a través de forma de percibir las sensibilidades de los fenómenos y la significación del lenguaje, atendiendo a los principios de determinación, corrección y sensibilidad que encauzan el ejercicio del pensar hermenéutico.

5.4. Paradigma de Investigación

Para este estudio el paradigma de investigación seleccionado fue el hermenéutico que facilita la interpretación de normas jurídicas para generar una explicación sobre el fenómeno que afecta el sistema financiero en Colombia a partir de las normas que regulan dicho comportamiento. Se puede aplicar al análisis de la TNA identificando patrones y tendencias en su aparición, entendiendo las causas subyacentes y desarrollando estrategias de prevención (Martínez, 2013).

Por otro lado, este paradigma se enfoca en la interpretación normativa, reconociendo la objetividad de regular los comportamientos sociales. Este enfoque permite comprender las experiencias de las víctimas, analizar la cultura organizacional de las instituciones financieras e interpretar discursos y narrativas sobre la TNA como se puede evidenciar en el estado el Arte (Quecedo, & Castaño, 2002).

5.5. Técnicas e Instrumentos de recolección de Datos

Como instrumentos de recolección de información se emplearán como primera instancia el análisis documental como normas jurídicas, jurisprudencia y la doctrina especializada, de igual manera se realizarán entrevistas dirigidas a jueces penales, investigadores judiciales, fiscales

para que den cuenta sobre las complejidades de tipificación del delito de transferencia no consentida de activos y se realizaran encuestas a diversas empresas del sector financiero sobre las afectaciones que ha causado este delito al patrimonio económico de los propietarios.

5.5.1. Fuentes de Datos

Las fuentes de datos para este estudio serán primarias y secundarias por medio de la revisión documental y entrevistas con expertos en ciberseguridad, profesionales del sector financiero y víctimas de delitos cibernéticos. Además, se considerarán datos provenientes de documentos oficiales, informes financieros y análisis de casos judiciales relacionados con la TNA.

5.5.1.1. Rastreo Bibliográfico

El rastreo bibliográfico permitió encontrar un número significativo de material investigativo compuesto por artículos, trabajos de grado y libros. Estos resaltaron temáticas tales como: (i) alcance dogmático del delito de transferencia no consentida de activos en Colombia; (ii) el impacto en la confianza de los usuarios a nivel económico y social respecto de la comisión del delito de transferencia no consentida de activos en el sector financiero en Colombia y (iii) Estructura de la integridad del sistema financiero en Colombia para la generación de respuesta a la comisión de delito de transferencia no consentida de activos. Los autores implementaron diferentes metodologías y variables temáticas en relación a la necesidad de reformar formal y sustancialmente, la forma de investigar y tipificar delitos trasnacionales que superan las barreras jurisdiccionales en Colombia e impide la efectiva respuesta institucional.

En el ejercicio de recolección de información pertinente para el proyecto tesis para optar al título de abogados, se establecieron tres ecuaciones de búsqueda que permiten identificar las categorías que se pretenden abordar en el desarrollo investigativo, las cuales son: (“Transferencia no consentida de activos OR “non-consensual transfer of assets”) AND (“Percepción de clientes victimas por Transferencia no consentida de activos OR “Perception of victim clients due to non-consensual transfer of assets”) AND (“Sistema financiero frente a delitos OR Financial system against crimes”).

El material fue seleccionado con criterios de pertinencia y veracidad, se utilizaron herramientas tanto de acceso abierto como por suscripción, para un total de (5) herramientas de búsqueda y se hallaron (4284) resultados de la siguiente manera: Scopus (90); Web of science (110); ScienceDirect (44); Redalyc (1990) y Google Scholar (2050), entre los años 2020 a 2024.

El autor más representativo fue Macias – Lara (2022) con 91 apariciones y Rodríguez – Vizuete con (79) apariciones. En suma, en cuanto a las publicaciones con más apariciones se encuentra el repositorio de la Universidad Libre de Colombia con (19) investigaciones y repositorio de la Universidad Santo Tomas con (11) investigaciones. La universidad que marco pauta fue la Universidad Libre de Colombia con (5) apariciones en el año 2024 y seguidas por las universidades Santo Tomas de Bogotá con (2) y Eafit con (1).

Finalmente, en cuanto a las palabras claves, luego de la revisión en una herramienta de nube de palabras llamada VOSviewer se identificaron las siguientes variables: la palabra crimen español e inglés suman (55) coincidencias, seguida de la palabra Gobernabilidad con (41) y las palabras que marcaron tendencia por si solas fueron valor original y blanqueo de dinero ambas con (31) apariciones.

Respecto de los resúmenes extraídos de los (48) resultados hallados a través de la herramienta generadora de nube de palabras VOSviewer se obtuvo la siguiente lectura: la palabra más recurrente fue crimen con (147) apariciones, seguida de consentimiento con (96).

5.5.1.2. Encuesta a Usuarios con productos financieros

De la misma manera, para determinar la percepción de usuarios victimas por delitos informáticos, especialmente por el de transferencia no consentida de activos fue necesario mediante la herramienta de formularios de Google, diseñar una encuesta que constó de (6) preguntas, dirigidas a (50) personas que participaron activamente en la diligencia, esta aplicación se llevó a cabo, teniendo en cuenta los protocolos de habeas data para el manejo de información personal, quienes decidieron aceptar el consentimiento informado antes de aplicar la encuesta, en donde se indicó que los resultados tenían una finalidad académica.

5.5.1.3. Entrevista a Entidades Nacionales

Con la finalidad de tener un sustento sobre la experiencia que han tenido los operadores judiciales como los fiscales y jueces y por supuesto la Superintendencia Financiera de Colombia frente al delito de transferencia no consentida de activos mediante derecho de petición se solicitó a las mismas un espacio a los correos documentalpqrs@fiscalia.gov.co; info@cendoj.ramajudicial.gov.co; super@superfinanciera@.gov.co, para lo cual no se obtuvo respuesta dentro de los términos legales (ver anexos).

Sin embargo, se enviaron a diferentes entidades bancarias comerciales de la ciudad de Medellín un cuestionario que constaba de (6) preguntas abiertas sobre la estructura de seguridad con la que contaban estas entidades para evitar y/o proteger los activos de los clientes y a su vez evidenciar como es la relación de confianza entre el usuario y su entidad financiera a pesar de las dificultades que produce el delito de transferencia no consentida de activos.

6. Resultados

6.1.Alcance dogmático del delito de transferencia no consentida de activos en Colombia

La génesis del delito de transferencia no consentida de activos obedece al desarrollo acelerado de la tecnología que a través de los procesos de globalización ha logrado derribar no solo los obstáculos físicos de la comunicación, sino que han permitido crear mecanismos suficientemente sofisticados que pueden afectar derechos fundamentales de personas, grupos y hasta conglomerados económicos que en un país como Colombia son quienes impulsan y sostienen la economía debido a la estabilidad laboral que ello supone en el sistema financiero (Astaiza & Cuellar, 2023).

Este auge ocurre a partir de la década de 1990, cuando se liberan las barreras comerciales existentes entre Colombia y Estados Unidos y por supuesto Europa, ocasionando una transferencia de información mediante las tecnologías de escala con la finalidad de acelerar procesos industriales. Una de las situaciones que afectaron este ingreso y actualización tecnológica fue que la formación académica fue tardía, lo que implicó una desventaja frente a otros países y hoy en día la infraestructura tecnológica es una copia de sistemas de información obsoletos en otros países.

Desde esta perspectiva se entiende porque Colombia es uno de los países más vulnerables en sistemas tecnológicos, pues su falta de capacidad instalada de tecnología de última generación impide anteponerse a los riesgos que implica este tipo de delitos que hasta la fecha envía un mensaje de impunidad e inseguridad jurídica. Si bien es cierto que desde punto de vista de la tipificación y la sanción la transferencia no consentida de activos evidencia penas que pueden llegar hasta 120 meses de prisión y una multa equivalente a 1500 salarios mínimos legales mensuales vigentes, el enfoque para mitigar el fenómeno no debe ser punitivo sino preventivo para no afectar la relación y la confianza entre los agentes que conforman el sistema financiero en el país.

El surgimiento de este delito está vinculado al aumento de las transacciones electrónicas y la digitalización de los servicios financieros, lo que ha proporcionado a los delincuentes nuevas oportunidades para cometer fraudes a gran escala. La legislación busca proteger tanto la seguridad de los sistemas informáticos como el patrimonio económico de los ciudadanos, adaptándose a las nuevas formas de criminalidad que emergen con el avance tecnológico.

Para realizar una comprensión dogmática de este delito y establecer las acciones que deben adoptar los operadores judiciales en su saber-hacer a continuación basado en la explicación esquemática del doctrinante Pabón Parra (2017) quien en su libro describe este tipo penal de la siguiente manera:

6.1.1. Clasificación del Delito de Transferencia no Consentida de Activos

De acuerdo con las conductas descritas en el tipo penal, se establece que a priori la transferencia no consentida de activos es un ***delito de resultado***. De acuerdo con Bernate (2006), los delitos de resultados "*Son aquellos que necesitan, para que se configuren, un efecto de vulneración material del bien jurídico ya sea su destrucción o su detrimento*" (pág. 48). Básicamente este tipo de delitos implica que el titular del derecho que se protege haya sido totalmente quebrantado en este sentido, teniendo en cuenta que existen fines de lucro, la afectación recae directamente sobre el patrimonio económico del usuario que fue transgredido a

su producto financiero con manipulación informática o por la creación o fabricación de un programa que produzca el perjuicio a un tercero.

De igual manera, este injusto también se clasifica como un ***delito de lesión***, teniendo en cuenta que la afectación o vulneración del patrimonio económico puede afectar un cuota parte del derecho y no la consumación total de este y básicamente este tipo de características son las que permiten aclarar los móviles en el proceso de investigación, ya que, muchos clientes y/o usuarios no denuncian porque la transferencia no consentida de activos porque en algunos casos la pérdida económica es irrisoria y normalizan esta conducta. De acuerdo con Perlaza & Rivera (2024), la transferencia no consentida de activos es un delito de lesión porque vulnera, transgrede o pone el peligro la estructura informática que diseñan las empresas financieras para almacenar las transacciones de los clientes y por supuesto proteger sus activos, en este entendido cuando el sujeto activo del delito a partir de sus habilidades manipula la información existente en dichos sistemas para su lucro y afectación del sujeto pasivo se produce lesiones no solo a información confidencial sino al patrimonio económico (Perlaza & Rivera, 2024).

Otro aspecto importante de este delito es que demanda una ***conducta instantánea***, es decir, La conducta instantánea se refiere a un tipo de delito cuya consumación ocurre en un solo acto o momento, sin extenderse en el tiempo. Este tipo de infracción se caracteriza por su ejecución inmediata, donde el acto delictivo se completa en el instante en que se realiza, sin necesidad de acciones continuas o repetidas. Aunque sus efectos pueden perdurar, la acción en sí misma no se prolonga (Salas, 2024). En este sentido, esta conducta puede tener efectos parciales si se logra recuperar el activo o parte de este o permanentes si efectivamente el dinero no se puede recuperar por su dificultad de rastrearlo y la incapacidad legislativa de acceder a otros sistemas, se debe recordar que este es un delito que se caracteriza por su transnacionalidad.

Asimismo, se establece que este delito se clasifica como ***Pluriofensivo***, sus efectos no solo vulneran un derecho especifico, sino varios para el caso en concreto la transgresión recae sobre el patrimonio económico y la seguridad informática. Un delito pluriofensivo es aquel que afecta simultáneamente a múltiples bienes jurídicos protegidos por la ley, ya que, involucra la violación de varios intereses legales, como el patrimonio, la integridad de los sistemas informáticos, y la seguridad de los datos. Este tipo de delito reconoce la complejidad de las acciones delictivas modernas, especialmente en el ámbito digital, donde una sola acción puede tener repercusiones en diversas áreas protegidas por el ordenamiento jurídico (Ávila, 2023).

Por último, esta conducta punible encaja en la clasificación de delitos de ***Tipo subsidiario alternativo***, lo anterior significa que solo es aplicable si esta no se adhiere a un delito de mayor sanción la transgresión del bien jurídico tutelado. El delito subsidiario o alternativo se refiere a la aplicación del derecho penal como último recurso, en consonancia con el principio de mínima intervención penal. Este enfoque prioriza la resolución de conflictos mediante métodos no penales, como la conciliación, antes de recurrir a sanciones penales y se aplica cuando el daño no es grave y el bien jurídico afectado no es de alta relevancia social (Guizado & Silva, 2024). Este principio busca evitar el uso excesivo del sistema penal, reservándolo para conductas que realmente amenazan la convivencia social, permitiendo así una justicia más eficiente y menos invasiva.

Indudablemente el delito de transferencia no consentida de activos tipificado en el artículo 269j de la Ley 599 de 2000 o código penal desde su clasificación exige una clasificación particular para hacerse valer por parte del fiscal como investigador en la audiencia de imputación

de cargos y en el juicio oral, pues el juez en su sana crítica y de manera objetiva evaluará cada uno de los elementos objetivos que acrediten la configuración o no de este hecho punible.

6.1.2. Elementos Normativos de Tipo Objetivo

En el sistema penal acusatorio en Colombia, los elementos normativos de tipo objetivo persiguen circunstancias meramente reguladas por el ordenamiento jurídico y que no implica una posición interna de las partes, sino de todo aquello que se pueda probar dentro del proceso. En este orden de ideas este acápite realiza una descripción del sujeto activo y pasivo en el delito, de la conducta, del objeto jurídico y material, su finalidad, el concurso con otros delitos y la admisión de tentativa y coparticipación.

La descripción típica de la conducta en comento establece como sujeto activo a cualquier persona en específico con el pronombre y conecto "***El que***", esto es, que el delito de transferencia no consentida de activos puede ser realizado por alguien indeterminado (Hombre, Mujer, profesional, no profesional, nacional, extranjero). El tipo penal indeterminado se refiere a un sujeto activo que no está claramente especificado dentro de la estructura gramatical del tipo penal, en otras palabras, es aquel sujeto que realiza la conducta descrita en el tipo penal, pero que no está definido de manera explícita en el texto legal (Vega, 2016).

Este concepto se utiliza para describir situaciones en las que la ley no identifica de manera precisa quién puede ser el autor del delito, permitiendo así que cualquier persona que realice la conducta prohibida pueda ser considerada como sujeto activo del delito. Esto es relevante en el análisis del tipo penal porque afecta la interpretación y aplicación de la norma penal, asegurando que no se limite la responsabilidad penal a un grupo específico de personas, sino que se extienda a cualquier individuo que incurra en la conducta tipificada (Vega, 2016).

Desde esta perspectiva se considera que una de las dificultades que recae sobre los investigadores judiciales como lo es la fiscalía en el sistema penal acusatorio en Colombia, indudablemente es la indeterminación del sujeto activo, ya que, a priori, por la naturaleza del delito se considera que corresponde a una persona con habilidades en sistemas, con experiencia en el mercado bursátil, experto en ciberseguridad y con un gran sistema de equipos sofisticados que le permitan vulnerar los sistemas informáticos de empresas financieras, sin embargo, la recomendación es ampliar el espectro, lo que implica mayor información de análisis.

Por otro lado, para referirse al sujeto pasivo, es de anotar que hasta aquí se ha mencionado que el delito de transferencia no consentida de activos es pluriofensiva, pues sus efectos afectan diversos bienes jurídicos tutelados, como el sistema informático en contra de la empresa que es la garante de asegurar los activos de sus clientes como el patrimonio económico, que en este caso afecta a ambos de manera proporcional, a los clientes por los activos contenidos en los diferentes productos financieros y el la empresa financiera por su desvalor comercial y corporativo como consecuencia de dicha vulneración.

En este sentido, los desafíos que enfrentan los operadores judiciales, especialmente los investigadores son los intereses de conflictos con las empresas financieras que comercialmente son herméticos con la información debido a los secretos corporativos y los protocolos y políticas de seguridad que impiden tener un acceso inmediato a los sistemas que permita definir la causalidad del injusto.

Asimismo, el tipo penal en su estructura gramatical especifica (2) conductas que se describen como "***Con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante***" y "***Quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito anterior***", bajo este entendido se esgrime que las conductas son complementarios, pues el diseñar un sistema o software tendiente a la vulneración de sistemas financieros para obtener provecho económico y manipular este para el mismo fin, desde todos los escenarios implica la necesidad de contar con el sistema informático sofisticado y adecuado y el recurso humano especializado en este tipo de análisis de información, ya que, esta conducta se ejecuta de manera intangible, es decir, no puede percibirse mediante los sentidos la transferencia no consentida de activos, sino que toca descifrarlo mediante algoritmos.

En este sentido, una de las situaciones más complejas que ocasiona dificultad para la imputación de este delito es su característica trasnacional, pues muchas veces quienes realizan dichos ataques al sistema o crean dichos programas no se asientan en el país, siendo complejo realizar el rastreo de información, desde aquí, se hace necesario fortalecer la cooperación internacional y trabajar mancomunadamente en aras que dichos rastreos se realicen en tiempo real entre los países que se vean afectados por dichas conductas.

Dentro del mismo escenario, como ya se ha evidenciado durante todo este capítulo, el objetivo jurídico del sujeto activo no es otro que la seguridad informática y el patrimonio económico y el objetivo material es el activo perteneciente al sujeto pasivo (particular o empresa). En este sentido, cuando en una conducta se presenten estas circunstancias de vulneración informática, económica y que implica un perjuicio a un tercero y existe la posibilidad de probarse, este tipo penal podría imputarse.

Por su naturaleza de ejecución este tipo penal tiende a tipificarse de manera independiente, en este sentido se excluyen las hipótesis sucesivas y simultaneas, es decir, no aplica el concurso con otros delitos, pero si la cláusula de subsidiariedad alternativa, es decir, aplicar mecanismos alternativos de resolución de conflictos para reversar los efectos que ocasionaron el injusto.

En cuanto a la admisión de tentativa, este delito de acuerdo con los actos ejecutorios para la configuración se asume dogmáticamente que, si es posible, pero desde dos ópticas independientes, la primera desde la creación del programa o sistema con la intención de realizar transferencias no consentidas, es decir, en este sentido el sujeto activo cuenta con los diseños, prototipos, infraestructura y la planeación para la creación del mismo. En la otra vertiente el sujeto activo manipula el sistema del cliente o empresa financiera pero no logra transferir activos por ausencia de estos en dicho momento, en este sentido aplicaría la tentativa.

Por último, en relación a la coparticipación, el delito por su estructura gramatical evidencia que facultativamente se admite la coautoría, la determinación y complicidad. Para el caso en concreto la coautoría implica la división de tareas para configurar el ilícito la persona que financia los equipos para la creación del software o en su efecto quien crea cuentas a nombre de terceros para evitar que se rastree el activo transferido. La determinación en el derecho penal implica aquel que incide o motiva por cualquier medio a otra persona para cometer hechos punibles, en este caso a crear programas y/o utilizarlos para tener provecho económico de activos de terceros. Entre tanto la complicidad demanda una ayuda simultanea de la conducta o posterior para bloquear la investigación judicial, esto es, el colaborador en la creación del programa, en la vulneración del sistema y en la recepción del activo transferido sin consentimiento del titular.

6.1.3. Elementos Normativos de Tipo Subjetivo

Los elementos subjetivos del delito son componentes internos que reflejan la intención o motivación del autor al cometer un acto ilícito, que incluyen el dolo, que implica conocimiento y voluntad de realizar la conducta delictiva, y otros elementos como la culpa y los ánimos especiales. Estos elementos son cruciales para determinar la responsabilidad penal, ya que configuran la tipicidad subjetiva y la antijuridicidad del comportamiento (Narvaéz, 2022).

Dogmáticamente la transferencia no consentida de activos corresponde indudablemente a una conducta meramente dolosa, ya que, se evidencia voluntad y conocimiento, pues crear un programa para manipular un sistema informático con la capacidad de transferir activos sin consentimiento es una evidencia de arbitrariedad, capacidad técnica y deseo de comportarse contrario a la normatividad.

En cuanto al complemento subjetivo, vale decir, que, sin duda alguna, a diferencia de los otros delitos informáticos al que se refiere la ley 1273 de 2009, este encausa su esencia en el lucro o beneficio económico, el uso de la informática es solo el medio necesario para facilitar el ilícito, pero la intención principal es generar un provecho económico mediante la defraudación de activos de terceros.

En definitiva, este delito no admite que se alegue atipicidad subjetiva por error de tipo debido a la ausencia de sujeto pasivo y objeto material, pues ya se mencionó que dentro de sus características el delito puede provocar afectaciones comerciales a las empresas, al no inscribir más cuentas o productos financieros, debido a la inseguridad o vulnerabilidad del sistema donde se aloja dichos activos, en este sentido, aunque no hayan activos en las cuentas vulneradas se produce afectaciones accesorias constitutivas de sanción.

6.2. El impacto en la confianza de los usuarios a nivel económico y social respecto de la comisión del delito de transferencia no consentida de activos en el sector financiero en Colombia

De acuerdo con Lozano (2017), la confianza desde el sistema financiero en Colombia puede entenderse como el atributo vertebral que coloca en funcionamiento la operacionalización del sistema financiero mediante la relación de demanda y oferta que se refleja entre los clientes y las organizaciones autorizadas para comercializar sus productos financieros a nivel nacional. En otras palabras, esta confianza es un elemento intangible pero vital, pues desde el enfoque de la banca implica la capacidad que tienen los clientes para asumir las obligaciones financieras y desde la postura del cliente la capacidad de responder a las necesidades de recaudación, inversión y crédito que tengan estas organizaciones para el soporte de proyectos de vida a corto, mediano y largo plazo.

Jurisprudencialmente la Corte Suprema de Justicia en sala de casación penal en Sentencia No. 15595 de 2003, en cabeza del Magistrado Ponente Dr. Yesid Ramírez Bastidas, indica que:

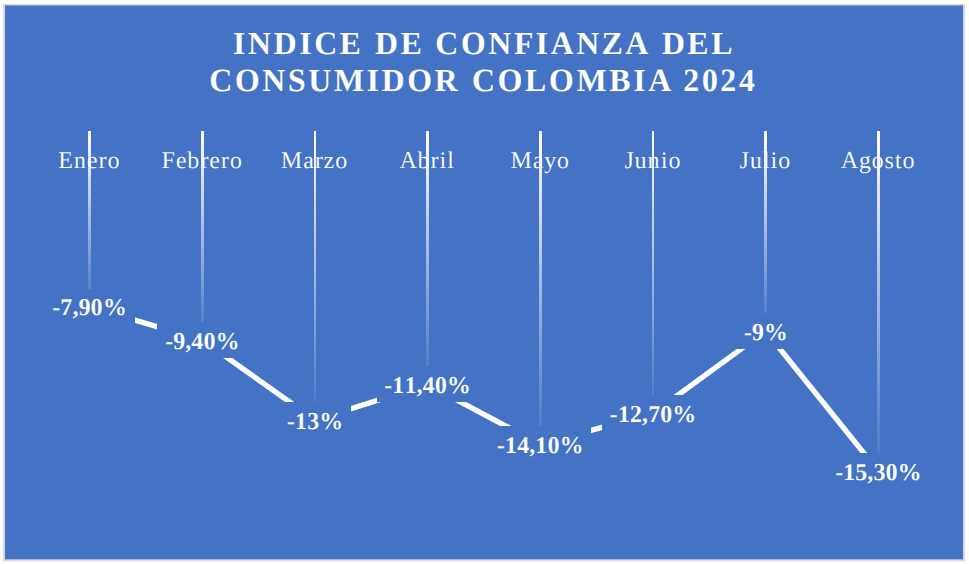
> La confianza es el principal activo no sólo de cualquier entidad que se dedique al negocio financiero, sino del sistema en general, pues únicamente sobre ese intangible es que se obtiene la circulación del dinero a través del sistema financiero, en desarrollo de las actividades de captación y colocación que en general caracterizan esa actividad (Sentencia No.15595, 2003).

En este sentido, la protección al consumidor financiero es crucial para fortalecer la confianza en el sistema financiero, pues, al garantizar acceso a información clara y precisa, se empodera a los usuarios para tomar decisiones informadas. Esto no solo protege sus intereses, sino que también fomenta un entorno estable y propicio para el crecimiento económico sostenible.

Vale decir, que la confianza en la economía se puede medir a través de varios indicadores económicos y financieros que reflejan la percepción de estabilidad y seguridad por parte de los consumidores e inversionistas. Algunos de estos indicadores incluyen la tasa de inflación, el crecimiento del Producto Interno Bruto (PIB), las tasas de interés, el índice de confianza del consumidor y el índice de confianza empresarial. Estos indicadores proporcionan una visión general de la salud económica de un país y la confianza que los agentes económicos tienen en su futuro.

De acuerdo con los reportes mensuales realizado por la Fundación para la Educación Superior y el Desarrollo, en adelante Fedesarrollo, que realizo encuestas durante los meses de enero hasta agosto de 2024, sobre el índice de confianza del consumidor, arrojando los siguientes resultados para Colombia:

Figura 1 - Índice de Confianza del Consumidor en Colombia para el Periodo 2024



Fuente: Fedesarrollo, 2024

En la actualidad, Colombia atraviesa por una dinámica de desconfianza financiera, pues su confianza en el consumo de productos financieros ha aumentado considerablemente de enero hasta el mes de agosto, es decir, se ha aumentado en un (-7,4%), lo que implica frente a los conceptos anteriormente señalados sobre confianza financiera, implica que el acceso a la información entre las empresas financieras y el usuario no es transparente, existe un aumento significativo en las tasas de interés o el decrecimiento del producto interno bruto, son escenarios que rompen esa estructura en el sector financiero.

Este fenómeno sobre desconfianza financiera, lo explica muy bien Palacios (2016), en su estudio, indico que, a mayor desconfianza hacia el sistema financiero, menor es la probabilidad de que las personas accedan a productos básicos ofrecidos por las entidades financieras, como cuentas de ahorro. Este efecto es tan relevante que, incluso cuando se controlan otros factores socioeconómicos como la edad, el nivel de educación, los ingresos y el género, la confianza sigue siendo un determinante clave.

El estudio utilizó un modelo econométrico, específicamente un modelo Logit binomial, para analizar esta relación y encuentra que la desconfianza reduce la probabilidad de acceder a servicios financieros en un (29%) aproximadamente. Además, se destaca que la confianza puede ser igual o más determinante que los costos y otras restricciones de acceso impuestas por la oferta de servicios financieros (Palacios, 2016).

En tal sentido, la desconfianza financiera se produce por una combinación de factores históricos, económicos y sociales. En el contexto de Colombia, varios elementos contribuyen a esta desconfianza:

- **Educación Financiera Insuficiente:** La falta de educación financiera adecuada limita la comprensión de los productos financieros y sus beneficios, lo que puede aumentar la

desconfianza. Las personas con menores niveles de educación tienden a desconfiar más del sistema financiero.

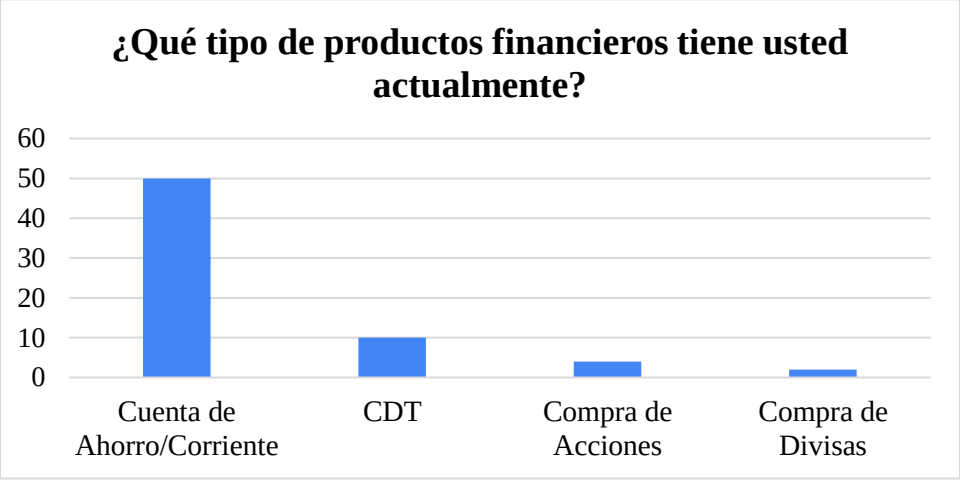
- **Desigualdad de Acceso:** La brecha en el acceso a servicios financieros entre diferentes grupos de ingresos también alimenta la desconfianza. Los sectores de menores ingresos, que a menudo tienen menos acceso a servicios financieros formales, pueden recurrir a alternativas informales, lo que refuerza su desconfianza hacia las instituciones formales.

- **Falta de Protección al Consumidor:** Debilidades en los mecanismos de protección al consumidor y poca flexibilidad en el marco legal para estimular la innovación en servicios financieros también contribuyen a la desconfianza.

En definitiva, la desconfianza financiera es un fenómeno complejo influenciado por experiencias pasadas, percepciones de riesgo, barreras económicas y falta de educación financiera. Para mejorar la confianza, es crucial abordar estos factores mediante políticas inclusivas, educación financiera y productos adaptados a las necesidades de todos los segmentos de la población.

Para conocer un panorama sobre la confianza existente sobre las entidades bancarias y los usuarios en la ciudad de Medellín, a continuación, se presentarán los resultados de la encuesta realizada a clientes con productos financieros que han padecido del delito de transferencia no consentida de activos.

Figura 2 - Pregunta 1 de encuesta dirigida a Clientes con Productos Financieros



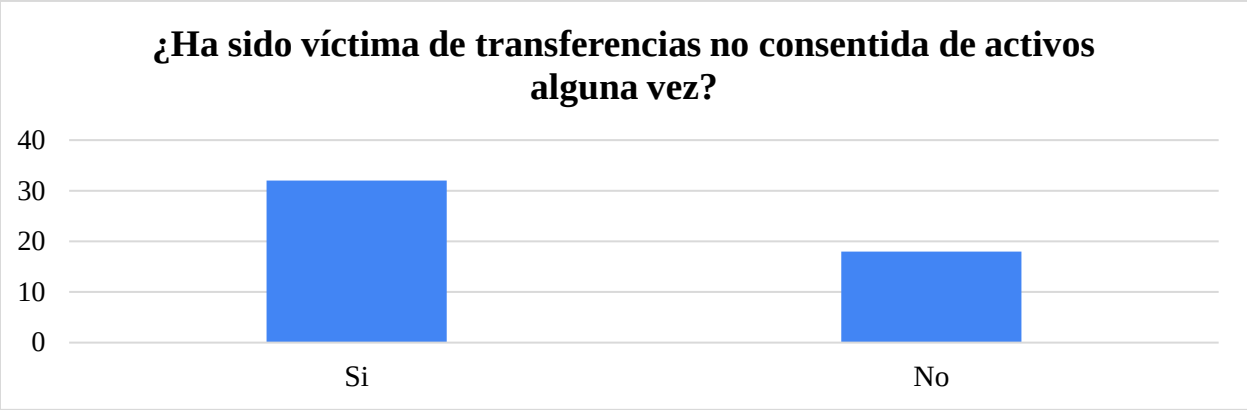
Fuente: Elaboración Propia

Se evidencia que la figura 2, que el (100%) de los encuestados cuenta con productos financieros donde se administran activos o que son sujetos de transferencias no consentidas de activos. De igual manera, el (100%) cuenta con cuenta de ahorros y/o corriente por temas de nómina o para recibir honorario, como inversión cuentan con CDTs, que, dentro del porcentaje anterior, está representado en un (20%), mientras que los productos de compra de acciones y divisas registran participaciones del (4%) y (2%), respectivamente.

Este panorama no es ajeno a la desconfianza que se vive actualmente en el país, ya que, solo el (26%) de los encuestados cuentan con productos financieros de inversión, considerando

que actualmente el sistema financiero no brinda garantías suficientes para realizar inversiones de suma media o grandes sumas, por temor a que sean permeadas por hackers.

Figura 3 - Pregunta 2 de la Encuesta Dirigida a Clientes con Productos Financieros



Fuente: Elaboración Propia

La Figura 3, evidencia que en efecto, al menos el (64%) de los encuestados ha sido víctima del delito de transferencia no consentida de activos, lo cual supone una gran susceptibilidad al menos en los productos de cuenta de ahorro/corriente que son los más comunes por su obligatoriedad para recibir pagos, ya sea, de un trabajo formal o no; y a su vez los que mayores riesgos supone como consecuencia de la desinformación o falta de formación de sus titulares, toda vez, que como lo indicaba Palacios (2016) a menor nivel de educación, mayor riesgo de vulneración de seguridad, debido a que no son capaces de diferenciar correos o mensaje de textos fraudulentos que se caracterizan por solicitar las credenciales de acceso a las cuenta como el usuario o cedula y la clave de la banca móvil o cajero, permitiendo la manipulación de activos y por supuesto la afectación a terceros.

Para efectos de la presente investigación se tomará como información de base a los encuestados que fueron víctimas del delito de transferencia no consentida de activos para comprender el respaldo del sistema financiero en Colombia.

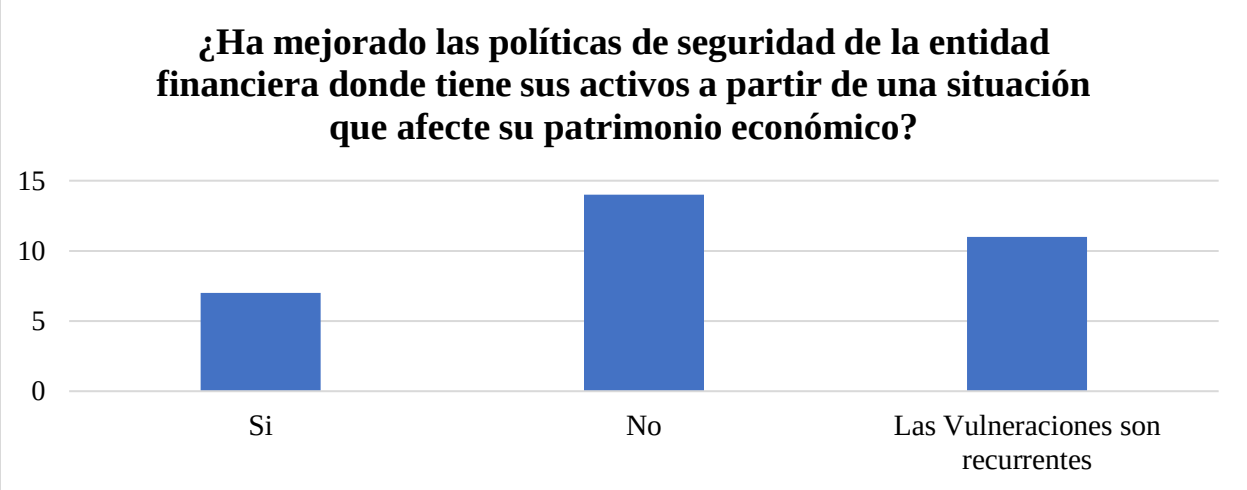
Figura 4 - Pregunta 3 de encuesta Dirigida a clientes con productos financieros

Fuente: Elaboración Propia

La figura 4, evidencia que en efecto la confianza del cliente se encuentra basada en su experiencia, en este sentido, el reintegro del dinero, donde el (94%) de los encuestados tuvieron esa resolución por parte de la entidad financiera, permite el fortalecimiento de ese activo intrínseco que es la confianza por la transparencia en que han actuado las mismas, quienes entienden los riesgos a los que se exponen los sistemas y establecen este tipo de medidas para salvaguardar las experiencias positivas y por supuesto la fidelidad del consumidor.

Indudablemente este tipo de proteccionismo frente a los clientes implica sacrificar un margen de la rentabilidad de estas entidades financieras que no es poco, para mantener latente la fidelidad del usuario que confía en las políticas comerciales de la empresa, sin embargo, en sentido estricto el funcionamiento de una estructura financiera demanda a todas luces acciones preventivas que ayude a disminuir la comisión del delito de transferencia no consentida de activos.

Figura 5 - Pregunta 4 de encuesta Dirigida a Clientes con productos financieros

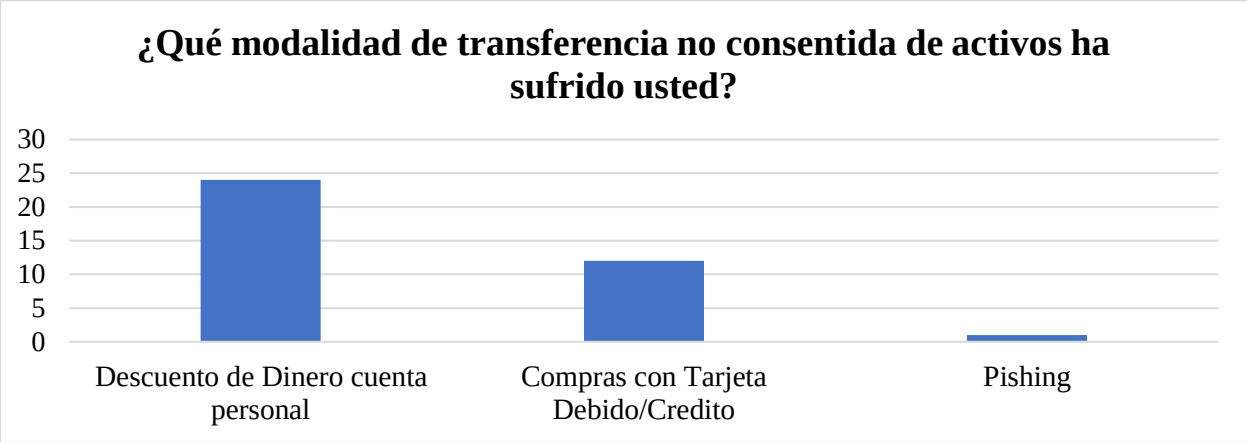


Fuente: Elaboración Propia

Los resultados de la figura 5, evidencian entonces que las políticas de seguridad en las entidades financieras siguen siendo vulnerables sobre los activos de los clientes, ya que, el (78,2%), de los encuestados consideran que no hay mejoría y que a su vez los casos de transferencias no consentida de activos son recurrentes, es decir, que no se hizo una reflexión sobre las lesiones aprendidas.

Lo que se presume es que, las entidades financieras comerciales y los entes de control del sistema financiero en Colombia, deberán interpretar de manera exhaustiva las formas como se dan estos ataques, indagando desde el desempeño del recurso humano de estas empresas, como la metodología que utilizan para acceder a las bases de datos y por supuesto, determinar el tipo de tecnología utilizada para generar dichas transferencias sin consentimiento y no menos importante verificar si los clientes cuentan con la información necesaria para prevenirlos de no brindar información confidencial en sitios web o mediante correos electrónicos, ya que, la clave y el usuario es de uso exclusivo del cliente.

Figura 6-Pregunta 5 de encuesta Dirigida a Clientes con productos financieros

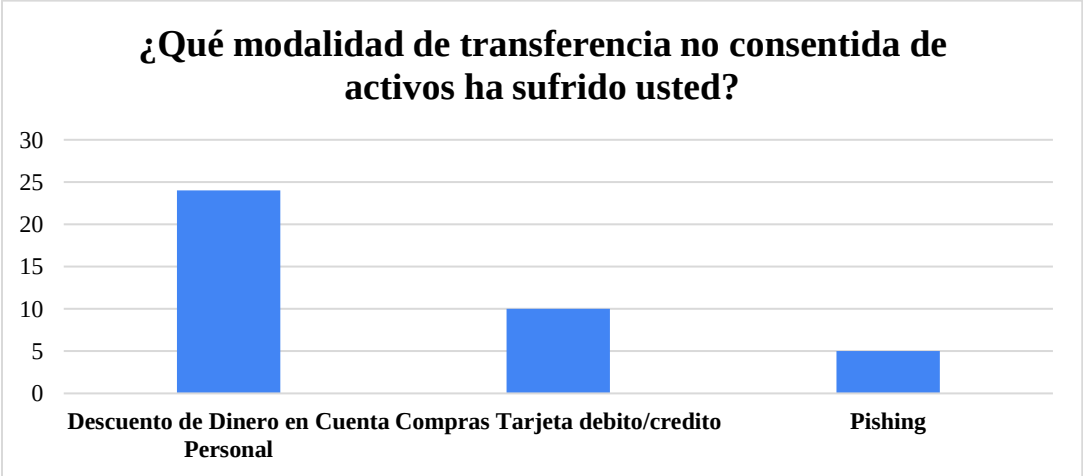


Fuente: Elaboración Propia

La figura 6, evidencia como consecuencia de lo anterior que su nivel de desconfianza actualmente es del (77%), es decir, que la regresión en la que se encuentra Colombia en el índice de confianza del consumidor no es alejada, pues si bien es cierto que siempre y cuando se demuestre que dichas vulneraciones a los sistemas y provoquen defraudación de los productos financieros de los clientes por falta de seguridad de la entidad, serán imputables a estos y asumen el deber de responder por dichos recursos, también es cierto que aunque los dineros se puedan recuperar no se genere la sensación de desconfianza, ya que, son episodios que siguen pasando de manera constante, ocasionando incertidumbre por activos de mayor valor o acrecentando el miedo para no invertir.

De acuerdo con estas situaciones es evidente que una de las acciones que produce dinámica al sistema financiero es el ahorro, y puede sucumbir frente a las amenazas constantes de los sujetos activos del delito, esto es, retirando la totalidad de los recursos una vez sean consignados los honorarios por el miedo a una posible vulneración del sistema.

Figura 7 - Pregunta 6 de encuesta Dirigida a Clientes con productos financieros



Fuente: Elaboración Propia

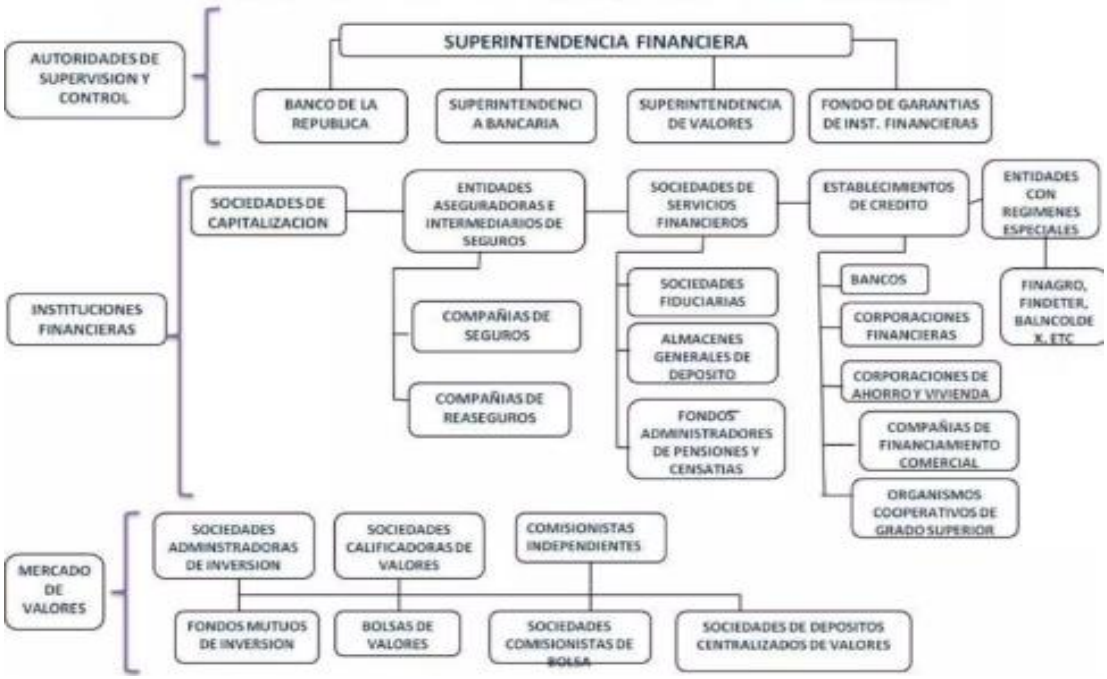
Finalmente, la figura 7, confirma la tendencia sobre la desconfianza que se ha venido analizando durante este segundo capítulo, ya que, el (75%) de los encuestados ha sido víctima de la forma común en que se lleva a cabo el delito de transferencia no consentida de activos y es el descuento de dinero de cuenta personal, debido a que es mucho más efectivo, teniendo en cuenta que sea una cuenta de nómina o no, en algún momento durante el mes se realizaran transacciones, lo cual crea la oportunidad para que los sujetos activos del delito puedan sacar provecho de la situación.

De acuerdo con las tendencias comportamentales evaluadas en este capítulo, se concluye entonces que las condiciones para fortalecer la confianza en el sistema financiero en Colombia actualmente se encuentra fragmentada debido a la falta de avances tecnológicos y políticas de seguridad que permitan a los clientes confiar en la seguridad que implicaba otorgar la administración de activos a las entidades financieras, pues dicha confianza se ha relevado a la administración del titular de los recursos, que prefiere realizar transacciones físicas por la falta de garantía.

6.3. Estructura de la integridad del sistema financiero en Colombia para la generación de respuesta a la comisión de delito de transferencia no consentida de activos

En cuanto a su estructura, el sistema financiero colombiano está estructurado para facilitar la transferencia de recursos desde sectores con excedentes hacia aquellos que requieren financiamiento. Se compone principalmente de dos mercados: el mercado bancario o intermediado, y el mercado de valores. El mercado bancario incluye bancos comerciales y otras instituciones financieras que actúan como intermediarios entre ahorradores e inversionistas. Por otro lado, el mercado de valores permite a los inversionistas realizar transacciones directamente en el mercado, reduciendo riesgos a través de intermediarios especializados.

Figura 8 - Estructura del Sistema Financiero en Colombia



Fuente: Rodríguez, 2011

Además, el sistema financiero colombiano ha evolucionado hacia un modelo de multibanca, especialmente desde la implementación de la Ley 45 de 1990, que introdujo el modelo de matrices y filiales, lo que ha permitido una mayor diversificación de servicios financieros y un control más efectivo sobre aspectos como la regulación, supervisión de conflictos de interés y riesgos de contagio (Ley 45, 1990). Los conglomerados financieros juegan un papel importante, aprovechando economías de escala y avances tecnológicos para ofrecer una amplia gama de servicios financieros tanto a nivel nacional como internacional, especialmente en Centroamérica.

Teniendo en cuenta que el delito de transferencia no consentida de activos se caracteriza por tener un enfoque trasnacional, es decir, que se puede cometer desde cualquier parte del mundo, como herramienta para la protección de este sistema financiero se encuentra el Convenio de Budapest suscrito por Colombia el 18 de junio de 1993. Tiene como finalidad principal establecer un marco común para combatir los delitos informáticos y las infracciones relacionadas con la tecnología de la información. Fue adoptado por el Consejo de Europa en 2001 y es el

primer tratado internacional que aborda específicamente los crímenes cometidos a través de internet y otras redes informáticas (Council de Europa, 2001).

Básicamente este convenio solicita a los Estados parte que dentro de sus legislaciones faciliten la posibilidad de armonizar las leyes a nivel internacional para sobreponerse a los delitos que se producen mediante el uso de la informática, promover la cooperación internacional, esto es, brindar facilidades para el desarrollo de investigaciones como acceso a bases de datos, aprovechamiento de nuevas tecnologías, etc.

Bajo esta perspectiva, se especifica que en efecto el Estado colombiano deberá analizar a partir de las lesiones aprendidas y de la depresión en la que se encuentra el sector bursátil por falta de confianza en los clientes, ocasionando poca liquidez y baja circulación del dinero lo cual extrapola otros sectores de la economía del país. En este sentido, evaluar cuál de los países que hacen parte del convenio cuenta con infraestructura tecnología para combatir este tipo de delitos y fortalecer las capacidades instaladas a los operadores judiciales, asimismo erradicar los obstáculos y la tramitología para acceder a sistemas de información internacional y brindar acceso privilegiado a la misma, pero de manera confidencial y con las garantías y reparaciones que esto supone.

A continuación, se presentarán resultados de la entrevista realizada a un gerente de una banca comercial de la ciudad de Medellín, quien brindo su apreciación sobre como su entidad se prepara para garantizar la salvaguarda de sus activos a partir de la aplicación de políticas de seguridad.

Como primer presupuesto se consultó **¿De qué manera su empresa garantiza la protección y seguridad de los productos financieros de los clientes?**

> **Gerente:** Nuestra entidad financiera garantiza la seguridad de los productos financieros mediante la implementación de múltiples capas de protección, que incluyen sistemas de encriptación avanzada, autenticación de múltiples factores (MFA) y monitoreo en tiempo real de las transacciones. Además, contamos con protocolos de ciberseguridad actualizados que cumplen con las normativas nacionales e internacionales para prevenir fraudes, accesos no autorizados y vulnerabilidades.

Lo anterior evidencia que la entidad financiera asegura la protección de sus productos mediante un enfoque integral de ciberseguridad como la encriptación avanzada para proteger los datos, junto con autenticación de múltiples factores (MFA) para verificar la identidad de los usuarios. El monitoreo en tiempo real permite detectar y responder rápidamente a actividades sospechosas. Además, los protocolos de ciberseguridad se actualizan regularmente para cumplir con las normativas vigentes, tanto nacionales como internacionales, garantizando así la prevención de fraudes, accesos no autorizados y otras vulnerabilidades potenciales en sus sistemas.

En segunda instancia, sobre las estrategias se preguntó **¿De qué manera fortalecen la estrategia para evitar que el sistema informático de su empresa sea vulnerado por expertos cibernéticos con la intención de lucrarse?**

> **Gerente:** De manera sistemática las políticas de seguridad de los sistemas se actualizan todo el tiempo mediante

> la adquisición de nuevas tecnologías que permitan detectar amenazas en tiempo real y alertar al administrador del mismo de un posible ataque y tomar las medidas necesarias para salvaguardar los activos propios y particulares de la organización.

Se puede inferir que las acciones inmediatas de ciberseguridad cumplen con las recomendaciones que se han venido mencionando a lo largo de esta investigación, como tratar de igualar o superar la infraestructura tecnológica con la que los sujetos activos del delito de transferencia no consentida de activos utilizan para manipular el sistema, esto implica contar con funcionarios capacitados y por supuesto brindar información sobre los riesgos a los clientes de manera focalizada que implique evadir las diferentes técnicas de sustracción de datos.

En relación al fortalecimiento técnico del recurso humano se indicó **¿Actualmente se brinda formación y capacitación al cliente que presenta mayor vulnerabilidad de ser vulnerado en sus productos financieros? ¿Explique de qué manera por favor?**

> **Gerente:** Los programas de formación y capacitación al interior de la organización es una política bandera para poder brindar el mejor servicio personalizado a los clientes, es por ello que todos deben aprender a manejar los dispositivos que la empresa disponga para el buen manejo por parte de los interesados.

Se considera que estos programas deben intensificarse por todos los canales disponibles y porque no realizar acompañamientos en lugares estratégicos de las diferentes ciudades que permitan identificar los riesgos que comúnmente se presentan al momento de adquirir productos financieros y evaluar el desempeño del recurso humano cuando se presenten crisis de información o ataques a la ciberseguridad de la misma.

Respecto al nivel de ataques cibernéticos que recibe la entidad se consultó **¿Con que frecuencia ocurren estos ataques cibernéticos en contra del sistema informático de su empresa?**

> **Gerente:** Si bien experimentamos intentos de acceso no autorizado casi diariamente, contamos con medidas robustas que impiden que estos ataques se materialicen. La mayoría son mitigados sin incidentes, y los casos graves son escasos debido a nuestras fuertes barreras de seguridad.

En la industria financiera, los intentos de ataques cibernéticos son una realidad diaria, sin embargo, la empresa ha implementado medidas de seguridad robustas que previenen la materialización de estos ataques. Gracias a estas defensas, la mayoría de los intentos de acceso no autorizado son mitigados sin causar incidentes y los casos graves son raros, lo que refleja la eficacia de las barreras de seguridad implementadas.

Sobre las garantías frente a los productos financieros, se preguntó **¿Cuál es el trámite que debe realizar un usuario víctima del delito de transferencia no consentida de activos frente a la entidad para recuperar lo perdido?**

> **Gerente:** En caso de que un cliente sea víctima de una transferencia no consentida, debe notificar de inmediato a la

> entidad a través de nuestros canales de atención (teléfono, app o presencial). Se abre una investigación interna para evaluar la transacción y, si se confirma el fraude, el banco procede a la reversión de los fondos en el menor tiempo posible. Durante este proceso, mantenemos una comunicación constante con el cliente para asegurar la resolución satisfactoria del caso.

Básicamente la entidad inicia una investigación interna para analizar la transacción, si se confirma que ha habido fraude, el banco revierte los fondos lo más rápido posible. Durante todo el proceso, la entidad mantiene una comunicación constante con el cliente para garantizar que el caso se resuelva de manera satisfactoria y eficiente, asegurando así la protección del cliente. Cabe señalar que esto se da siempre y cuando se determine que el fraude fue objeto por falta de garantías de la entidad, si se demuestra que el cliente brindo información confidencial haciendo caso omiso a los programas de formación y los comunicados al celular y correo electrónico, dicha responsabilidad no podrá ser imputable a la entidad financiera.

Finalmente, sobre el habeas data y la administración de información del recurso humano se estableció **¿Cómo es el protocolo para el tratamiento de datos personales de los clientes por parte de los colaboradores de la empresa?**

> **Gerente:** Nuestro protocolo de tratamiento de datos personales sigue estrictamente las normativas de protección de datos vigentes, tanto locales como internacionales. Los colaboradores reciben capacitación regular sobre la importancia de la confidencialidad y el manejo seguro de la información de los clientes. Accedemos a los datos bajo estrictas medidas de control y utilizamos encriptación y políticas de acceso limitado para asegurar que sólo el personal autorizado pueda gestionar la información de los clientes. Además, realizamos auditorías regulares para asegurar el cumplimiento de estas políticas.

En esta empresa se implementan medidas de control estrictas, como la encriptación y políticas de acceso limitado, para garantizar que solo el personal autorizado pueda gestionar los datos de los clientes y se realizan auditorías periódicas para asegurar el cumplimiento de estas políticas y proteger la información.

De acuerdo con la estructura del sistema financiero en Colombia, los postulados del convenio de Budapest, el nivel de confianza del consumidor, y los avances que han venido ejerciendo las empresas financieras del sector privado para proteger los activos de los clientes, brindando garantías integrales para la tranquilidad de inversiones o ahorros, se concibe que es necesario realizar esfuerzos por parte del Estado a través de las entidades competentes para que se pueda facilitar las acciones de investigación que se ven obstruidas por permisos y reglamentos externos que impiden rastrear los fondos en tiempo real, especialmente a países que son paraísos fiscales. De esta manera se pueden obtener mejores resultados y al menos procurar porque los activos no sean defraudados y reflejar efectividad en la posición de garante que tiene el gobierno nacional para hacer cumplir la ley penal en relación al delito de transferencia no consentida de activos.

Conclusiones

El estudio destaca la necesidad de mejorar las capacidades de investigación y prevención de delitos informáticos en Colombia, toda vez, que los jueces y fiscales enfrentan dificultades al aplicar la normativa actual, lo que subraya la importancia de contar con políticas de seguridad informática estandarizadas y supervisadas por organizaciones de calidad internacional. Que implique un verdadero fortalecimiento de los sistemas de información administrados por las bancas comerciales.

Respecto al alcance dogmático del delito de transferencia no consentida de activos se pudo determinar que urge que el Estado pueda afianzar acciones administrativas y legislativa que supongan brindar mayor celeridad a las instancias de investigación y sanción, teniendo en cuenta que descriptivamente el comportamiento se encuentra bien tipificado y con sanciones y penas adecuadas al tipo de bien que se afecta, sin embargo al tratarse de recursos financieros se hace necesario que este no se vea sustraído de los sistemas que lo administran para no afectar la confianza de los actores que pertenecen a dicho sector.

Por otro lado, en relación a la confianza que se presenta en el sistema financiero en Colombia cabe decir que se encuentra con una tendencia a la baja, como consecuencia de la falta de efectividad por parte de las entidades competentes para reprimir estos actos delictivos. Es de anotar que se hace necesario desde una perspectiva gubernamental dotar a dichas entidades de una infraestructura de última generación, actualizar los convenios internacionales y por supuesto realizar pasantías internacionales de algunos funcionarios para que puedan contar con capacidad técnica suficiente para detectar sigilosamente los autores materiales de estos hechos.

Por último, respecto de la estructura financiera en Colombia, vale decir que en la actualidad es vulnerable frente a los ataques de los hackers porque se ha priorizado en desarrollar tecnología para aumentar el consumo de los clientes y no han invertido suficiente por soportar de manera adecuada los sistemas de ciberseguridad que puedan amparar la política de información que implique un fortalecimiento en la confianza comercial y la seguridad jurídica.

Referencias

Acosta, M., Benavides, M., & García, N. (2020). Delitos informáticos: Impunidadorganizacional y su complejidad en el mundode los negocios. *Revista Venezolana de Gerencia, 25*(89), 1-14. Obtenido de https://www.redalyc.org/journal/290/29062641023/html/

Aranzazu, M., & Delgado, D. (2018). *Eficacia Legislativa y Normativa sobre los delitos informaticos en Colombia.* Obtenido de https://repository.unilibre.edu.co/bitstream/handle/10901/26654/EFICACIA%20NORMATIVA%20SOBRE%20LOS%20DELITOS%20INFORM%C3%81TICOS%20EN%20COLOMBIA%20PDF.pdf?sequence=1&isAllowed=y

ASOBANCARIA. (2019). *Desafios del riesgo cibernetico en el sector financiero para Colombia y America Latina.* Obtenido de https://www.asobancaria.com/wp-content/uploads/20191010-asobancaria-OEA_min.pdf

Asobancaria. (2022). *La reinvención financiera en la era digital.* Obtenido de https://asobancaria.com/wp-content/uploads/La_reinvencion_financiera_en_la_era_digital-2022.pdf

Astaiza, P., & Cuellar, V. (2023). *Analisis dogmatico de los delitos informaticos o ciberdelitos en Colombia.* Obtenido de https://repository.unilibre.edu.co/bitstream/handle/10901/29295/An%C3%A1lisis%20Dogm%C3%A1tico%20de%20los%20Delitos%20Inform%C3%A1ticos%20o%20Ciberdelitos%20en%20Colombia.pdf?sequence=3&isAllowed=y

Astaiza, P., & Cuellar, V. (2023). *Analisis dogmatico de los delitos informaticos o ciberdelitos en Colombia.* Obtenido de https://repository.unilibre.edu.co/bitstream/handle/10901/29295/An%c3%a1lisis%20Dogm%c3%a1tico%20de%20los%20Delitos%20Inform%c3%a1ticos%20o%20Ciberdelitos%20en%20Colombia.pdf?sequence=3&isAllowed=y

Ávila, A. (2023). Analisis del delito de fraude informatico. *Vox Juris*, *42*(1), 159-173. Obtenido de https://portalrevistas.aulavirtualusmp.pe/index.php/VJ/article/view/2654/3534

Bechara, Y., Mosquera, A., & Ledezma, E. (2020). *Analisis juridico de la Ley 1273 de 2009 y el surgimiento y expansión del delito de hurto y semejantes por medios informaticos.* Obtenido de https://repository.ucc.edu.co/server/api/core/bitstreams/25b22101-a13a-4eeb-a50d-ac9cecb8e4c0/content

Bernate, O. (2006). *Estudios de derecho penal economico.* Bogotá: Grupo Editorial Ibañez.

Calvo, M. (2023). La responsabilidad civil de los bancos en los delitos de esta por "Phishing". *Actualidad Juridica Iberoamericana*(18), 1778-1809. Obtenido de https://revista-aji.com/articulos/2023/18/AJI18_64.pdf

Castillo, J. (2018). *El delito informático y su implicación en el patrimonio económico en Colombia.* Obtenido de https://repository.unimilitar.edu.co/bitstream/handle/10654/17914/CastilloMellizoJorgeAlberto2018.pdf.pdf?sequence=2&isAllowed=y

Congreso de la República de Colombia. (18 de Diciembre de 1990). Ley 45. *Por la cual se expiden normas en materia de intermediación financiera, se regula la actividad aseguradora, se conceden unas facultades y se dictan otras disposiciones*. Bogotá, Colombia.

Congreso de la República de Colombia. (05 de Enero de 2009). *Ley 1273.* Obtenido de Por medio de la cual se modifica el Código Penal se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

Congreso de la República de Colombia. (17 de Octubre de 2012). Ley 1581. *Por la cual se dictan disposiciones generales para la protección de datos personales.* Bogotá, Colombia: Diario Oficial 48587.

Council de Europa. (23 de Noviembre de 2001). Convenio sobre la Ciberdelincuencia. Budapest, Hungria.

Diario las Americas. (22 de Septiembre de 2023). *Delitos cibernéticos, una amenaza en ascenso con un costo de $10.5 billones*. Obtenido de https://www.diariolasamericas.com/tecnologia/los-delitos-ciberneticos-pueden-alcanzar-los-105-billones-dolares-2025-n5343714

Fedesarrollo. (10 de Septiembre de 2024). *Boletín Encuesta de Opinión del Consumidor.* Obtenido de https://www.repository.fedesarrollo.org.co/handle/11445/36

FLAI. (25 de Mayo de 2020). *Informe de la asociación de examinadores de fraude certificados (ACFE).* Obtenido de https://laflai.org/informe-de-la-asociacion-de-examinadores-de-fraude-certificados-acfe/

Forero, Y., & Galeano, L. (2016). *Detección, prevención de transacciones fraudulentas con tarjeta de credito en almacenes fallabella.* Obtenido de https://ciencia.lasalle.edu.co/cgi/viewcontent.cgi?article=1613&context=contaduria_publica

Gamba, J. (2019). *El delito informatico en el marco juridico colombiano y el derecho comparado: Caso de la transferencia no consentida de activos.* Obtenido de https://bdigital.uexternado.edu.co/server/api/core/bitstreams/2e7e30f3-4a1f-45f6-b59a-dae6012b7210/content

Garzón, V., & Quintero, S. (2021). *Riesgos juridico penales que se derivan de la practica del comercio electronico en Colombia.* Obtenido de https://repository.upb.edu.co/bitstream/handle/20.500.11912/9762/Riesgos%20jur%C3%ADdico%20penales.pdf?sequence=1&isAllowed=y

Gonzalez, D. (2017). *La protección de información y los datos en el marco de la Ley 1273 de 2009: Un estudio del dato y la información como objeto material en el tipo penal hurto por medios informáticos.* Obtenido de https://repository.ugc.edu.co/bitstream/handle/11396/4273/Dato_informaci%C3%B3n_delitos_inform%C3%A1ticos.pdf

Grisales, G. (2013). *Análisis dogmático de las conductas deHurto por medios informáticos ysemejantes (Art. 269i) y Transferencia noconsentida de activos (Art. 269j) Ley 1273de 2009.* Obtenido de https://repository.eafit.edu.co/server/api/core/bitstreams/f4d5ecfb-76fb-4e37-91c9-d86557d9c4cf/content

Guerrero, B., & Castillo, D. (2017). *Desafios Tecnicos y Juridicos frente al Ciberdelito en el sector bancario colombiano.* Obtenido de https://repository.unad.edu.co/bitstream/handle/10596/13387/52498805.pdf?sequence=5&isAllowed=y

Guizado, A., & Silva, M. (2024). *La posibilidad de conciliación en los delitos de estafa y el principio de mínima intervención penal.* Obtenido de http://dspace.unach.edu.ec/bitstream/51000/13714/1/Guizado%20Arteaga%20A%20y%20Silva%20Toro%2c%20M%282024%29%20La%20posibilidad%20de%20conciliaci%c3%b3n%20en%20los%20delitos%20de%20estafa%20y%20el%20principio%20de%20m%c3%adnima%20intervenci%c3%b3n%20penal

Lozano, M. (2017). *Sistema Financiero Colombiano.* Obtenido de https://digitk.areandina.edu.co/server/api/core/bitstreams/b4ad6835-697c-4325-b72e-017acf53f726/content

Martinez, J. (2023). *Hurto a través de medios informáticos y otras conductas delictivas semejantes en Colombia 2022.* Obtenido de https://repository.ucatolica.edu.co/server/api/core/bitstreams/e21a70d5-f51b-4c06-b5ea-47a50d3d8551/content

Montañez, A. (2017). *Analisis de los delitos informaticos en el actual sistema Colombiano.* Obtenido de https://repository.unilibre.edu.co/bitstream/handle/10901/11041/AN%C3%81LISIS%20DE%20LOS%20DELITOS%20INFORM%C3%81TICOS%20EN%20EL%20ACTUAL%20SISTEMA%20PENAL%20COLOMBIANO%20revisado%20NHJ%20OK.pdf?sequence=3

Naciones Unidas. (25 de Octubre de 2011). *UNODC estima en 1,6 billones de dólares lavado de dinero en 2009*. Obtenido de https://news.un.org/es/story/2011/10/1228761

Narvaéz, O. (2022). *Los elementos subjetivos distintos del dolo, del tipo o del injusto: una inclusión de la jurisprudencia nacional para la descripción de la conducta punible.* Obtenido de https://repository.ugc.edu.co/server/api/core/bitstreams/0284ec68-8b95-49e2-a064-06d6e78011b5/content

Nobles, E., Narváez, E., & Rúgeles, A. (2020). *Ámbito de Validez de la Prueba Electrónica en los Delitos Informáticos.* Obtenido de https://alejandria.poligran.edu.co/bitstream/handle/10823/2155/El%20%C3%A1mbito%20de%20validez%20de%20la%20prueba%20electr%C3%B3nica%20en%20los%20delitos%20informaticos.pdf?sequence=2&isAllowed=y

Palacios, A. (2016). *Confianza e inclusión financiera en Colombia.* Obtenido de https://www.eafit.edu.co/programas-academicos/posgrado/maestria-administracion-

financiera/investigacion/Documents/confianza%20e%20inclusi%C3%B3n%20financiera%20en%20Colombia.pdf

Peréz, A. (2019). *Delitos contra el patrimonio economico.* Bogotá D.C.: Editorial Temis S.A.

Perlaza, C., & Rivera, J. (2024). *Actuación del Estado en el delito de transferencia no consentida de activos en Colombia, periodo 2020-2023.* Obtenido de https://repositorio.uceva.edu.co/bitstream/handle/20.500.12993/4600/TG-cperlaza-jrivera.pdf?sequence=1&isAllowed=y

Posada, M. (2017). El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual. *Nuevo Foro Penal, 13*(188), 72-112.

Posada, R. (2012). El delito de Transferencia no consentida de activos. *Revista de Derecho, Comunicaciones y Nuevas Tecnologias*(8), 1-27.

Ricaurte, T. (2022). *La Transformación Digital en el Sector Financiero.* Obtenido de https://ciencia.lasalle.edu.co/cgi/viewcontent.cgi?article=1678&context=finanzas_comercio

Rueda, J. (2020). *Impacto de la tecnica de ataque de Pishing en Colombia durante los ultimos cinco años.* Obtenido de https://repository.unad.edu.co/bitstream/handle/10596/38721/jaruedaq.pdf?sequence=1&isAllowed=y

Salas, R. (2024). El delito permanente y el delito habitual. *Revista de Ciencias Juridicas*(164), 1-24.

Salazar, J. (2011). Situación normativa de la Sociedad de la Información en Colombia. *Criterio Jurídico, 9*(1), 89-103.

Sánchez, Z. (2017). *Analisis de la Ley 1273 de 2009 y la evolución de la ley con relación a los delitos informaticos en Colombia.* Obtenido de https://repository.unad.edu.co/bitstream/handle/10596/11943/1053323761.pdf?sequence=1&isAllowed=y

Sentencia de Casación, 42724 (Corte Suprema de Justicia 11 de Febrero de 2015). Obtenido de https://www.cortesuprema.gov.co/corte/wp-content/uploads/relatorias/pe/b1mar2015/SP1245-2015.pdf

Sentencia No.15595 (Corte Suprema Justicia 03 de Diciembre de 2003).

Suarez, A. (2019). *El delito informatico en el marco juridico Colombiano y el Derecho Comparado: Caso de la Transferencia no consentida de activos.* Obtenido de https://bdigital.uexternado.edu.co/server/api/core/bitstreams/2e7e30f3-4a1f-45f6-b59a-dae6012b7210/content

Vásquez, D., Camacho, I., Medina, K., Torres, L., Mejia, N., Torres, L., & Mejia, N. (2023). *Proyecto de investigación para el proceso de selección de personal en la empresa Scotiabank Colpatria.* Obtenido de https://repository.unad.edu.co/bitstream/handle/10596/57296/dmvasquezh.pdf?sequence=1&isAllowed=yhttps://www.researchgate.net/publication/222103312_La_gestion_del_tal

ento_en_las_organizaciones_Su_alineamiento_estrategico_y_coherencia_operacionalhttp://rep

Vega, H. (2016). El analisis gramatical del tipo penal. *En justicia*(29), 53-71. Obtenido de http://www.scielo.org.co/pdf/just/n29/n29a05.pdf

Anexos

Medellín, veintiuno (21) de agosto de 2024.

Fiscalía General de la Nación
Avenida Calle 24 No. 52 -01 Ciudad Salitre
Bogotá, D.C.
E. S. D.

Asunto: Derecho de petición, solicitud información.

De manera respetuosa nos dirigimos a su Despacho, con el fin de solicitar información sobre cuántas indagaciones e investigaciones se han aperturado durante los últimos diez años en la Fiscalía General de la Nación de Colombia acerca del **delito Transferencias no Consentida de Activos**, en el actual entorno digital, el sector financiero enfrenta desafíos cada vez más complejos relacionados con la seguridad de la información y la protección de activos. Uno de los problemas más urgentes en este contexto es la transferencia no consentida de activos como delito informático, que representa una amenaza significativa para la estabilidad y la confianza en las instituciones financieras. Nos referimos a aquellas transacciones que los ciudadanos titulares de cuenta no autorizan, problemática que nos aqueja constantemente. Dicha información la solicitamos para anexarla a nuestro proyecto de grado, el cual se encuentra direccionado a este fenómeno que se presenta con la digitalización y que cada vez es más común. Del que somos conscientes que, aunque existe, no tenemos una regulación completamente definida para dichos casos.

Notificaciones

Para efectos de notificaciones por favor enviar la respuesta a los correos; alexandra.pulgarin8686@unaula.edu.co, federico.munoz9147@unaula.edu.co líneas telefónicas: 3117134621, 3006327000.

Cordialmente,

Alexandra Pulgarín Pulgarín
C.C. 1.037.498.686
Estudiante Universidad Autónoma Latinoamericana de Medellín
Programa de derecho

Federico Augusto Muñoz Zapata
C.C. 71.229.147
Estudiante Universidad Autónoma Latinoamericana de Medellín
Programa de derecho

Derecho de petición

ALEXANDRA PULGARIN PULGARIN <alexandra.pulgarin8686@unaula.edu.co>

Mié 21/08/2024 16:12

Para:ges.documentalpqrs@fiscalia.gov.co <ges.documentalpqrs@fiscalia.gov.co>;jur.notificacionesjudiciales@fiscalia.gov.co <jur.notificacionesjudiciales@fiscalia.gov.co>;juridicanotificacionestutela@fiscalia.gov.co <juridicanotificacionestutela@fiscalia.gov.co>
Cco:FEDERICO AUGUSTO MUNOZ ZAPATA <federico.munoz9147@unaula.edu.co>

1 archivos adjuntos (34 KB)

Derecho de petición Fiscalía General de la Nación.pdf;

Medellín, veintiuno (21) de agosto de 2024.

Fiscalía General de la Nación
Avenida Calle 24 No. 52 -01 Ciudad Salitre
Bogotá, D.C.
E. S. D.

Asunto: Derecho de petición, solicitud información.

Medellín, veintiuno (21) de agosto de 2024.

Señores
Superintendencia Financiera de Colombia
Calle 7 No. 4 - 49
Bogotá, D.C.
E. S. D.

Asunto: Derecho de petición, solicitud información.

De manera respetuosa nos dirigimos a su Despacho, con el fin de solicitar información sobre cuántas PQRS existen durante los últimos diez años en la Superintendencia Financiera de Colombia acerca del **delito Transferencias no Consentida de Activos**, en el actual entorno digital, el sector financiero enfrenta desafíos cada vez más complejos relacionados con la seguridad de la información y la protección de activos. Uno de los problemas más urgentes en este contexto es la transferencia no consentida de activos como delito informático, que representa una amenaza significativa para la estabilidad y la confianza en las instituciones financieras. Nos referimos a aquellas transacciones que los ciudadanos titulares de cuenta no autorizan, problemática que nos aqueja constantemente. Dicha información la solicitamos para anexarla a nuestro proyecto de grado, el cual se encuentra direccionado a este fenómeno que se presenta con la digitalización y que cada vez es más común. Del que somos conscientes que, aunque existe, no tenemos una regulación completamente definida para dichos casos.

Notificaciones

Para efectos de notificaciones por favor enviar la respuesta a los correos; alexandra.pulgarin8686@unaula.edu.co, federico.munoz9147@unaula.edu.co líneas telefónicas: 3117134621, 3006327000.

Cordialmente,

Alexandra Pulgarín Pulgarín
C.C. 1.037.498.686
Estudiante Universidad Autónoma Latinoamericana de Medellín
Programa de derecho

Federico Augusto Muñoz Zapata
C.C. 71.229.147
Estudiante Universidad Autónoma Latinoamericana de Medellín
Programa de derecho

Derecho de petición

ALEXANDRA PULGARIN PULGARIN <alexandra.pulgarin8686@unaula.edu.co>

Mié 21/08/2024 16:15

Para:super@superfinanciera.gov.co <super@superfinanciera.gov.co>;notificaciones_ingreso@superfinanciera.gov.co <notificaciones_ingreso@superfinanciera.gov.co>
Cco:FEDERICO AUGUSTO MUNOZ ZAPATA <federico.munoz9147@unaula.edu.co>

1 archivos adjuntos (34 KB)

Derecho de petición Superintendencia Financiera de Colombia.pdf;

Medellín, veintiuno (21) de agosto de 2024.

Señores
Superintendencia Financiera de Colombia
Calle 7 No. 4 - 49
Bogotá, D.C.
E. S. D.

Asunto: Derecho de petición, solicitud información.

Medellín, veintiuno (21) de agosto de 2024.

Rama Judicial
Calle 12 No. 7 - 65, Palacio de Justicia Alfonso Reyes Echandía
info@cendoj.ramajudicial.gov.co
Bogotá, D.C.
E. S. D.

Asunto: **Derecho de petición, solicitud información**.

De manera respetuosa nos dirigimos a su Despacho, con el fin de solicitar información sobre cuántas sentencias condenatorias se han emitido durante los últimos diez años en la Rama Judicial de Colombia acerca del **delito Transferencias no Consentida de Activos**, en el actual entorno digital, el sector financiero enfrenta desafíos cada vez más complejos relacionados con la seguridad de la información y la protección de activos. Uno de los problemas más urgentes en este contexto es la transferencia no consentida de activos como delito informático, que representa una amenaza significativa para la estabilidad y la confianza en las instituciones financieras. Nos referimos a aquellas transacciones que los ciudadanos titulares de cuenta no autorizan, problemática que nos aqueja constantemente. Dicha información la solicitamos para anexarla a nuestro proyecto de grado, el cual se encuentra direccionado a este fenómeno que se presenta con la digitalización y que cada vez es más común. Del que somos conscientes que, aunque existe, no tenemos una regulación completamente definida para dichos casos.

Notificaciones

Para efectos de notificaciones por favor enviar la respuesta a los correos; alexandra.pulgarin8686@unaula.edu.co, federico.munoz9147@unaula.edu.co líneas telefónicas: 3117134621, 3006327000.

Cordialmente,

Alexandra Pulgarín Pulgarín
C.C. 1.037.498.686
Estudiante Universidad Autónoma Latinoamericana de Medellín
Programa de derecho

Federico Augusto Muñoz Zapata
C.C. 71.229.147
Estudiante Universidad Autónoma Latinoamericana de Medellín
Programa de derecho

Derecho de petición

ALEXANDRA PULGARIN PULGARIN <alexandra.pulgarin8686@unaula.edu.co>

Mié 21/08/2024 16:09

Para:info@cendoj.ramajudicial.gov.co <info@cendoj.ramajudicial.gov.co>
Cco:FEDERICO AUGUSTO MUNOZ ZAPATA <federico.munoz9147@unaula.edu.co>

1 archivos adjuntos (35 KB)
Derecho de petición Rama Judicial.pdf;

Medellín, veintiuno (21) de agosto de 2024.

Rama Judicial
Calle 12 No. 7 - 65, Palacio de Justicia Alfonso Reyes Echandía
info@cendoj.ramajudicial.gov.co
Bogotá, D.C.
E. S. D.

Asunto: Derecho de petición, solicitud información.