UNIVERSIDAD DE TECNOLOGIA Y COMERCIO

Facultad de Ciencias Jurídicas y Sociales

Proyecto monográfico para optar al título de

Licenciado en Derecho:

Aplicación ley 1042 "ley especial de ciberdelitos" en la investigación del delito fraude informático, estudio de casos en Managua, primer trimestre 2023

Autores:

1. Br. Juan Pablo Centeno Benavidez
2. Br. Mirna de los Ángeles Ramírez Pérez

Tutor:

1. MSc. Perla Marina Tablada Peralta
2. Dra. Jossarys Massielle Gazo Robles

Managua, octubre 2023

DEDICATORIA

A nuestros queridos padres, a nuestros compañeros de vida y a nuestros adorados hijos que son la fuerza y razón que nos han impulsado durante estos años de estudio a lograr nuestros objetivos trazados de graduarnos como licenciados en derecho.

A Comisionado General Victoriano Ruíz Urbina por su apoyo incondicional, amistad, cariño y calidad de compañía. A nuestra familia y todas las personas que de una u otra manera influyeron y están relacionados durante esta etapa y siempre dándonos motivación de seguir adelante.

AGRADECIMIENTOS

Agradecemos a **Dios**, por darnos la oportunidad de vivir, quien con su amor y misericordia nos ha permitido salud y sabiduría para poder culminar esta tesis.

Agradecemos a nuestros hijos por el sacrificio del tiempo que no hemos compartido con ellos por esforzarnos y asistir durante un poco más de cuatro años a la universidad para lograr la meta de culminar nuestra formación profesional.

Agradecemos a todos los maestros que con esmero y cariño pusieron a nuestra disposición sus enseñanzas y experiencia en los salones de clases para formar nuestros conocimientos que servirán para el buen desempeño como futuros profesionales del Derecho en Nicaragua.

En especial agradecemos a nuestros tutores, Msc. Perla Marina Tablada Peralta y Dra. Jossarys Massielle Gazo Robles por su amable disposición y por todo el tiempo que nos han dedicado en el desarrollo de este proyecto monográfico.

ÍNDICE

RESUMEN

El presente trabajo investigativo es realizado con el objetivo de evaluar la efectividad de la LEY N°. 1042, Ley especial de ciberdelitos en cuanto a la investigación, persecución y prevención de los casos de fraude informático. El diseño metodológico que caracteriza esta investigación es mixto, la recolección de información y datos se realizó a través análisis documental, el empleo de la técnica de observación en expedientes y la aplicación de instrumentos con la técnica de muestreo aleatorio simple, cuyo fin responde únicamente a medir el nivel de conocimiento y percepción sobre la efectividad de la ley en la población seleccionada.

El procesamiento de los datos y la información permitió llegar a las siguientes conclusiones:

La investigación de los fraudes informáticos surgen a raíz de una denuncia, en Managua la responsabilidad de investigar recae en los detectives policiales quienes practican técnicas y diligencias investigativas entre las que resalta el análisis forense como uno de los más importantes, el estudio de la percepción permitió conocer que a criterio de las victimas la ley de ciberdelitos si es efectiva, sin embargo, existen aspectos que deben ser mejorados en el futuro, entre estos resalta la necesidad de establecer una cuantía para determinar la gravedad del delito.

Palabras Claves: Ciberdelitos, hackers, tecnología, programa malicioso, ciberseguridad.

ABSTRACT

The present investigative work called LEGAL ANALYSIS OF LAW 1042: “SPECIAL CYBERCRIME LAW” AND ITS EFFECTIVENESS IN FIGHTING COMPUTER FRAUD, CASE STUDY IN MANAGUA, FIRST QUARTER 2023 is carried out with the objective of evaluating the effectiveness of the cybercrime law of Nicaragua in the investigation, prosecution and prevention of cases of computer fraud that occurred in the city of Managua during the first quarter of 2023. The methodological design that characterizes this investigation is Mixed, the collection of information and data was carried out through documentary analysis, the use of the observation technique in files and the application of instruments with the simple random sampling technique, whose purpose is solely to measure the level of knowledge and perception about the effectiveness of the law in the selected population. The processing of the data and information allowed us to reach the following conclusions:

The investigation of computer fraud arises from a complaint, and in Managua, the responsibility for investigating falls on police detectives who practice various investigative techniques, with forensic analysis standing out as one of the most important. The perception study revealed that, according to victims, the cybercrime law is effective; however, there are aspects that need improvement in the future, notably the need to establish a threshold to determine the severity of the offense.

Keywords: Cybercrimes, hackers, technology, malware, cybersecurity.

I. INTRODUCCIÓN

En todo el mundo y en especial en nuestra Nicaragua la inseguridad en el ámbito virtual es una realidad cada vez más compleja, la era digital ha transformado la forma en que interactuamos, trabajamos y compartimos. Lo que ha dado lugar a un aumento significativo en la delincuencia cibernética y específicamente al delito denominado fraude informático, fenómeno que refleja un acelerado crecimiento. Ante esta imperante realidad se promulgo en el año 2020 la Ley No. 1042, Ley Especial de Ciberdelitos, con la que el gobierno de Nicaragua busca frenar y prevenir hechos antijurídicos determinados en esta nueva norma legal.

En este contexto, surge una pregunta fundamental: ¿Está siendo efectiva la Ley Especial de Ciberdelitos, como es su aplicación en el enfrentamiento al fraude informático? esta interrogante cobra especial relevancia en el primer trimestre de 2023, en la ciudad de Managua, donde este delito sigue representando una amenaza creciente para individuos, empresas y organismos gubernamentales, reflejando en comparación con el mismo periodo del año anterior registro un aumento significativo en el número de casos denunciados ante la policía nacional.

El objetivo central de este proyecto monográfico es abordar el problema de investigación mediante un análisis jurídico profundo de la Ley 1042, Ley Especial de Ciberdelitos y una evaluación de su impacto en la lucha contra el fraude informático en Managua durante el primer trimestre de 2023. Para alcanzar este objetivo, se llevará a cabo un estudio de casos que permitirá examinar cómo la legislación ha

sido implementada y aplicada, se aplicarán instrumentos para conocer desde la óptica de las víctimas de este delito sus consideraciones sobre la efectividad de la ley, así como de las autoridades sobre las que recae su aplicación.

Este estudio no solo se centrará en determinar la efectividad de la ley, sino también en identificar los factores que están influyendo positiva o negativamente en su aplicación en la investigación policial de este delito. Se analizarán las fortalezas y debilidades de la Ley 1042, Ley Especial de Ciberdelitos y se identificarán las dinámicas legales, tecnológicas y sociales que inciden en la efectividad de la legislación.

En resumen, este proyecto monográfico busca conocer la efectividad de la Ley 1042, Ley Especial de Ciberdelitos de Nicaragua en el enfrentamiento al fraude informático en Managua durante el primer trimestre de 2023. A través de un análisis exhaustivo y la identificación de factores claves, que pueden influir positiva o negativamente en la eficiencia y eficacia de la misma, con este estudio se espera proporcionar información valiosa que contribuya a una futura mejora de la legislación y de las estrategias de lucha aplicada por las autoridades competentes contra los delitos cibernéticos en el país y en específico contra el fraude informático.

Para el cumplimento de los objetivos propuestos en la presente investigación se realizó un análisis exhaustivo de literatura, se observó expedientes investigativos y se participó como observador del trabajo policial realizado por el departamento de investigación de delitos informáticos de la Dirección de Auxilio Judicial de la Policía

Nacional, durante un periodo de dos meses, tiempo en el que se seleccionó y se aplicó instrumentos de recolección de datos a víctimas que formularon denuncias seleccionadas por conveniencia.

II. ANTECEDENTES

2.1. Internacional

Desde la creación del internet, diversas modalidades delictivas han surgido y se han cometido por personas que, haciendo uso de la tecnologías y haciendo uso de diversos métodos delictivos virtuales lo que actualmente conocemos como ciberdelitos. Al respecto de este fenómeno, diversos investigadores especialistas en informática, en leyes, y en fenómenos sociológicos han plasmado en sus tesis investigativas argumentos y elementos propios de las realidades que se viven en cada país, sin embargo, lejos de ser una realidad diferenciada, el tema de los ciberdelitos constituye una problemática global, cuyo enfrentamiento debe ser un esfuerzo coordinado.

En el campo internacional, existen variedad de tesis doctorales, libros, monografías y artículos de revistas científicas, sin embargo, para fines de esta investigación se seleccionaron las siguientes:

El artículo científico por (Gamon, 2017) publicado en la revista Latinoamericana de Estudios de seguridad titulado: Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad ofrece una amplia reseña histórica sobre el surgimiento, la proliferación y el enfrentamiento de los delitos cometidos con el internet a nivel global, la visión histórica planteada por el autor tiene amplia relación con el presente trabajo investigativo por que ofrece una amplia visión del tiempo y las realidades en que la ciberdelincuencia actúa en Nicaragua.

En la tesis Análisis del delito de fraude electrónico: modalidad tarjeta de crédito, Díaz y Barboza (2018) publicado en la Universidad Cooperativa de Colombia, los autores realizan un amplio análisis jurídico sobre el fraude electrónico en Colombia, por lo que para fines de la presente investigación el marco legal colombiano y su aplicación en los casos citados por estos autores constituye una excelente materia para el uso del derecho comparado.

Otro estudio de referencia lo constituye la tesis doctoral de (Rodríguez, 2019) denominado Los Desafíos del Derecho de las Tecnologías de la Información y las Comunicaciones (TIC) en la Sociedad de la Información en el Siglo XXI: Una puerta a la cooperación internacional, publicada en la Universidad Rey Juan Carlos de España, esta tesis fue del tipo explicativo y desarrollada con una metodología cualitativa en la que el uso de estadísticas y datos se empleó únicamente para sustentar los argumentos del autor.

Otra investigación internacional es la tesis de maestría titulada: La responsabilidad de las entidades financieras por fraudes electrónicos por (Hernández, 2020) publicada en la Universidad Pontificia Bolivariana de Medellín, la investigación describe la responsabilidad legal que tiene las entidades bancarias de Colombia para sus clientes cuando son víctimas de fraude, por lo que guarda pertinencia y relación respecto a la presente investigación para establecer una base comparativa sobre la responsabilidad de los bancos a nivel internacional versus la responsabilidad que toma el sistema bancario nicaragüense con sus clientes cuando son víctimas de fraude informático.

El más reciente antecedente internacional lo constituye la tesis de licenciatura Delitos informáticos en la actualidad costarricense (Esquivel y Romero, 2021) publicado por la Universidad de Costa Rica, dicha investigación tuvo como objetivo analizar la legislación penal costarricense en materia de delitos informáticos con la finalidad de identificar carencias para plantear soluciones. Dada la similitud de las realidades sociales de Costa Rica con Nicaragua, la comparación de ambos marcos legales para la presente investigación constituirá un relevante aspecto referencial.

2.2. A nivel nacional

En nuestro país diversos autores han realizado investigaciones sobre ciberdelitos, en dichas investigaciones han realizado definiciones, comparación, y aplicación del análisis doctrinal para definir los aspectos novedosos de los ciberdelitos en nuestro país, a esta fecha, no existe una investigación que aborde en específico el tema del fraude informático en Nicaragua; sin embargo, existen trabajos investigativos que abordan la problemática de los delitos cibernéticos que para este trabajo hemos utilizado únicamente como marco referencial y de consulta didáctica. Entre los resultados más notorios que constituyen un antecedente investigativo para el presente trabajo están los siguientes:

La tesis de licenciatura denominada: Análisis de amenazas relacionadas a los metadatos y correo electrónico, e implementación de un aplicativo como herramienta para disminuir el riesgo de un ataque en el que se empleen estos elementos (Altamirano y Sequeira, 2016) publicada por la Universidad Nacional de Ingeniería UNI, aborda la problemática de los ciberdelitos y los fraudes informáticos desde la perspectiva experta de un ingeniero en computación, por lo que esta tesis guarda una

relación importante y relevante con el presente trabajo investigativo al momento de proponer medidas que permitan blindar los sistemas informáticos para la prevención del fraude.

Otro antecedente a mencionar es el artículo científico Perfiles del Ciberdelito: un campo de estudio inexplorado por Barahona (2021) publicado en la revista de derecho de la UCA, en este se realiza un análisis de la incidencia y expansión de los ciberdelitos en general haciendo uso de los métodos de estudio de la criminología.

La tesis por (Gómez y Hernández,2022) titulado: Análisis Jurídico de la Ley No 1042 Ley Especial de Ciberdelitos en relación al acoso sexual cibernético que pueden llegar a sufrir los niños, niñas y adolescentes, en el segundo trimestre del año 2021, publicado por la UNAN Managua, nos acerca al tema a tratar en la presente investigación, si bien es cierto las definiciones conceptuales son similares, por tratarse de la misma ley, la tipicidad y la antijuridicidad son completamente diferentes, por lo que el ámbito de aplicación de la ley, la jurisprudencia y el análisis doctrinal son completamente distintos.

2.3. A nivel Local

En la ciudad de Managua, sitio donde se delimita la presente investigación, no existen antecedentes de investigaciones sobre el tema, por lo que el análisis jurídico de la ley 1042, Ley Especial de Ciberdelitos para evaluar su efectividad en el enfrentamiento al fraude informático, constituye una temática novedosa e inexplorada por otros investigadores y será la primera investigación de grado académico realizada en este tema en específico.

III. Planteamiento del problema

A nivel internacional, con la globalización y la llegada de la era virtual, el fraude informático como hecho delictivo, se ha convertido en una preocupación creciente debido a su alarmante aumento y a la sofisticación de las técnicas utilizadas. Estos actos ilícitos tienen un impacto significativo en la economía, la seguridad y la confianza en el entorno digital. Por ello, los países de manera individual o colectiva han creado leyes y asumido acuerdos y tratados internacionales para el enfrentamiento de estas nuevas modalidades delictivas.

En Nicaragua, el fraude informático también representa una amenaza cada vez mayor. A medida que la sociedad nicaragüense se vuelve más digitalizada, los delincuentes cibernéticos aprovechan las vulnerabilidades en la seguridad informática para perpetrar fraudes financieros, robar datos personales y realizar actividades ilícitas en línea. En este contexto, es fundamental examinar la efectividad de la ley de ciberdelitos de Nicaragua y evaluar si proporciona un marco legal sólido para prevenir, investigar y sancionar adecuadamente estos delitos.

En Managua, centro económico del país, el fraude informático plantea desafíos particulares. Con la era digital las empresas, microempresas y emprendimientos desarrollan su actividad comercial física y digital, lo que los expone a un mayor riesgo debido a la concentración de recursos y la amplia variedad de actividades comerciales en la ciudad, en todos los casos ocurridos el uso de herramientas tecnológicas puede presentar vulnerabilidades que los delincuentes cibernéticos pueden explotar.

Según cifras del departamento de investigación de delitos informáticos de la DAJ, durante el año 2022 en la ciudad de Managua fueron realizadas 70 denuncias sobre este delito; en contraste, durante el primer trimestre del presente año se han realizado 200 denuncias del mismo hecho, reflejando crecimiento del 185.1% en la ocurrencia de esta figura delictiva en el primer trimestre del corriente año en comparación con el periodo 2022, por lo tanto, es necesario analizar cómo la Ley Especial de Ciberdelitos de Nicaragua se ha aplicado a casos concretos ocurridos en la ciudad de Managua y qué resultados se han obtenido en términos de prevención e investigación de los fraudes informáticos.

Es por ello que sobreviene la interrogante ¿Está siendo efectiva la Ley Especial de Ciberdelitos de Nicaragua en el enfrentamiento al fraude informático, como es su aplicación en la investigación de este delito? ¿Cuáles son los factores que están influyendo positiva o negativamente en la efectividad de la ley durante la investigación de este delito en la ciudad de Managua durante el primer trimestre 2023?

IV. OBJETIVOS

4.1. General

Evaluar la efectividad de la Ley Especial de Ciberdelitos de Nicaragua en la investigación, y prevención de los casos de fraude informático ocurridos en la ciudad de Managua durante el primer trimestre 2023.

4.2. Específicos

- Identificar los factores que influyen positiva o negativamente en la efectividad de la aplicación de la ley especial de ciberdelitos y su influencia en la investigación de los casos de fraude informático.
- Examinar expedientes investigativos de casos de fraude informático ocurridos en la ciudad de Managua durante el año 2023 para la identificación de las técnicas investigativas aplicadas por las autoridades policiales en la investigación de este delito.
- Indagar la percepción de las víctimas de este delito sobre la efectividad de la ley en la investigación y prevención de los casos de fraude informático ocurridos en la ciudad de Managua durante el primer trimestre 2023.

V. HIPÓTESIS

La Ley No. 1042, Ley Especial de Ciberdelitos y su aplicación en la investigación al fraude informático en la ciudad de Managua ha sido efectiva durante el primer trimestre 2023. Esta legislación proporciona un marco legal sólido y actualizado, lo que ha facilitado la prevención e investigación de los delitos informáticos, logrando una disminución significativa en la incidencia del delito.

VI. MARCO TEÓRICO

6.1. Historia de la computación

En el desarrollo de la historia de la humanidad, diversos hombres de ciencia aportaron pequeños avances que conllevaron a la creación de la primera computadora digital, dentro de las acciones más reconocidas en la antigüedad pioneras de la computación se encuentran: la invención del ábaco para contabilizar año 1000 A.C, la invención de los logaritmos de napier en 1617, la regla deslizante de Ouhgtred en 1621, la calculadora mecánica de Schickard en 1623, la calculadora de Pascal en 1642, la maquina analítica de Babbage en 1833 y finalmente la creación de la Mark 1 en Harvard, la pionera de las computadoras actuales.

A partir de la creación de la primera computadora digital han existido diversas etapas de actualización y mejoría de los sistemas computarizados, con la invención del internet en 1993 se ha ido incorporando nuevas tareas y funciones en los ordenadores que ha conllevado a la creación de grandes redes cibernéticas que tiene la capacidad controlar el funcionamiento de la infraestructura económica, productiva, comunicativa, militar, educativa, productiva y científica de la humanidad.

En las últimas dos décadas, el acceso a los sistemas computarizados se globalizó y se convirtió en parte de la vida de todas las personas, con la invención de las redes sociales la humanidad alcanzó la era de la digitalización, permitiendo a cada persona del mundo tener acceso a la red al alcance de la mano, facilitando con ello una serie de

oportunidades que a elección del portador del aparato informático puede constituir una acción productiva o caer en conductas que podrían ser penalizadas por el marco jurídico de los países.

6.2. El internet, su origen, desarrollo histórico e importancia

La red informática mundial por la cual se transfieren datos e información conocida popularmente como el internet, es la vía de comunicación más utilizada actualmente y bajo la cual muchos de los sistemas industriales, militares, científicos o tecnológicos sustentan o sincronizan su funcionamiento.

Esta red tuvo diversas etapas evolutivas hasta convertirse en lo que actualmente conocemos y tenemos al alcance de la mano. El punto de partida de la era virtual se logró con el lanzamiento al espacio del primer satélite soviético, el Sputnik, en octubre de 1957, en pleno auge de la guerra fría, la industria militar estadounidense se vio en la necesidad de diseñar un método que permitiese la sincronización de sus comunicaciones, es así que en el año 1962 surge el proyecto denominado Internet, producto del interés de los Estados Unidos por crear una red de militar capaz de soportar las comunicaciones de esta esfera bajo las condiciones de un ataque nuclear procedente de la entonces Unión Soviética y otros países del campo socialista.

Entre 1962 y 1970, diversos contratistas militares estadounidenses diseñaron prototipos de redes de comunicación que permitían conectar en tiempo real los sistemas defensivos norteamericanos, sin embargo, aún el internet era exclusivamente una

herramienta de uso militar. En la década de los 80 y principio de los 90, el sistema precursor del internet moderno dejo de ser exclusivo para uso militar y las redes fueron evolucionando lograr la capacidad de intercambiar mensajería electrónica entre diversos sistemas computarizados que podían enlazarse de un país a otro volviendo las redes cada vez más amplias, robustas y capaces de servir a comunidades mayores.

A mediados de los años 90, el internet se convirtió en un fenómeno global, con el surgimiento de los motores de búsqueda como AOL, Yahoo y Ask, el acceso a la red electrónica llego a todos los hogares al alcance de un ordenador, actualmente todos los sistemas comunicativos y muchos de los sistemas de control de las industrias que mueven el mundo se encuentran conectados a la red, de igual manera, con el auge de la telefonía inteligente el uso de internet pasó de ser una herramienta a convertirse en una necesidad de todos los seres humanos.

Sin embargo los beneficios de estar conectados al entorno virtual también representa una oportunidad para que personas o grupos utilicen el entorno virtual para cometer hechos que transgreden la ley, obligando a los estados a promulgar leyes especializadas para enfrentar este fenómeno, en el caso de nuestro país, la Ley 1044, Ley Especial de Ciberdelitos la que contempla una serie de hechos punibles que pueden ser cometidos con el uso de medios electrónicos conectados a la red, sin embargo nuestro estudio se limitará al fenómeno del fraude informático.

6.3. Definición y reseña histórica de los delitos cibernéticos

En la vida cotidiana, todo ser humano define y delimita el rumbo de sus acciones por las normas dictadas por la ética, la moral, la costumbre y la ley, todos aquellos actos que contradice lo establecido por la ley es una conducta transgresora y por lo tanto punible, cuando esta circunstancia ocurre se puede afirmar que se está en la presencia de un delito.

Flores Salgado, (2014), p. 17 define: El derecho informático es un conjunto de principios y normas que regulan los efectos jurídicos de la relación entre EL Derecho y la Informática.

Para Julio Téllez Valdés, el Derecho Informático es... “Una rama de las ciencias jurídicas que considera a la Informática como instrumento (Informática Jurídica) y objeto de estudio (Derecho de la Informática).

Llinares (2012) define el Ciberdelito desde el sentido tipológico y normativo, al respecto nos refiere:

Si utilizamos el término de forma amplia, podremos definir como cibercriminal cualquier comportamiento delictivo realizado en el ciberespacio, entendiendo además por el mismo el ámbito virtual de interacción y comunicación personal definido por el uso de las tecnologías de la información y comunicaciones (TIC), y dando cabida, por tanto, a conductas cuyo contenido ilícito es nuevo y se relaciona directamente con los nuevos intereses o bienes sociales existentes en el ciberespacio, así como también a comportamientos tradicionalmente ilícitos en los que únicamente cambia que ahora se llevan a cabo por medio de Internet.

Delincuencia Informática

La define Gómez Perals como conjunto de comportamientos dignos de reproche penal que tienen por instrumento o por objeto a los sistemas o elementos de técnica informática, o que están en relación significativa con ésta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos.

La misma definición aporta Correa incidiendo en la Recomendación. Del Comité de Ministros del Consejo de Europa considerando que la delincuencia informática suele tener carácter transfronterizo que exige una respuesta adecuada y rápida y, por tanto, es necesario llevar a cabo una armonización más intensa de la legislación y de la práctica entre todos los países respecto a la delincuencia relacionada con el computador.

Los delitos cibernéticos tienen su origen con la creación de la computación y la proliferación del uso del internet, al globalizarse la red y convertirse en una herramienta de gran utilidad, los delincuentes vieron la oportunidad de utilizar la red para cometer delitos en los que no necesitaban hacer presencia física, escondiendo así su identidad y su ubicación, dificultando a los estados la persecución de un delito en el que el autor puede estar en un país y la víctima en otro, al respecto del surgimiento de los ciberdelitos

Quezada (2021) afirma: Con el surgimiento y desarrollo de la informática, la humanidad entera observa la creación del mundo virtual, cuyas actividades se realizan en el Ciberespacio, y se materializan estas con el uso de la computadora, teléfonos móviles, Tablet, herramientas que han incursionado en todos los aspectos de la vida diaria de los seres sociales, corporaciones, naciones o Estados, pero el uso indiscriminado, sin control, ha dado paso al surgimiento de conductas en mala parte, conductas nocivas y que tiene como fin atacar todo lo relacionado a los programas informáticos. (p.7)

6.4. El Fraude Informático

El fraude informático es toda aquella acción dolosa, mediante la cual haciendo uso de un medio electrónico se pretende guiar hacia el engaño a un tercero con la finalidad de obtener un beneficio económico, la definición jurídica de este delito se encuentra contenida en la ley especializada en la materia.

El delito de fraude informático, guarda una estrecha relación con el delito de estafa ya que muchas de las características de este último son utilizadas por el sujeto activo para guiar a la víctima hacia el engaño o la manipulación, sin embargo, la diferencia entre ambos es el uso de un medio electrónico o de comunicación como herramienta o como medio para consumar el delito.

6.5. Sujetos del Fraude Informático

En derecho penal, la ejecución de la conducta transgresora de la ley supone la existencia de dos sujetos, un sujeto activo y otro pasivo. Los sujetos activos y pasivos

del delito pueden ser uno o varios y a su vez pueden ser personas naturales o jurídicas, el bien jurídico protegido será el elemento localizador de los sujetos y de su posición frente al delito.

6.5.1. El sujeto activo

El sujeto activo es quien comete el hecho punible o realiza toda o una parte de la acción para la comisión de un delito. Las personas que los cometen poseen ciertas características que no presentan el denominador de los delincuentes comunes, los sujetos activos de esta ley tienen habilidades para el manejo de los sistemas informáticos y generalmente cuentan con la colaboración de personas que se encuentran en lugares estratégicos donde se maneja información sensible, o bien son hábiles en el uso de los sistemas informáticos.

Por otro lado tenemos el sujeto pasivo que es la persona natural o jurídica titular del bien que la ley protege y sobre la cual recae la actividad típica del sujeto activo. El sujeto pasivo o víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso del fraude informático, las víctimas pueden ser individuos, empresas, instituciones financieras, entes del estado, etcétera, todo aquel sujeto que usa sistemas automatizados para el almacenamiento y procesamiento de datos o que realiza transacciones financieras electrónicas, perfectamente puede ser una víctima más de este delito que presenta un acelerado crecimiento en el país.

6.5.2. El bien jurídico tutelado

El bien jurídico tutelado es todo bien o valor de la vida de las personas que es protegido por la ley, en este caso el bien jurídico tutelado es meramente relacionado a la integridad de los datos informáticos de las personas naturales o jurídicas, y entre sus principales aspectos tenemos los siguientes:

- La calidad, pureza e idoneidad de la información contenida en un sistema informático.
- La confianza de los ciudadanos en el correcto funcionamiento de los sistemas informáticos.
- La protección de los bienes y recursos financieros privados y estatales.

6.6. Modalidades del fraude informático

Existen diversas modalidades o métodos bajo los cuales los delincuentes informáticos pueden enmascarar sus acciones para lograr engañar a sus víctimas, dentro de las modalidades más conocidas están las siguientes:

Uso de datos falsos o engañosos: Conocido también como introducción de datos falsos, es una manipulación de datos de entrada al computador con el fin de producir o lograr movimientos falsos en transacciones de una empresa. Este tipo de fraude informático conocido también como manipulación de datos de entrada, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir.

Manipulación de programas: Esta modalidad consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas

rutinas y de forma encubierta utilizando un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

La técnica del salami: Es una técnica especializada que se denomina “técnica del salchichón” en la que pequeñas transacciones, se van sacando repetidamente de una cuenta y se transfieren a otra. Por lo general el defraudador introduce al sistema bancario unas instrucciones para que remita a una determinada cuenta los céntimos de dinero de muchas cuentas corrientes pertenecientes a sus víctimas.

Falsificaciones informáticas: Ocurre cuando se alteran datos de los documentos almacenados en forma computarizada o cuando las computadoras se utilizan para efectuar falsificaciones o alteraciones fraudulentas.

Manipulación de los datos de salida: Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos.

Pishing: Es una modalidad de fraude informático diseñada con la finalidad de robarle la identidad al sujeto pasivo. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños.

VII.MARCO JURÍDICO

La presente investigación tiene su génesis en la realización de un análisis del cuerpo de leyes existentes en nuestro país en las que se sustenta la investigación del fraude informático, en derecho un análisis legal debe abordar los aspectos significativos de cada ley y las facultades o limitaciones que estas confieren a los ciudadanos y al estado, haciendo uso de la pirámide de jerarquía de leyes encontramos que en el caso de los delitos informáticos la investigación y judicialización de estos se facultan de la siguiente manera:

La presente investigación tiene su génesis en la realización de un análisis del cuerpo de leyes existentes en nuestro país en las que se sustenta la investigación del fraude informático, en derecho un análisis legal debe abordar los aspectos significativos de cada ley y las facultades o limitaciones que estas confieren a los ciudadanos y al estado, haciendo uso de la pirámide de jerarquía de leyes encontramos que en el caso de los delitos informáticos la investigación y judicialización de estos se facultan de la siguiente manera:

La Constitución Política

La constitución de nuestro país establece derechos deberes y garantías para todos los ciudadanos nicaragüenses, dentro de estos derechos de manera implícita y explicita se encuentran los derechos a la privacidad de los datos, la protección de los recursos financieros de cada ciudadano y finalmente el derecho de cada persona a denunciar ante las autoridades cuando es víctima de un delito, de igual manera la constitución es la que faculta a las autoridades competentes para investigar, acusar y juzgar cuando

ocurra un delito y es de estas facultades brindadas por la constitución que posteriormente se desprenderán las leyes que rigen a cada una de estas instituciones, así como las leyes especiales y procedimentales que facultaran la persecución de un delito.

Nuestra Constitución Política en su artículo 97 faculta a la Policía Nacional para desempeñar su actuar, se establece que tiene por misión garantizar el orden interno, la seguridad de los ciudadanos, la prevención y persecución del delito

De igual manera nuestra carta magna en su artículo 159 da la facultad de juzgar delitos a los jueces estableciendo literalmente que las facultades jurisdiccionales de juzgar y ejecutar lo juzgado corresponden exclusivamente al Poder Judicial.

Es importante destacar que la Policía Nacional y la Corte Suprema de Justicia son instituciones clave en el sistema de justicia de Nicaragua, cada una con sus respectivas funciones y responsabilidades. La Policía tiene la tarea de llevar a cabo investigaciones iniciales y recopilar pruebas en casos de delitos, mientras que la Corte Suprema, como órgano judicial supremo, tiene la facultad de conocer y resolver los asuntos judiciales y garantizar que se aplique la ley de manera justa y equitativa.

Ley N° 872, Ley de Organización, funciones, carrera y régimen especial de seguridad social de la Policía Nacional.

Es la norma jurídica que rige el funcionamiento, la carrera y la función que desempeña la policía de Nicaragua en la prevención e investigación de los delitos, el artículo 2 de

esta ley, establece que la misión de esta institución es proteger la vida, la integridad y la seguridad de las personas y sus bienes, así como la prevención, la persecución e investigación del delito en general.

Es bajo estas facultades que la institución policial como órgano auxiliar de la justicia tiene el papel de investigar los ciberdelitos, entre estos el fraude informático, para ello la institución policial se vale de fuerzas especializadas y medios tecnológicos que coadyuvan a las actividades investigativas en contra de este flagelo de acelerado crecimiento en el país.

Ley No. 1042, Ley Especial de Ciberdelitos.

Esta ley vino a llenar el vacío existente en nuestro marco legal que por años careció de una ley especializada en la materia, si bien es cierto dada la similitud del fraude informático con otros delitos tipificados en el código penal, el uso de medios informáticos era visto como un medio para la comisión de los delitos y no como un delito en si, por ello con la puesta en vigencia de la ley de ciberdelitos se logró establecer una serie de figuras delictivas nuevas que no estaban contenidas en la ley penal.

En su artículo 1, establece que su finalidad y objeto es “la prevención, investigación, persecución y sanción de los delitos cometidos por medio de las Tecnologías de la Información y la Comunicación, en perjuicio de personas naturales o jurídicas”

De igual manera en el artículo 12, establece la correcta conceptualización del delito Fraude informático, del cual es objeto esta investigación, permitiendo al investigador policial y al fiscal acusador la correcta tipificación de la figura delictiva antes de formular la acusación ante el juez correspondiente.

Ley No. 406, Código Procesal Penal.

Regula los procedimientos y normas a seguir en el ámbito penal del sistema judicial nicaragüense. Su principal objetivo es garantizar el debido proceso, la protección de los derechos de los imputados, y el acceso a la justicia de las víctimas de delitos entre estos, el fraude informático.

Establece principios fundamentales que rigen el proceso penal en Nicaragua, describe las diferentes etapas del proceso penal, desde la denuncia, la fase de investigación, hasta llegar al juicio y la posible apelación de las sentencias, regula las medidas cautelares que pueden ser impuestas y establece la forma en que se debe desarrollara el juicio oral y público.

En el caso de la ley de ciberdelitos y en específico del delito Fraude informático, el código procesal penal brinda el mismo tratamiento y el mismo procedimiento que se debe realizar en con cualquier delito que se dirima en la parte penal.

Ley No.641, Código Penal

El código penal es un conjunto de normas jurídicas con las que se castigan los delitos. El código penal establece los delitos y las sanciones o penas que corresponde por cometerlos.

Ley No. 561, Ley General de Bancos, Instituciones Financieras no Bancarias y Grupos Financieros.

Regula la actividad bancaria y financiera en el país, por medio de esta ley el estado establece los lineamientos y parámetros que el sistema bancario debe cumplir y aplicar a sus clientes para un correcto funcionamiento y para garantizar la estabilidad económica del país, en el caso del delito en el que se basa el presente estudio , la ley de bancos es un elemento importantísimo ya que generalmente las principales víctimas del fraude informático son clientes de los distintos bancos y es con la aplicación de esta ley que el estado puede obligar al sistema bancario a aplicar medidas más eficientes para proteger los datos de sus clientes y evitar que estos sean víctimas de este delito.

Ley No. 787, Ley de Protección de Datos Personales.

Esta ley tiene como objeto la correcta protección y preservación de los datos personales que las instituciones públicas y privadas tienen de los ciudadanos y sus clientes, como es plenamente conocido en al caso de la ley de ciberdelitos se deja establecido que los datos digitales que de los ciudadanos deben preservarse correctamente, cuando ocurre el delito de fraude cibernético, muchas veces los datos personales y financieros de la víctima son obtenidos de manera ilegal para usarse como un medio para la consumación del delito, es ahí que existe una estrecha relación entre la ley de ciberdelitos y la ley anteriormente mencionada.

Ley No. 182, Ley de Defensa de los Consumidores y su Reglamento

Esta ley, fue creada para proteger los intereses legítimos de los consumidores frente a los abusos o violaciones de las empresas que prestan un servicio, entre estos el sistema bancario del país, en el caso de las víctimas del fraude informático, la ley de defensa del consumidor puede aplicarse en aquellos casos que se demuestre que el delito se produjo por la negligencia de alguna institución financiera, en ese caso la victima tiene el derecho de responsabilizar civilmente a la institución que propicio o facilito las condiciones para la comisión del delito.

VIII. JUSTIFICACIÓN

La presente investigación pretende desde el punto de vista jurídico realizar un análisis que arroje claridad sobre la efectividad de la ley de ciberdelitos en Nicaragua en el enfrentamiento al fraude informático en la ciudad de Managua, este trabajo es pertinente y de gran importancia ya que el delito estudiado representa una amenaza cada vez más frecuente y sofisticada en nuestro país, afectando tanto a individuos como a instituciones.

La comprensión y evaluación de la efectividad de la legislación vigente en la lucha contra este tipo de delito permitirá identificar posibles vacíos legales, incoherencias o debilidades en la normativa. Además, este análisis brindara recomendaciones para fortalecer la legislación y mejorar los mecanismos de prevención, persecución y sanción a las personas comisores del delito, contribuyendo así a la protección de los ciudadanos, la seguridad de la información y la confianza en los sistemas electrónicos en Nicaragua.

Del mismo modo, este trabajo tiene una relevancia social significativa. Al comprender y evaluar la efectividad de la legislación existente, esta investigación puede tener los siguientes impactos sociales: Protección de los ciudadanos al proponer mejoras y medidas de protección más efectivas para salvaguardar los derechos e intereses de las personas frente al fraude informático; respuesta efectiva, al proponer mejoras en los mecanismos de respuesta y finalmente es relevante socialmente ya que de esta

investigación podría derivarse la base para el fortalecimiento del marco legal con recomendaciones concretas para mejorar la legislación existente.

Estas recomendaciones podrían ser consideradas por los legisladores y las autoridades competentes para la actualización y mejora de la ley.

Finalmente, la presente investigación tiene implicación práctica, ya que con el presente trabajo se pretende generar un producto y este producto se basará en la propuesta de medidas acertadas, especificas, tangibles y aplicables a la legislación y a la realidad nicaragüense con la finalidad de mejorar la capacidad de respuesta estatal en la persecución, prevención y judicialización del fraude informático.

IX. DISEÑO METODOLÓGICO

9.1. Paradigma

El hombre es un ser abierto y capacitado para construir su realidad, así como su propio conocimiento de la realidad “el sujeto construye el conocimiento de la realidad a través de los mecanismos cognitivos de que dispone. De manera que el conocimiento se logra a través de la actuación sobre la realidad, experimentando con situaciones y objetos y, al mismo tiempo, transformándolos” (Araya, et al., 2007, p.77).

Se seleccionó el paradigma constructivista: Con la presente investigación, se pretende realizar una propuesta de medidas alcanzables, accesibles y pertinentes que pueden ser utilizadas por los legisladores, las autoridades competentes, las instituciones financieras afectadas y las victimas de fraude informático para ejecutar acciones que mejoren la investigación y prevención de este delito.

9.2. Tipo de estudio

En los estudios descriptivos se busca especificar las propiedades y las características del fenómeno. “Es decir, únicamente pretenden medir o recoger información de manera independiente o conjunta sobre los conceptos o las variables a las que se refieren, su objetivo no es indicar cómo se relacionan éstas” (Sampieri, 2014, p.92).

La presente investigación es exploratoria, dado que la temática del fraude informático en Nicaragua no ha sido estudiada previamente y descriptiva porque tiene como objetivo analizar la ley 1042: “Ley especial de ciberdelitos” y su eficacia en la prevención e investigación de los delitos cometidos por medio de las Tecnologías de la

Información y la Comunicación, en perjuicio de personas naturales o jurídicas. Este estudio se basa en el análisis de casos para identificar los aspectos positivos y las brechas existentes en la aplicación de la ley.

9.3. Enfoque de la investigación

“Los métodos mixtos representan un conjunto de procesos sistemáticos, empíricos y críticos de investigación e implican la recolección y el análisis de datos cuantitativos y cualitativos, así como su integración y discusión conjunta, para realizar inferencias producto de toda la información recabada y lograr un mayor entendimiento del fenómeno bajo estudio” (Sampieri, 2014, p.546).

La presente investigación es de enfoque mixto, los elementos de tipo cualitativo se aplican en el proceso de plantear el problema investigado, en la elaboración de un marco teórico y un marco jurídico y en el análisis de las características y las cualidades del fenómeno estudiado mediante el estudio de expedientes de caso, los elementos que corresponden al enfoque cuantitativo utilizados para dar respuesta al planteamiento del problema se realizaron mediante recolección de los datos y la aplicación de un instrumento para darle un valor numérico a la investigación, ejecutándolo bajo el método de muestreo aleatorio simple no probabilístico empleando para este fin la encuesta.

La utilización de este enfoque permitió la realización un análisis exhaustivo de las características del fenómeno estudiado y a la vez la medición de la percepción que las

víctimas de este delito tienen respecto a la eficacia de la ley en estudio y es en base a los resultados obtenidos que se brindarán los aportes y recomendaciones para mejorar los aspectos perseguidos en los objetivos de la investigación.

9.4. Población y muestra

9.4.1. La población

La población no sólo depende de los objetivos de la investigación y la calidad de la selección no depende de la cantidad. “La calidad de un estudio no se refleja por tener una población más grande; la calidad de un trabajo investigativo radica en delimitar claramente la población con base en el planteamiento del problema” (Sampieri, 2014, p.568).

En la presente investigación la población está comprendida por el universo al que denominaremos “victimas del fraude informático”, estas serán personas identificadas por medio del estudio de expedientes de los casos judicializados y de aquellas que en búsqueda de acceso a la justicia hayan interpuesto denuncias en la ciudad de Managua durante el primer trimestre 2023.

Según cifras aportadas por el departamento de investigación de delitos informáticos de la Dirección de Auxilio Judicial de la Policía Nacional, en el primer trimestre del año en curso en la ciudad de Managua, doscientas personas formularon denuncias de fraudes informáticos, esta cifra constituye nuestra población.

9.4.2. La muestra

El tipo de muestra tomada fue seleccionada por conveniencia, los sujetos del muestreo deben cumplir con las mismas características y deben ser parte de las víctimas de fraude informático que constituyen la población. Dado que la población está constituida por 200 personas que presentaron denuncias ante la policía nacional en la ciudad de Managua en el primer trimestre 2023 la muestra seleccionada será de 20 personas, el muestreo buscara obtener datos que permitan medir eficazmente el grado de respuesta que la muestra ha recibido de las autoridades en sus respectivos casos.

9.5. Métodos, técnica e Instrumentos de recolección de Datos

9.5.1. Técnica e instrumentos de recolección de datos

Dado que el presente trabajo investigativo plantea la realización de un estudio de casos, la técnica de recolección de datos se realizará por medio de la observación, los resultados de la misma se plasmarán en una bitácora donde el investigador reflejará los aspectos importantes detectados en el estudio de expedientes que permitan responder plenamente al problema de investigación. Los expedientes a estudiar se obtuvieron del archivo de expedientes investigativos de la Dirección de Auxilio Judicial, instancia competente en la investigación de este delito, del mismo modo, se aplicó entrevista con preguntas abiertas a un experto en la investigación de este delito para obtener una visión más acertada de las características y cualidades del fenómeno en investigación.

Como técnica secundaria de la investigación se eligió la encuesta, esta lleva preguntas cerradas y consta de tres puntos. El primero, busca de manera introductoria conocer si

el encuestado conoce la existencia de la ley de ciberdelitos y su reciente aplicación. En el segundo punto, se busca conocer y evaluar la respuesta que las autoridades han brindado a la víctima de fraude informático y si logro la adecuada obtención de justicia. En el tercer punto se buscará evaluar la apreciación de las víctimas de fraude informático sobre la efectividad de la ley en la investigación, persecución, sanción y prevención del fraude informático.

9.5.2. Métodos

9.5.2.1 Método bibliográfico

La presente investigación tuvo su base teórica en la investigación bibliográfica, para ello se seleccionó un grupo de autores especialistas en derecho y en informática para lograr un acercamiento más directo al fenómeno estudiado, la descripción detallada de los autores consultados se encuentra plasmado en la referencia bibliográfica.

.

9.5.2.2 Método especializado

El método principal aplicado en la presente investigación es el análisis de los datos, en el estudio de casos, todos los aspectos contenidos en la bitácora de observación que respondan al problema de investigación serán sintetizados y plasmados en la discusión de los resultados con la finalidad de tener una correcta apreciación del nivel de efectividad de la ley, principal motivación de este estudio.

Del mismo modo, al aplicar la encuesta y posterior recolección de datos se utilizará el programa Microsoft Excel, en el que se ingresará la información recolectada, para

obtener el análisis de resultados reflejado en gráficos de barra, haciendo de esta manera un análisis numérico y porcentual más exacto y de fácil comprensión para el lector.

9.5.3. Matriz de operacionalización de variables.

Tema de la investigación: ANÁLISIS JURÍDICO LEY 1042: “LEY ESPECIAL DE CIBERDELITOS” Y SU EFECTIVIDAD EN LA INVESTIGACION AL FRAUDE INFORMÁTICO, ESTUDIO DE CASOS EN MANAGUA, PRIMER TRIMESTRE 2023					
Objetivos	Variables	Definición de la variable	Sub variables / categoría	Indicadores o variable operativa	Método, instrumento, técnica para recolectar información
➢ Identificar los factores que inciden positiva o negativamente en la efectividad de la aplicación de	Investigación de los casos de fraude informático	Procesos jurisdiccionales en el que las autoridades buscan garantizar la seguridad jurídica y la persecución y prevención de los delitos.	• Incidencia del delito • Procedimientos investigativos aplicados • Resultados del proceso investigativo	Porcentajes denuncias y sus resultados.	1 Entrevista abierta

la ley especial de ciberdelitos y su influencia en la investigación de los casos de fraude informático			• Factores internos y externos q influyen en el trabajo investigativo		
➢ Analizar expedientes investigativos de casos de fraude informático ocurridos en	Expedientes policiales de casos de fraude informático	Documento de carácter jurídico administrativo que contiene toda la información de un proceso investigativo.	• Reseñas de los casos estudiados. • Característica de las víctimas. • Características de los victimarios. • Apreciación de la	Porcentaje del total de 200 casos denunciados Se accedió	5 Bitácora

la ciudad de Managua durante el año 2023 para la identificación de la respuesta investigativa de las autoridades en los casos de fraude informático			repuesta de las autoridades competentes.	únicamente a cinco expedientes de casos investigados (criterio de la muestra teórica)	❖ 1Entrevista abierta
➢ Inquirir la percepción de las víctimas de este delito	Percepción de las víctimas del	Visión y criterio de cada individuo	• Percepción positiva.		

sobre la efectividad de la ley en prevención de los casos de fraude informático ocurridos en la ciudad de Managua durante el primer trimestre 2023	fraude informático sobre la efectividad de la ley	sobre una realidad individual	• Percepción negativa. • Aspectos a mejorar a percepción de las víctimas del delito ❖ Modalidades del delito	Cantidades de aprobación o desaprobación del trabajo policial en la investigación del fraude informático.	20 Encuestas cerradas

X. Análisis de datos

El análisis de los datos tuvo su génesis en la recolección de información con la aplicación de una entrevista abierta a funcionario experto, la implementación de veinte encuestas a víctimas del delito y el análisis de datos vitales encontrados en expedientes investigativos de casos en concreto plasmados en bitácoras.

10.1. La investigación policial en los casos de fraude informático

Constitucionalmente se encuentra establecido el papel que desempeña la Policía Nacional para salvaguardar el orden interno en el país, así como la prevención y persecución del delito en todas sus modalidades. La ley de funciones y carrera policial establece el ordenamiento interno de la institución, delegando a la Dirección de Auxilio Judicial- DAJ, la responsabilidad de realizar todos los actos investigativos en los hechos delictivos consumados como órgano auxiliar del sistema de justicia del país; para el cumplimiento de su función jurisdiccional la DAJ, se divide en siete departamentos especializados, entre estos el departamento de investigación de delitos informáticos.

Fundado en el año 2020 a raíz de la aprobación de la ley especial de ciberdelitos, el departamento de Investigación de delitos informáticos tiene como función la investigación de todos los delitos tipificados en esta ley, practicando todas las diligencias necesarias para la comprobación de los delitos, la detención de los investigados y la elaboración del expediente investigativo policial que servirá como insumo al Ministerio Publico para formular la acusación al juez competente.

Mediante entrevista aplicada al jefe del Departamento de Investigación de delitos informáticos Capitán Corea (2023) afirma que:

La investigación de los casos de fraude informático tiene su punto de partida en la denuncia formulada por las víctimas, en el caso de Managua la competencia en la investigación de este delito recae en los detectives policiales de la DAJ, quienes poseen las habilidades y competencias técnico- científicas para investigar este tipo de casos, para ello practican un sinnúmero de diligencias policiales con la finalidad de descubrir a los hechores, capturarlos, recolectar indicios y piezas de convicción, estructurar el expediente investigativo policial y una vez finalizados los actos investigativos remitirlos al MP para su siguiente etapa en la vía judicial penal.

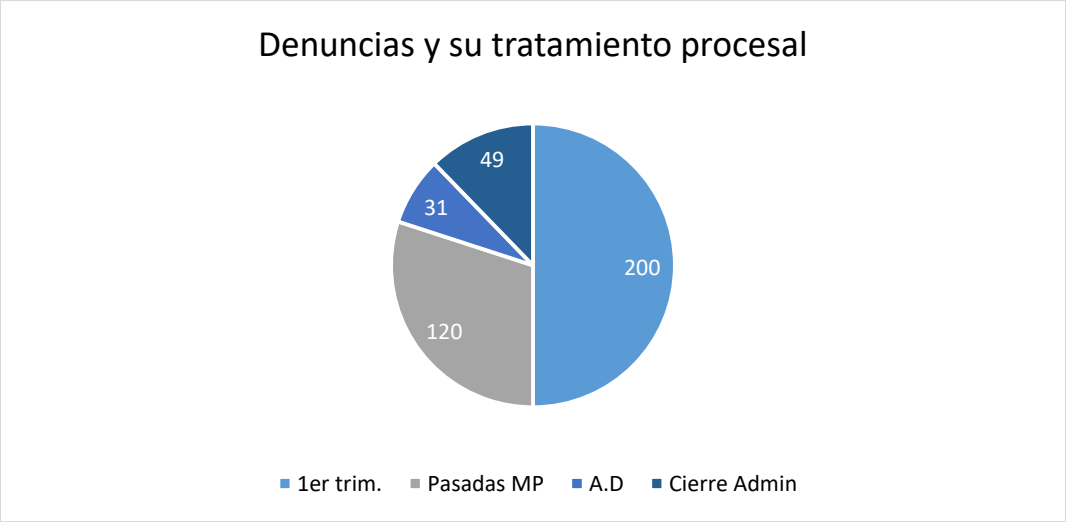
10.1.1. Incidencia del fraude virtual en la ciudad de Managua durante el primer trimestre 2023

Respecto a la incidencia del delito y el tratamiento investigativo de las denuncias de fraude informático recabadas por los detectives DAJ, Corea (2023) manifiesta:

Los delitos informáticos en nuestro país no es algo que la población denuncia de manera cotidiana, debido a que es una materia relativamente nueva y hay desconocimiento de muchos conceptos que permitan a la población discernir y estar claro de la seguridad de sus datos e identificar aquello que lo hace vulnerable en el ciberespacio que los hace ser víctima de delitos, a raíz de la aprobación de la ley en el año 2020 el número de denuncias fue relativamente bajo en comparación con otros delitos como por ejemplo la estafa; sin embargo, en el primer trimestre del año en curso el número de denuncias en la ciudad de

Managua se elevó significativamente respecto a todo el periodo anterior llegando en solo tres meses a recabarse 200 denuncias de las cuales 120 fueron expedientadas y pasadas al MP, en 31 de estos casos el autor no se identificó por ser extranjero y los restantes 49 casos fueron cerrados administrativamente por desistimiento de las víctimas.

Grafico. 1 Denuncias recibidas en el departamento de investigación de delitos informáticos, primer trimestre 2023.



10.2. El expediente investigativo policial en los casos de fraude informático

Una vez interpuesta la denuncia, el detective policial debe iniciar el proceso investigativo y realizar las diversas diligencias mencionadas en el capítulo anterior, todas estas diligencias deben organizarse y estructurarse en orden cronológico para dar forma al informe policial que será elevado al MP para que formule su denuncia al juez, este expediente debe confeccionarse acorde al procedimiento establecido por el

Sistema Automatizada de Investigación Policial en adelante SAIP y debe resguardarse tanto física como digitalmente.

Respecto a los elementos que deben dar forma al expediente policial Policía Nacional (2010) define:

> El expediente policial contendrá toda la información que se produzca durante el desarrollo de la investigación policial entre estos: informe de investigación policial, la denuncia, el acta de inspección de la escena del crimen, croquis y foto tablas ilustrativas, actas de detención, órdenes de allanamiento, actas de resultado de allanamiento; acta de reconocimiento de personas, resultados de peritajes y resultados de valoraciones medico legales cuando la situación lo amerite (p.62)

10.2.1. Caracterización de las víctimas y victimarios en los casos de fraude informático

A criterio del entrevistado, el patrón común bajo el cual pueda establecerse una relación entre las víctimas de fraude informático quienes más resaltan son los emprendedores que desarrollan sus actividades comerciales en línea, hecho que los hace más vulnerables a ser víctimas de este delito; sin embargo, amas de casa, particulares, profesionales y ciudadanos en general que realizan transacciones en línea o que poseen cuentas bancarias y hacen usos de ellas en el entorno digital han sido víctimas de este delito.

Respecto a los victimarios si existen factores determinantes en la actividad delictiva que estos realizan, los comisores de este delito; casi en su totalidad son personas con

experiencia y preparación en el manejo de sistemas informáticos y bancarios o tienen acceso a bases de datos empresariales con información personal que luego utilizan para convencer a sus víctimas que son funcionarios reales, cuando en realidad solo usan la información para engañar a las personas y bajo ese engaño logran que la misma victima sea quien facilite sus datos vitales con los cuales pueden extraer sus recursos financieros.

Otro aspecto relevante detectado en los comisores de este delito, Corea (2023) sostiene:

En muchos de los casos investigados, se ha detectado que la mayoría de los autores del delito son extranjeros, por lo general estos son miembros de grupos organizados en las cárceles de Costa Rica, Venezuela y Ecuador y se dedican a realizar llamadas por medio de la aplicación WhatsApp a números al azar de ciudadanos nicaragüenses a quienes se les identifican como funcionarios de los diversos bancos mencionando que les llaman porque hay una alerta en el sistema bancario, en algunas ocasiones por el desconocimiento de la población los ciudadanos caen en la trampa y en el transcurso de la llamada terminan brindándole todos los datos de su cuenta al delincuente, quien procede con el apoyo de cómplices a transferir el dinero de la víctima a múltiples cuentas en el extranjero y cuando la víctima se percata su dinero ya desapareció.

Los hechos afirmados por el entrevistado son reales y se verificaron en el análisis de expedientes de casos en concreto que desarrollaremos en el siguiente capítulo.

10.3. Breve reseña de los casos en los expedientes estudiados

Para la realización de este estudio, se seleccionaron como muestra cinco expedientes policiales de los casos investigados durante el primer trimestre del año 2023. El estudio de estos expedientes permitió observar la ejecución de todas las diligencias investigativas establecidas por el manual policial de investigación de delitos y su aplicación a casos concretos de fraude informático, acción que permitió comparar si lo manifestado por el experto entrevistado en el capítulo anterior corresponde a la realidad reflejada en los expedientes estudiados, comprobando como verdaderos todos los hechos manifestados por el experto en la entrevista, he aquí una breve descripción de los hechos observados en los expedientes analizados:

Expediente A-0162-2023-00137: En este caso el denunciante manifiesta que, en el mes de marzo 2023, publicó en la plataforma Marquet place de Facebook la venta virtual de prendas de vestir para dama facilitando su número de teléfono para contacto de potenciales clientes. Horas después de realizada la publicación fue contactado por una persona que manifestó ser originaria de Jalapa y que estaba interesada en adquirir varias prendas de vestir, en el transcurso de la conversación; el victimario selecciono una gran cantidad de prendas de vestir y la víctima le facilito un número de cuenta bancaria para que se le realizara el pago de los productos por medio de un deposito, acordando que una vez realizado el pago de las prendas se presentaría a la tienda de la víctima un delivery que se encargaría de recibir los productos.

Transcurridos unos minutos, el victimario contactó nuevamente a la víctima y le envió fotografía de un boucher de depósito bancario manifestando que el delivery se encontraba en la tienda y que necesitaba que los productos fueran entregados brevemente por que debían ser trasladados a la terminal de buses del mercado mayoreo para ser enviados hasta jalapa, por lo que la víctima procedió a entregar todos los productos sin asegurarse de que el deposito ya estuviera reflejado en su cuenta bancaria. Transcurrido un tiempo procedió a verificar su banca en línea y observo que el deposito no estaba reflejado por lo que realizo una llamada telefónica al número del supuesto cliente y este ya se encontraba desactivado por lo que llamó al banco y le manifestaron que ningún deposito se había realizado a su cuenta, recomendándole proceder a interponer la respectiva denuncia.

Con esta narración de los hechos formulada en la denuncia por la víctima y el número telefónico con el que el victimario se contactó, el investigador policial procede a realizar diligencias investigativas en búsqueda de esclarecer el caso, una de estas diligencias es la solicitud formal de oficio judicial para que la empresa de telefonía celular proporcione los datos del propietario del número telefónico usado para cometer el delito, en este caso en específico el número telefónico no tenía ningún registro que permitiera identificar al usuario, por lo que el expediente se encuentra en condición de autor desconocido, hecho que conlleva al estancamiento de la investigación y al posterior cierre administrativo de la misma.

Expediente A-0162-2023-00045: En este expediente, el denunciante manifiesta que el día 06-01-2023 se presentó a un negocio X, ubicado en un reconocido centro comercial de Managua. Durante su estancia en el local, el denunciante manifiesta que consumió alimentos y algunas bebidas alcohólicas junto a sus tres acompañantes. Al concluir el consumo procedió a hacer uso de su tarjeta de crédito para cancelar la cuenta, entregándosela al mesero quien se retiró a caja y se presentó con el respectivo boucher que acreditaba el pago de la cuenta.

Transcurrida una semana, al revisar su estado de cuenta observó que en este se reflejaban un sinnúmero de compras que nunca realizo, entre estas compras se encontraban consumo en locales de comida y compras en línea paginas como Alibaba y Shein por un monto de diez mil seiscientos córdobas, por lo que procedió a comunicarse con su banco para hacer el reclamo correspondiente, siendo notificado por la institución financiera que presentase la denuncia ante la Policía Nacional.

En este caso, el detective policial luego de recabar la denuncia solicito al judicial oficio para que la institución bancaria brindara información sobre la fecha y los lugares donde fueron realizadas las compras, con esa información procedieron a solicitar videos de vigilancia de los locales y en base a esos indicios recabados pudieron capturar a los investigados.

Expediente A-0162-2023-00134: En esta denuncia, la victima menciona que el día 21-01-2023, recibió un mensaje vía WhatsApp de un numero con foto de perfil con el emblema de un banco X, el mensaje era enviado por un supuesto agente del

departamento de seguridad financiera del banco en cuestión, manifestándole que el sistema bancario en línea reflejaba una alerta de transacción sospechosa por lo que necesitaban validar si esa transacción verídicamente la había realizado el, al responderle que no había realizado ninguna transacción bancaria reciente, el supuesto agente bancario menciono que necesitaba hacerle varias preguntas de seguridad para cancelar la transacción y que para este fin le enviaría un formulario y un enlace a la plataforma bancaria para confirmar los datos, procediendo la victima a seguir paso a paso el llenado del formulario con la asesoría del supuesto agente.

Una vez que finalizo el llenado del formulario, el supuesto agente le menciono que por seguridad la banca en línea en el teléfono de la víctima se cerraría por unas horas y que luego se actualizaría, procediendo a cortar la llamada. Sin embargo, pasaron las horas y la banca en línea permanecía sin darle acceso a la víctima, por lo que procedió a dirigirse a una sucursal del banco X y al plantear la situación el agente procedió a revisar, notificándole casi la totalidad de los fondos habían sido transferidos a diversas cuentas

La investigación de este caso fue sumamente compleja, el banco involucrado por orden judicial suministro la información de los propietarios de las cuentas a las que se les deposito el dinero de la víctima y con la detención de estos se determinó que sin conocer del hecho y de manera aislada todos los involucrados bajo engaño facilitaron sus cuentas a conocidos de origen costarricenses que les habían pedido el favor de recibirles dinero. Este caso es una de las evidencias que en esta figura delictiva existe

la participación de grupos organizados desde el exterior que usan esta modalidad del delito para operar en nuestro país.

Expediente A-0162-2023-00006:

Las circunstancias de este caso son similares al anteriormente descrito, en la denuncia la victima menciona que el 04-01-2023 recibió llamada telefónica en la que una dama manifestó ser agente de un banco X y que se encontraban realizando una encuesta para medir el nivel de seguridad de su plataforma bancaria, la victima al ser cliente de ese banco creyó que la llamada era autentica y fácilmente brindo sus datos personales y bancarios, dándose cuenta casi a lo inmediato que su banca en línea no le permitía acceso, por los que procedió a cortar la llamada ya dirigirse a la sucursal bancaria más cercana donde le informaron que fue víctima de fraude y la remitieron a interponer la formal denuncia.

El desarrollo investigativo en este caso en específico sufrió estancamiento hasta llegar al cierre administrativo ya que, tanto el hechor como el número telefónico utilizado para cometer el hecho fueron rastreados hasta una cárcel costarricense.

Expediente A-0162-2023-00097: Al denunciar este hecho, la victima manifestó que en un grupo de compraventas de Facebook ofreció sus servicios como topógrafo certificado, colocando su número de teléfono y cuenta de correo como contacto para las personas interesadas. El día 06-02-2023 le llego un mensaje de WhatsApp desde un numero con prefijo nacional, el mensaje consistía en una supuesta promoción de aniversario de la ferretería X y conducía a un enlace en el que al darle clic redirigía a la

página de dicha ferretería en la que se anunciaba que a quienes le dieran me gusta a la página y llenaran un formulario podrían ganar una dotación de herramientas y materiales de construcción. La victima procedió a llenar el formulario y quedo en espera de ser notificado si resultaba ganador.

Unos días después se dirigió al cajero automático a retirar dinero y al acceder a su cuenta observo que se encontraba sin fondos, por lo que presento reclamo al banco y estos lo remitieron a poner formal denuncia.

La investigación de este hecho tuvo resultados satisfactorios, por medio de orden judicial la empresa telefónica facilito los datos y ubicación del número utilizado para cometer el delito, descubriendo que el hechor era un menor de edad que utilizo los recursos obtenidos para realizar compras de puntos para juegos en línea, en el desarrollo del caso investigativo la victima al parecer realizó un arreglo extrajudicial con los padres del menor, eliminando así la posibilidad de que el caso se ventilara en juzgados.

10.3.1. La respuesta policial en los casos de fraude informático estudiados

Para identificar la respuesta policial en casos en concreto se realizó análisis de cinco expedientes investigativos y se comparó lo afirmado en la entrevista realizada al Capitán Javier Corea, jefe del departamento de investigación de delitos informáticos DAJ, con lo practicado por los detectives policiales durante el desarrollo de las investigaciones anteriormente descritas, logrando conocer que en los casos de fraude

virtual al igual que en otros delitos los métodos investigativos son prácticamente similares a los ejecutados en los delitos comunes; sin embargo, existe un elemento indispensable que no debe obviarse en la investigación de este y todos los delitos tipificados en la ley de ciberdelitos y este elemento es el análisis informático forense de equipos electrónicos.

Del mismo modo en que el dictamen médico legal es vital para determinar mano criminal en un deceso, el análisis forense de equipos electrónicos es el elemento más importante para determinar la persona, el lugar, los métodos y hasta nexos entre varios hechores de ciberdelitos. Este análisis es realizado por peritos informáticos expertos del laboratorio de criminalística de la Policía Nacional y el dictamen emitido por estos tiene validez legal y es admitido como evidencia en todos los casos que son elevados a instancia penal.

Otras diligencias policiales practicadas por los detectives policiales y que tienen una gran importancia para el esclarecimiento de este tipo de hechos son la solicitud de información a bancos, a empresas telefónicas y a proveedores de internet, para conservar las formalidades legales requeridas estas solicitudes se realizan mediante oficios judiciales, lo que le da valor y respaldo legal a estas actuaciones en caso de que lleguen a ventilarse en un juicio.

Mediante el análisis de los expedientes de casos de fraude informáticos podemos afirmar que, en la investigación de los caos de fraude informático, la ley de ciberdelitos

es eficiente ya que la simple existencia de una tipificación delictiva obliga a la autoridad policial a brindar una respuesta cuando ocurre la conducta transgresora tipificada, por lo que en este punto la finalidad de la ley de fomentar la persecución de este delito se cumple cabalmente al momento que la autoridad competente inicia un proceso investigativo y el hecho que los detectives policiales practiquen un sinnúmero de diligencias para lograr esclarecer el delito es muestra de la voluntad de la autoridad policía de dar solución al fenómeno social que motivo la creación de la ley.

Entre las diligencias que predominan en los expedientes estudiados se encuentran las siguientes:

Tab. 1 Tabla de diligencias policiales indispensables practicadas en los expedientes analizados

Número de expediente	**Denuncia**	**Análisis Forense de E.L**	**Detenciones**	**Allanamientos**	**Informe policial al M.P**
A-0162-2023-00137	03-03-2023	No	No	No	Si
A-0162-2023-00045	06-01-2023	Si	Si	Si	Si
A-0162-2023-00134	21-01-2023	No	No	No	No
A-0162-	04-01-2023	Si	Si	Si	Si

2023-00006					
A-0162-2023-00097	06-02-2023	Si	Si	Si	Si

Los números de expedientes fueron cambiados para mantener la confidencialidad de los casos.

En el análisis de los expedientes se observó que en dos de los casos no se practicó algunas diligencias vitales que permitieran el esclarecimiento de los casos, esto ocurrió ya que los comisores del delito no pudieron ser identificados y la investigación policial arrojo que estos son de origen extranjero, aspecto que a criterio policial merma la capacidad de respuesta en estos casos.

10.4. Factores que influyen en la capacidad de respuesta policial en la investigación del fraude informático

Toda investigación policial encuentra obstáculos que merman o dificultan su resultado en mayor y menor medida, casi por regla general, estos obstáculos son generados por factores externos que no están relacionados con la labor institucional. Para superar estos obstáculos, el detective policial debe hacer uso de las herramientas legales y de las habilidades dadas por la capacitación y la experiencia para llevar su investigación a buen fin. En este sentido, Corea (2023) afirma:

> Durante el desarrollo de la investigación de los casos de fraude virtual siempre existen factores de origen externo que a veces limitan los resultados, la limitación principal de los resultados de la investigación es que en muchos de los casos los autores del delito son de origen extranjero, existen bandas organizadas en Costa

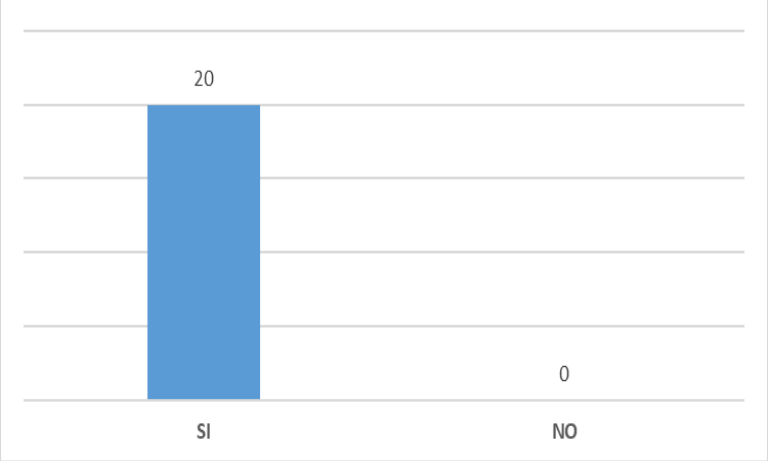
Rica o en Sur América que se dedican a realizar llamadas haciéndose pasar como agentes bancarios y en estas llamadas convencen a la víctima de brindar sus datos bancarios y una vez que los obtiene transfieren el dinero a cuentas en su respectivo país y extraen el dinero, el hecho que el autor sea extranjero dificulta su identificación y estanca la investigación. Otro factor que incide mucho es que casi siempre las victimas prefieren recuperar sus recursos y cuando el autor es detenido muchos prefieren mediar con su victimario y una vez que recuperan sus recursos desisten y el caso no llega a ventilarse en los juzgados.

A nivel interno, existen factores que influyen positivamente en los resultados de la investigación de este delito, entre los más importantes se pueden mencionar el enfoque sistémico policial, las coordinaciones institucionales, el alto grado de capacitación de los detectives policiales y la incorporación de modernos equipos tecnológicos en el laboratorio de criminalística con los cuales se realizan los análisis científicos de los aparatos electrónicos utilizados por los investigados.

10.5. La percepción de las víctimas del delito sobre la efectividad de la ley en la investigación y prevención del fraude informático.

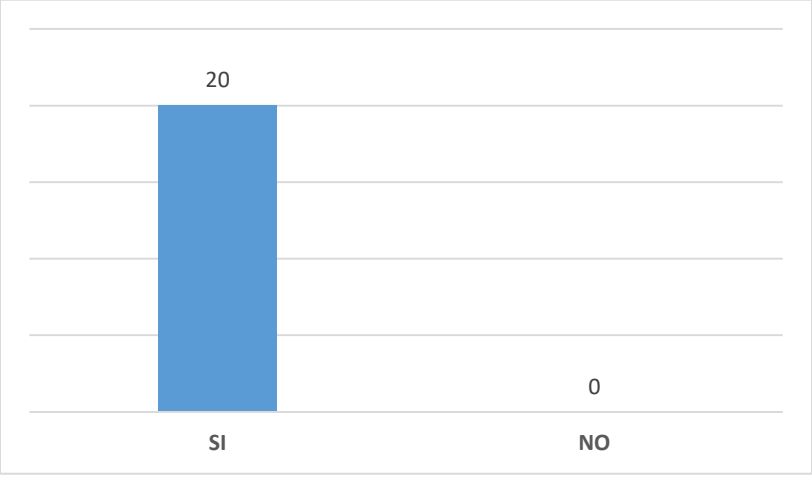
Para indagar la percepción de las víctimas se aplicó encuestas cerradas con opciones de selección múltiple con la finalidad de conocer a visión de los denunciantes sus consideraciones respecto al papel de la ley y las fortalezas que esta brinda a los investigadores policiales para desarrollar su trabajo investigativo, en este sentido los resultados fueron los siguientes:

Grafico. 2 Aplicación de encuesta exclusiva a víctimas del delito



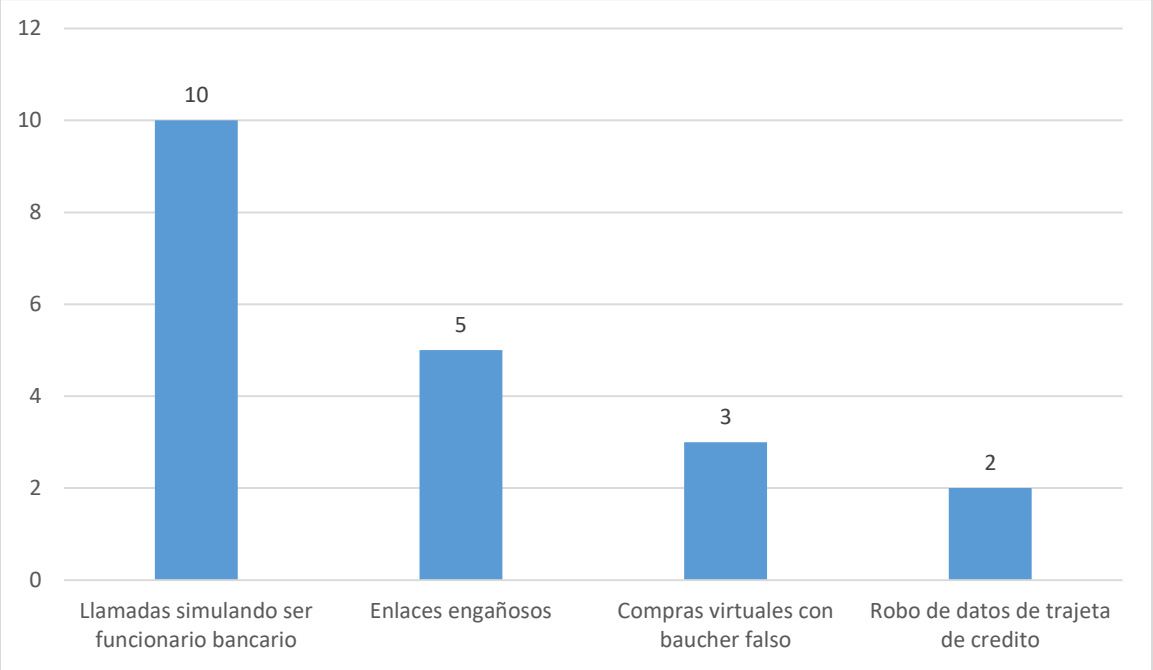
La encuesta se aplicó a 20 personas, el 100% de los encuestados confirmo haber denunciado haber sido víctima del delito fraude virtual en la ciudad de Managua en el primer trimestre 2023.

Grafico. 3 Conocimiento de las victimas sobre la existencia de la ley de ciberdelitos.



La totalidad de los encuestados manifestó conocer plenamente sobre la existencia de la ley y los delitos en ella tipificados.

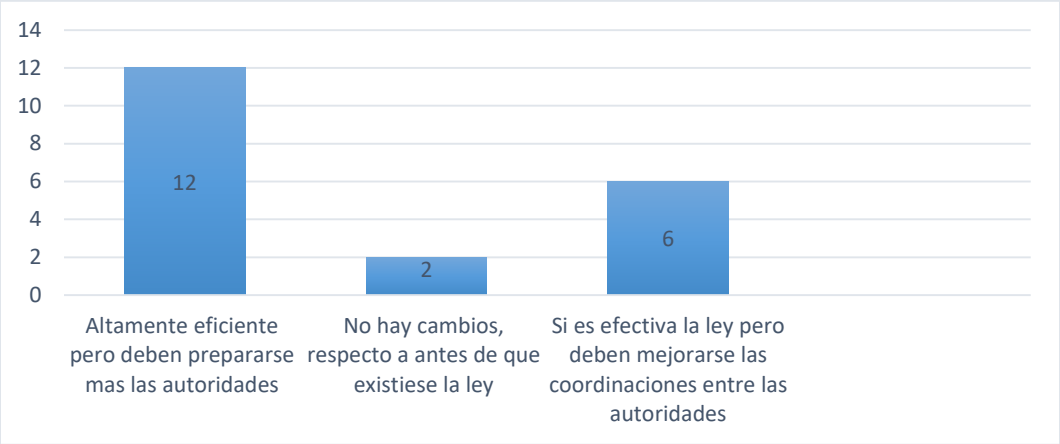
Grafico. 4 Modalidades de fraude virtual de las que fueron victima los encuestados



De los veinte encuestados, cuatro fueron las modalidades del delito de las que estos fueron víctimas, predominando las llamadas telefónicas engañosas en las que el comisor del delito simula ser un funcionario bancario para solicitarle a la víctima datos de sus bancas en línea y una vez obtenidos los datos transfieren los fondos a otras cuentas para extraer los recursos bancarios.

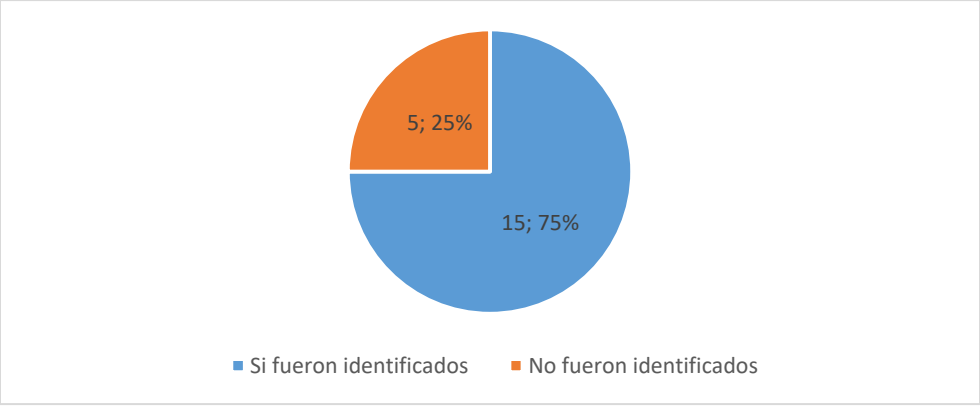
Los datos obtenidos en encuesta corresponden a la realidad observada en el desarrollo del análisis de expedientes ya que en los expedientes estudiados se reflejan estas modalidades del delito.

Grafico. 5 Percepción de los encuestados sobre el papel de la ley en la investigación y prevención del fraude informático



Del total de los encuestados, el 60 % menciona que la ley está siendo altamente eficiente en la investigación y prevención del delito, sin embargo, menciona que deben mejorarse la preparación y la coordinación de las autoridades.

Grafico. 6 Los autores del delito fueron identificados durante la investigación policial

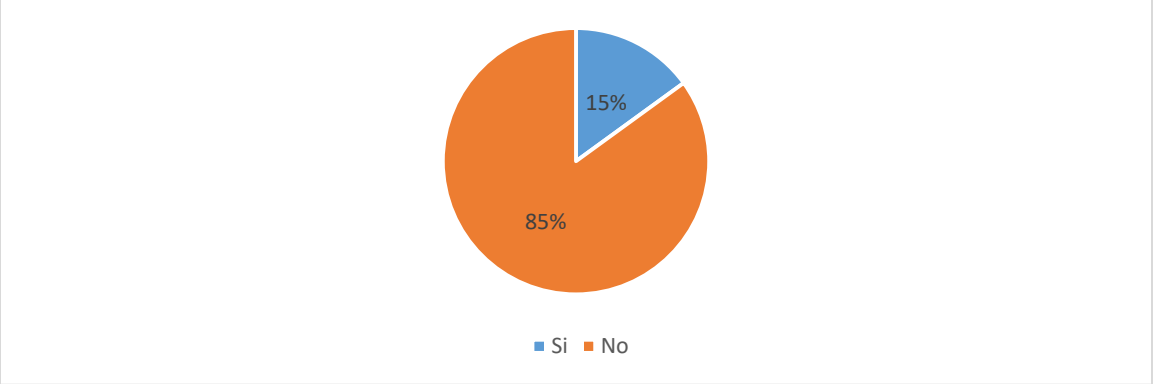


En relación a esta gráfica, el 75 % de los encuestados manifestó que en relación al delito del que fueron víctimas durante la investigación policial fueron identificados, el restante 25% manifiestan que no se logró identificar a los autores, siendo este aspecto uno de los principales obstáculos en la investigación policial.

Con los datos aquí obtenidos se demuestra que, aunque la investigación policial se desarrolle acorde a los procedimientos legales establecidos, la naturaleza del delito en estudio presenta desafíos que merman la capacidad de esclarecer los hechos, lo que corrobora lo manifestado por el experto al mencionar en entrevista que hay factores desfavorables entre estos el hecho de que la víctima no tenga contacto visual con el victimario o que este último opere a distancia desde el exterior.

Grafico. 7 La denuncia que interpuso fue tramitada hasta llegar a juicio

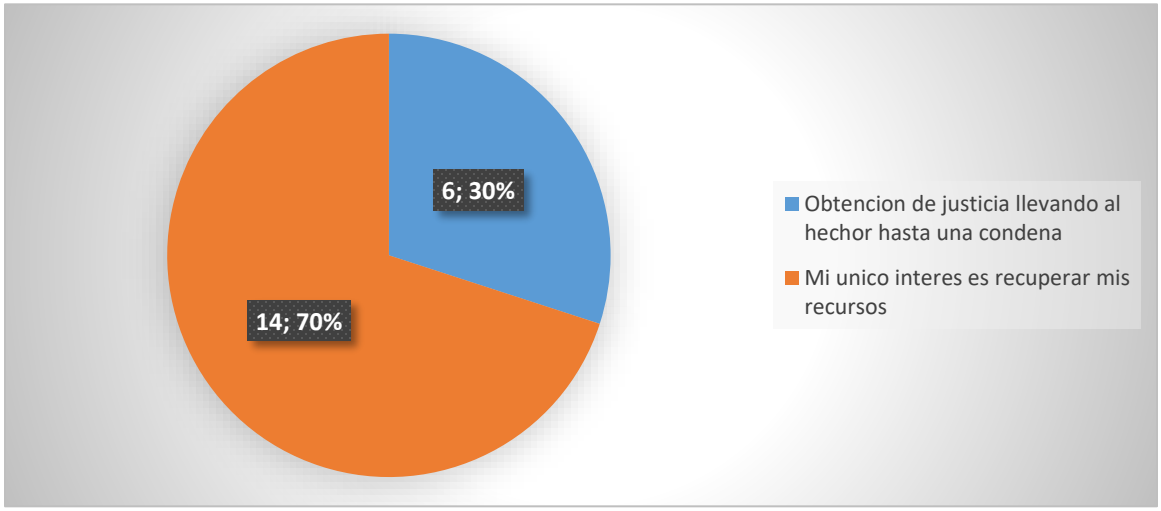
Grafico. 8



Del total de los encuestados 17 manifestaron que sus casos no llegaron a etapa de juicio y únicamente en tres de los casos la denuncia paso todas las etapas penales hasta llegar al judicial.

Esto demuestra el hecho de que este delito tenga una baja taza de judicialización el hecho que esto ocurra se debe a diversas circunstancias que serán ampliadas en la discusión de los resultados.

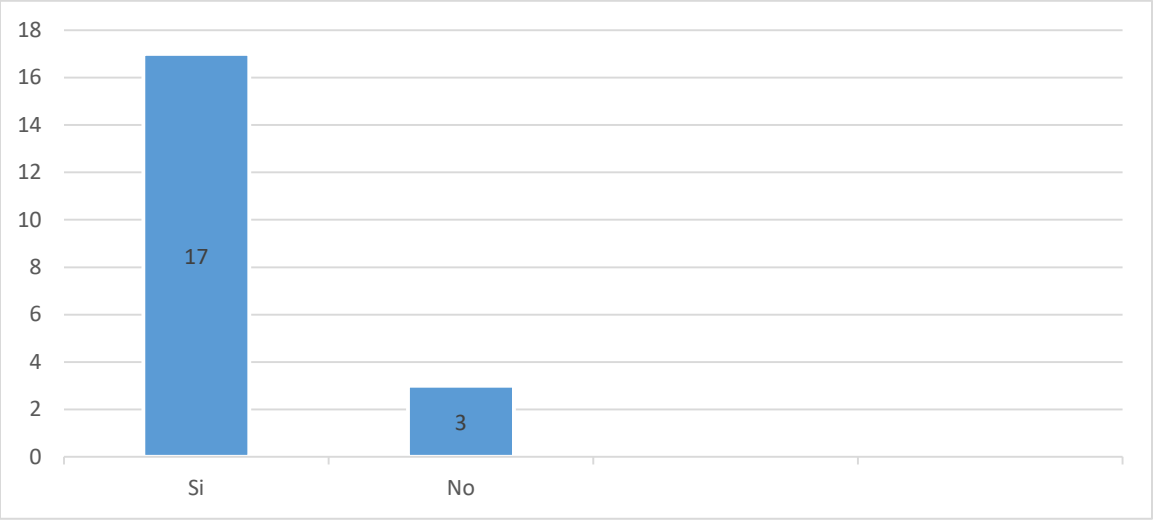
Grafico. 9 Propósito de los denunciantes respecto a su caso



Respecto a esta gráfica, al consultarle a los encuestados sobre el propósito de su denuncia, el 70% manifestó que únicamente tienen el interés de que con la denuncia recuperar sus recursos, el restante manifestaron el interés que el delito se procese y llegue a las instancias judiciales.

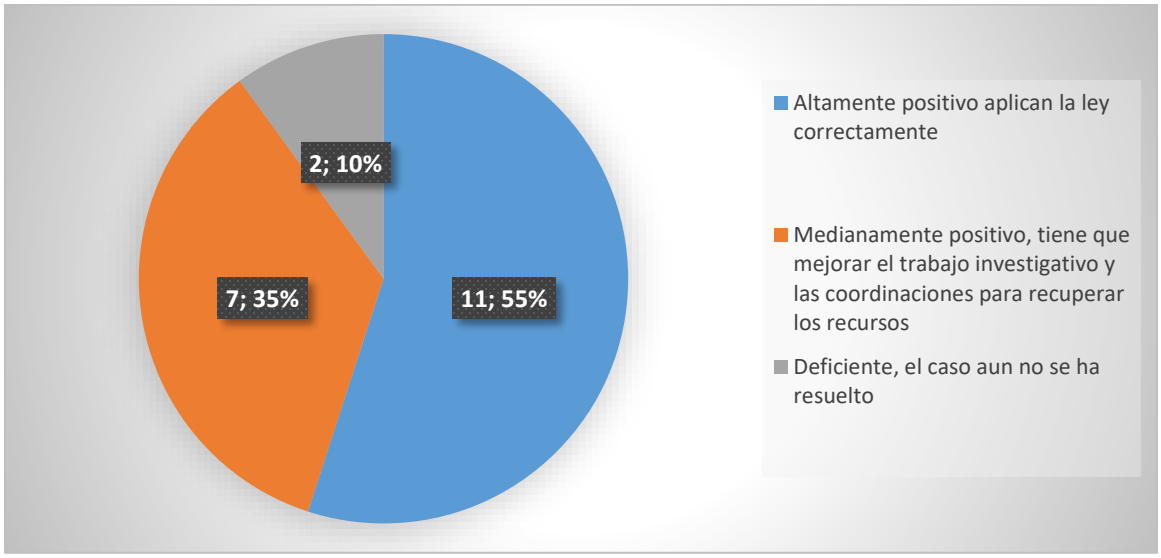
Estos datos guardan estrecha relación con la gráfica anterior y demuestra el por qué algunas de las víctimas al llegar a arreglo con sus victimarios desisten de sus denuncias acortando y limitando los resultados de las investigaciones.

Grafico. 10 Los recursos que financieros involucrados en el delito del que fue víctima, fueron extraídos de alguna entidad bancaria



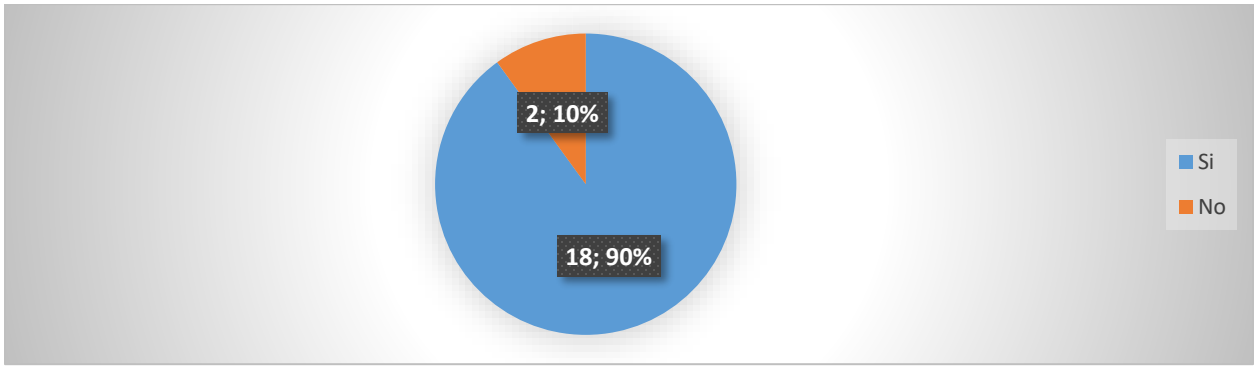
Al consultarle a los encuestados donde estaban sus recursos y si estos fueron extraídos de una entidad bancaria el 85% manifestaron que sí, el restante manifestó que no.

Grafico. 11 Cómo valora la actuación de la autoridad respecto a la aplicación de la ley en la investigación de los casos de fraude informático



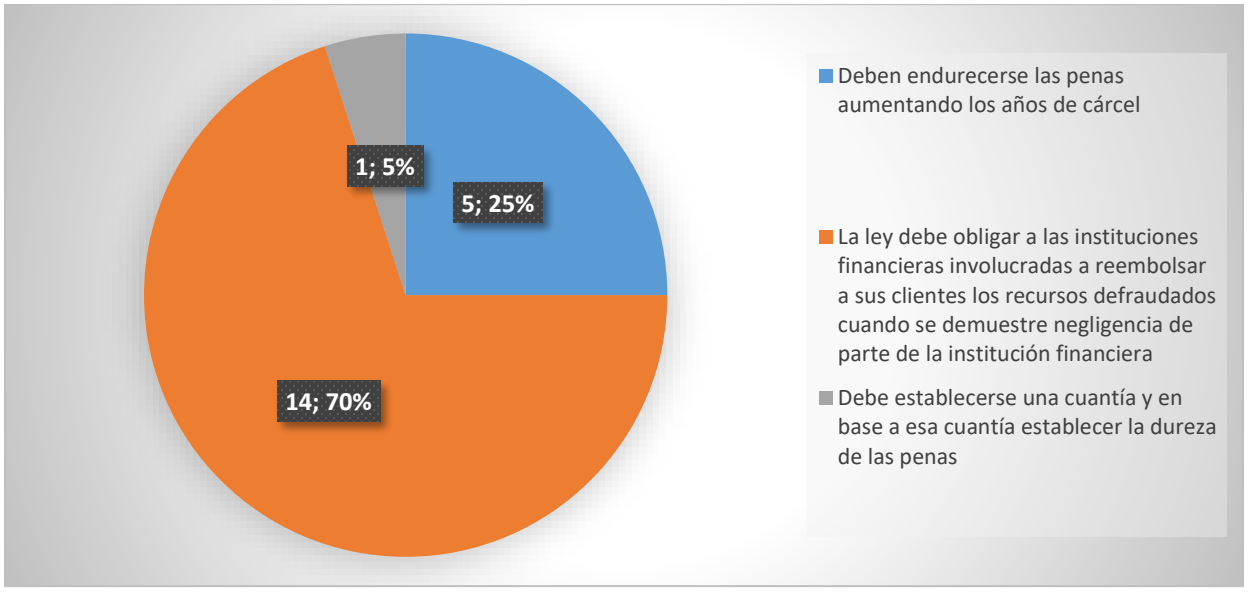
Respecto al gráfico anterior, al consultar a los encuestados su valoración de la aplicación de la ley en la investigación de este delito, el 55% la valora altamente positiva, el 35 % lo valora medianamente positiva y mencionan que aún hay aspectos que mejorar. El restante 10% valora deficientemente la labor investigativa respecto a este delito.

Grafico. 12 Consideran los encuestados que la ley de ciberdelitos contenga aspectos que deban ser mejorados o ampliados respecto al fraude informático



Al consultarle a los encuestados sobre si consideran que la ley de ciberdelitos tenga aspectos que deban en el futuro ser ampliados o mejorados, el 90% respondió que si consideran que a la ley deban en el futuro realizársele reformas que adicionen o amplíen los elementos actuales que esta contiene.

Grafico. 13 Elementos considera que deban ampliarse o mejorarse en la ley



Respecto a este gráfico, al brindarle a los encuestados la opción de seleccionar los aspectos que a su criterio deban adicionarse en la ley en un futuro, el 70% plantea que la ley debe obligar a las instituciones financieras a reembolsar los recursos que sus clientes pierden al ser víctimas de este delito.

XI. DISCUSIÓN DE RESULTADOS

Finalizado el análisis de los resultados de la entrevista, podemos concluir que la investigación policial de los casos de fraude informático nace a raíz de la denuncia interpuesta por las víctimas de este delito. La instancia competente para investigar estos hechos es la Dirección de Auxilio Judicial por medio del departamento de investigación de delitos informáticos, conformado por detectives policiales capacitados y con plena experiencia técnico científica para investigar este tipo de casos.

Todos los procedimientos investigativos son plasmados en un expediente de carácter administrativo en el cual se ordenan cronológicamente todas las actuaciones y diligencias realizadas por el detective policial, este expediente es vital para la posterior etapa del proceso penal, ya que es en base a este expediente que el Ministerio Público acusa ante el juez a los autores del delito.

A criterio del experto entrevistado, existen dos factores externos que limitan la capacidad de respuesta institucional para investigar este delito, uno de estos es que en muchos casos los autores del delito son extranjeros y al no existir contacto entre víctima y victimario la identificación de estos hechores se dificulta, estancando en muchos de los casos el avance de la investigación. Otro de los factores que incide negativamente es el hecho que muchas de las victimas llegan a mediación con el autor del delito y declinan de seguir con el proceso, impidiendo de esta manera que los casos se ventilen en la instancia judicial.

Del mismo modo, el experto manifestó que el delito en estudio no distingue categorías de personas; sin embargo, las principales víctimas son ciudadanos que se dedican a actividades comerciales en línea ya que, al colocar información de sus negocios en redes sociales los delincuentes toman esta información para utilizarla como anclaje y preparar condiciones para engañar a la víctima y robarle sus recursos financieros aplicando diversos métodos y modalidades de este delito.

Con la implementación del estudio de casos plasmados en bitácora se logró comparar lo afirmado por el experto en la entrevista con lo observado en los expedientes, concluyendo que estas afirmaciones son reales ya que en dos de los expedientes analizados la investigación policial se estancó ya que los hechores no fueron identificados y según lo afirmado por los denunciantes estos tenían acento extranjero.

De igual manera la implementación de la bitácora permitió identificar los métodos de investigación aplicados por los detectives policiales, siendo los predominantes la recepción de la denuncia, la remisión de equipos al experto forense, la aplicación de allanamientos, la captura de los investigados y la elaboración del informe policial para elevar el caso al Ministerio público.

Finalmente, la aplicación de encuesta permitió conocer la percepción de las víctimas de este delito respecto la efectividad de la ley en la prevención del delito, la percepción del trabajo investigativo policial, las modalidades de este delito más predominantes, así como los aspectos que deban mejorarse a futuro en la ley.

Referente a las modalidades más usadas por los delincuentes al cometer fraude informático, en el 50% de los casos las más utilizadas son las llamadas simulando ser

un funcionario bancario, el 25% fue él envió de enlaces engañosos por redes sociales, el 15% fueron compras en línea utilizando boucher de depósitos falsos y el restante 10% fue el robo de datos de tarjetas de crédito.

En lo concerniente a la apreciación positiva y negativa de los encuestados sobre el trabajo investigativo policial, el 55% lo valora como altamente efectivo, el 35% como mediamente efectivo ya que consideran que existen aspectos aún debe mejorarse y únicamente el 10% los considera deficiente porque sus casos aún no han sido esclarecidos.

Respecto a las consideraciones de los encuestados sobre que la ley de ciberdelitos contenga aspectos que deban ser mejorados o ampliados respecto al fraude informático, el 90% de los encuestados manifestó que si consideran que la ley debe ser mejorada en el futuro. En cuanto a los aspectos que los encuestados consideran que deben mejorarse en la ley, el 70% manifestó que la ley debe obligar a las instituciones financieras a reembolsar los recursos defraudados cuando se demuestre que el hecho ocurrió por vulnerabilidades sus sistemas para proteger a sus clientes, el 25% considera que deben endurecerse las penas establecidas en la ley y el 5% manifestó que la ley debería establecer una cuantía para determinar la gravedad del delito y en base a esa cuantía endurecer las penas.

XII.CONCLUSIONES

La aplicación de los instrumentos de recopilación de datos permitió la obtención de la información necesaria para conocer la falta de desconocimiento de algunas personas en los casos de ciberdelitos, siendo el problema la falta de información y el procedimiento que se realiza en estos tipos de delitos.

En base a los resultados obtenidos, al finalizar este proyecto de tesis de Licenciatura en derecho, se menciona las siguientes conclusiones:

Se logró identificar los factores que influyen positiva y negativamente en el desarrollo de la investigación de los casos de fraude informático ocurridos en la ciudad de Managua durante el primer trimestre 2023, determinando que los factores externos que no están bajo el control de la institución policial son los que reducen la capacidad de respuesta, uno de estos factores es que al ser un delito en el que la víctima no tiene contacto directo con el victimario y que muchas veces los hechores son extranjeros, las investigaciones se estancan y no generan resultados, otro de los factores es que al ser un delito donde existe un interés económico de por medio; las víctimas en muchas ocasiones solo pretenden recuperar sus recursos, por lo que llegan a mediación con su victimario y desisten de la denuncia, eliminando así toda posibilidad de elevar el caso a instancias judiciales.

La aplicación de entrevista al experto permitió conocer el desarrollo de la investigación de este delito, la plena capacidad científica de los investigadores expertos en este tema y la vital importancia del expediente policial como antesala de la acusación del Ministerio público ante judicial competente.

El estudio de casos en concreto permitió identificar los métodos y técnicas investigativas aplicadas por los detectives policiales en los casos de fraude informático, logrando conocer que una de las diligencias más importantes es el análisis forense de medios electrónicos, el resultado de este análisis emitido por un perito policial experto se convierte en una pieza de convicción vital para demostrar ante el judicial los hechos y permite la obtención de justicia a las víctimas.

La aplicación de encuesta a víctimas del delito, permitió conocer la percepción que estas tienen del trabajo investigativo policial en sus respectivos casos, logrando conocer que la percepción es mayoritariamente positiva y consideran que la ley es efectiva para prevenir la incidencia del delito, sin embargo, plantean algunos aspectos que su criterio deben tomarse en cuenta para futuras reformas o adiciones a la ley, predominando en este sentido, la posibilidad de que la ley obligue al sistema financiero a reembolsar a las victimas sus recursos y del mismo modo proponen que la ley establezca una cuantía y en base a esa cuantía se agrave el delito y por ende las penas que deban imponerse.

Finalmente, podemos afirmar que la hipótesis planteada se verifica como positiva, ya que en el desarrollo del presente trabajo investigativo se logró comprobar que la implementación de la ley de ciberdelitos ha venido a permitir a las víctimas del fraude informático un mejor acceso a la justicia, esta legislación permite a las autoridades implementar mecanismos legales para perseguir y prevenir este delito y a su vez, el simple hecho de la existencia de esta ley ha servido como medio disuasivo para que

quienes se dedican a ejecutar este acto delictivo, deberán abstenerse de hacerlo por las consecuencias legales que enfrentarían, por lo que podemos decir que la ley es efectiva ya que cumple su objeto de castigar los delitos cibernéticos en sus diferentes modalidades.

XIII. RECOMENDACIONES

Basado en los resultados obtenidos con la aplicación de los instrumentos de recolección de datos aplicados para dar respuesta a los objetivos de esta investigación se propone una serie de recomendaciones que deberán ser tomadas en cuenta en el mediano y largo plazo para futuras investigaciones relacionadas al delito en estudio, siendo estas las siguientes:

Fortalecimiento de la cooperación internacional: Dada la naturaleza transfronteriza en muchos casos de fraude informático ocurridos en la ciudad de Managua, así como la participación frecuente de hechores de origen extranjero, se recomienda fortalecer la cooperación internacional en la investigación de estos delitos principalmente con los países de mayor predominancia en los casos investigados. La institución policial, debe establecer mecanismos eficaces de colaboración con agencias de aplicación de la ley de otros países para mejorar la capacidad de seguimiento y persecución de los perpetradores.

Incentivar la denuncia y desincentivar la mediación: Con el objetivo de mejorar la tasa de denuncias y evitar la mediación que muchas veces corta el proceso legal, se sugiere implementar campañas de concientización dirigidas a las víctimas de fraude informático. Estas campañas deben destacar la importancia de denunciar y darle continuidad al proceso legal hasta llegar a juicio, resaltando el impacto negativo en términos de prevención del delito al fomentar en los hechores la normalización de la mediación como método para evitar una sentencia privativa de libertad

Reforzar la capacitación y mejorar la tecnología disponible para los análisis forenses de medios electrónicos: Dado que el análisis forense de medios electrónicos es crucial en

la investigación de los casos de fraudes informáticos, se recomienda continuar y fortalecer la formación de los detectives en estas técnicas. Además, es importante mantener actualizadas las herramientas y tecnologías utilizadas en el análisis forense para asegurar la efectividad y validez de los resultados periciales presentados ante los tribunales.

Revisión y mejora del marco legal: A raíz de las percepciones de las víctimas, se sugiere una revisión del marco legal relacionado con el fraude informático. Se debe considerar a futuro la inclusión en la ley de adiciones que obliguen al sistema financiero a reembolsar a las víctimas y establecer una escala de agravantes basada en la cuantía del fraude. Estas medidas podrían actuar como disuasivos adicionales y mejorar la protección de los afectados.

Capacitación en sensibilización y Prevención: Implementar programas educativos dirigidos a la población en general sobre la prevención de fraudes informáticos y la importancia de la seguridad cibernética. Esto podría contribuir a reducir la incidencia de estos delitos al tiempo que empodera a los ciudadanos para protegerse mejor.

Finalmente, se recomienda la realización de un estudio más amplio que aborde todas las atapas del proceso penal en los casos de fraude informático y en base a ese estudio fortalecer las recomendaciones propuestas anteriormente.

XIV. REFERENCIAS BIBLIOGRÁFICAS

Barahona, S. S. (2021). Perfiles del ciberdelito: un campo de estudio inexplorado. *Revista de Derecho UCA*. doi:https://doi.org/10.5377/derecho.v1i30.12223

Berenguer, E. O. (2004). *Manual de derecho penal parte general.* Managua, Nicaragua: CAJ/FIU-USAID.

Botero, J. H. (2020). *La responsabilidad de las entidades financieras por fraudes electronicos.* Tesis de Maestria, Medellin. Obtenido de https://repository.upb.edu.co/bitstream/handle/20.500.11912/6161/La%20responsabilidad%20de%20las%20entidades%20financieras%20por%20fraudes%20electr%C3%B3nicos.pdf?sequence=1

Gamon, V. P. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *Revista latinoamericana de estudios de seguridad*. doi:https://doi.org/10.17141/urvio.20.2017.2563

Irma Solangue Gómez, J. Y. (s.f.). *Análisis Jurídico de la Ley No 1042 Ley Especial de Ciberdelitos en relación al acoso sexual cibernético que pueden llegar a sufrir los niños, niñas y adolescentes, en el segundo trimestre del año 2021.* Managua: Unan Managua. Obtenido de https://catalogosiidca.csuca.org/Record/UNANM.2381/Details

Llinares, F. M. (2012). *Femenologia y crimonologia de la delincuencia en el ciberespacio.* Madrid: Marcial Pons.

Nacional, A. (1987). *Constitucion Politica de Nicaragua.* Managua: La Gaceta.

Nacional, A. (1994). *Ley 182, ley de defensa al consumidor.* Managua: La Gaceta.

Nacional, A. (1998). *Ley 260, ley organica del poder judicial.* Managua: La Gaceta.

Nacional, A. (2000). *Ley346, ley organica del Ministerio Publico.* Managua: La Gaceta.

Nacional, A. (2001). *Ley 406, codigo procesal penal .* Managua: La Gaceta.

Nacional, A. (2005). *Ley 561, ley general de bancos e intituciones financieras .* Managua: La Gaceta.

Nacional, A. (2012). *Ley 787, ley de proteccion de datos personales.* Managua: La Gaceta.

Nacional, A. (2014). *LEY DE ORGANIZACIÓN, FUNCIONES, CARRERA Y RÉGIMEN ESPECIAL DE SEGURIDAD SOCIAL DE LA POLICÍA NACIONAL.* Managua: La Gaceta.

Nacional, A. (2020). *Ley 1042, ley especial de ciberdelitos.* Managua: La Gaceta.

Nacional, A. (2020). *Ley 1044 "Ley especial de ciberdelitos".* Managua: La Gaceta.

Páiz, J. F. (2022). Cibercriminalidad como modalidad comisiva del delito de. *Revista Constructos criminologicos*. Obtenido de file:///E:/Downloads/Revista+Constructos+Criminol%C3%B3gicos+-+Vol+2,+N%C3%BAm+3,+2022+-+Flores+-+PP09-30%20(3).pdf

Roberto Sampieri, C. F. (2014). *Metodologia de la investigacion.* Mexico DF: McGraw Hil interamericana editores.

Salmeron, C. E. (2021). *Delitos informaticos en la actualidad costarricense.* Tesis de Licenciatura, Universidad de Costa Rica, San Jose. Obtenido de http://repo.sibdi.ucr.ac.cr:8080/jspui/bitstream/123456789/18007/1/45958.pdf

Sebastian Diaz Jimenez, J. C. (2018). *ANÁLISIS DEL DELITO DE FRAUDE ELECTRONICO: MODALIDAD TARJETA DE CRÉDITO.* Monteria: UNIVERSIDAD COOPERATIVA DE COLOMBIA. Obtenido de

https://repository.ucc.edu.co/server/api/core/bitstreams/779709a1-437b-45f6-9396-cf2a9838ace9/content

Sequeira, N. A. (2016). *ANÁLISIS DE AMENAZAS RELACIONADAS A LOS METADATOS Y CORREO ELECTRÓNICO, E IMPLEMENTACIÓN DE UN APLICATIVO COMO HERRAMIENTA PARA DISMINUIR EL RIESGO DE UN ATAQUE EN EL QUE SE EMPLEEN ESTOS ELEMENTOS.* Managua: Universidad nacional de ingenieria. Obtenido de https://ribuni.uni.edu.ni/1824/1/90240.pdf

Suarez, D. R. (2019). *Los Desafíos del Derecho de las TIC en la Sociedad de la informacion.* Tesis Doctoral, Universidad Rey Juan Carlos, Madrid. Obtenido de https://burjcdigital.urjc.es/bitstream/handle/10115/17560/TESIS%20DOCTORAL%20DANIEL%20RODR%C3%8CGUEZ.pdf?sequence=1&isAllowed=y

Valeria Araya, M. A. (2007). Constructivismo: Origenes y pesrpectivas. *Laurus, Revista de educacion*, 76-92. Obtenido de www.redalyc.org/pdf/761/76111485004.pdf

ANEXOS

Anexo N°1. Modelo de Entrevista abierta

Datos Generales

Nombre del entrevistado_____ Edad:_____

Sexo:_____ Fecha de la entrevista:_____ Inicio-finalización:_____ Lugar de trabajo:_____ Cargo:_____ años de laborar:_____

Contenido

Objetivo específico 1

1. ¿Podría compartir un poco acerca de su trayectoria profesional y su experiencia en el direccionamiento de investigaciones de delitos informáticos?

2. ¿Qué tan a menudo la ciudadanía presenta denuncias de fraude informático, cuales son las estrategias utilizadas por los delincuentes para cometer este delito?

3. Este es un delito tipificado muy recientemente ¿Coméntenos su perspectiva sobre cómo la ley especial de ciberdelitos ha impactado el trabajo de la policía nacional en la detección y persecución de este delito?

4. Descríbanos cómo se desarrolla una investigación de fraude informático y cuál es el lineamiento a seguir y su diferencia respecto a la investigación de delitos comunes.

5. ¿Cuáles son los resultados más comunes que se obtiene de la investigación de los fraudes informáticos que son denunciados?

6. ¿Cuáles son los factores internos o externos que influyen positiva o negativamente en los resultados de una investigación de fraude virtual?

7. ¿Cuáles son las vulnerabilidades más frecuentes que son utilizadas por los investigados para cometer el fraude informático?

8. En su experiencia ¿cuál es la característica, más común que se observa en las victimas de fraude informático?

9. ¿En el desarrollo de las investigaciones policiales, cual es el denominador común que identifica a un sospechoso de fraude virtual?

Agradecemos su apoyo incondicional al desarrollo de esta entrevista.

Anexo N°2. Modelo de encuesta cerrada

Datos Generales:

Edad: _____ Sexo: _____ Oficio: _____

Fecha de la encuesta: _____

Inicio-finalización: _____

1. ¿Ha sido usted víctima del ciberdelito denominado fraude virtual?

a. Si b. No

2. ¿Conoce usted de la existencia de una ley especial de ciberdelitos?

a. Si b. No

3. Si su respuesta a la pregunta anterior fue “Si”, indíquenos que papel considera usted que desempeña la aplicación de esta nueva ley en la prevención del delito del que usted fue víctima.

4. ¿El autor del delito del cual usted fue víctima, fue identificado?

a. Si b. No

5. ¿Su denuncia fue tramitada por las autoridades correspondiente hasta llegar a un juicio?

a. Si b. No

4. Si su respuesta anterior fue “SI”. ¿Cómo considera usted el trabajo de las autoridades competentes respecto a su denuncia?

a. Respuesta rápida y altamente eficiente

b. Respuesta lenta y negligente, pero con resultados.

c. Sin respuesta, el caso quedo en la impunidad.

5. De qué manera ocurrió el delito del que usted fue víctima.

a. Uso de enlaces falsos enviados en redes sociales para extraer recursos bancarios.

b. Simulación de un depósito bancario mediante bouchers falsos al hacer compras online.

C. Robo de datos de tarjetas de crédito-debito.

d. Simulación de ser funcionarios bancarios para solicitar datos y luego extraer todos los recursos de una cuenta bancaria.

e. Compras en tiendas online que cobran mucho más del precio que señalaban por un producto.

f. Simulación de vender un producto online y al recibir el pago no lo entregaron.

6. En el caso que su delito no pudo llegar a juicio, que explicación le brindo el investigador policial al respecto

a. El autor del delito no logro ser identificado.

b. El autor del delito es extranjero.

c. El autor logro ser inidentificado, pero no capturado.

d. No me interesa llegar a juicio, solo quiero recuperar mis recursos.

7. ¿Ha denunciado usted o alguien de su círculo cercano otro tipo de delito común?

a. Sí b. No

8. Si su respuesta a la pregunta anterior fue “Si”, sírvase a indicarnos ¿Noto usted alguna diferencia en el actuar de las autoridades al investigar el fraude informático del cual fue víctima?

9. ¿En el fraude del cual usted fue víctima, los recursos fueron extraídos de sus ahorros en alguna entidad bancaria o financiera?

a. Si b. No

10. Si su respuesta fue “si” ¿Cómo considera usted que la entidad bancaria o financiera responsable del resguardo de sus recursos colaboro con las autoridades competentes para el esclarecimiento del delito del que usted fue víctima?

a. Fueron responsables y colaboraron con las autoridades

b. Fueron negligentes y solo aportaron información sin relevancia

C. Deslindaron responsabilidades y se negaron a aportar información

11. A su consideración, ¿cómo considera el papel de las autoridades competentes respecto a la correcta aplicación de la ley?

a. Altamente positivo, aplican la ley correctamente priorizando la obtención de justicia a la víctima.

b. Medianamente positivo, aplican la le ley negligentemente, pero se obtuvieron resultados.

c. Deficiente. No existió aplicación de ley, el caso está en la impunidad.

12. Según su apreciación ¿Considera que los funcionarios competentes en la investigación y judicialización de este delito están plenamente capacitados para esta labor?

a. Si b. No

13. ¿Considera usted que la Ley especial de ciberdelitos contenga aspectos que deban ser mejorados respecto al delito denominado fraude informático?

a. Si b. No

12. A su criterio, señale el aspecto que considera debe mejorarse en la ley.

a. Deben endurecerse las penas aumentando los años de cárcel.

b. Debe establecerse una cuantía y en base a esa cuantía establecer la dureza de las penas.

c. La ley debe obligar a las instituciones financieras involucradas a reembolsar a sus clientes los recursos defraudados cuando se demuestre negligencia de parte de la institución financiera.

Anexo N° 3. Modelo de bitácora de observación de expedientes

I. Generalidades:

Número de expediente policial:

Nombre de los investigados:

Nombre de la víctima:

Fecha de realización de la denuncia:

Nombre del investigador policial:

II. Aplicación de instrumento:

Objetivo:

Actos investigativos realizados:

Pasada a M.P: SI NO

Existencia de piezas de convicción físicas: SI NO

Piezas de convicción:

Detención exitosa de los investigados: SI NO

Método utilizado por los investigados para la acción delictiva

III. Dictamen Final:

Breve descripción de los hallazgos más importantes en el expediente que den repuesta al objetivo de investigación:

Anexo N°4. Certificación emitida por las autoridades policiales de la instancia donde se realizó la investigación.

REPÚBLICA DE NICARAGUA
POLICÍA NACIONAL
DIRECCIÓN DE AUXILIO JUDICIAL
"JUNTO A LA COMUNIDAD, COMPROMETIDOS CON TU SEGURIDAD"

Lunes ,02 de octubre 2023.

El suscrito Jefe Dirección Auxilio Judicial de la Policía Nacional, Comisionado General Victoriano Ruiz Urbina, hace constar que los estudiantes de la Carrera de Derecho Mirna de los Ángeles Ramírez Pérez identificada con cedula número 001-061189-0043Q y Juan Pablo Centeno Benavidez identificado con cedula número 1272509900000H, realizarán un proyecto de investigación científico denominado "FRAUDE INFORMATICO" en el departamento de Delitos Informáticos de la Dirección de Auxilio Judicial, el cual realizara del 12 de octubre dos mil veintitrés al treinta de noviembre del mismo año y consistirá en realizar una entrevista al Jefe del Departamento de Delitos Informáticos y responder una encuesta que se realizara a las víctimas del Delitos de Fraude Informático la que demorara aproximadamente 10 minutos.

La información registrada será confidencial y los nombres de los participantes en dicha encuesta serán omitidos tampoco se recibirá ninguna retribución para brinda esa información a los estudiantes Mirna de los Ángeles Ramírez Pérez y Juan Pablo Centeno Benavidez.

Se extiende la presente, para lo fines que estime pertinente.

Dado en la Ciudad de Managua, a los dos días del mes de octubre del año dos mil veintitrés.

Atentamente;

Comisionado General
VICTORIANO RUIZ URBINA
Jefe Dirección Auxilio Judicial

HONOR, SEGURIDAD, SERVICIO
Email:investigacionescriminales@policia.gob.ni
Teléfono: 22267800 – 22267801 Ext.-100-102

Anexo 5. Cronograma de la investigación.

CRONOGRAMA DE ACTIVIDADES		2023							
NUMERO	ACTIVIDADES	MAYO	JUNIO	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE
1	Planteamiento del problema	x	x	x					
2	Marco Teórico	x		x					
3	Metodología de la investigación				x				
4	Primera Revisión				X				
5	Levantamiento de Observaciones					x			
6	Aprobación del proyecto de Tesis					x			
7	Trabajo de campo						x		
8	Procesamiento estadístico						x		
9	Análisis de datos							x	
10	Revisión del informe final							x	
11	Aprobación de la Tesis								x
12	Sustentación								x