UNIVERSIDAD CENTRAL

VICERRECTORÍA ACADÉMICA

CARRERA DE DERECHO

TEMA

ANÁLISIS NORMATIVO Y JURISPRUDENCIAL SOBRE LA RESPONSABILIDAD DE LOS BANCOS ESTATALES PARA CON LOS CLIENTES, EN CASOS DE FRAUDES ELECTRÓNICOS -ENTRE LOS AÑOS 2019 AL 2023-

MODALIDAD DE TESIS

PARA OPTAR POR EL GRADO DE LICENCIATURA EN DERECHO

SUSTENTANTE

MARIELA QUESADA CASTRO

TUTOR

LIC. CRISTIAN MASIS ROJAS

SEDE CENTRAL

ABRIL, 2024

DEDICATORIA Y AGRADECIMIENTO

A Dios,

Por la vida, por la paciencia, por la sabiduría, por todo lo que me das y que me niegas, porque el tiempo de Dios es perfecto.

A mis padres y hermanos,

Por la educación que me dieron, gracias a ellos soy la mujer que soy hoy en día.

A mi esposito,

Por absolutamente todo el apoyo que me ha dado durante la carrera y en el hogar, esta carrera nos unió y nos mantiene cada vez más unidos con ayuda del amor de Dios, gracias por toda tu ayuda incondicional, por levantarme en cada paso en falso, por tus palabras de ánimo y todo el amor que me das.

A todos los profesores,

Que día a día dieron su mejor esfuerzo por nuestra educación, en especial a doña Ligia por todo su amor y cariño, a Winter por la paciencia con la que nos enseñó y su amistad, y a mi tutor Cristian por todo lo que nos instruyó durante la carrera y por toda su dedicación y colaboración durante este último paso.

A todos infinitas gracias.

CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

CAPÍTULO I: PROBLEMA DE INVESTIGACIÓN

En este apartado se define el problema de investigación, para lo cual se desarrolla un objetivo general y los objetivos específicos, así como una justificación con la cual se expone la importancia de este. Con respecto a los antecedentes, se detalla el fundamento histórico que le precede; por último se proyectan los resultados esperados.

1.1 Planteamiento del Problema

Los fraudes electrónicos en la actualidad representan un problema nacional e internacional que progresa conforme la tecnología avanza, y uno de sus blancos son los clientes bancarios. Dentro de los ciberdelitos de ataque financiero se encuentran el *phishing*, *pharming*, tráfico cifrado o encriptado y las *key logger*. Las cifras de los usuarios bancarios que son víctimas en los fraudes electrónicos van en aumento según diversos estudios (BPDC, s.f., parr. 01-05).

Consecuentemente, los Bancos Estatales no están exentos de sufrir los fraudes electrónicos en perjuicio de sus clientes. En ese sentido, el presente trabajo proyecta determinar la normativa y Jurisprudencia que señala la responsabilidad directa de los Bancos Estatales de Costa Rica con los clientes en casos de fraudes electrónicos. Este capítulo abarca el desarrollo del problema de investigación, las interrogantes que dieron origen a la tesis, los objetivos del estudio y la justificación.

Desde finales del siglo pasado, e inclusive durante el desarrollo de este, la tecnología ha avanzado a pasos desproporcionados, otorgando una serie de herramientas a los individuos que quizás ni se imaginaban. Si bien es cierto, el avance de la ciencia y la tecnología han venido a facilitar las labores diarias de un mundo moderno y globalizado, también se han convertido en instrumentos que facilitan actos delictivos contrarios al fin para el cual han sido creados (Salas, 2010).

En Costa Rica, producto del comienzo de los delitos informáticos, se empieza a normar estos tipos de delitos de carácter privado. Es a partir del año 2001, con la entrada en vigor de la Ley 8148, que se adicionan al Código Penal, los artículos 196 bis, 217 bis y 229 bis, respectivamente son Violación de comunicaciones electrónicas, Fraude Informático y Alteración de datos y sabotaje informático, con el objetivo de reprimir y sancionar a los infractores de este tipo de estafas informáticas (Bonilla, 2019).

En el año 2012, se promulga la Ley No. 9048, denominada “Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal”, la cual decreta la reforma de varios artículos (167, 196, 196 bis, 214, 217 bis, 229 bis y 288) y modificación de la Sección VIII, denominada delitos informáticos y conexos, del Título VII del Código Penal:

> Donde los cambios se produjeron principalmente en el aumento de las penas, y se incluyeron conductas relacionadas con el uso de redes sociales, medios informáticos, entre otros. Por otra parte, se adicionó un inciso 6 al Artículo 229, correspondiente al “Daño Agravado”, ubicado en el Título correspondiente a los “Delitos contra la propiedad”, donde también se incorpora, un artículo 229 ter, correspondiente al “Sabotaje Informático”. (Bonilla, 2019, p.222)

En el 2015, la Ley No. 9048 sufrió modificaciones producto de la resolución de la Sala Constitucional N° 5615 del 22 de abril de 2015, en la que se anuló el artículo 288 del Código Penal. Además, mediante la misma resolución se modificó el inciso b del artículo 196 bis, quedando redactado de la siguiente manera: “O estén contenidos en bases de datos públicas”, anulando la frase “cuando los datos sean de carácter públicos” (artículo 196 bis).

Seguidamente, los Bancos Estatales producto del auge tecnológico posterior a la crisis sanitaria por COVID-19 en los años 2021 y 2022, en donde las formas primarias de comercio y consumo eran mediante actividades digitales, sufrieron un aumento considerable de transacciones electrónicas realizadas por medios tecnológicos, así mismo aumentaron las estafas informáticas. Los primeros cuatro meses del 2022, el OIJ recibió el 50% de las denuncias de todo el año del 2021 (BPDC, s.f., parr. 01-02).

Para la presente investigación se entiende como fraude informático la definición de Gutiérrez (1991, citando a Camacho Losa), que señala que es toda conducta fraudulenta mediante el uso indebido o manipulación fraudulenta de elementos informáticos, realizadas a través o con la ayuda de un sistema informático, mediante la cual alguien trata de obtener un beneficio patrimonial ilícito.

Al analizar este tema, los estudiosos en la materia señalan que el fraude informático se debe en gran medida al aumento y aceptación de las transferencias bancarias realizadas a través del internet, ya que ha beneficiado a los clientes con el traslado y ahorro de tiempo, al no tener la necesidad de acudir a una sucursal bancaria (Salas, 2010).

Consecuentemente, el aumento de las transacciones bancarias mediante plataformas digitales crea también vulneración para que ciberdelincuentes se beneficien patrimonialmente de forma ilícita. Utilizan estrategias como engaños y manipulación verbal para que los usuarios les brinden información sensible como elementos de legitimación, datos personales, claves de acceso (PIN) y su identificación, para realizar los actos delictivos. Así mismo, manipulan, abusan o interfieren en el funcionamiento de sistemas de tratamiento automatizado de datos con la intención maliciosa de producir un perjuicio económico (Gutiérrez, 1991).

Por otra parte, diferentes investigaciones (Salas, 2010) describen que existe una oposición entre los usuarios y los bancos, en cuanto a la responsabilidad objetiva entre los mismos, por cuanto los usuarios alegan que el servicio que se les brinda se considera riesgoso y no contempla las medidas de seguridad necesarias y suficientes.

Aunado a esto se encuentra la posición de los bancos donde se resalta que no deben asumir el riesgo causado por un tercero. Indican que no pueden controlar las actuaciones negligentes de la víctima por un mal manejo de su información, imprudencias al acceder a páginas electrónicas del banco, suministro de contraseñas o de datos confidenciales a terceros y demás posibilidades.

Por tanto, se plantea la siguiente pregunta de investigación: ¿Existe una norma que defina la responsabilidad de los Bancos Estatales con los clientes, en casos de fraudes electrónicos, entre los años 2019 al 2023? y ¿cuál es la posición de las diferentes instancias judiciales con relación a los fraudes electrónicos bancarios?

1.2 Objetivos

1.2.1 Objetivo General

- Analizar la normativa y Jurisprudencia costarricense sobre la responsabilidad de los Bancos Estatales para con los clientes en casos de fraudes electrónicos, entre los años 2019 al 2023.

1.2.2 Objetivos Específicos

- Estudiar los tipos de responsabilidad que se aplican en el Sistema Jurídico Costarricense en las estafas informáticas.
- Examinar Jurisprudencia sobre la responsabilidad de los Bancos Estatales con los clientes en relación con los fraudes electrónicos.
- Ahondar en las medidas de seguridad desarrolladas por los Bancos Estatales de Costa Rica para mitigar los efectos de las estafas electrónicas.

1.3 Justificación

La presente investigación se motiva en el aumento desproporcionado que se dio en las estafas informáticas durante y posteriormente a la crisis sanitaria por COVID-19 en los años 2021 y 2022, en donde las formas primarias de comercio y consumo eran mediante actividades digitales a raíz del confinamiento ordenado por el Gobierno de la República.

Es importante recalcar que el presente trabajo investigativo no es per se un estudio técnico que se enfoca en las tecnologías que utilizan los bancos y los usuarios para el acceso a sus cuentas, sin embargo, sí es necesario ahondar en terminologías técnicas para una mejor comprensión. No obstante, la investigación se enfoca en un estudio jurídico de normas y Jurisprudencia que mostrará la responsabilidad objetiva de los Bancos Estatales de Costa Rica para con los clientes cuando sufren estafas electrónicas.

Con esta investigación se concluirá si, de acuerdo con la normativa y Jurisprudencia, los Bancos Estatales tienen la responsabilidad de cubrir el daño patrimonial que sufren sus clientes producto de las estafas informáticas realizadas por los sistemas ofrecidos por los entes bancarios, o si, de lo contrario, no existe responsabilidad objetiva por las entidades financieras en dichos casos. Dentro de este, se analizará los derechos humanos y las garantías constitucionales, plasmadas en nuestra normativa y normas internacionales.

Simultáneamente, el aporte que el presente trabajo espera alcanzar en el campo jurídico costarricense será identificar el rol y la responsabilidad de los Bancos Estatales en las estafas electrónicas sufridas por los clientes y brindar una propuesta a los entes bancarios para disminuir las repercusiones negativas patrimoniales a los usuarios.

Finalmente, no se puede negar el rápido avance de las tecnologías, las facilidades a la población moderna que cada vez es más tecnológica y con menor disponibilidad de horarios para asistir a sucursales bancarias físicas, razón por la que utilizan los medios tecnológicos ofrecidos por los Bancos Estatales para realizar sus transacciones bancarias, convirtiéndose posiblemente en una población vulnerable ante la tecnología en las estafas informáticas. Es una realidad no solo de nuestra sociedad, si no a nivel mundial junto con países como Chile, México, España y Brasil que tienen sistemas normativos similares al nuestro, en relación con los fraudes electrónicos.

1.4 Antecedentes

En este apartado se muestran diferentes trabajos de investigación y documentos, tanto a nivel nacional como internacional. Adicionalmente, la importancia de estos se relaciona con el tema de interés en estudio, el cual trata sobre la responsabilidad directa de los Bancos Estatales de Costa Rica con los clientes en las estafas electrónicas. Por su parte, es trascendental mencionar que existe una escasa literatura sobre este tema, tanto a nivel documental como de investigación. Sin embargo, constan diversos artículos científicos e informes sobre el fondo de esta tesis.

1.4.1 Antecedentes internacionales

En relación con los antecedentes internacionales, el artículo de Balmaceda (2011), "El delito de estafa en la Jurisprudencia chilena", establece como objetivo la interpretación del delito de estafa que se estima han asumido los tribunales chilenos.

La metodología empleada en esta crónica se basa en el análisis jurisprudencial y normativo de la legislación. La conclusión a la cual llegó Balmaceda es que la Jurisprudencia chilena en materia de estafa ha sido coherente con la identidad normativa, sin embargo, para la determinación del engaño y su suficiencia, la Jurisprudencia mayoritaria establece que la figura básica de estafa la deben encontrar en el art. 468 del Código Penal, y para determinar la suficiencia se debe recurrir a la teoría de la imputación objetiva del resultado.

Devia (2017) expone en su tesis doctoral, "Delito Informático: Estafa Informática del Artículo 248.2 del Código Penal", como objetivo entregar una revisión sintética pero integral sobre los requisitos típicos del delito informático, de manera tal que se pueda obtener una perspectiva acerca de cuáles son sus antecedentes normativos y las implicancias en el mundo jurídico.

En esta exposición la metodología empleada se basa en el análisis de la legislación y doctrina. El doctorando determina que es aplicable el tipo básico de estafa para el fraude informático, y aunque Chile fue pionero en Latinoamérica respecto de la promulgación de una ley que sanciona los delitos informáticos, la legislación penal referente a esa materia no ha sido actualizada, existiendo dos proyectos en el parlamento que esperan ser aprobados, Chile ha protegido la empresa, protegiendo los datos en sí mismo como parte integrante del sistema de tratamiento de la información, dejando de lado al usuario los delitos informáticos.

En la Revista Chilena de Derecho y Tecnología, en el artículo de Mayer y Oliver (2020), el objetivo propuesto fue analizar el delito de fraude informático, con énfasis en su concepto y delimitación, examinando su relación con los demás delitos informáticos, así como su vínculo con otras figuras delictivas.

En esta publicación la metodología empleada fue de revisión documental. En su principal conclusión determinaron que es necesario regular dicho delito en torno a tres requisitos, primero que la conducta típica consista en manipular datos o programas de sistemas de tratamiento automatizado de la información, segundo que exista un perjuicio patrimonial y tercero que coexista un ánimo de lucro del ciberdelincuente. Así mismo, concluyeron que deben regular en el ordenamiento jurídico penal chileno algunas de las directrices contenidas en el artículo 8 del Convenio sobre Ciberdelincuencia del Consejo de Europa.

Por su parte, Alves, Ivo y Moretti (2022) plantean en su artículo "El malware como medio de obtención de pruebas y su implementación en el sistema jurídico brasileño", que el objetivo de los autores fue analizar los principales aspectos que involucran el uso de *malware* en el ámbito investigativo y el posible uso en el sistema legal de Brasil, y bajo que términos el uso sería legal.

Esta narración utilizó la metodología de revisión documental. Los autores concluyen que el uso de *malware* es imposible de utilizar con base en la legislación brasileña vigente. Así mismo, proporcionaron parámetros que orientan al legislador a construir una norma que regule esta medida en Brasil.

Asimismo, Anzola y Oliveira (2022) exponen en su ensayo "La regulación de blanqueo de capitales y la responsabilidad penal de la persona jurídica en España: el cumplimiento como clave para los proveedores de servicio con activos virtuales" un estudio del alto riesgo de sus actividades en el aumento del blanqueo de capitales y cuáles son las normas legales en España sobre el tema. Además, en este artículo se investigó si se puede imponer a los *exchangers* directrices existentes en la Unión Europea.

Este artículo basó la metodología de investigación en el análisis de la legislación y doctrina. Los autores determinan que el cumplimiento corporativo es un medio necesario para la prevención del lavado de dinero dentro de los proveedores de servicios virtuales convertibles. Adicionalmente, concluyeron que la legislación española tiene una sólida estructura de cumplimiento para los *exchangers*, pero necesita ser actualizada.

Por último, Calvo (2022) exterioriza en el artículo “La responsabilidad civil de los bancos en los delitos de estafa por “phishing”” que el objeto de análisis de su investigación es saber cuáles son los instrumentos de defensa a disposición de los particulares en caso de ser víctimas, y cuál es la responsabilidad que asumen las entidades bancarias frente a este nuevo tipo de delito informático.

Dicho artículo basó su metodología de investigación en el análisis de la legislación y doctrina. La profesora Calvo, discernió que la Jurisprudencia es unánime a la hora de considerar que el Banco debe restituir las cantidades antijurídicamente sustraídas por un tercero, en tanto que, como depositaria de los fondos, tiene la obligación legal de conservar y devolver el dinero depositado. Concluyó que únicamente se les podrá exonerar de dicha obligación cuando pudieran acreditar que el cliente ha actuado fraudulentamente o con negligencia grave a la hora de proteger sus datos personales y confidenciales.

1.4.2 Antecedentes nacionales

Dentro de los antecedentes nacionales el Centro de Información Jurídica en Línea (2009a), en la investigación sobre el “fraude informático”, se aborda el tema desde una perspectiva penal y la novedosa rama del derecho informático, se realiza un análisis doctrinal del concepto de fraude informático, así como las generalidades del tipo delictivo en conjunto con las clasificaciones del hacking. Además, se abarca el artículo 217 bis del Código Penal y extractos jurisprudenciales sobre los requisitos que configuran el delito informático.

La metodología de investigación utilizada fue teórico-dogmática. Se concluye que el fraude informático es una conducta fraudulenta realizada a través o con la ayuda de un sistema tecnológico, por medio del cual alguien trata de obtener un beneficio ilícito.

El Centro de Información Jurídica en Línea (2009b) en el informe sobre la “responsabilidad objetiva de los bancos por delitos informáticos”, realizó una breve recopilación doctrinaria y jurisprudencial sobre el tema de interés, y se analizó Jurisprudencia relativa al artículo 35 de la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor.

En dicho informe de investigación privó la metodología teórico-dogmática. Dentro de lo concluido por el autor se estableció que los bancos deben responder por los fraudes en perjuicio de sus clientes, salvo que se trate de fuerza mayor o de culpa de la víctima, como cuando esta entrega a un extraño, datos sensibles.

Adicionalmente, Salas (2010), en su tesis “Responsabilidad civil bancaria frente al cliente por delitos informáticos”, pretende brindar un criterio sobre la resolución del conflicto, analizando de forma integral las distintas aristas que forman parte del problema.

El estudio basó su metodología de investigación en el análisis de la doctrina y la legislación. Determinó que en Costa Rica, la jurisprudencia sobre Responsabilidad Objetiva es abundante y ha aumentado a raíz de la Ley de Protección al Consumidor, que incluye en el artículo 35 el régimen de responsabilidad entre las relaciones de consumo, fundamentándose en la teoría del riesgo creado. Al comprobar la hipótesis planteada por la investigadora, se ha demostrado la existencia de responsabilidad objetiva en el tema en cuestión, con la posibilidad de exonerar la obligación si se comprueba la existencia de un eximente de responsabilidad, es decir, por fuerza mayor, culpa de la víctima o hecho de un tercero.

Adicionalmente, Bonilla (2019), en el artículo científico titulado "El espectro actual de los delitos informáticos", señaló que el constante progreso tecnológico que experimenta la sociedad afecta el aumento en las formas de delinquir, dando lugar a nuevos actos ilícitos y, por lo tanto, a nuevos conceptos. La metodología utilizada en este artículo fue de revisión documental. La autora concluyó que la ciberdelincuencia llegó y crece constantemente, por lo que el derecho debe evolucionar y buscar los mecanismos necesarios para avanzar con mayor celeridad.

Calderón (2021) defendió su tesis de postgrado denominada: “Construcción legislativa y aplicación jurisprudencial del delito de “estafa” informática en Costa Rica del año 2014 al 2019. Énfasis en el uso indebido de datos”. El objetivo general de esta investigación fue analizar las diferencias y similitudes entre el delito de estafa y el de estafa informática y los supuestos fácticos en la normativa costarricense.

La metodología utilizada en esta investigación fue teórico-dogmática, así como normativa y empírica. El estudio concluyó que la estafa informática tipificada en el Código Penal carece de componentes, no contempla elementos objetivos, lo que si describe es la pérdida del patrimonio para la víctima. Además, concluye que la norma referente a estafa informática contenida en el Código Penal tiende a ser confusa y repercute negativamente en la comprensión de esta, así como que las penas no sé adaptan al principio de proporcionalidad.

El informe de investigación realizado por Salazar para el Centro de Información Jurídica en Línea (2023), denominado “Jurisprudencia sobre Responsabilidad Bancaria por el Delito de

Estafa Informática", plasma una reseña considerando los supuestos normativos del artículo 271 Bis del Código Penal y el criterio que al respecto de esta norma han elaborado las Salas Primera y Tercera de la Corte Suprema de Justicia, además del Tribunal de Apelación de la Sentencia Penal.

La metodología de investigación se basó en el análisis de la doctrina y la Jurisprudencia. Concluye en primera instancia con relación a la responsabilidad civil objetiva del Banco en el delito penal que habiéndose demostrado el vínculo de servicio y el daño generado a la ofendida, por intervención delictiva de una funcionaria del Banco, sin que pudiera demostrarse alguna circunstancia que excluyera la responsabilidad objetiva, debe condenarse en la reparación del daño civil al Banco, conforme a Derecho.

En segunda instancia, la responsabilidad objetiva de la Administración al poner a disposición de sus clientes el servicio de banca electrónica, concluye que no resulta admisible, de acuerdo a los principios de razonabilidad y proporcionalidad, relevar al cliente de sus deberes de prudencia en aquellos aspectos que forman parte de su ámbito personal de control, como lo es el lugar donde realiza la conexión, así como utilizar equipos de cómputo y los programas informáticos adecuados para garantizar la seguridad de la información.

Todos los anteriores, tienen gran importancia con relación a la presente investigación, ya que conceptualizan términos informáticos que se echan de menos en el área jurídica. Asimismo, delimitan la normativa relacionada con este tipo de delitos, amplía los conceptos básicos y determinan su aplicación en el crimen cibernético.

1.5 Proyecciones

Dentro de la presente investigación se pretende la determinación de si existe responsabilidad de los Bancos Estatales de Costa Rica con los clientes en las estafas electrónicas entre los años 2019 al 2023. Para ello es necesario ampliar todos los términos informáticos relacionados con este tipo delictivo, así como su delimitación en la normativa y realidad costarricense.

De esta manera, la metodología a utilizar será la dogmático-realista, que nos permitirá establecer la normativa y Jurisprudencia, así como, el análisis de campo con la aplicación de una encuesta y el estudio de casos concretos. La investigación se basará en los Bancos Estatales de

Costa Rica, los cuales son el Banco Nacional de Costa Rica, Banco de Costa Rica y Banco Popular y de Desarrollo Comunal.

De ser necesario, a raíz de la investigación se presentará una propuesta de mejora sea en la normativa o en el mejoramiento del suministro de información a los clientes, con el fin de disminuir los casos de estafa informática, basándose en el análisis teórico, jurisprudencial y de campo realizado.

1.6 Limitaciones

Dentro de esta investigación se cuentan con ciertas dificultades, de las cuales podemos señalar:

- La sensibilidad de la información bancaria ocasiona dificultades en el acceso a los datos bancarios con relación al tema, esto por cuanto se manejan como datos confidenciales.
- Se cuenta con limitaciones longitudinales, en cuanto al tiempo para investigar, esto por horario de trabajo, sin embargo, se cuenta con personas profesionales en derecho relacionadas con el tema de fácil acceso, lo que contra resta ligeramente esta limitación.

CAPÍTULO II: MARCO TEÓRICO

En este capítulo se desarrollan los conceptos para una mejor comprensión de la normativa y la jurisprudencia sobre la responsabilidad de los Bancos Estatales para con los clientes en casos de fraudes electrónicos. A lo largo del tiempo, los fraudes electrónicos han experimentado un aumento significativo, particularmente antes, durante y después de la pandemia por el coronavirus de 2019 (COVID-19), virus que provocó el aislamiento de la mayoría de la población a nivel mundial. Como consecuencia, se incrementaron las transacciones bancarias digitales, así como la utilización de los medios informáticos para llevar a cabo las actividades diarias.

Debido a lo anterior, los ciberdelincuentes también han modificado o modernizado los métodos utilizados para obtener información sensible y confidencial de los clientes bancarios. Los transgresores emplean diversas estrategias para cometer dichos delitos. Ahora bien, existen dos ramas del Derecho relacionadas con estos hechos: la penal y la responsabilidad civil, siendo esta última la que se enfoca en esta investigación.

2.1. Sistema Jurídico Costarricense

El sistema jurídico se define como aquel que comprende "la totalidad de las normas que se correlacionan en virtud de la unidad que integran a partir de la Constitución, y se compone por una secuencia de conjuntos de normas vigentes en momentos distintos" (Huerta, 2007, p. 271).

Por otro lado, para González (2021, citando a Zárate, Martínez y Ríos, 1997) los sistemas jurídicos se pueden definir como aquel conjunto articulado y coherente de instituciones, métodos, procedimientos y reglas legales que constituyen el derecho positivo de un lugar y tiempo determinados. Cada Estado soberano cuenta con un sistema jurídico propio.

De acuerdo con Kelsen (1925/1949) la pirámide kelseniana es una representación gráfica del sistema jurídico escalonado, el sistema no es otra cosa que la forma en que se relacionan un conjunto de normas jurídicas y la principal forma de relacionarse entre sí es sobre la base del principio de jerarquía.

Según el artículo 6 de la Ley General de la Administración Pública, la jerarquía de las fuentes del ordenamiento jurídico administrativo se estructura de la siguiente forma:

- La Constitución Política;
- Los tratados internacionales y las normas de la Comunidad Centroamericana;

- Las leyes y los demás actos con valor de ley;
- Los decretos del Poder Ejecutivo que reglamentan las leyes, los de los otros Supremos Poderes en la materia de su competencia;
- Los demás reglamentos del Poder Ejecutivo, los estatutos y los reglamentos de los entes descentralizados; y
- Las demás normas subordinadas a los reglamentos, centrales y descentralizadas.

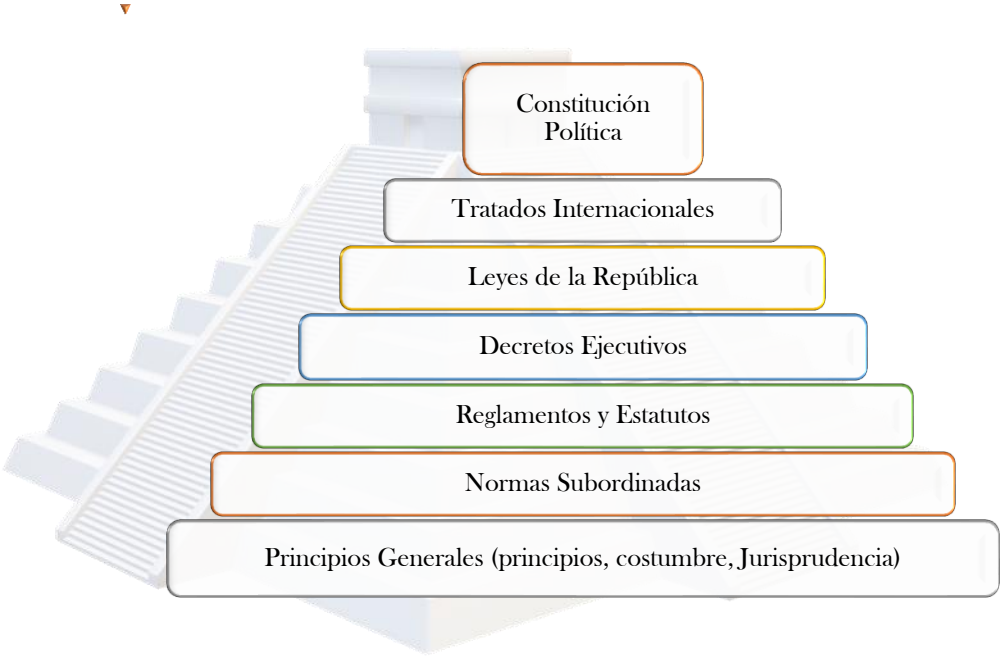

Figura 1: Pirámide de Kelsen

Fuente: Elaboración propia, 2024.

2.1.1. Norma

Dentro de las normas, existen diferentes tipos, pero para esta investigación interesa el concepto de la norma jurídica. Según el Diccionario Usual del Poder Judicial (2020), la norma jurídica es la regla de conducta de carácter legal y prescriptivo, encaminada a ordenar diferentes facetas del comportamiento humano. Por lo general, confiere derechos e impone deberes. "Sobre la naturaleza de la norma jurídica, la teoría se inclina a ver en ella un mandato, antes que un simple juicio o hipótesis. Constituyen sus elementos: a) un supuesto de hecho (por ejemplo, 'si alguien compra una cosa'); b) una afirmación de derecho ('estará obligado a pagar su precio'); c) una sanción ('o deberá indemnizar los daños y perjuicios que ocasione al vendedor')".

Para Hierro (2003) una norma jurídica existe si pertenece a un sistema jurídico existente. Sin embargo, un sistema jurídico no es otra cosa que un determinado conjunto organizado de normas.

De los conceptos anteriores se resalta que las normas son el eje central de los sistemas jurídicos. Además, establecen los derechos y deberes obligados a respetar en nuestro comportamiento humano. El no acatamiento de las normas establecidas en cada sistema jurídico provoca la sanción por su irrespeto.

2.1.2. Jurisprudencia

La Jurisprudencia es la interpretación reiterada que los tribunales supremos de justicia efectúan, en cuanto a la aplicación de la ley, en casos similares en una materia determinada. Además, coadyuvan a la interpretación de la ley, y su aplicación a casos determinados, realizada por los jueces. Así mismo, también se les conoce como el conjunto de sentencias y análisis jurídico que en ellas se hace sobre temas semejantes (Poder Judicial, 2020).

2.1.3. Sala Primera de la Corte Suprema de Justicia

La Sala Primera de la Corte Suprema de Justicia es la instancia superior que atiende principalmente recursos de casación y revisión en materia civil, misma en la que se basa esta investigación, por esto es importante que se conozca que de acuerdo con el artículo 54 de la Ley Orgánica del Poder Judicial, las competencias de esta son atender principalmente los recursos de casación y revisión en materia civil y comercial, con salvedad de los asuntos referentes al Derecho de familia y a juicios universales, entre otras funciones. Las resoluciones que emite la Sala Primera de la Corte Suprema de Justicia son fuente de Jurisprudencia en el tema que nos ocupa en esta investigación.

2.1.4. Jurisdicción Contencioso-Administrativo y Civil de Hacienda

La Jurisdicción Contencioso-Administrativo es la encargada de dirimir los litigios relacionados con estafas informáticas en perjuicio de los clientes financieros de los Bancos Estatales, así consagrado en el artículo 49 de la Constitución Política que señala que dicha jurisdicción tiene por objeto garantizar la legalidad de la función administrativa del Estado, de sus instituciones y de toda otra entidad de derecho público, protegiendo los derechos subjetivos y los intereses legítimos de los administrados.

Así mismo, como lo establece el artículo 2, inciso b, del Código Procesal Contencioso-Administrativo, conocerá las cuestiones de responsabilidad patrimonial de la Administración Pública y sus funcionarios, siendo la primera instancia judicial en conocer las demandas sobre estafas informáticas en detrimento del patrimonio de los usuarios de la Banca Estatal.

2.1.5. Ministerio de Economía, Industria y Comercio (MEIC)

El Ministerio de Economía, Industria y Comercio es la institución del Estado encargada de conocer los conflictos sobre la responsabilidad objetiva que nos ocupa en la investigación con relación a las estafas informáticas, donde funge como Tribunal Administrativo (MEIC, 2021).

Dentro de las funciones del MEIC, mediante la Ley de Promoción de la Libre Competencia y Defensa Efectiva del Consumidor, de acuerdo con el artículo 47, se crea la Comisión Nacional del Consumidor, como órgano de máxima desconcentración, para velar por el cumplimiento de las normas que garanticen la defensa efectiva del consumidor, órgano encargado de recibir, celebrar y resolver las denuncias de los consumidores.

2.2. Bancos Estatales de Costa Rica

De acuerdo con el Diccionario Usual del Poder Judicial (2020), la banca estatal es un sistema de entidades bancarias de derecho público que pertenecen al Estado o a sujetos públicos. Sin embargo, en Costa Rica, es un conjunto de bancos conformados como instituciones autónomas de derecho público, con personería jurídica propia e independencia administrativa.

2.2.1. Banco Central de Costa Rica

El Banco Central de Costa Rica (BCCR), se rige por la Ley Orgánica del Banco Central de Costa Rica, cuyo principal objetivo es controlar la inflación, realiza labores juntamente con el Consejo Nacional de Supervisión de Sistema Financiero para cumplir con sus objetivos.

2.2.2. Consejo Nacional de Supervisión del Sistema Financiero (CONASSIF)

En el mismo cuerpo normativo, en el artículo 119, se establece que el consejo dictará las normas generales que sean necesarias para el establecimiento de sanas prácticas bancarias de gobierno corporativo, incluidas las de idoneidad de miembros del órgano de dirección y puestos claves de la organización, así como de gestión de riesgos y de registro de las transacciones, entre otros aspectos, todo en salvaguarda del interés de la colectividad.

De acuerdo con el Diccionario Usual del Poder Judicial (2020), el CONASSIF es un órgano colegiado de dirección superior encargado de uniformar e integrar las actividades de regulación y supervisión del sistema financiero costarricense. Ejerce la actividad directiva sobre la Superintendencia General de Entidades Financieras.

2.2.3. Superintendencia General de Entidades Financieras

Bajo la misma Ley Orgánica del Banco Central de Costa Rica, en el artículo 115, se crea la Superintendencia General de Entidades Financieras (SUGEF), por el interés público de fiscalización de las entidades financieras del país, como órgano de desconcentración máxima del Banco Central de Costa Rica.

En Costa Rica, de acuerdo con el Diccionario Usual del Poder Judicial (2020) el sistema bancario está integrado por el Banco Central de Costa Rica, el Banco de Costa Rica, el Banco Nacional de Costa Rica, el Banco Popular y de Desarrollo Comunal y el Banco Crédito Agrícola de Cartago. Sin embargo, este último en el 2017, el Gobierno acordó el cierre de operaciones comerciales debido a su mal desempeño financiero. Es mediante la Ley 9605 que se acuerda la fusión por absorción del Banco Crédito Agrícola de Cartago por parte del Banco de Costa Rica.

Debido a lo anterior esta investigación se centra en el Banco Nacional de Costa Rica, Banco de Costa Rica y Banco Popular y de Desarrollo Comunal, como Bancos Estatales activos.

2.3. Tipos de responsabilidades jurídicas

Según Fernández (2014) existen formas de estructurar las responsabilidades jurídicas, mediante dos grandes sistemas, el primero la responsabilidad subjetiva y el segundo la responsabilidad objetiva. Las diferencias entre ambos son muy importantes para determinar e imputar el daño a un responsable.

2.3.1. Responsabilidad Subjetiva

Menciona Fernández (2014) que la principal característica de la responsabilidad subjetiva es la conducta, siendo que la culpa del autor es la conducta determinante para la imputabilidad de la responsabilidad, por ello es muy importante analizar detalladamente la acción u omisión y el grado de culpa en que incurrió, para con ello determinar la responsabilidad.

2.3.2. Responsabilidad Objetiva

Esta es establecida como la “obligación indemnizatoria por un daño, sin culpa, provocado directa e inmediatamente y que sobreviene como resultado del accionar de quien lo provoca o por cosas que le pertenecen o que están bajo su guarda o custodia” (Diccionario Usual del Poder Judicial, 2020).

Adicionalmente, Fernández (2014) menciona que la responsabilidad objetiva es por riesgo creado, e implica que cualquier situación que se genere y por su propia naturaleza ocasione un riesgo a los terceros se tiene como responsabilidad objetiva. Por el simple hecho de encontrarse en este supuesto de riesgo, se tiene como responsable y se tiene que reparar el daño generado y los perjuicios causados.

2.3.3. Responsabilidad Civil

Para Calvo (2022) la responsabilidad civil se define como la obligación de reparar los daños y/o perjuicios causados a una persona o grupo de personas. Dicho daño puede ser provocado por un incumplimiento contractual, o por la ocurrencia de un hecho lesivo sin vinculo contractual previo (extracontractual).

Adicionalmente, el Diccionario Usual del Poder Judicial (2020) define la responsabilidad civil como la obligación personal y patrimonial, de carácter causal, para resarcir o reparar un daño o perjuicio causado por uno mismo o por un tercero.

2.3.3.1. Contractual.

Dentro del concepto de responsabilidad contractual, Salas (2010) señala que:

> Funciona como una garantía ante el incumplimiento de lo que fue previamente pactado entre las partes. Surge una vez que no se ha hecho efectivo tal y como se pactó el cumplimiento de la prestación debida, pero para valorarse ese incumplimiento no solamente se toma en cuenta lo que el contrato indica, sino también lo que la Ley determina, por ejemplo, la buena fe, principio bajo el cual deben actuar las partes. (p.22)

2.3.3.2. **Extracontractual.**

De acuerdo con Salas (2010), en la responsabilidad civil extracontractual, aunque no hay un vínculo preexistente entre quien depara el daño y el sujeto dañado, siempre se genera una responsabilidad. Dicho hecho se produce cuando una persona violenta el interés que es jurídicamente relevante para el otro, y no existe una relación jurídica entre ambos.

2.3.3.3. Directa.

En el caso de la responsabilidad directa como lo indica Fernández (2014), no existe problema en identificar al obligado y al responsable, esto por cuanto es la misma persona. Así mismo reúne las siguientes características:

1. Debe actuar a nombre propio, es decir no está bajo las órdenes o en representación de un tercero.

2. Debe ser mayor de edad y tener capacidad jurídica.

Esta responsabilidad se le aplica directamente al ejecutor del daño, y se le obliga a resarcir el daño causado por imprudencia o culpa, o a la indemnización por daños y perjuicios.

2.3.3.4. Indirecta.

Por otra parte, para el mismo autor, en la responsabilidad indirecta no existe identificación del sujeto que comete el hecho ni del que está obligado a repararlo, que no necesariamente es la misma persona, como pasa con los incapaces o menores de edad bajo la tutela o patria potestad de otro.

Es por esto por lo que se señala que una persona indirecta es el responsable civil para el pago o la indemnización por daños y perjuicios que ocasione el menor o incapaz, en este ejemplo. Por lo anterior, se señala que el responsable de un acto en perjuicio de otro no es necesariamente el obligado a resarcir el daño.

2.4. Estafas informáticas

Burgos (2020, citando a Salt, 1994) define el fraude informático como "la manipulación ilícita, a través de la creación de datos falsos o la alteración de datos o procesos contenidos en sistemas informáticos, realizadas con el objeto de obtener ganancias indebidas" (p. 178).

En Costa Rica, las estafas informáticas están tipificadas en el Código Penal en el artículo 217 bis, con el siguiente tipo penal:

> Se impondrá prisión de tres a seis años a quien, en perjuicio de una persona física o jurídica, manipule o influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos, programación, valiéndose de alguna operación informática o

> artificio tecnológico, o bien, por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro. (Código Penal, 217 bis)

De acuerdo con el mismo artículo, la pena será mayor si "las conductas son cometidas contra sistemas de información públicos, sistemas de información bancarios y de entidades financieras, o cuando el autor es un empleado encargado de administrar o dar soporte al sistema o red informática o telemática" (ídem).

El delito de estafa visto desde los tribunales chilenos, según Balmaceda (2011) no es definido en el Código Penal de Chile, por lo que se ha determinado mediante la doctrina y la Jurisprudencia que deben presupuestarse cuatro elementos, sean el engaño, error, disposición patrimonial y perjuicio. No obstante, la realidad se centra solo en el engaño y el perjuicio.

Las técnicas utilizadas para obtener la información son variadas, sin embargo, existen dos principales, las cuales son mediante la ingeniería social y la suplantación de identidad, las que se desarrollan de seguido.

2.4.1. Ingeniería Social

Para Salas (2010) la ingeniería social se refiere a la manipulación de las personas para que voluntariamente realicen actos que por lo general no harían. El objetivo es engañar a las personas para que revelen contraseñas, ingresen a sitios fraudulentos con apariencia lícita u cualquier otra información que comprometa la seguridad del sistema objetivo.

Devia (2017) señala que la ingeniería social es la acción o práctica que tiene por fin, obtener información confidencial, a través de la manipulación de usuarios legítimos. Especifica que esta práctica es utilizada por investigadores privados o delincuentes informáticos, para tener información o acceso a sistemas de información que les permitan realizar algún acto que perjudique o exponga a la persona u organismo comprometido a riesgos o abusos. La ingeniería social se sustenta en que es vulnerable y por ende el eslabón débil es el usuario.

2.4.2. *Suplantación de identidad*

La suplantación de identidad en asuntos informáticos es un delito que implica simular la identidad de una persona física, jurídica o una marca comercial en cualquier red social, sitio de

internet, medio electrónico o tecnológico de información. También existe la suplantación de identidad de equipos, que consiste en reemplazar un equipo o servidor informático por otro, con el propósito de obtener información privada de un cliente o usuario (Diccionario Usual, 2020).

Según el Código Penal, será sancionado "con pena de prisión de uno a tres años quien suplante la identidad de una persona en cualquier red social, sitio de Internet, medio electrónico o tecnológico de información" (artículo 230).

Existe una diferencia entre estafas y ataques informáticos. La estafa implica la manipulación ilícita de un tercero mediante la creación de datos falsos o la alteración de datos o procesos contenidos en sistemas informáticos, con el objetivo de obtener ganancias indebidas. Por otro lado, el ataque informático, según Devia (2017), son programas que muestran lo que el usuario ve en su ordenador, son técnicas para espiar a personas mediante un acceso remoto, monitoreando lo que el usuario está haciendo en cada instante, como capturar la digitación que se realiza en ese momento en el teclado y obtener las contraseñas que muestra la pantalla. Es importante resaltar que no todos los ataques informáticos concluyen en una estafa informática; además, también existen mecanismos de defensa contra ellos.

2.5. Tipos de estafas electrónicas

Dentro de las principales estafas electrónicas tenemos los siguientes métodos que utilizan los estafadores para poder sustraer el patrimonio de sus víctimas.

2.5.1. Phishing

El termino phishing proviene del vocablo en ingles fishing cuyo significado en español es pescando, lo relacionan porque los responsables de este fraude se encuentran pescando información personal. El phishing es la acción fraudulenta a través de la cual se procura conseguir información confidencial, mediante diferentes técnicas, por ejemplo, por imitación de correo electrónico de una institución financiera o por técnicas más avanzadas como imitación de páginas electrónicas donde los clientes introducen sus datos personales (Salas, 2010).

Este método se relaciona muy estrechamente con la técnica utilizada mediante la ingeniería social, esto por cuanto existe mayor facilidad para obtener los datos de los usuarios si realizan el proceso de ingeniería social para adquirir los datos sensibles en el cometido de los fraudes.

2.5.2. Smishing

El smishing es una variante del phishing pero con el uso de los mensajes cortos o SMS (Short Message Service, por sus siglas en inglés). También es llamado SMS phishing. La técnica smishing consiste en el envío de mensajes de texto (SMS) cuya actividad criminal es la de obtener, mediante engaños a los usuarios de telefonía móvil, información privada o suscripciones falsas online y ofertas de trabajo en sitios web, para luego introducir spyware o programas con intenciones maliciosas sin el consentimiento del usuario (Devia, 2017).

2.5.3. Vishing

El vishing también es otra variante del phishing pero mediante teléfono. Consiste en el envío de un correo electrónico en el cual los delincuentes consiguen detalles de datos bancarios mediante un número telefónico gratuito, en la cual una voz computarizada de aspecto profesional requiere de las víctimas la confirmación de su cuenta bancaria, solicitándoles el número de cuenta, tarjeta, PIN, etc. (Devia, 2017).

Dentro de estas variantes, según señala Quesada (2023), se ubican las modalidades de estafa más comunes en Costa Rica siendo: el falso funcionario bancario, el falso empleador, y otros.

2.5.4. Falso funcionario bancario

Esta modalidad pertenece al grupo de estafas enmarcadas en la ingeniería social, abarcando también las técnicas de phishing y vishing. Según lo describe Alvarado (2022), en esta modalidad los sospechosos utilizan números enmascarados de los números oficiales de las entidades financieras y líneas IP (VoIP) vía Internet (de acuerdo con Cisco (2024), VoIP se refiere a la transmisión del tráfico de voz sobre redes basadas en Internet). Los estafadores engañan a sus víctimas indicándoles que están transfiriendo dinero de sus cuentas sin su autorización y que deben bloquearlas. Mediante un segundo medio de contacto (WhatsApp o correo electrónico), le indican a la persona, a través de varios hipervínculos, que deben frenar esos movimientos y que para hacerlo deben seguir los hipervínculos enviados.

2.5.5. Falso empleador

Los ciber estafadores en esta modalidad postean anuncios falsos en las diferentes redes sociales como Facebook, Whatsapp, Telegram y otros, en donde anuncian plazas vacantes y solicitan remitir el currículum a buzones que incluyen el nombre de alguna reconocida empresa. Una vez remitido, ya los estafadores tienen la base para realizar la ingeniería social y a partir de

ahí, utilizan números enmascarados con los números reales de esas empresas o bien líneas IP. Durante la llamada, estas personas le indican a la víctima que está contratada, pero que requiere obtener la firma digital, es ahí donde caen en el engaño (Alvarado, 2022).

2.6. Tipos de ataques informáticos

Como se explicó previamente, existe una diferencia entre estafas y ataques informáticos, los ataques informáticos que realizan los infractores no siempre concluyen en la consumación de una estafa informática. Si el cometido es la estafa informática, pueden utilizar las diferentes formas que de seguido se desarrollan con el fin de obtener los datos de ingreso o la información sensible de los clientes bancarios, utilizando los siguientes tipos de ataques.

2.6.1. Malware

Este se refiere a cualquier programa diseñado con intenciones maliciosas, el más conocido de ellos es el troyano. Este se utiliza para introducir un keylogger, lo que en nuestra lengua quiere decir que es un programa que al ejecutarlo lee todo lo ingresado en el teclado y así robar la información que el usuario digite (Regis, 2022).

2.6.2. Spoofing

De acuerdo con el mismo autor, este término se refiere a la estafa en la que el infractor cibernético roba la identidad del usuario u organización con malas intenciones y así adhiere un malware y/o virus al dispositivo o red de la organización.

2.6.3. Pharming

De acuerdo con la explicación amplia proporcionada por Salas (2010), se trata de una práctica delictiva realizada por un pirata informático, que consiste en desviar el tráfico de internet de un sitio web legítimo hacia otro sitio falso similar, con el propósito de obtener los nombres y contraseñas de acceso que los usuarios ingresan, los cuales son registrados en la base de datos del sitio falso. Esto se hace con la intención de cometer estafas suplantando la identidad de los usuarios. El desvío del tráfico entre los sitios web se lleva a cabo mediante la modificación de los DNS (Domain Name System, por sus siglas en inglés) o Servidores de Nombres de Dominio, los cuales son los datos que relacionan la página auténtica con su dirección IP (Internet Protocol) o protocolo de internet, lo que hace que el usuario crea que está accediendo al sitio genuino.

2.7. Medidas de seguridad de los bancos

Las medidas de seguridad que los bancos establecen para asegurar la información, el Banco Central de Costa Rica (BCCR) lo define como la conservación de la confidencialidad, integridad y disponibilidad de la información; incorporando otras propiedades de igual importancia como son la autenticidad, la responsabilidad, el no repudio, e inclusive la certeza (BCCR, 2024). Estas medidas son implementadas por los bancos y deben ser de aplicación por los usuarios.

2.7.1. Factor de doble autenticación

La autenticación de doble factor es un modo robusto de identificarse en el que se utilizan dos factores que aporta el usuario, uno es algo que es de su conocimiento (puede ser una contraseña) y segundo algo que tiene (puede ser un teléfono, un token o huella dactilar). Dentro del segundo factor se suele utilizar el envío de un SMS al teléfono asociado a dicha cuenta bancaria (LISA Institute, 2024).

Así mismo, de acuerdo con el voto Nº 26–2023 del Tribunal Contencioso Administrativo Sección I, del 24 de marzo del 2023 de las 16:10, la autenticación, "se va a entender como la forma en que un sistema verifica o se asegura que un usuario que intenta acceder y realizar acciones dentro del sistema, es quien dice ser y que tiene autorización para hacer lo que pretende" (ídem).

2.7.2. Nombre de usuario

En el entorno de las redes informáticas: "un usuario se refiere a una persona o entidad que utiliza los recursos y servicios de una red para realizar tareas específicas. Un usuario puede ser un individuo, una organización u otros" (Polaridad.es, 2024, párr. 2).

Un usuario de acuerdo con el mismo autor citado anteriormente "es un individuo o entidad que utiliza los recursos y servicios de una red para realizar tareas específicas". Adicionalmente señala que "los usuarios generalmente tienen cuentas de inicio de sesión únicas que les permiten acceder a los recursos y servicios de la red" (ídem).

El nombre de usuario es un identificador único de cliente mediante el cual el propietario de un sistema informático elige identificar a un usuario que visita su sitio web o aplicación móvil (Google Ads, 2024).

2.7.3. Contraseña

Scarfone (2009) define la contraseña como una secuencia de caracteres secretos (combinación de letras, dígitos o signos) que el usuario utiliza para autentificar su identidad en un

sistema informático, con el fin de proteger datos, sistemas y redes. Adicionalmente, las contraseñas pueden ser de menor visibilidad, mediante un dispositivo biométrico que genera una contraseña basada en huellas dactilares, o también mediante un número de identificación personal o conocido comúnmente como PIN (Personal Identification Number por sus siglas en inglés).

2.7.3.1. PIN.

Un PIN es relativamente corta (generalmente de 4 a 6 caracteres) y consta únicamente de números. Los PIN son utilizados para sistemas de alarma, cajeros automáticos o ATM (Automated Teller Machine por sus siglas en inglés), dispositivos de token de seguridad y otros dispositivos que tienen teclados pequeños. Los PIN rara vez se utilizan como única forma de autenticación para acceder al sistema informáticos. (Scarfone, 2009)

2.7.3.2. Identificación por huella dactilar.

Rojas (2023) define las huellas dactilares, como "únicas para cada individuo (incluso en gemelos idénticos de misma bolsa), son inmutables y son perennes, características que las hacen uno de los mejores rasgos biométricos para poder identificar personas ya sea con fines forenses o de control de acceso" (párr. 19).

2.7.4. Antivirus

De acuerdo con la página de ESET (2024), el termino antivirus generalmente se refiere al software (de acuerdo con la Real Academia Española es un conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora) de seguridad que, a través de múltiples capas de protección, detecta, bloquea y elimina el malware y protege a los usuarios de las ciber amenazas.

2.7.5. Sitio web seguro

El Digital Server (2024) señala que un sitio seguro es aquel que utiliza protocolo HTTPS o Hypertext Transfer Protocol Secure (se puede traducir al español como protocolo de transferencia de hipertexto seguro), para asegurar que la información intercambiada entre el usuario y el servidor no puede ser vista o manipulada por terceros.

2.7.6. Red segura

Según Rudra (2023), una red segura es “una red privada protegida por un cortafuegos y con acceso externo limitado. En otras palabras, es un sistema cerrado que sólo permite a determinadas personas acceder a recursos específicos como archivos, carpetas y aplicaciones”. También puede denominarse red privada o intranet.

2.7.7. Alertas de transacciones

De acuerdo con Visa (2024), el servicio de alertas ayuda a evitar fraude y mantener las cuentas seguras, ya que los tarjetahabientes pueden identificar transacciones fraudulentas casi en tiempo real, recibiendo un mensaje de texto al celular, correo electrónico o a la aplicación, alertándote de una compra inusual en base a tu historial y a los parámetros establecidos.

CAPÍTULO III: MARCO METODOLOGÍCO

Para la investigación del presente tema se implementará la investigación documental, ya que el tema en estudio se desarrollará con fuentes de investigación que incluyen libros, artículos científicos, normativa, Jurisprudencia y demás fuentes formales. Además, se utilizará investigación de campo mediante entrevistas a expertos y encuestas.

3.1 Enfoque de la investigación

El enfoque por utilizar para el desarrollo de este estudio es el mixto. Para Hernández, Baptista y Fernández (2014, citando a Hernández y Mendoza, 2008), definen el método de investigación mixto como un conjunto de procesos sistemáticos, empíricos y críticos, que implican la recolección y el análisis de datos tanto cuantitativos como cualitativos, para su integración y discusión conjunta, con el objetivo de obtener deducciones producto de toda la información recabada (metainferencias) y lograr un mayor entendimiento del fenómeno bajo estudio.

De igual manera Gregorio (2023) define la investigación mixta, como la agrupación de información y datos de los métodos cualitativo y cuantitativo, empleando técnicas de los dos enfoques a la vez, valora ambas perspectivas para fundir, integrar y complementar información, así como las fuentes y técnicas cualitativas y cuantitativas, con el propósito de realizar un análisis integrador en el problema.

Por lo anterior, el enfoque mixto se ajusta a la investigación en curso, porque el protagonismo se orienta en las normas y Jurisprudencia, sin embargo, analizar los datos cuantitativos es relevante para esta investigación. En este ensayo la observación de los diferentes antecedentes jurisprudenciales es muy importante, para definir la responsabilidad directa de los Bancos Estatales con los clientes en las estafas electrónicas, así como las estadísticas derivadas.

3.2 Métodos de Investigación

Dentro de la presente investigación se utilizará el método deductivo, el cual Tena y Rivas (1995) lo definen como un método de razonamiento teórico, que parte del estudio de hechos prácticos y concretos, formando un sistema axiomático (que pretende ir más allá de las mismas disciplinas formales que le han dado origen) totalmente ideal, que no corresponde a una realidad, que permite manejarla y calcularla.

Así mismo, Rodríguez (2005) explica que es un proceso que consiste en obtener conclusiones particulares a partir de una ley universal. Este método consta en determinar los hechos

más importantes, deducir las relaciones constantes de naturaleza uniforme que dan lugar al fenómeno, con base en las anteriores se formula la hipótesis, se observa la realidad para comprobarla y de esto, se deducen leyes. Este método parte de verdades generales y progresa por el razonamiento.

Por lo tanto, el método deductivo es el que se adecua al ensayo. Esto porque se analizará desde lo general de la normativa y Jurisprudencia hasta poder llegar a las conclusiones, acerca de la responsabilidad directa de los Bancos Estatales con los clientes en el tema que nos ocupa.

3.3 Tipos de investigación

El tipo de investigación a utilizar es el Fenomenológico. Taylor y Bodgan (1984) mencionan que "el fenomenólogo busca comprensión por medio de métodos cualitativos tales como la observación participante, la entrevista en profundidad y otros, que generan datos descriptivos" (p.16).

El método fenomenológico se ajusta a la investigación ya que nos permite observar los diferentes criterios y normas en profundidad. Al respecto, Hernández et al. (2014) señala que: "Su propósito principal es explorar, describir y comprender las experiencias de las personas con respecto a un fenómeno y descubrir los elementos en común de tales vivencias" (p. 493).

3.4 Fuentes de información.

Para López (2017) las fuentes de información de acuerdo con la literatura clásica se clasifican dependiendo de la perspectiva desde la que se traten, pero las más reconocidas son de acuerdo con el nivel de información, y se clasifican en primarias, secundarias, terciarias y obras de consulta y referencia.

3.4.1. Primarias

Las fuentes de información primarias según López (2017) son "aquellos que tienen un carácter original, que no han sufrido ningún proceso de transformación o cambio, por ejemplo un libro, un periódico, una revista" (p. 27).

Para la presente investigación se utilizarán como fuentes primarias: obras literarias, normativa legal, publicaciones ide revistas digitales periódicas, documentos gubernamentales, trabajos finales de graduación, expertos en el tema presentados en conferencias o seminarios virtuales a través de la internet, así como entrevistas físicas al personal jurídico relevante para la

obtención de la información elemental para la investigación, entre los sujetos a entrevistar se acudirá a: Administrativos, jefaturas, abogados públicos y privados de la banca estatal y de los despachos legales.

3.4.2. Secundarias

Como fuentes de información secundarias Cordón et al., citado por López (2017), las define como "aquellos que resultan del análisis y del tratamiento de los documentos primarios y dan lugar a un documento diferente, por ejemplo, una bibliografía, una base de datos de resúmenes" (p. 28).

Las fuentes secundarias por utilizar en la investigación consistirán en: Análisis de Jurisprudencia de los tribunales nacionales y de las diferentes Salas de la Corte Suprema de Justicia, bibliografías, índices y compilación general de información.

3.4.3. Terciarias

Así mismo, las fuentes documentales terciarias para Cordón et al., citado por López (2017), son "aquellos que someten a revisión los materiales primarios y secundarios, por ejemplo, una bibliografía de bibliografías o un índice bibliográfico" (p. 28).

3.5 Sujetos de información

3.5.1. Población

De acuerdo con Hernández y Mendoza (2018, citando a Chaudhuri, 2018 y Lepkowski, 2008) la población es el conjunto de todos los casos que coinciden en una serie de especificaciones.

3.5.2. Muestra

Según Gómez (2006) la muestra es una unidad de análisis o un grupo de ellas, sobre las que se recolectan datos, sin que sean necesariamente representativas de la población que se estudia.

3.5.2.1. Tipo de muestra.

Las muestras se clasifican en dos grandes ramas: las no probabilísticas y las probabilísticas, para efectos de esta investigación se trabaja con la primera, la cual se define de la siguiente manera.

En las muestras no probabilísticas, la elección de los elementos no depende de la probabilidad, sino de causas relacionadas con las características de la investigación o de quien hace

la muestra. Aquí el procedimiento “no es mecánico, ni con base en fórmulas de probabilidad” (Gómez, 2006, p. 111).

Dentro del muestreo no probabilístico tenemos el intencional y el accidental, entre otros. Para los fines de esta teoría se utiliza el muestreo intencional, que según Flores (2014): “es un procedimiento que permite seleccionar los casos característicos de la población limitando la muestra a estos casos” (p. 113).

3.6 Consideraciones éticas

Para Galeano (2004) las consideraciones éticas en la investigación social cualitativa son frecuentemente menos vistas y más sutiles que cuando se hacen en los métodos cuantitativos. Se asume la ética como práctica, modo de vida, y se presentan como los ejes éticos básicos la integridad del proceso, responsabilidad hacia los informantes (consentimiento informado, confidencialidad, anonimato y derechos de autor), pertinencia de las técnicas de recolección y registro de la información, manejo del riesgo y reciprocidad.

3.7 Variables de análisis

Objetivo	**Variables**	**Subvariables**	**Fuentes de Información**
Estudiar los tipos de responsabilidad que se aplican en el Sistema Jurídico Costarricense en las estafas informáticas.	Sistema Jurídico Costarricense	Norma Jurisprudencia Sala Primera Jurisdicción Contencioso-Administrativo y Civil de Hacienda MEIC	Huerta (2007) González (2021) Kelsen (1925/1949) Diccionario Usual del Poder Judicial (2020) Hierro (2003) Ley Orgánica del Poder Judicial () Constitución Política (1949) Código Procesal Contencioso-Administrativo () MEIC (2023) Ley de Promoción de la Libre Competencia y Defensa Efectiva del Consumidor () Fernández (2014) Calvo (2022)
	Tipos de responsabilidades jurídicas	Subjetiva Objetiva Civil	
Definición conceptual			

Tipos de responsabilidades jurídicas en el Sistema Jurídico Costarricense para las estafas informáticas			
Definición operacional			
Responsabilidad Subjetiva	Responsabilidad Objetiva	Responsabilidad Civil	
Definición instrumental			
Fuentes de información primara	Fuentes de información primara	Fuentes de información primara	
Objetivo	**Variables**	**Subvariables**	**Fuentes de Información**
Examinar Jurisprudencia sobre la responsabilidad directa de los Bancos Estatales de Costa Rica con los clientes en relación con los fraudes electrónicos	Responsabilidad Civil	Contractual Extracontractual Directa Indirecta	Salas (2010) Fernández (2014)
	Bancos Estatales de Costa Rica	BCCR CONNASSIF SUGEF BNCR BCR BPDC	Diccionario Usual del Poder Judicial (2020) Ley Orgánica del Banco Central de Costa Rica
	Estafas informáticas	Ingeniería Social Suplantación de Identidad Phishing Smishing Vishing Falso funcionario bancario Falso empleador	Burgos (2020) Código Penal Salas (2010) Diccionario Usual del Poder Judicial (2020) Devia (2017) Quesada (2023) Alvarado (2022)
	Ataques informáticos	Malware Spoofing Pharming	Regis (2022) Salas (2010)

<table>
<tr><td colspan="4">Definición conceptual
Responsabilidad directa de los Bancos Estatales de Costa Rica en estafas informáticas</td></tr>
<tr><td colspan="4">Definición Operacional</td></tr>
<tr><td>Responsabilidad Civil</td><td>Bancos Estatales de Costa Rica</td><td colspan="2">Estafas y ataques informáticos</td></tr>
<tr><td colspan="4">Definición instrumental</td></tr>
<tr><td>Encuesta</td><td>Encuesta</td><td colspan="2">Encuesta</td></tr>
<tr><td>Objetivo</td><td>Variables</td><td>Subvariables</td><td>Fuentes de Información</td></tr>
<tr><td>Ahondar en las medidas de seguridad desarrolladas por los Bancos Estatales de Costa Rica para mitigar los efectos de las estafas electrónicas</td><td>Medidas de seguridad de los bancos</td><td>Factor de doble autenticación
Nombre de usuario
Contraseña
PIN
Identificación por huella dactilar
Antivirus
Sitio web seguro
Red segura
Alertas de transacciones</td><td>BCCR (2024)
LISA Institute (2024)
Tribunal Contencioso Administrativo
Google Ads (2024)
Scarfone (2009)
Rojas (2023)
ESET (2024)
Digital Server (2024)
Rudra (2023)
Visa (2024)</td></tr>
<tr><td colspan="4">Definición conceptual
Medidas de seguridad bancarias</td></tr>
<tr><td colspan="4">Definición Operacional</td></tr>
<tr><td colspan="2">Utilización de medidas de seguridad</td><td colspan="2">Tipos de Medidas de Seguridad</td></tr>
<tr><td colspan="4">Definición instrumental</td></tr>
<tr><td colspan="2">Encuesta</td><td colspan="2">Encuesta</td></tr>
</table>

3.8 Técnicas

Tal como lo indica Ramírez (2018), las técnicas en la metodología cualitativa son los recursos que se pueden utilizar que permiten obtener información que ayude a identificar y describir las cualidades del objeto en estudio. Así mismo, existen diferentes técnicas para recolectar información cualitativa; sin embargo, las más utilizadas son la observación, la entrevista, la historia de vida, el grupo focal, el grupo de discusión y la información documental.

De las anteriores, la observación se define según Ramírez (2018, citando a Hernández, Fernández y Baptista, 2010) como el registro sistemático de comportamientos y situaciones, realizadas a partir de los sentidos, para buscar información específica. La observación se subdivide en: directa, indirecta, no participante, participante, no estructurada, estructurada, de campo, de laboratorio, individual y grupal.

Por otro lado, la entrevista según Ramírez (2018, citando a Hernández, Fernández y Baptista, 2010) es una conversación entre dos o más personas, donde el entrevistador hace preguntas para comprender las perspectivas, situaciones, problemas y soluciones de los consultados con sus propios términos. Esta se puede realizar mediante una guía estructurada, semiestructurada o abierta.

Así mismo, la otra técnica de importancia para la realización de esta investigación es la información documental, que de acuerdo con Ramírez (2018, citando a Ramírez, s.f.) señala que es una recopilación de datos hecha a partir de fuentes bibliográficas, iconografías, entre otros, que permiten explicar como sucedió un acontecimiento y orientar hacia otras fuentes de investigación. Esta se divide en dos tipos, los documentos escritos y los materiales audiovisuales.

3.9 Instrumentos

La elaboración de instrumentos para la obtención de información sobre una determinada construcción teórica exige una fundamentación técnica sobre aquello que queremos medir, y una construcción de instrumentos contrastados con la opinión de expertos y con la plausibilidad de que sea aplicable realmente en la recopilación de datos, comprobable mediante su aplicación y valoración de efectividad en lo pretendido (Martínez, 2014).

Para la presente investigación se utilizarán los siguientes instrumentos de medición:

- **Información documental**: La información documental consiste en la lectura y comprensión de las diferentes fuentes de información primarias escritas, como lo son el análisis de normativa y Jurisprudencia a profundidad.
- **Encuesta**: un conjunto de preguntas, normalmente de varios tipos, preparado sistemática y cuidadosamente, sobre los hechos y aspectos que interesan en una investigación o evaluación, y que puede ser aplicado en formas variadas, entre las que destacan su administración a grupos o su envío por correo.

- **Entrevistas no estructuradas**: Es una de las fuentes más utilizadas en la investigación. Mediante esta una persona (entrevistador) solicita información a otra (entrevistado). Puede ser uno de los instrumentos más valiosos para conseguir información, se puede definir como: El arte de escuchar y captar información.

3.10 Proceso para la Recolección y Análisis de Datos

Una de las formas de procesar los acontecimientos es mediante la triangulación de datos, y según Martínez (2014) esta se define como:

> La triangulación es una técnica que utiliza diferentes tipos de fuentes para asegurar las evidencias. El principio que subyace es el de recoger observaciones de una situación desde una variedad de perspectivas para después compararlas y contrastarlas. La investigación cualitativa utiliza diversidad de fuentes y técnicas de recogida de datos para evitar sesgos y asegurar la exactitud. (p. 95)

La recopilación de datos mixta es de naturaleza exploratoria, implica un análisis e investigación a profundidad. Los métodos de recolección de datos mixto no se enfocan en un método especifico, se profundiza de diversas formas para su recopilación.

Dado que la investigación es limitada a una población particular sea esta la Banca Estatal y a los clientes, entre éstos los que han sufrido estafas informáticas, se procede a establecer un mecanismo de investigación científica a través del uso del muestreo por conveniencia no probabilístico y no aleatorio.

Para la presente investigación se hará uso de la entrevista no estructurada y del muestreo por conveniencia, el cual según los autores Hernández, Baptista y Fernández (2014) se trata de una técnica de muestreo no probabilístico y no aleatorio utilizada para crear muestras de acuerdo con la facilidad de acceso, la disponibilidad de las personas de formar parte de la muestra en un intervalo de tiempo dado o cualquier otra especificación práctica de un elemento particular.

El investigador elige a los miembros solo por su conveniencia y no considera si realmente estos representan muestra representativa de toda la población o no. Cuando se utiliza esta técnica, se pueden observar hábitos, opiniones y puntos de vista de manera más fácil.

De acuerdo con Hernández, Baptista y Fernández (2014), los investigadores utilizan técnicas de muestreo en situaciones en las que hay grandes poblaciones para ser evaluadas, ya que,

en la mayoría de los casos, es casi imposible realizar pruebas a toda una población, incluso aunque muchos evitan implementar esta técnica, el muestreo por conveniencia es clave en situaciones en las que un investigador pretende obtener información en un lapso más corto y sin invertir demasiado dinero.

CAPÍTULO IV: ANÁLISIS NORMATIVO Y JURISPRUDENCIAL

Dentro del objetivo principal de esta investigación es el análisis normativo y jurisprudencial sobre la responsabilidad de los Bancos Estatales para con los clientes en casos de fraudes electrónicos, entre los años 2019 al 2023, por lo que a continuación se analiza la normativa relacionada, así como la Jurisprudencia de interés.

4.1 Normativa

Se analiza la normativa nacional e internacional relacionada con la investigación, la misma esta estructura siguiendo el orden jerárquico de la pirámide de Kelsen, por lo que se incorporan las directrices internacionales dentro de este apartado.

4.1.1 Constitución Política

A través de toda la investigación es claro que existe un acelerado crecimiento tecnológico en la sociedad, y como reflejo de ello nuestra Carta Magna también se actualiza para abarcar y proteger todos los derechos de los ciudadanos costarricenses, es por esto que el 29 de noviembre del 2023 mediante la Ley N° 10385 se adiciona un fragmento de esta Norma Suprema, que dice: "(…) toda persona tiene el derecho fundamental al acceso a las telecomunicaciones, y tecnologías de la información y comunicaciones en todo el territorio nacional. El Estado garantizará, protegerá y preservará este derecho" (art. 24).

Resulta una obligación del Estado garantizar el acceso a las tecnologías de la información para toda la población, incentivando el uso de estas. Producto de este principio al aumentar el acceso a la tecnología y como medida de protección, se debe capacitar a la población, para disminuir los riesgos informáticos a los que están expuestos, siendo uno de estos, el riesgo a las estafas informáticas.

Al mismo tiempo el artículo 46 de la Ley Fundamental establece entre otras cosas que: "(…) los consumidores y usuarios tienen derecho a la protección de su salud, ambiente, seguridad e intereses económicos; a recibir información adecuada y veraz; a la libertad de elección, y a un trato equitativo" (art. 46).

Por lo tanto, el Estado está en la obligación de proteger la seguridad e intereses económicos de los usuarios bancarios, razón por la que debe de tomar las medidas necesarias para velar por su cumplimiento, dentro de las facultades como Estado, al Poder Legislativo se le faculta la creación

o modificación de leyes que le permita cumplir con este principio fundamental, y de esta forma disminuir los riesgos a los ataques y estafas informáticas, a las que se exponen los consumidores y usuarios de los servicios bancarios.

4.1.2 Ley 7472, Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor

Con el objetivo de proteger, efectivamente, los derechos y los intereses legítimos del consumidor, se proclama la Ley 7472; dentro de esta, se delimita la responsabilidad objetiva ante el consumidor, específicamente en el artículo 35, el cual señala:

> Artículo 35.- Régimen de responsabilidad.
>
> El productor, el proveedor y el comerciante deben responder concurrente e independientemente de la existencia de culpa, si el consumidor resulta perjudicado por razón del bien o el servicio, de informaciones inadecuadas o insuficientes sobre ellos o de su utilización y riesgos.
>
> **Sólo se libera quien demuestre que ha sido ajeno al daño**.
>
> Los representantes legales de los establecimientos mercantiles o, en su caso, los encargados del negocio son responsables por los actos o los hechos propios o por los de sus dependientes o auxiliares. Los técnicos, los encargados de la elaboración y el control responden solidariamente, cuando así corresponda, por las violaciones a esta Ley en perjuicio del consumidor. (**La negrita no pertenece al original**)

Dentro del ámbito jurídico definido, se establecen las obligaciones y derechos recíprocos entre el consumidor y en el caso que nos ocupa, los Bancos; este último teniendo la obligación de suministrar el servicio de forma segura, ininterrumpida y de manera informada. Por lo que debe proporcionar al cliente información suficiente para que este tome una decisión con un panorama completo de riesgos y beneficios.

Se establece que el proveedor del servicio, independientemente de la existencia de culpa, si el consumidor se ve perjudicado producto del riesgo que conlleva, el comerciante, en este caso los Bancos Estatales, deben resarcir el daño patrimonial acontecido producto del riesgo.

Ahora bien, de acuerdo con el articulo 35 ya citado, solo se libera el que demuestre que es ajeno al daño, lo que quiere decir, que, si los Bancos Estatales demuestran que no tuvieron culpa, porque se cumplieron las medidas de seguridad establecidas, y la falta fue de la víctima o por fuerza

mayor o hechos de un tercero, entonces se exonera de dicha responsabilidad y por lo tanto de resarcir el daño patrimonial provocado mediante una estafa informática.

Este artículo es medular en el análisis que para los efectos realizan las diferentes instancias judiciales y administrativas, ya que delimita bajo que circunstancias se debe resarcir el daño patrimonial provocado por los riesgos del servicio, y bajo que hipótesis se excluye dicha responsabilidad.

4.1.3 Código de Comercio

En el Código de Comercio se establecen algunas características de la relación comercial entre los consumidores y los entes bancarios, de seguido se puntean los artículos más relevantes.

> Artículo 613, la apertura de una cuenta corriente es facultativa de los bancos, para lo cual podrán establecer las condiciones que estimen necesarias.
>
> Artículo 614, el contrato de cuenta corriente, ya se origine en depósito o en crédito debe ser expreso y constar por escrito.
>
> Artículo 615, Las cuentas corrientes bancarias son inviolables y los bancos solo podrán suministrar información sobre ellas a solicitud o con autorización escrita del dueño, o por orden de autoridad judicial competente. Se exceptúa la intervención que en cumplimiento de sus funciones determinadas por la ley haga la Superintendencia General de Entidades Financieras, o la Dirección General de Tributación autorizada al efecto. (Código de Comercio)

De los artículos anteriores se desprende que el servicio de cuentas bancarias es facultativo de los bancos, y pueden establecer las condiciones que ellos estimen necesarias, entre estas podemos señalar las cláusulas del servicio de banca por internet o aplicaciones móviles, donde se expresan las condiciones para brindar el servicio, así como la responsabilidad de los usuarios, con el manejo que le den a la información confidencial, para el ingreso a estas fuentes de acceso electrónico.

Así mismo, de acuerdo con el artículo 614, es necesario que los contratos sean expresos y deben constar por escrito, bajo el resguardo del ente bancario.

El último artículo referenciado, señala la privacidad de la información del cliente, como es asentado en la Carta Magna que, bajo algunas excepciones, dentro de lo que nos compete en la

investigación, los Banco Estatales no pueden brindar la información de los usuarios. Por lo que es el responsable de velar por el cumplimiento de este principio fundamental, y de mitigar el riesgo de una eventual pérdida o fuga de información.

4.1.4 Código Penal

Es importante señalar que los delitos de estafa están tipificados en el Código Penal, sin embargo, se hace mención, pero no hay que dejar de lado que en esta investigación lo que se pretende demostrar es la responsabilidad civil de los Bancos Estatales, sin embargo, es conveniente señalar los tipos penales relacionados con el tema de investigación.

Dentro de los delitos de estafa tenemos los siguientes artículos relacionados en este cuerpo normativo.

> Artículo 216. Quien induciendo a error a otra persona o manteniéndola en él, por medio de la simulación de hechos falsos o por medio de la deformación o el ocultamiento de hechos verdaderos, utilizándolos para obtener un beneficio patrimonial antijurídico para sí o para un tercero, lesione el patrimonio ajeno, será sancionado en la siguiente forma:
>
> 1.-Con prisión de dos meses a tres años, si el monto de lo defraudado no excediere de diez veces el salario base.
>
> 2.-Con prisión de seis meses a diez años, si el monto de lo defraudado excediere de diez veces el salario base.
>
> Las penas precedentes se elevarán en un tercio cuando los hechos señalados los realice quien sea apoderado o administrador de una empresa que obtenga, total o parcialmente, sus recursos del ahorro del público, o por quien, personalmente o por medio de una entidad inscrita o no inscrita, de cualquier naturaleza, haya obtenido sus recursos, total o parcialmente del ahorro del público. (ídem)

Del artículo anterior se desprende como sí los recursos son sustraídos por un individuo o por medio de una entidad financiera se incrementa la pena en un tercio, siendo un agravante el hecho de que la sustracción sea del ahorro del público, como lo son los fondos que administran los Bancos Estatales.

> Artículo 217 bis. Estafa informática. Se impondrá prisión de tres a seis años a quien, en perjuicio de una persona física o jurídica, manipule o influya en el ingreso, en el

> procesamiento o en el resultado de los datos de un sistema automatizado de información, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos, programación, valiéndose de alguna operación informática o artificio tecnológico, o bien, por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro.
>
> La pena será de cinco a diez años de prisión, si las conductas son cometidas contra sistemas de información públicos, sistemas de información bancarios y de entidades financieras, o cuando el autor es un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos. (ídem)

Este artículo señala los tipos asociados al delito de estafa informática, y de acuerdo con los conceptos desarrollados se incluyen tanto los tipos de estafas informáticas, como la ingeniería social, la suplantación de identidad, el phishing, entre otros, así como los ataques informáticos por malware o pharming, siendo un agravante si las estafas son cometidas contra sistemas de información bancarios.

> Artículo 229 ter. Sabotaje informático. Se impondrá pena de prisión de tres a seis años al que, en provecho propio o de un tercero, destruya, altere, entorpezca o inutilice la información contenida en una base de datos, o bien, impida, altere, obstaculice o modifique sin autorización el funcionamiento de un sistema de tratamiento de información, sus partes o componentes físicos o lógicos, o un sistema informático.
>
> La pena será de cuatro a ocho años de prisión cuando:
>
> a) Como consecuencia de la conducta del autor sobrevenga peligro colectivo o daño social.
>
> b) La conducta se realice por parte de un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.
>
> c) El sistema informático sea de carácter público o la información esté contenida en bases de datos públicas.

> d) Sin estar facultado, emplee medios tecnológicos que impidan a personas autorizadas el acceso lícito de los sistemas o redes de telecomunicaciones. (ídem)

En este artículo de acuerdo con los conceptos desarrollados, se relaciona estrechamente con el ataque informático denominado pharming, donde se realiza un desvío de datos de un sitio web seguro a uno falso, esto por cuanto está modificando un sistema informático para obtener un beneficio patrimonial propio o a favor de un tercero.

> Artículo 230. Suplantación de identidad. Será sancionado con pena de prisión de uno a tres años quien suplante la identidad de una persona física, jurídica o de una marca comercial en cualquiera red social, sitio de Internet, medio electrónico o tecnológico de información. (ídem)

La suplantación de identidad de una persona física o un sitio web bancario es sancionada con este tipo penal, bajo estas circunstancias se están utilizando estafas mediante engaño como la ingeniería social o con ataques informáticos como el pharming, con un sitio web falso homogéneo al real, para obtener las credenciales de acceso y demás información relevante para el ciberdelincuente.

> Artículo 231. Espionaje informático. Se impondrá prisión de tres a seis años al que, sin autorización del titular o responsable, valiéndose de cualquier manipulación informática o tecnológica, se apodere, transmita, copie, modifique, destruya, utilice, bloquee o recicle información de valor para el tráfico económico de la industria y el comercio. (ídem)

La persona que realice este tipo delictivo no es necesariamente el que obtenga un provecho patrimonial de un tercero, esto por cuanto, la persona que realiza el espionaje puede trasmitir los datos obtenidos a un tercero, para que realice la estafa electrónica. Por ello, es muy importante de resaltar, que, aunque no sea el ciberdelincuente que obtiene el patrimonio de un tercero, pero si colaboró para obtener las credenciales de acceso u otra información para cometer el delito, igual tiene pena privativa de libertad.

> Artículo 232. Instalación o propagación de programas informáticos maliciosos. Será sancionado con prisión de uno a seis años quien, sin autorización, y por cualquier medio, instale programas informáticos maliciosos en un sistema o red informática o telemática, o en los contenedores electrónicos, ópticos o magnéticos. (ídem)

La misma pena se impondrá en los siguientes casos:

a) A quien induzca a error a una persona para que instale un programa informático malicioso en un sistema o red informática o telemática, o en los contenedores electrónicos, ópticos o magnéticos, sin la debida autorización.

b) A quien, sin autorización, instale programas o aplicaciones informáticas dañinas en sitios de Internet legítimos, con el fin de convertirlos en medios idóneos para propagar programas informáticos maliciosos, conocidos como sitios de Internet atacantes.

c) A quien, para propagar programas informáticos maliciosos, invite a otras personas a descargar archivos o a visitar sitios de Internet que permitan la instalación de programas informáticos maliciosos.

d) A quien distribuya programas informáticos diseñados para la creación de programas informáticos maliciosos.

e) A quien ofrezca, contrate o brinde servicios de denegación de servicios, envío de comunicaciones masivas no solicitadas, o propagación de programas informáticos maliciosos.

La pena será de tres a nueve años de prisión cuando el programa informático malicioso:

i) Afecte a una entidad bancaria, financiera, cooperativa de ahorro y crédito, asociación solidarista o ente estatal.

ii) Afecte el funcionamiento de servicios públicos.

iii) Obtenga el control a distancia de un sistema o de una red informática para formar parte de una red de ordenadores zombi.

iv) Esté diseñado para realizar acciones dirigidas a procurar un beneficio patrimonial para sí o para un tercero.

v) Afecte sistemas informáticos de la salud y la afectación de estos pueda poner en peligro la salud o vida de las personas.

vi) Tenga la capacidad de reproducirse sin la necesidad de intervención adicional por parte del usuario legítimo del sistema informático. (ídem)

Este tipo penal aumenta la privación de libertad si el delito es cometido con el fin de afectar a una entidad bancaria como lo son los Bancos Estatales, lo que ampara a las instituciones financieras contra estos delitos informáticos, en los que hemos visto, como aumentan las penas si los actos delictivos son cometidos contra los intereses del patrimonio de la sociedad que se resguarda en los entes financieros.

> Artículo 233. Suplantación de páginas electrónicas. Se impondrá pena de prisión de uno a tres años a quien, en perjuicio de un tercero, suplante sitios legítimos de la red de Internet.
>
> La pena será de tres a seis años de prisión cuando, como consecuencia de la suplantación del sitio legítimo de Internet y mediante engaño o haciendo incurrir en error, capture información confidencial de una persona física o jurídica para beneficio propio o de un tercero. (ídem)

Esta norma está relacionada y deslumbra la pena que obtiene una persona que realice pharming, lo que quiere decir que obtenga datos sensibles a partir de la homologación o suplantación de páginas web bancarias, mediante el engaño o haciendo incurrir en error a los usuarios, que piensan que están frente a un sitio web seguro, y no lo es, si no por el contrario, está un tercero obteniendo la información de las credenciales y demás datos de interés, para sustraerle el dinero de sus cuentas bancarias. La pena es mayor si con la suplantación el imputado obtiene un beneficio propio o para un tercero.

4.1.5 Ley de protección de la persona frente al tratamiento de sus datos personales

Dentro de la investigación es importante señalar que los Bancos Estatales tienen la obligación de resguardar la información confidencial de los clientes, en amparo de los principios fundamentales de la Carta Magna, así como de la directriz internacional referida, y de las normas específicas comentadas anteriormente, donde la seguridad de la información se debe respetar y resguardar bajo todas las medidas necesarias.

> Es por ello, que la Ley de protección de la persona frente al tratamiento de sus datos personales, en la sección III, denominada seguridad y confidencialidad del tratamiento de los datos, señala lo siguiente: Artículo 10. Seguridad de los datos
>
> **El responsable de la base de datos** deberá adoptar las medidas de índole técnica y de organización necesarias **para garantizar la seguridad de los datos de carácter personal**

> y evitar su alteración, destrucción accidental o ilícita, pérdida, tratamiento o acceso no autorizado, así como cualquier otra acción contraria a esta ley.
>
> **Dichas medidas deberán incluir**, al menos, **los mecanismos de seguridad física y lógica más adecuados de acuerdo con el desarrollo tecnológico actual**, **para garantizar la protección de la información almacenada**.
>
> No se registrarán datos personales en bases de datos que no reúnan las condiciones que garanticen plenamente su seguridad e integridad, así como la de los centros de tratamiento, equipos, sistemas y programas.
>
> Por vía de reglamento se establecerán los requisitos y las condiciones que deban reunir las bases de datos automatizadas y manuales, y de las personas que intervengan en el acopio, almacenamiento y uso de los datos. **(La negrita no es del original)**

Por lo anterior y en acatamiento a todas las normas relacionadas, los Bancos Estatales están en la obligación de adquirir e implementar todos los mecanismos de seguridad, físicos y tecnológicos, para el resguardo de la información de los clientes bancarios, garantizando la seguridad y la disminución del riesgo por pérdida de información.

Este acatamiento le es favorable a los Bancos Estatales, porque se asegura que, al contrarrestar los riesgos por pérdida de información, les coadyuba a las condiciones eximentes de la responsabilidad objetiva referida en el artículo 35 de la Ley de promoción de la competencia y defensa efectiva del consumidor.

4.1.6 Ley General de la Administración Pública

Como estamos ante una investigación competente con los Bancos Estatales y, por lo tanto, de carácter público, es necesario señalar la responsabilidad de éstos, mediante el artículo 190, inciso 1, que dice: “la Administración responderá por todos los daños que cause su funcionamiento legítimo o ilegítimo, normal o anormal, salvo fuerza mayor, culpa de la víctima o hecho de un tercero” (art. 190).

De esta norma se desprende, como la Administración, llámese en este caso, los Bancos Estatales, es responsable por los daños causados a raíz de su funcionamiento, muy relacionado con los artículos descritos anteriormente, como el artículo 35 de la Ley de promoción de la competencia

y defensa efectiva del consumidor, dentro de esta responsabilidad encaja la objetiva, producto de las estafas informáticas sufridas por los clientes bancarios.

Sin embargo, este artículo también excluye como responsable a la Administración, si existió fuerza mayor, culpa de la víctima o hecho de un tercero, por lo que, para los Bancos Estatales, es imprescindible demostrar la culpa de la víctima o hecho de un tercero, ostentando que son ajenos al daño, si pretenden no resarcir el daño patrimonial sufrido por los clientes.

4.1.7 Reglamentos de los Bancos Estatales

Dentro de la investigación es menester ahondar en los reglamentos de los servicios de los Bancos Estatales, por lo que de seguido se señalan los principales hallazgos.

- **Reglamento de servicios para Banca en Línea del Banco Popular y de Desarrollo Comunal (2024)**

Dentro del reglamento de servicios para la Banca en Línea del Banco Popular y de Desarrollo Comunal, es menester señalar los artículos 4 y 8 que expresamente establecen lo siguiente:

> Artículo 4. Contraseña de Acceso:
>
> La contraseña de acceso o la correcta validación del Certificado Digital, es la prueba irrefutable de que es el usuario quien accedió al sistema y que todas las operaciones realizadas a través de este medio han sido aceptadas consciente y voluntariamente por él. Es por esta razón que el usuario se obliga a no compartir su contraseña con otra persona, de hacerlo, asumirá la responsabilidad por el uso que esta persona le dé, relevando al BANCO de toda responsabilidad por tal hecho…
>
> Artículo 8. Uso del servicio:
>
> El BANCO excluye y declina cualquier responsabilidad que pudiera derivarse de la transmisión de información entre usuarios a través de la red Internet y no adquiere ninguna responsabilidad por causa de problemas técnicos o fallos mecánicos en los equipos informáticos producidos durante la conexión a la red Internet, ya sea a través de la WEB del BANCO Popular o de WEB de terceros. Del mismo modo, el BANCO declina cualquier responsabilidad derivada de la transmisión de virus informáticos o derivados de daños

causados por terceras personas que, de forma no autorizada, interactúen a través de las páginas WEB del BANCO.

El BANCO no será, en ningún caso, responsable de cualquier reclamo efectuado por el mal uso que el usuario haga del sitio WEB, POPULAR EN LINEA. (Reglamento de servicios para Banca en Línea del Banco Popular y de Desarrollo Comunal, 2024)

Mediante los artículos 4 y 8 del reglamento antes mencionado se traslada al usuario la responsabilidad por el mal uso que se le dé al servicio ofrecido de Banca en Línea, sin embargo, en este no se observa ningún artículo relacionado a capacitar, asesorar o explicar el uso o las medidas de seguridad que deben de tener los usuarios al utilizar este servicio digital.

Dejando de lado la obligación del Estado de proteger al consumidor, fomentando la elaboración de programas y mecanismos para ayudar a que éstos adquieran el conocimiento y competencias que sean necesarias para poder disminuir los riesgos o que comprendan a los que están sometidos por el consumo de un bien o servicio, como en este caso en concreto, un servicio tecnológico.

- **Reglamento para los servicios de Banca Electrónica del Banco de Costa Rica (2016)**

Dentro del reglamento para los servicios de Banca Electrónica del Banco de Costa Rica, es importante ahondar en los artículos 8, 9 y 10, que explícitamente establecen lo siguiente:

Artículo 8. Seguridades (Obligaciones de los clientes)

El uso de los servicios de Banca Electrónica implica que los clientes tienen los siguientes deberes y obligaciones:

a) Conocer y aplicar de manera correcta y segura las instrucciones de operación y los dispositivos de seguridad de los sistemas ofrecidos por el Banco.

b) Tener los cuidados necesarios a efectos de que la clave, PIN y dispositivo de seguridad no sean conocidos por terceras personas.

c) Adoptar y utilizar las medidas de seguridad que el Banco ha sugerido convenientes, respecto de los Sistema electrónicos y de los Servicios Bancarios.

d) Usar personalmente los servicios de la Banca Electrónica y no mostrar a nadie las claves de acceso; en caso contrario, será de su exclusiva responsabilidad cualquier consecuencia dañosa que resultare.

(…)

g) Hacer caso omiso de correos electrónicos que no provengan del Banco y en los que se le solicite información personal, afiliación a cualquier sistema electrónico o similar, debiendo eliminarlo inmediatamente de su buzón.

h) Acceder a los servicios de Banca Electrónica del Banco, únicamente a través del sitio web oficial del Banco, utilizando equipos seguros, dotados de software de seguridad (antivirus, antispyware, entre otros) de una compañía reconocida internacionalmente, debidamente instalado y actualizado de acuerdo a las especificaciones y actualizaciones que el fabricante del antivirus mantenga disponible para el público, omitiendo el acceso a través de otros sitios de referencia (links) a efectos de prevenir accesos o intromisiones ilegítimas. Además, el cliente debe estar seguro de que cuenta con seguridades que impidan la manipulación del hardware y la instalación de dispositivos que permitan el acceso fraudulento a sus datos por parte de terceros…

Artículo 9. Obligaciones del Banco

Con el propósito de cumplir el derecho de acceso a la información previsto en las leyes, y en cumplimiento con el principio del Consentimiento Informado, el Banco asumirá las siguientes obligaciones:

a) Entregar al cliente de manera confidencial la clave secreta o PIN y el dispositivo de seguridad.

b) Informar de manera clara, veraz y oportuna las particularidades de los servicios que se brindan a través de Banca Electrónica…

Artículo 10. Límites de responsabilidad respecto al Banco

En la prestación de servicios por banca electrónica se aplican los siguientes criterios que relevan al Banco de responsabilidad.

a) El incumplimiento en las obligaciones o mal uso de los servicios que se prestan por Banca Electrónica, por parte del cliente o sus autorizados, relevan al Banco de toda responsabilidad por los daños y los perjuicios que puedan resultar.

b) Cuando el cliente o sus autorizados desaplican, inutilizan, o utilizan incorrectamente la clave secreta o PIN y los dispositivos de seguridad a ella asociados.

c) Cuando el cliente o sus autorizados no adoptan ni inutilizan las medidas de seguridad que el Banco ha sugerido convenientes, respecto de los sistemas electrónicos y de los servicios bancarios.

(…)

l) Cuando se produzca algún daño o perjuicio al cliente, producto de la desatención o inadecuadamente utilización de los sistemas electrónicos y medidas de seguridad que el Banco ha sugerido por parte del usuario.

n) Si a pesar de la advertencia anterior, el usuario resultare perjudicado por acciones delictivas efectuadas con la utilización de la clave secreta personal y del dispositivo de acceso, a los cuales los ejecutores de la delincuencia tuvieron acceso por haberlo voluntaria o involuntariamente facilitado el cliente, al realizar el ingreso a bancobcr.com a través de equipos inseguros y deficiente custodia, y el fraude hubiere ocurrido debido a las fragilidades del software o a la manipulación del hardware por tratarse de equipos librados al acceso público, o no haya implementado las seguridades en su equipo indicadas en el artículo 8 de este Reglamento. (Reglamento para los servicios de Banca Electrónica del Banco de Costa Rica, 2016)

Como se puede observar el reglamento para los servicios de Banca Electrónica del Banco de Costa Rica, es muy claro y preciso, e incorpora las medidas necesarias conforme la normativa descrita anteriormente, sin embargo se echa de menos la obligación del Estado de capacitar, asesorar o explicar el uso o las medidas de seguridad que deben de tener los usuarios al utilizar este servicio informático, el reglamento expresa que el cliente debe conocer y acatar las medidas de seguridad, no así, que el Banco brinde el conocimiento necesario para que los clientes determinen si asumen el riesgo de su utilización.

Siendo reiterada la escasa protección al consumidor que brinda el Estado mediante los Bancos Estatales, en su obligación de proteger al consumidor, fomentando la elaboración de programas y mecanismos para ayudar a que éstos adquieran el conocimiento y competencias que sean necesarias para poder reconocer los riesgos a los cuales se someten con su uso.

- **Reglamento de los términos y condiciones de uso de registro de dispositivos móviles en el Banco Nacional de Costa Rica (2023)**

El reglamento con los términos y condiciones de uso de registro de dispositivos móviles del Banco Nacional de Costa Rica establece las obligaciones de seguridad, que deben mantener los clientes en la cláusula quinta, que se transcribe a continuación:

> QUINTA: OBLIGACIONES DE SEGURIDAD. El servicio de registro de dispositivo móvil en el Banco Nacional es un mecanismo de seguridad adicional a las medidas de seguridad existentes... El Cliente en su condición de titular de una clave de acceso y tecnologías de protección que el Banco Nacional brinda para el servicio, se compromete a no suministrar, divulgar o de ninguna forma facilitar el acceso a terceras personas, información asociada a los métodos de autenticación o esquemas de seguridad, tales como: contraseñas, PIN, Token, códigos de seguridad, códigos de verificación, entre otros; y a observar las más estrictas normas de confidencialidad y resguardo de su información personal y de seguridad. Durante el tiempo de uso del servicio el Cliente debe verificar que la computadora y los dispositivos móviles cuenten con la más reciente versión y actualizaciones del APP, navegador o "browser", sistema operativo y antivirus. El Cliente se compromete a mantener sus equipos y dispositivos móviles en óptimas condiciones, libres de virus informáticos, con programas "anti-spyware" (que evitan el ingreso de programas espías) y resguardados de manera tal que no perjudiquen los equipos o sistemas del Banco o la intercepción de los códigos de ingreso. En forma adicional el cliente se compromete a acceder el servicio únicamente en el sitio oficial del Banco HTTPS://www.bncr.fi.cr o a través del software dispuesto por el Banco en las Tiendas oficiales en Apple Store, Google Play o AppGallery. El incumplimiento de estas obligaciones por parte del Cliente, libera al Banco Nacional de todo tipo de responsabilidad con ocasión de eventos que hayan perjudicado al Cliente por violaciones al sistema de seguridad del propio Cliente..., el Cliente se compromete a acatar las recomendaciones que

en materia de seguridad emita el Banco Nacional, entre estas, pero no limitadas a las siguientes:

a) Evitar acceder hipervínculos o ejecutar archivos adjuntos en mensajes de correo electrónico o SMS.

b) No proporcione información personal o referente a sus claves de acceso o Tokens cuando es solicitada por medio de correo electrónico, teléfono (llamada telefónica o SMS) o cualquier otro medio.

c) Nunca ingrese información en un sitio sin haber verificado que el ambiente es seguro, esto se puede reconocer buscando "https://" en la barra de dirección, junto con un candado en la parte inferior derecha de su buscador.

d) Realizar sus transacciones únicamente en sitios seguros o aplicaciones oficiales, asegúrese que cuenta con los requerimientos de seguridad necesarios, de lo contrario no proceda a realizar sus transacciones desde ahí.

e) Utilizar siempre las opciones tecnológicas para la generación de claves aleatorias (OTP), seguros, firma digital y cualquier otro mecanismo que el Banco Nacional brinde e implemente a futuro.

f) Mantener actualizado los sistemas operativos de sus computadores y dispositivos móviles (aplique los parches y recomendaciones del proveedor), el software antivirus, el antispyware y active las funcionalidades de seguridad de su sistema operativo.

g) Reportar a cualquiera de nuestras oficinas, o al teléfono 2212-2000 del

Centro de Contacto del Banco Nacional o a la cuenta de correo bnseg@bncr.fi.cr todo correo sospechoso.

h) Eliminar correos sospechosos o que no conoce su procedencia. Sospeche de direcciones numéricas o vínculos desconocidos que se presenten visualmente parecidos a los presentados por el Banco Nacional.

i) Sospechar de llamadas telefónicas mediante las cuales se ofrezcan negocios fáciles, premios o se realicen promociones donde medie la entrega de información confidencial,

como claves, correos electrónicos o números de tarjetas de crédito o débito, claves aleatorias (OTP) Token, códigos de seguridad, códigos de verificación, entre otros.

j) Nunca brinde sus claves o accesos de servicios electrónicos a otras personas.

k) Ninguna entidad bancaria les solicitará a sus clientes información confidencial como claves, pines o tokens de acceso ni números de tarjetas de débito o crédito. Tampoco lo hará mediante mensajes de texto o de correo electrónico. Reporte inmediatamente al Banco Nacional si detecta una situación sospechosa.

l) Se aconseja no utilizar las mismas claves para ingresar a sitios de banca

electrónica, en otros servicios como redes sociales o cuentas de correo.

m) No se recomienda utilizar los servicios de Wi-Fi públicos para realizar transacciones bancarias, porque otros podrían estar mirando su información. Las transacciones bancarias solo deben realizarse en conexiones de internet privadas.

n) Active el servicio gratuito de alertas en su celular y reciba notificaciones cada vez que realice transacciones.

El incumplimiento de estas obligaciones facultará al Banco Nacional a suspender el servicio. (Reglamento de los términos y condiciones de uso de registro de dispositivos móviles en el Banco Nacional de Costa Rica, 2023)

El Banco Nacional mediante esta norma, es muy explícito y amplio en las medidas de seguridad que se deben realizar para salvaguardar la información confidencial de los usuarios, explica de forma clara y sin términos confusos las medidas que se deben de seguir.

Es muy importante que los Bancos Estatales pongan en conocimiento de los usuarios estas recomendaciones, en primera instancia para trasladar la información a los usuarios y segundo para cumplir con las normativas internas e internacionales que protegen al consumidor, para mitigar los efectos de las estafas informáticas.

Como se puede observar los tres Bancos Estatales cuentan con reglamentos en los que se le informa al cliente de su responsabilidad con el manejo y uso de sus datos confidenciales, sin embargo, se echa de menos la obligación de los entes bancarios de proteger la seguridad de los

consumidores, así como las técnicas de divulgación de información suficientes, para que los usuarios con el conocimiento adecuado asuman el riesgo que conlleva los servicios digitales.

4.2 Jurisprudencia

En este apartado se realiza el análisis jurisprudencial de cinco votos de los veintisiete estudiados con relación a la responsabilidad objetiva en los casos de estafas informáticas en los Bancos Estatales.

4.2.1 Resolución 000300-F-S1-2009

Caso: El expediente 08-000123-0161-CA, Resolución 000300-F-S1-2009, emitida por la Sala Primera de la Corte Suprema de Justicia el 26 de marzo de 2009 a las 11:25, que involucra un proceso de conocimiento en el Tribunal Contencioso Administrativo y Civil de Hacienda interpuesto por la señora María de los Ángeles Arroyo Vargas contra el Banco de Costa Rica.

Hechos: En este caso, la demandante reclama el reintegro de las sumas sustraídas de sus cuentas bancarias a través de fraude electrónico, solicitando también el pago de intereses y costas procesales. El Banco demandado contestó negativamente y opuso varias excepciones, sin embargo, el Tribunal rechazó las defensas y declaró la demanda con lugar. El Banco presentó un recurso de casación argumentando una indebida valoración de la prueba testimonial-pericial y la falta de aplicación de algunas normas legales y reglamentos.

Argumentos legales: En la resolución, el Magistrado González Camacho analiza detalladamente los argumentos presentados por ambas partes. En relación con el numeral 35 de la Ley del Consumidor, de la cual se desprenden una serie de elementos condicionantes de su aplicación, desde el plano de los sujetos, quien causa el daño y quien lo sufre, la aplicación de este régimen de responsabilidad se encuentra supeditada a que en ellos concurran determinadas calificaciones. Así, en cuanto al primero, se exige que sea un productor, proveedor o comerciante, sean estos personas físicas o jurídicas. Por su parte, en cuanto al segundo, la lesión debe ser irrogada a quien participe de una relación jurídica en donde se ubique como consumidor, en los términos definidos en el cuerpo legal de referencia y desarrollados por esta Sala.

Se requiere, entonces, que ambas partes integren una relación de consumo, cuyo objeto sea la potencial adquisición, disfrute o utilización de un bien o servicio por parte del consumidor. Asimismo, del precepto bajo estudio se desprende, que el legislador fijó una serie de criterios de

atribución con base en los cuales se puede imputar la responsabilidad objetiva que regula este cardinal, dentro de los que se encuentra la teoría del riesgo.

Concomitantemente, importa realizar algunas precisiones en cuanto a los riesgos aptos para la generación de la responsabilidad, ya que no todo riesgo implica el surgimiento, en forma automática, de esta. Es importante mencionar que en una actividad es dable encontrar distintos grados de riesgo, los cuales deben ser administrados por aquel sujeto que se beneficia de esta, circunstancia que ejerce una influencia directa en el deber probatorio que le compete, ya que resulta relevante para determinar la imputación en el caso concreto, aunado a la existencia de causales eximentes demuestra que la legislación en comentario no constituye una transferencia patrimonial automática.

Decisión: Concluyendo que no existen vulneraciones a la normativa aplicable ni errores en la interpretación de la responsabilidad del Banco en el caso del fraude electrónico sufrido por la demandante. Se rechaza el recurso presentado y se establece que las costas corren por cuenta del recurrente.

Análisis: En resumen, la resolución confirma la responsabilidad objetiva del Banco de Costa Rica en el caso del fraude electrónico sufrido por la demandante, rechazando las objeciones planteadas por el Banco en su recurso de casación, principalmente porque el Banco no presenta causal excluyente con relación al canon 35 de la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor.

4.2.2 Resolución 000394-F-S1-2009

Caso: El expediente 08-000116-1027-CA, Resolución 000394-F-S1-2009, emitida por la Sala Primera de la Corte Suprema de Justicia el 23 de abril de 2009 a las 10:20, que involucra un proceso de conocimiento en el Tribunal Contencioso Administrativo y Civil de Hacienda interpuesto por Inversiones K M K Sociedad Anónima contra el Banco de Costa Rica.

Hechos: En este caso, la demandante reclama el reintegro de las sumas sustraídas de su cuenta corriente a través de una transferencia electrónica no autorizada, solicitando también el pago de intereses y costas procesales. El Banco demandado contestó negativamente y opuso la defensa previa de falta de integración de litis consorcio necesaria, así como las excepciones de falta de derecho, falta de legitimación activa y pasiva. Sin embargo, el Tribunal resolvió a favor de la demandante, condenando al Banco a reintegrar la cantidad sustraída, pagar intereses y costas

judiciales. El Banco presentó un recurso de casación alegando la indebida interpretación de la Ley de Defensa del Consumidor en cuanto a la responsabilidad por el servicio de banca electrónica, también alegó falta de aplicación de normas contractuales del Banco y violación de principios constitucionales de razonabilidad y proporcionalidad.

Argumentos legales: En la resolución, el Tribunal consideró que el Banco debía responder por el riesgo de su servicio, independientemente de la participación del cliente en la sustracción de la información de su cuenta. Además, rechazó los argumentos del casacionista, indicando que la responsabilidad del banco se basaba en el funcionamiento de su servicio, no en el incumplimiento de cláusulas contractuales por parte del cliente.

De acuerdo con la interpretación del artículo 35 de la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor, el casacionista apunta que la violación aducida se produce al entender que la responsabilidad objetiva por el servicio de banca electrónica se extiende a todos los focos de riesgos que le resultan ajenos, tornando imposible concretar este criterio como eximente de responsabilidad.

Para la Sala no lleva razón el recurrente en cuanto a la vulneración que endilga a la sentencia del Tribunal. En lo que se refiere a la responsabilidad, se pueden ubicar dos grandes vertientes, una subjetiva, en la cual se requiere la concurrencia, y consecuente demostración, del dolo o culpa por parte del autor del hecho dañoso, y otra objetiva, que se caracteriza, en lo esencial, por prescindir de dichos elementos, siendo la imputación del daño el eje central sobre el cual se erige el deber de reparar.

Además, se encuentra el numeral 35 de la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor, en donde el comerciante, productor o proveedor, responderá por aquellos daños derivados de los bienes transados y los servicios prestados, aún y cuando en su actuar no se detecte negligencia, imprudencia, impericia o dolo. Asimismo, es importante considerar, que los elementos determinantes para el surgimiento de la responsabilidad civil, sea esta subjetiva u objetiva, son: una conducta lesiva, la existencia de un daño y un nexo de causalidad que vincule los dos anteriores.

Es importante aclarar que la comprobación de las causas eximentes (culpa de la víctima, de un hecho de tercero o la fuerza mayor), actúa sobre el nexo de causalidad, descartando que la conducta atribuida a la parte demandada fuera la productora de la lesión sufrida.

Coherentemente, importa realizar algunas precisiones en cuanto a los riesgos aptos para la generación de la responsabilidad, ya que no todo riesgo implica el surgimiento, en forma automática, de esta. En una actividad es posible encontrar distintos grados de riesgo, los cuales deben ser administrados por aquel sujeto que se beneficia de esta, situación que ejerce una influencia directa en el deber probatorio que le compete, ya que resulta relevante para determinar la imputación en el caso concreto, aunado a la existencia de causales eximentes que demuestra que la legislación en comentario no constituye una transferencia patrimonial automática.

Decisión: Concluyendo que no existen vulneraciones a la normativa aplicable ni errores en la interpretación de la responsabilidad del Banco en el caso de la sustracción electrónica sufrida por la demandante. Se rechaza el recurso presentado y se establece que las costas corren por cuenta del recurrente.

Análisis: En resumen, la resolución confirma la responsabilidad objetiva del Banco de Costa Rica en el caso de la sustracción electrónica sufrida por la demandante, rechazando las objeciones planteadas por el Banco en su recurso de casación, principalmente porque el Banco no presenta causal eximente con relación al numeral 35 de la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor.

Para estas fechas y aún posteriores, los bancos no utilizaban el doble factor de autenticación, existiendo muchas falencias en la autenticación y acceso a las cuentas bancarias mediante internet, por lo que los bancos no demostraban ante el Tribunal Contencioso Administrativo que eran ajenos al daño, no podían demostrar que era culpa de las víctimas, por lo que la posición y resoluciones de la judicatura eran que existía responsabilidad objetiva por la teoría del riesgo, y así se condenó a los diversos bancos a solventar el daño patrimonial sufrido por los consumidores.

En concordancia con los cambios y evolución en las estafas informáticas, tanto de la realidad, como de la teoría del riesgo y la responsabilidad objetiva aplicable en la materia, del mismo modo, la Jurisprudencia ha venido a responder a estos cambios.

4.2.3 Resolución Nº 01607 - 2012

Caso: El expediente 09-001097-1028-CA, Resolución Nº 01607 - 2012, emitida por la Sala Primera de la Corte Suprema de Justicia el 06 de diciembre del 2012 a las 09:15, que involucra un proceso de conocimiento en el Tribunal Contencioso Administrativo y Civil de Hacienda interpuesto por Fabio Vargas Arias contra el Banco Nacional de Costa Rica.

Hechos: En este caso, el demandante reclama el reintegro de las sumas por la sustracción de sus ahorros a través de Internet Banking, solicitando también el pago de intereses, indexación y costas procesales. El Banco demandado contestó negativamente y opuso las excepciones de falta de derecho, hecho de un tercero y culpa de la víctima. Sin embargo, el Tribunal declaró con lugar la demanda, condenando al Banco a resarcir los daños y perjuicios ocasionados, así como al pago de daño moral y costas procesales. El Banco Nacional formuló un recurso de casación argumentando que el Tribunal aplicando el artículo 35 de la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor, revirtió la carga de la prueba, estimando que el Banco no logró demostrar eximentes que rompieran el nexo de causalidad, a saber, la culpa de la víctima y hecho de un tercero que el recurrente había establecido como defensas.

Argumentos legales: En la resolución, el Tribunal consideró que el Banco no aportó pruebas suficientes para desvirtuar la presunción de buena fe del demandante. Además, se menciona que el Banco prescindió de presentar la prueba ofrecida durante la audiencia preliminar, lo que reforzó la responsabilidad del Banco en el caso. El recurrente señala que con este criterio se torna el sistema de responsabilidad objetiva en un "*callejón sin salida para el demandado*", donde la parte actora, con su simple dicho, le exige al Banco el deber de probar fehacientemente la culpa del cliente, lo cual resulta imposible pues se trata de actos que suceden en su esfera de intimidad o en la de los sujetos autorizados por él.

Adicionalmente, hace alusión al régimen de responsabilidad por riesgo en materia del consumidor. Se ha reiterado que la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor estipula una responsabilidad objetiva para las relaciones de consumo, por la cual, los inconvenientes de una actividad lucrativa han de ser asumidos por quien la desarrolla de acuerdo con el canon 35. Tal como es el caso de la actividad bancaria. Ahora bien, pese a la objetividad, la atribución de responsabilidad al agente, quien asume el riesgo o inconveniente, no opera de pleno derecho. El consumidor, debe demostrar la lesión y el nexo de causalidad con la acción que despliega el sujeto al que la reclama. Este último, debe acreditar el rompimiento de ese vínculo por ajenidad en el daño; esto es, si comprueba los eximentes de hecho de un tercero o culpa de la víctima.

Decisión: Finiquitando que en su impugnación no identifica de qué otros elementos admitidos y practicados se podría concluir la suficiencia de los sistemas de seguridad que

implementó el Banco, y esa carencia es el motivo principal por el cual el Tribunal le atribuyó responsabilidad, de manera que no combate el fallo. Por lo que se resuelve que no existen vulneraciones a la normativa aplicable ni errores en la interpretación de la responsabilidad del Banco en el caso de la sustracción indebida sufrida por el demandante. Se rechaza el recurso presentado y se establece que las costas corren por cuenta del recurrente.

Análisis: En resumen, el Tribunal consideró que, dado el riesgo inherente a las operaciones bancarias en línea, la responsabilidad del Banco debía ser asumida debido a las deficiencias en los sistemas de seguridad y a la falta de pruebas contundentes que eximieran al Banco de responsabilidad en la sustracción de los fondos del demandante con relación al numeral 35 de la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor, si no por el contrario desistió del testigo perito que lo podría demostrar.

4.2.4 Resolución Nº 2606 - 2020

Caso: El expediente 15-000179-0183-CI, Resolución Nº 2606 - 2020, emitida por la Sala Primera de la Corte Suprema de Justicia el 12 de noviembre del 2020 a las 15:22 que involucra un proceso de conocimiento en el Tribunal Contencioso Administrativo y Civil de Hacienda interpuesto por Dorian Brenes Fonseca contra el Banco de Costa Rica.

Hechos: En este caso, el señor Dorian Brenes Fonseca demandó al Banco de Costa Rica por una transferencia fraudulenta realizada desde su cuenta bancaria a la cuenta de otra persona. El demandante solicitó el reintegro del monto sustraído, daños y perjuicios, intereses, indexación, gastos en el proceso penal, honorarios, y daño moral. El demandado contestó negativamente y opuso las excepciones de falta de derecho. Sin embargo, el Tribunal declaró improcedente la demanda, acogiendo la excepción de falta de derecho y señalando que las costas serían a cargo del demandante. El demandante interpuso un recurso de casación alegando que no se valoraron adecuadamente la evidencia y que se aplicó incorrectamente el régimen de responsabilidad.

Argumentos legales: En la resolución, la Cámara respaldó la decisión del Tribunal al considerar que el demandante fue imprudente al revelar la totalidad de su clave dinámica, lo cual permitió la sustracción de fondos por parte de un tercero. Se concluyó que el Banco no fue responsable, ya que el fraude se basó en la información provista por el cliente y no en una vulneración de los sistemas de seguridad del Banco. El demandante apunta, que contrario al criterio de los Juzgadores de instancia en el caso concreto no resulta aplicable tal régimen de

responsabilidad contenido en la Ley General de la Administración Pública, sino el establecido en la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor, dada la relación de consumo existente entre el BCR y su persona.

Sin embrago, los jueces alegan que el régimen de responsabilidad en el derecho del consumidor es de naturaleza objetiva, lo que conlleva a que se deba responder por todo daño cometido en el ejercicio de la actividad, independientemente de que haya mediado culpa o dolo, pues basta con demostrar el nexo causal entre la conducta u omisión desplegada y el resultado dañoso, siempre que en la comisión de este último no medien causas eximentes de responsabilidad (culpa de la víctima, fuerza mayor o hecho de un tercero) las cuales en el derecho del consumidor se denominan como ajenidad del daño.

Así mismo, el Tribunal concluye que tanto la responsabilidad del cliente al suministrar sus datos, de forma consciente o no, pero con causa en su exclusivo actuar, como la conducta desplegada por un tercero, produjeron dos eximentes que hacen que el Banco no deba responder por el reclamo planteado, a saber, culpa de la víctima y hecho de un tercero, o ajenidad en el daño, tal y como lo indica el artículo 190 de la Ley General de la Administración Pública y el artículo 35 de la Ley de la Promoción de la Competencia y Defensa Efectiva del Consumidor.

Decisión: Siendo que el señor Brenes Fonseca obvió las medidas de seguridad y las advertencias difundidas por el Banco, en cuanto a los elementos de protección a observar para este tipo de gestiones en línea, en especial respecto a la no solicitud de la información completa de la clave dinámica. Al demostrarse que los sistemas del Banco no fueron violentados y que se utilizó la clave dinámica de don Dorian para la trasferencia en disputa, resulta evidente que no se dio una función anormal del servicio, por ende, el daño ocasionado deriva de la imprudencia o falta al deber de cuidado de la víctima en el manejo de su información (culpa de la víctima). En consecuencia, dada la existencia de un elemento de ruptura del nexo causal, la responsabilidad objetiva que acusa el recurrente deviene improcedente, de conformidad con el ordinal 35 de la Ley de la Promoción y Defensa Efectiva del Consumidor. Por lo que estima esta Cámara que la valoración probatoria y la aplicación normativa efectuada en el fallo impugnado resultan conforme a derecho. Se declara sin lugar el recurso, con sus costas a cargo de la parte actora.

Análisis: En base a la información presentada previamente, se determinó que el Banco había cumplido con proveer medidas de seguridad y campañas informativas a sus clientes, pero la

responsabilidad recae en el demandante por no resguardar adecuadamente sus datos confidenciales. Ocasionando la ruptura del nexo causal contemplado en el numeral 35 de la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor.

4.2.5 Resolución Nº 00127 - 2020

Caso: El expediente No. 18-007920-1027-CA, resolución Nº 00127 – 2020, emitida por el Tribunal Contencioso Administrativo, Sección IV, el 19 de noviembre del 2020 a las 10:17, que involucra un proceso de conocimiento interpuesto por Desconocido contra el Banco Popular y de Desarrollo Comunal.

Hechos probados:

- El demandante tenía una cuenta de ahorros en el Banco demandado.
- El demandante intentó usar su tarjeta de débito, pero encontró su cuenta sin fondos debido a una transferencia de ¢2.880.000 no autorizada.
- El demandante denunció el fraude ante la Unidad de Prevención y Monitoreo del Banco.
- El Banco mediante oficio UPM-0166-2018 del 25 de enero de 2018 le informó que la transferencia se realizó con la información de usuario y contraseña del cliente.
- El Banco mediante oficio SGN-0433-2018 del 1 de marzo de 2018, de la Sugerencia General de Negocios rechazó el reclamo del accionante.

Hechos no probados:

- No se demostró que los sistemas informáticos del Banco fueran vulnerados para la transferencia no autorizada.

Posiciones de las partes:

- Actor: Alega irresponsabilidad del Banco y reclama daños y perjuicios. Asimismo, manifiesta, que, con lo dicho por la Subgerencia General de Negocios en su respuesta, que el Banco Popular ha realizado una gran cantidad de campañas publicitarias en torno al tema de acceso seguro a la página transaccional, en las que advierte a los clientes que deben estar alertas y guardar las medidas de seguridad requeridas, se evidencia que dicha entidad ya tenía conocimiento de que se estaban presentando situaciones de fraude como la ocurrida a él. Concluyendo que queda completamente acreditado que existió una relación de consumo

entre él y el ente accionado, lo que da surgimiento a la configuración de una Responsabilidad Civil Extracontractual Objetiva y que a la luz de la Teoría del Riesgo en relación con el artículo 35 de la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor.

- Demandado: Se defiende argumentando que el fraude fue resultado de una falsificación de página web y que el cliente reveló su información de forma imprudente. Deduciendo, que del mismo dicho del accionante se desprende que lamentablemente fue objeto de un fraude del cual es ajeno el Banco. Señala que el Banco Popular, así como los Bancos del Sistema Bancario Nacional, a raíz de los fraudes de 'phishing" que se dieron entre el 2006 y 2008, en acatamiento de la Jurisprudencia de Sala Primera, se implementaron sistemas de doble autenticación, el primero con firma digital y el segundo con contraseña, aunado a que este último tiene otro sistema de seguridad conocido como OTP (por sus siglas en inglés one time password o "Código de un solo uso"), que remite un correo electrónico al cliente registrado en los sistemas del Banco, para su autorización sobre transacciones sensibles, tales como transferencias de dinero, adelantos de efectivo, inclusión de cuentas, entre otros. De tal manera, el Banco Popular implementó estas medidas de seguridad desde el año 2010. Por lo tanto, el Banco resulta ajeno al daño.

Fundamento y conclusión: La sentencia concluye que el Banco no tiene responsabilidad por el daño ocasionado debido a la imprudencia del cliente y al acto de un tercero. Se destaca la importancia de la diligencia por parte de los usuarios en la protección de su información confidencial. Y se rechaza la demanda contra el Banco por falta de nexo causal entre la conducta del Banco y el daño reclamado. Por lo anterior, se acoge la excepción de falta de derecho opuesta por el demandado y se declara sin lugar la demanda interpuesta por el demandante. Se determina que el demandante debe pagar las costas procesales y personales al ser vencido en el caso.

En resumen, la sentencia concluye que el Banco no es responsable por el daño causado debido a la imprudencia del cliente y a la acción de un tercero basándose en el numeral 35 de la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor, siendo que existe un eximente para romper el nexo causal entre las partes, por lo que se rechaza la demanda y se condena al demandante a pagar las costas del proceso.

Producto del análisis realizado se concluye que la línea jurisprudencial va orientada en el sentido de que, en cuanto a la responsabilidad objetiva, en materia de protección al consumidor, se ha establecido que existen obligaciones que deben ineludiblemente de cumplir tanto las entidades bancarias como quienes utilizan sus servicios, excluyéndose por tanto la existencia de una suerte de “responsabilidad automática” de las primeras, pero es necesario que demuestren el rompimiento del nexo causal de la relación de consumo producto de unas de las eximentes establecidas en las normas ya citadas.

De seguido adjunto cuadro de todas las resoluciones analizadas con relación a la responsabilidad objetiva de los Bancos Estatales en los fraudes informáticos, en los que se analiza las causales eximentes del canon 35 de la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor, y algunos de ellos también el numeral 190 de la Ley General de la Administración Pública.

Tabla 1

Resoluciones analizadas de la Sala Primera de la Corte Suprema de Justicia y del Tribunal Contencioso Administrativo y Civil de Hacienda.

Expediente	Sentencia	Despacho	Fecha
08-000123-0161-CA	Res. Nº 00300 – 2009	Sala Primera de la Corte	26 de marzo del 2009 a las 11:25
12-001911-1027-CA	Res. Nº 00385 – 2015	Sala Primera de la Corte	25 de marzo del 2015 a las 10:45
08-000116-1027-CA	Res. 000394-F-S1-2009	Sala Primera de la Corte	23 de abril del 2009 a las 10:20
16-004454-1027-CA	Res. Nº 00604 – 2021	Sala Primera de la Corte	16 de marzo del 2021 a las 10:55
12-004684-1027-CA	Res. Nº 00658 – 2018	Sala Primera de la Corte	13 de julio del 2018 a las 09:30
11-005470-1027-CA	Res. Nº 00686 – 2014	Sala Primera de la Corte	28 de mayo del 2014 a las 09:15
10-003907-1027-CA	Res. Nº 00778 – 2012	Sala Primera de la Corte	03 de julio del 2012 a las 09:40
10-003391-1027-CA	Res. Nº 00783 – 2016	Sala Primera de la Corte	21 de julio del 2016 a las 09:25
18-004107-1027-CA	Res. Nº 01116 – 2023	Sala Primera de la Corte	05 de julio del 2023 a las 11:21
13-007379-1027-CA	Res. Nº 01123 – 2017	Sala Primera de la Corte	14 de setiembre del 2017 a las 15:20
13-003573-1027-CA	Res. Nº 01289 – 2017	Sala Primera de la Corte	26 de octubre del 2017 a las 10:20
19-004967-1027-CA	Res. Nº 01307 – 2023	Sala Primera de la Corte	27 de julio del 2023 a las 09:28
09-002163-1027-CA	Res. Nº 01431 – 2012	Sala Primera de la Corte	23 de octubre del 2012 a las 14:20
10-004318-1027-CA	Res. Nº 01568 – 2012	Sala Primera de la Corte	29 de noviembre del 2012 a las 09:30
09-001097-1028-CA	Res. Nº 01607 – 2012	Sala Primera de la Corte	06 de diciembre del 2012 a las 09:15
15-009564-1027-CA	Res. Nº 02056 – 2022	Sala Primera de la Corte	29 de setiembre del 2022 a las 10:55
13-007991-1027-CA	Res. Nº 02190 – 2020	Sala Primera de la Corte	13 de agosto del 2020 a las 11:27
15-000179-0183-CI	Res. Nº 02606 – 2020	Sala Primera de la Corte	12 de noviembre del 2020 a las 15:22
21-001244-1027-CA	N° 2023006486	Tribunal Contencioso Administrativo Y Civil De Hacienda	15 de diciembre del 2023 a las 14:33

22-001162-1028-CA	N° 2023005234	Tribunal Contencioso Administrativo Y Civil De Hacienda, Sección Tercera	08 de noviembre del 2023 a las 8:00
20-004623-1027-CA	Nº 51-2023-IV	Tribunal Procesal Contencioso Administrativo, Sección Cuarta	29 de mayo del 2023 a las 11:58
20-000537-1027-CA	No. 026-2022-IX	Tribunal Contencioso Administrativo Y Civil De Hacienda, Sección Primera	30 de mayo del 2022 a las 16:15
21-000586-1027-CA	Res. Nº 00026 – 2023	Tribunal Contencioso Administrativo Sección I	24 de marzo del 2023 a las 16:10
16-004454-1027-CA	Res. Nº 00006 – 2020	Tribunal Contencioso Administrativo Sección IV	29 de enero del 2020 a las 14:30
18-007920-1027-CA	Res. Nº 00127 – 2020	Tribunal Contencioso Administrativo Sección IV	19 de noviembre del 2020 a las 10:17
18-007920-1027-CA	Res. Nº 00112 – 2022	Tribunal de Casación Contencioso Administrativo y Civil de Hacienda	12 de mayo del 2022 a las 09:03
20-000537-1027-CA	Res. 000128-F-TC-2023	Tribunal De Casación De Lo Contencioso Administrativo Y Civil De Hacienda	13 de julio del 2023 a las 14:42

Fuente: Elaboración propia, 2024.

De las resoluciones anteriores es importante aclarar que se realiza un análisis jurisprudencial desde el 2019, sin embargo, tanto la Sala Primera de la Corte Suprema de Justicia como el Tribunal Contencioso Administrativo y Civil de Hacienda, hacen referencia a los diferentes votos analizados anteriores a esta fecha, es por ello por lo que se toman como referencia.

De estas resoluciones se desprende que la línea jurisprudencial antes del 2010 era condenatoria para los Bancos Estatales, esto de acuerdo a la responsabilidad objetiva referida en el numeral 35 de la Ley de Promoción de la Competencia y Efectiva Defensa del Consumidor, basando su criterio no en la sustracción del dinero por un tercero, sino en la existencia de un riesgo, así mismo, solo se libera el que demuestre que es ajeno al daño, se exonera de culpa si se demuestra que existió culpa de la víctima, fuerza mayor o hecho de un tercero.

Véase el siguiente extracto de la resolución 000394-F-S1-2009 de Sala Primera, de las diez horas veinte minutos del veintitrés de abril del dos mil nueve, sobre la responsabilidad de los bancos en este tipo de casos.

En el caso en concreto, las pretensiones de la sociedad actora fueron acogidas por el Tribunal, quién consideró que el funcionamiento del sistema de banca electrónica presenta

> una peligrosidad tal que permite imputar los daños irrogados al banco. La experiencia confirma que las transacciones realizadas por Internet presentan cierto nivel de riesgo, por lo que las generalidades apuntadas en el considerando anterior resultan aplicables. La función esencial de la entidad bancaria es la intermediación financiera, que incluye la captación de fondos provenientes del ahorro del público, concepto que lleva implícita su custodia, tanto desde el punto de vista físico, como del registro electrónico correspondiente. No cabe duda de que se encuentra sometida a una ineludible obligación de garantizar la seguridad de las transacciones realizadas, ya sea en ventanilla o mediante cualquier otro medio puesto a disposición de los clientes, la cual debe abarcar, necesariamente, el uso de todos aquellos mecanismos disponibles que le permitan contar con un mayor grado de certeza en cuanto a la identificación de las personas que se encuentran facultadas para realizar transacciones electrónicas desde las cuentas. La responsabilidad que le fue imputada al Banco se fundamenta, no en la sustracción del dinero por un tercero, sino en la existencia de un riesgo, según lo expuesto en el considerando III, en el funcionamiento propio del servicio que ofrece, lo que permite imputar el origen del daño al funcionamiento del servicio. Aunado a lo anterior, la prueba evacuada no permite acreditar que en el caso concreto se dé la concurrencia de alguna causa eximente de responsabilidad de la cual se extraiga la ajenidad del demandado respecto del daño.

Para estas fechas y aún posteriores, los bancos no utilizaban el doble factor de autenticación, existiendo muchas falencias en la autenticación y acceso a las cuentas bancarias mediante internet, por lo que los bancos no demostraban ante el Tribunal Contencioso Administrativo y Civil de Hacienda que eran ajenos al daño, no podían demostrar que era culpa de las víctimas, por lo que la posición y resoluciones de la judicatura eran que existía responsabilidad objetiva por la teoría del riesgo, y así se condenó a los diversos bancos a solventar el daño patrimonial sufrido por los consumidores.

En concordancia con los cambios y evolución en las estafas informáticas, tanto de la realidad, como de la teoría del riesgo y la responsabilidad objetiva aplicable en la materia, del mismo modo, la jurisprudencia ha venido a responder a estos cambios, siendo así que, podemos citar el Voto 28-2014 del 5 de mayo de 2014, del Tribunal Contencioso Administrativo, Sección V, el cual indica:

> … SOBRE EL CASO CONCRETO… Tampoco fue acreditado que las entidades bancarias demandadas no se prepararan con sistemas de seguridad eficientes, no fue aportada prueba técnica que pudiera demostrar que los sistemas de seguridad de los demandados fueren ineficientes u obsoletos de acuerdo con la tecnología que se contaba en el país, en los años en que se produjeron la mayor cantidad de fraudes informáticos. **No fue acreditado que la seguridad del usuario en sus transacciones electrónicas dependa únicamente de la institución bancaria; por el contrario, entiende este órgano colegiado que, al tratarse de una relación contractual entre cada institución bancaria y su cliente, existen derechos y obligaciones para ambas partes**. La negrita y subrayado no corresponde al original.

En la misma línea de pensamiento, tenemos la Sentencia No. 127-2020-IV Sección Cuarta del Tribunal Contencioso Administrativo, de las diez horas diecisiete minutos del diecinueve de noviembre de dos mil veinte, que establece:

> De entrada, ha de indicarse que la demanda incoada ha de ser declarada sin lugar en todos sus extremos, en tanto en la especie nos encontramos ante las **eximentes de responsabilidad culpa de la víctima y hecho de un tercero**. Y siendo ello así, al resultar **el Banco accionado ajeno al daño que se reclama, no existe nexo de causalidad entre el referido daño y alguna conducta de dicho ente**… De ahí que la Sala Primera de la Corte Suprema de Justicia ha señalado que "(...) **la responsabilidad objetiva no puede ser vista como una transferencia patrimonial automática**... Ahora bien, no cuestiona esta Sala que en el subjúdice existe una parte afectada... No obstante, tal circunstancia, por sí

> sola, **no trae aparejada la imputación de responsabilidad exclusiva a la entidad bancaria**… **El manejo y uso de los datos bancarios... son exclusivos del usuario, a quien le corresponde proteger y ser garante de dicha información**.... Así las cosas, no existe en esta materia la responsabilidad automática de las entidades bancarias, siendo como se ha podido apreciar a partir del Fallo parcialmente transcrito, que **existe un ineludible deber de diligencia de los usuarios bancarios**, en cuanto al resguardo de claves, tarjetas y en general, de su información confidencial. La negrita y subrayado no corresponde al original.

Adicionalmente en diversos fallos de los analizados la judicatura se ha referido a la responsabilidad objetiva por riesgo en materia del consumidor y sobre la carga de la prueba en el tema que nos ocupa, como se observa de seguido:

> **Responsabilidad objetiva por riesgo en materia del consumidor**. En lo que se refiere a la responsabilidad, se pueden ubicar dos grandes vertientes, una subjetiva, en la cual se requiere la concurrencia, y consecuente demostración, del dolo o culpa por parte del autor del hecho dañoso (v.gr. el cardinal 1045 del Código Civil), y otra objetiva, que se caracteriza, en lo esencial, por prescindir de dichos elementos, siendo la imputación del daño el eje central sobre el cual se erige el deber de reparar. Como ejemplo de lo anterior, se encuentra el numeral 35 de la Ley de Defensa Efectiva del Consumidor, en donde el comerciante, productor o proveedor, responderá por aquellos daños derivados de los bienes transados y los servicios prestados, aún y cuando en su actuar no se detecte negligencia, imprudencia, impericia o dolo. En asuntos como el presente, esta Sala ha mencionado sobre la **carga de la prueba**, en primer término, que la parte actora se encuentra en una situación donde le resulta muy difícil o prácticamente imposible comprobar algunos de los hechos o presupuestos esenciales para su pretensión, colocándola ante una posible indefensión.

> Producto de lo anterior, se redistribuye el deber de demostración entre las partes litigantes, en donde el onus probandi (deber probatorio) le corresponde a quien se encuentre en mejores condiciones para aportar el elemento probatorio al proceso. La negrita no es del original.

Es decir, que la línea jurisprudencial va orientada en el sentido de que, en cuanto a la responsabilidad objetiva, en materia de protección al consumidor, se ha establecido que existen obligaciones que deben ineludiblemente de cumplir tanto las entidades bancarias como quienes utilizan sus servicios, excluyéndose por tanto la existencia de una suerte de "responsabilidad automática" de las primeras. Además, de que la carga de la prueba se revierte, y es el Banco quien debe demostrar que es ajeno al daño y por lo tanto que le aplican las causas eximentes del artículo 35 de la Ley de la Promoción de la Competencia y Defensa Efectiva del Consumidor o del 190 de la Ley General de la Administración Pública.

Consecuentemente, la línea jurisprudencial se basa en analizar cada caso individual, esto por cuanto la resolución judicial va a depender de la prueba aportada por las partes, en especial por el Banco, según se señaló anteriormente que es quien tiene la carga probatoria, basándose en la misma para determinar si existe ajenidad al daño por el proveedor, o alguna de las causales eximentes del canon 190 de la Ley General de la Administración Pública.

4.3 Remedios procesales

Dentro de los medios procesales a los que se puede acudir cuando se sufre una estafa informática, se tiene la denuncia o reclamo administrativo, posteriormente, si existe disconformidad y agotada la vía administrativa, se puede acudir a sede judicial, en el caso de investigación hablamos de Bancos Estatales, por lo que se debe acudir al Tribunal Contencioso Administrativo y Civil de Hacienda.

4.3.1 Proceso Administrativo

Cuando se sufre una estafa informática, se debe seguir un proceso en sede administrativa, el cual detallo a continuación:

1. Si está siendo víctima de fraude electrónico debe llamar o acudir a la sucursal bancaria de inmediato, con el fin de evitar que se sigan haciendo transacciones bancarias.
2. Interponer el reclamo administrativo en el Banco, los diferentes bancos ponen a disposición diversas formas para hacerlo, puede ser vía telefónica llamando al centro de atención al

cliente o físicamente en alguna sucursal, cuando realiza la misma, le generan un listado de las transacciones con el fin de que identifique los movimientos fraudulentos.

Sin embargo, es muy importante que el usuario aporte la prueba adicional que estime necesaria, por ejemplo, si cuando llamo al Banco no le contestaron las llamadas, aportar el historial de llamadas de la empresa telefónica con el fin de demostrar que sufrió un daño mayor al no poder suspender los accesos a los ciberdelincuentes, así mismo, cualquier otra prueba que considere necesaria.

Los Bancos les instan a los usuarios a interponer la denuncia en el Organismo de Investigación Judicial y después la aporten como prueba en el reclamo, sin embargo, no es requisito obligatorio.

3. Cuando se recibe la resolución administrativa con el resultado de la investigación, si esta no es de su satisfacción, puede interponer un recurso de revocatoria con apelación en subsidio, para que sea reconsiderado y conocido por la instancia administrativa superior.

Importante señalar, que para acudir a sede administrativa no es necesario contar con patrocinio letrado, sin embargo, se puede acudir a un abogado de confianza para presentar tanto la denuncia como los medios de revocatoria y apelación.

Con la resolución de la Gerencia General del Banco o dependencia autorizada por él para emitir la resolución del recurso de apelación, se agota la vía administrativa. Si la resolución es desfavorable para el usuario, éste puede acudir a sede judicial.

4.3.2 Proceso Judicial

1. En el tema que nos ocupa al ser contra el Estado es necesario agotar la vía administrativa para interponer el litigio judicial, por lo que describo el proceso a seguir: Con la resolución del recurso de apelación y antes de un año a partir de su notificación, se presenta la demanda y todas las pruebas necesarias al Tribunal Contencioso Administrativo y Civil de Hacienda, para interponer ésta, es necesario contar con patrocinio letrado, lo que quiere decir, con abogado defensor.

   En el tribunal se llevará a cabo todo el proceso correspondiente, de contestación de la demanda, conciliación, audiencia preliminar, juicio oral y público, y sentencia.
2. La parte afectada con sentencia en contra podrá interponer recurso de casación. Este recurso se interpone ante el Tribunal de Casación o Sala Primera, según corresponda en cada caso, en un plazo de quince días hábiles contados a partir del día hábil siguiente a la notificación

de la resolución a todas las partes, de acuerdo con el artículo 139 del Código Procesal Contencioso-Administrativo.

3. Como última instancia y de ser necesario se podrá interponer un recurso extraordinario de revisión ante la Sala Primera.
4. Resueltos los recursos presentados se debe ejecutar la sentencia final por el victorioso para que le otorguen lo condenado en la misma, si así se resuelve en sentencia. Si la sentencia no otorga ningún derecho de resarcimiento no es necesario acudir a la vía ejecutoria.

Por lo expuesto anteriormente se deduce que existen suficientes medios tanto administrativos como judiciales para solicitar el resarcimiento del daño causado. Sin embargo, es necesario contar con la suficiente prueba para demostrar que el proveedor del servicio no es ajeno al daño, o no le aplica ninguna de las eximentes vistas anteriormente, o de lo contrario, cuando se acuda a sede judicial, de acuerdo con la línea jurisprudencial, puede ser condenado y tener que sufragar las costas procesales por interponer la demanda y recursos, además de averse sufrido ya un daño patrimonial por la estafa informática.

4.4 Recomendaciones Internacionales

4.4.1 Directrices para la Protección del Consumidor

Costa Rica es Estado miembro de la Organización de las Naciones Unidas (ONU) desde el 02 de noviembre de 1945, además es la sede de la Corte Interamericana de Derechos Humanos. De acuerdo con la Carta de las Naciones Unidas, Capítulo IV: La Asamblea General, artículo 10, se establecen las funciones de la Asamblea General, que dice:

> La Asamblea General podrá discutir cualesquier asuntos o cuestiones dentro de los límites de esta Carta o que se refieran a los poderes y funciones de cualquiera de los órganos creados por esta Carta, y salvo lo dispuesto en el Artículo 12 podrá hacer recomendaciones sobre tales asuntos o cuestiones a los Miembros de las Naciones Unidas o al Consejo de Seguridad o a este y a aquéllos. (art. 10)

Las Directrices de las Naciones Unidas para la Protección del Consumidor son un conjunto valioso de recomendaciones y principios diseñados para orientar a los Estados miembros a que establecen las principales características que deben tener las políticas y leyes para la de protección al consumidor, así como, las instituciones encargadas de aplicarlas y los sistemas de compensación para que sean eficaces. Ayudando a los Estados Miembros interesados a formular y aplicar leyes,

normas y reglamentos nacionales y regionales, adaptados a sus circunstancias económicas, sociales y ambientales.

Las Directrices de las Naciones Unidas para la Protección del Consumidor son un conjunto valioso de recomendaciones y principios diseñados para orientar a los Estados miembros a que establecen las principales características que deben tener las políticas y leyes para la de protección al consumidor, así como, las instituciones encargadas de aplicarlas y los sistemas de compensación para que sean eficaces. Ayudando a los Estados Miembros interesados a formular y aplicar leyes, normas y reglamentos nacionales y regionales, adaptados a sus circunstancias económicas, sociales y ambientales.

Las Directrices para la Protección del Consumidor, fueron aprobadas por la Asamblea General en su resolución 39/248, del 16 de abril de 1985, ampliadas posteriormente por el Consejo Económico y Social en su resolución 1999/7, del 26 de julio de 1999, y revisadas y aprobadas por la Asamblea General en su resolución 70/186, del 22 de diciembre del 2015.

Dentro de las Directrices de las Naciones Unidas (2015) para la protección del consumidor, establece dentro de los principios generales que corresponde a los Estados Miembros formular, fortalecer o mantener una política enérgica de protección del consumidor, teniendo en cuenta las directrices que figuran más adelante y los acuerdos internacionales pertinentes. Al hacerlo, cada Estado Miembro debe establecer sus propias prioridades para la protección de los consumidores, según las circunstancias económicas, sociales y ambientales del país y las necesidades de su población y teniendo presentes los costos y los beneficios de las medidas que se propongan.

Dentro de los principios para unas buenas prácticas comerciales, se establecen los siguientes que son relevantes con la investigación.

> d) Educación y sensibilización: Las empresas deben elaborar, según proceda, programas y mecanismos para ayudar a los consumidores a adquirir los conocimientos y competencias necesarios para comprender los riesgos, incluidos los riesgos financieros, tomar decisiones bien fundadas y acceder a servicios competentes y profesionales de asesoramiento y asistencia, prestados preferiblemente por terceros independientes, cuando sea necesario.
>
> e) Protección de la privacidad: Las empresas deben proteger la privacidad de los consumidores mediante una combinación de mecanismos adecuados de control, seguridad,

transparencia y consentimiento en lo relativo a la recopilación y utilización de sus datos personales.

En el primero de estos se fomenta la elaboración de programas y mecanismos para ayudar a los consumidores a adquirir el conocimiento y competencias que sean necesarias para poder disminuir los riesgos o comprender a los que están sometidos por el consumo de un bien o servicio. Dentro de este inciso se incluyen los riesgos financieros, por lo que es necesario que el Estado, sea por su cuenta o por medio de los Bancos Estatales, asesore de manera profesional a los consumidores sobre los riesgos patrimoniales a los que se presentan, al utilizar los servicios digitales ofrecidos por los Bancos, en concordancia con el avance tecnológico, con el fin de minimizar los riesgos económicos.

Otro de los principios relevantes de esta directriz es la protección de la privacidad de los consumidores, mediante mecanismos adecuados de control, seguridad y otros, es por ello, que el Estado debe proteger la información de sus consumidores, y para ello debe adecuar los mecanismos necesarios para ofrecer a los usuarios seguridad, y dentro de esta, la seguridad bancaria. Uno de los mecanismos que los Bancos Estatales utilizan para brindarla son las medidas de doble factor de autenticación, pero sin el acompañamiento del principio anterior, no tienen el mismo efecto positivo en los consumidores.

Por lo que es necesario que los Bancos Estatales además de fomentar medidas de seguridad bancaria, se preocupen por ofrecer la adecuada capacitación a los usuarios, con el objetivo de disminuir el riesgo delictivo al que están expuestos al utilizar medios informáticos.

CAPÍTULO V: ANÁLISIS DE RESULTADOS

Para la realización de la presente investigación se utiliza una metodología inductiva, el cual se basa en el razonamiento teórico que parte del estudio de lo particular a lo general, formando ideas individuales de lo que se estudia. Es decir, el objetivo principal de la investigación es el de crear un cuerpo de conocimientos teóricos a raíz del razonamiento de lo investigado.

Se caracteriza como un proceso que estudia casos particulares, y de donde se obtienen conclusiones o leyes universales que explican o relacionan los fenómenos estudiados. Este método se basa en la observación directa de los fenómenos, la experimentación y el estudio de las relaciones entre sí.

Se considera fenomenológico, porque como lo señalan Taylor y Bodgan (1984) busca comprensión por medio de la observación participante, la entrevista y otros, además generan datos descriptivos. El método se ajusta a la investigación ya que nos permite observar los diferentes criterios y normas en profundidad. Como lo indican Hernández et al. (2014), su propósito principal es explorar, describir y comprender las experiencias de las personas con respecto a un fenómeno y descubrir los elementos en común de la investigación.

La elaboración de la presente investigación ha utilizado los instrumentos que más confiabilidad ofrecen a la hora de recabar la información necesaria para cumplir con los objetivos planteados.

La aplicación de lo anteriormente explicado se realiza por medio una serie de entrevistas no estructuradas a 4 personas y encuestas con preguntas cerradas a 116 personas por medio de un trabajo de campo virtual utilizando la herramienta digital Google Forms con la siguiente dirección online: https://docs.google.com/forms/d/e/1FAIpQLSdOOjOSyeLhTIEz_IMap-aaIPX-ptfh-_mS5tIaVLtwJd7Bgw/, así como diferentes medios tecnológicos.

Tabla 2

Aceptación de que los datos suministrados sean utilizados en la investigación con fines académicos.

Respuesta	Cantidad	Porcentaje
No	10	8,62%
Sí	106	91,38%
Total de encuestados	**116**	**100%**

Fuente: Elaboración propia, 2024.

Resultados e interpretación: Como se logra apreciar en la tabla anterior: Se aplicó la encuesta a un total de 116 personas de las cuales 106 autorizaron el uso de sus datos en la presente investigación, siendo equivalente a un porcentaje de 91.38%, y 10 sujetos no autorizaron el uso de los datos suministrados, siendo el 8,62%. Debido a lo anterior, los siguientes resultados se analizan solamente con las personas que autorizaron su utilización, por lo que a continuación cuando se indique encuestados se debe entender como los 106 acreditados.

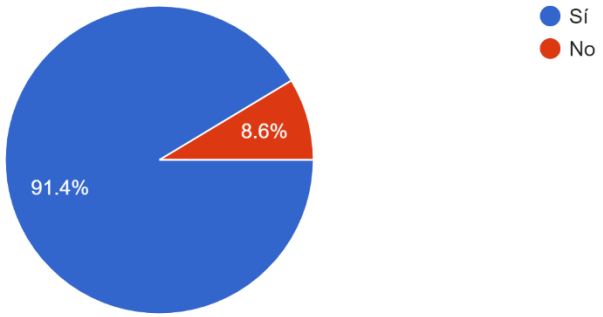

Figura 2. Aceptación de que los datos suministrados sean utilizados en la investigación con fines académicos.

Fuente: Elaboración propia, 2024.

Tabla 3

Rango de edad de los encuestados.

Respuesta	Cantidad	Porcentaje
18 - 25 años	6	5,66%
26 - 35 años	36	33,96%
36 - 45 años	39	36,79%
46 - 55 años	19	17,92%
56 - 65 años	5	4,72%
66 - 75 años	1	0,94%
76 años en adelante	0	0%
Total de encuestados	**106**	**100%**

Fuente: Elaboración propia, 2024.

Resultados e interpretación: De la tabla anterior se extrae lo siguiente: De las 106 personas valorables se logró llegar a un público variado, siendo del rango de edad de 18 a 25 años, 6 personas completaron la encuesta, siendo un 5,66%. Entre los 26 a 35 años se encuestaron a 36 personas, para un porcentaje de 33,96%. De los 36 a 45 años se logró sondear a 39 individuos, con una representación del 36,79%. Contestaron el estudio 19 personas entre los 46 a 55 años, con una participación del 17,92%. Externaron su opinión 5 personas con un rango de edad de los 56 a los 65 años, representando un 4,72% del total de encuestados. Así mismo, solamente 1 persona entre los 66 a los 75 años completo la encuesta, lo que equivale a 0,94%. Ninguna persona mayor a 75 años respondió. El promedio de personas que estuvo más anuente a contestar esta entre el rango de los 26 hasta los 55 años, siendo esto la población laboralmente activa en promedio de nuestro país. Estos comprenden un 88.68% del total de encuestados.

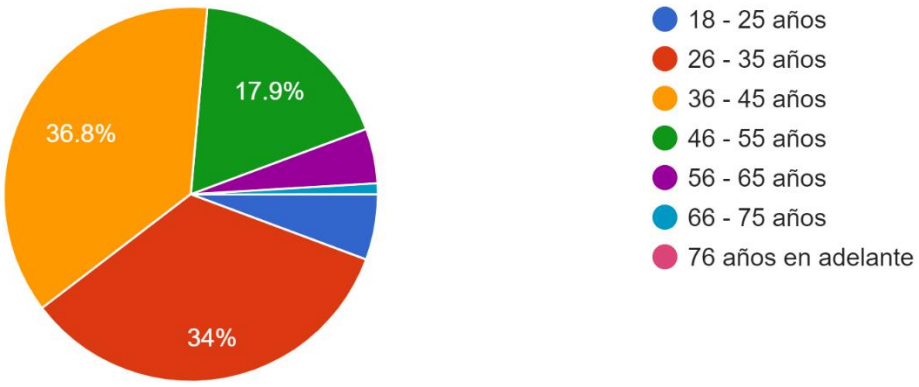

Figura 3. Rango de edad de los encuestados.

Fuente: Elaboración propia, 2024.

Tabla 4

Conocimiento de los encuestados sobre que es una estafa informática.

Respuesta	**Cantidad**	**Porcentaje**
No	9	8,49%
Sí	97	91,51%
Total de encuestados	**106**	**100%**

Fuente: Elaboración propia, 2024.

Resultados e interpretación: La información que arroja esta pregunta de investigación, la cual se encuentra tabulada en la tabla anterior muestra que del total de 106 respuestas, 97 personas o el 91,51 % afirman que conocen qué es una estafa informática. Ahora bien, el dato extraído de 9 encuestados o un 8,49 % que desconocen que es una estafa informática, es preocupante, esto por cuanto demuestra el desconocimiento de la población en estos temas y eventualmente podrían ser víctimas de estas. Por lo que es muy importante facilitar de conocimiento a la mayor población bancaria, para disminuir aún más este porcentaje.

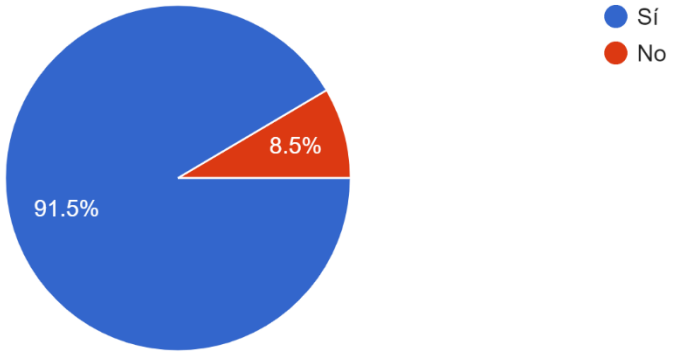

Figura 4. Conocimiento de los encuestados sobre que es una estafa informática.

Fuente: Elaboración propia, 2024.

Tabla 5

Conocimiento de los encuestados sobre cuáles son los Bancos Estatales de Costa Rica.

Respuesta	**Cantidad**	**Porcentaje**
No	5	4,72%
Sí	101	95,28%
Total de encuestados	**106**	**100%**

Fuente: Elaboración propia, 2024.

Resultados e interpretación: De la tabla anterior se logra extraer lo siguiente: que, de un total de 106 personas encuestadas, 101 individuos que representan un 95,28% de los criterios emitidos conocen cuales son los Bancos Estatales de Costa Rica, esta interrogante es relevante para la investigación porque la misma engloba solo dicho fragmento del Sistema Bancario Nacional. Por otra parte, 5 sujetos indican desconocer cuáles son los Bancos Estatales, comprendiendo solamente un 4,72 %, siendo un porcentaje minoritario y aceptable.

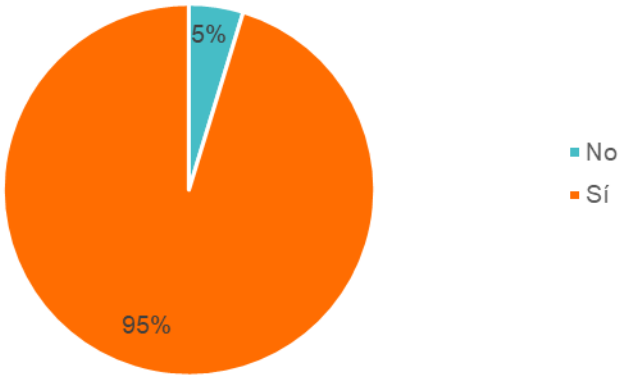

Figura 5. Conocimiento de los encuestados sobre cuáles son los Bancos Estatales de Costa Rica.

Fuente: Elaboración propia, 2024.

Tabla 6

Cantidad de personas víctimas de estafas informáticas.

Respuesta	**Cantidad**	**Porcentaje**
No	86	81,13%
Sí	20	18,87%
Total de encuestados	**106**	**100%**

Fuente: Elaboración propia, 2024.

Resultados e interpretación: De un total de 106 personas encuestadas 86 no han sido víctimas de estafas, siendo un 81,13%. Sin embargo, 20 personas que representan un 18,87% si han sido víctimas de estafas informáticas, siendo un porcentaje muy alto.

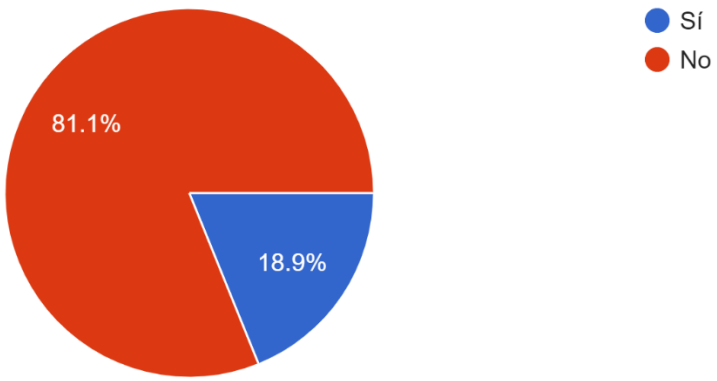

Figura 6. Cantidad de personas víctimas de estafas informáticas.

Fuente: Elaboración propia, 2024.

Tabla 7

Método utilizado para sustraer información.

Respuesta	**Cantidad**	**Porcentaje**
Correo electrónico	1	5,00%
Llamada telefónica	8	40,00%
Mensaje de texto SMS	2	10,00%
Ingeniería Social	4	20,00%
Ataque informático	2	10,00%
Desconocido	3	15,00%
Total de encuestados	**20**	**100%**

Fuente: Elaboración propia, 2024.

Resultados e interpretación: Siguiendo la tabla anterior, de las 20 personas estafadas, 1 sufrió la sustracción de la información mediante correo electrónico, representando un 5% de los sujetos estafados. El medio más utilizado para la sustracción de la información fue por llamada telefónica con 8 personas, lo que representa un 40% de las víctimas. Otro método utilizado es mediante mensajes de texto SMS con 2 damnificados, equivalente a un 10%. Mediante la

utilización del engaño por ingeniería social se lesiono a 4 personas, proporcional al 20%. Otra forma que utilizan los ciberdelincuentes para sustraer la información es mediante ataques informáticos, con malwares y otros, con una representación del 10% o 2 víctimas en esta investigación. Por otra parte, 3 personas indican desconocer el medio por el cual se les sustrajo la información, siendo un 15%.

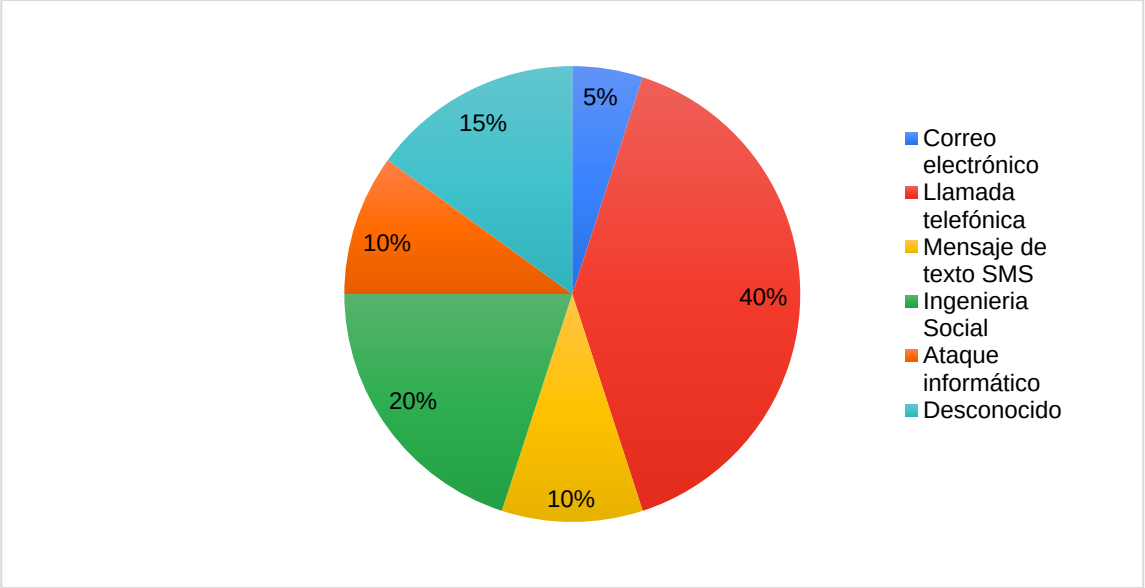

Figura 7. Método utilizado para sustraer información.

Fuente: Elaboración propia, 2024.

Tabla 8

Banco en que sufrió el daño patrimonial.

Respuesta	**Cantidad**	**Porcentaje**
Banco de Costa Rica	2	10,00%
Banco Nacional de Costa Rica	6	30,00%
Banco Popular	7	35,00%
Otro	5	25,00%
Total de encuestados	**20**	**100%**

Fuente: Elaboración propia, 2024.

Resultados e interpretación: Siempre trabajando con las 20 víctimas de estafas informáticas, se desprende que solamente 2 personas sufrieron sustracción en el Banco de Costa Rica, lo que equivale a un 10%. Para el Banco Nacional de Costa Rica el número aumenta a 6 clientes, siendo un 30%. El banco con el mayor número de lesionados es el Banco Popular con 7 personas con un 35% de damnificados. Por otro lado, 5 individuos o un 25%, sufrieron el daño en otros bancos, pero esta investigación se concentra en los Bancos Estatales.

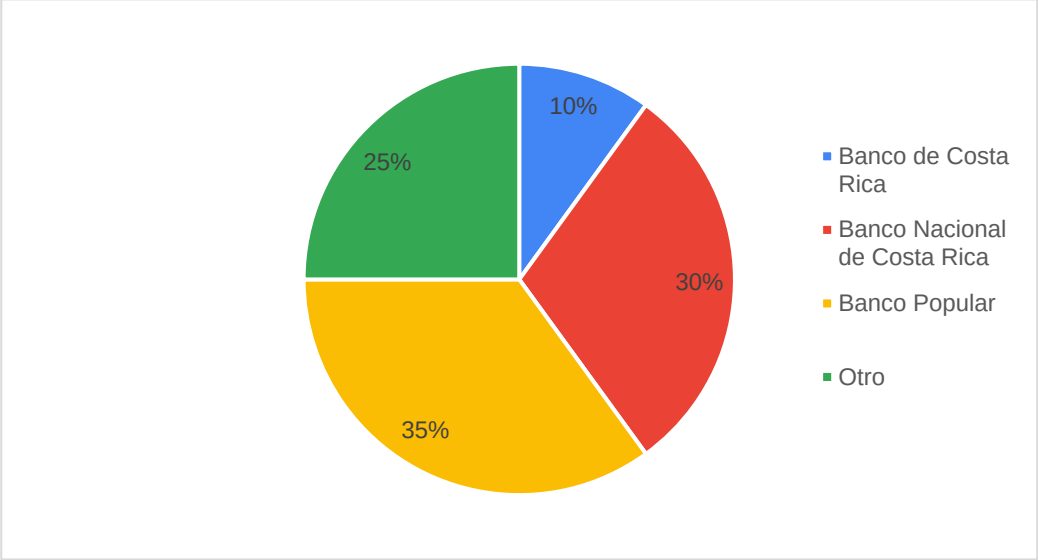

Figura 8. Banco en que sufrió el daño patrimonial.

Fuente: Elaboración propia, 2024.

Tabla 9

Percepción de los clientes sobre si debe el banco responder por el dinero sustraído.

Respuesta	Cantidad	Porcentaje
No	1	5,00%
Sí	19	95,00%
Total de encuestados	**20**	**100%**

Fuente: Elaboración propia, 2024.

Resultados e interpretación: De las 20 víctimas de estafa informática, nótese que solamente 1 persona señala que no considera que el banco deba devolverle el dinero sustraído, es decir, solo un 5%. Por el contrario 19 individuos señalaron que el banco si debe devolverles su patrimonio, para un 95%.

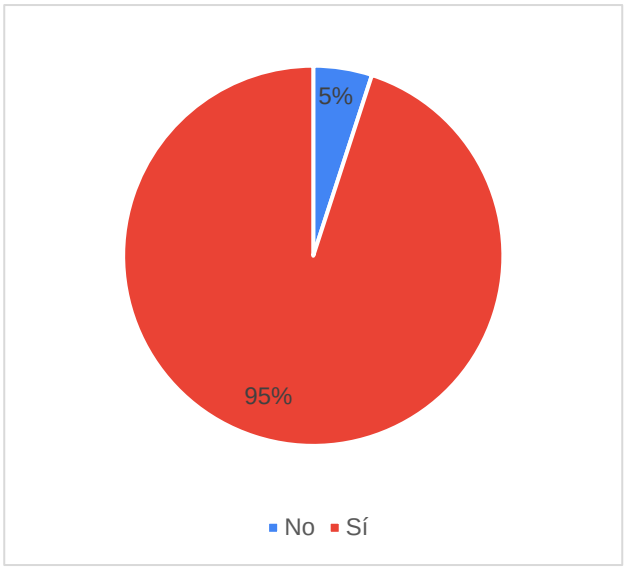

Figura 9. Percepción de los clientes sobre si debe el banco responder por el dinero sustraído.

Fuente: Elaboración propia, 2024.

Tabla 10

El Banco devolvió el dinero.

Respuesta	Cantidad	Porcentaje
No	10	50,00%
Si	10	50,00%
Total de encuestados	**20**	**100%**

Fuente: Elaboración propia, 2024.

Resultados e interpretación: Los bancos les devolvieron el dinero sustraído a 10 personas de las 20 víctimas de estafa informática, siendo una devolución del 50%, lo que señala que los

bancos están asumiendo la responsabilidad objetiva y le realiza la devolución del dinero sustraído a la mitad de los usuarios. Por otro lado, el otro 50% o 10 personas no recibieron la devolución económica por parte del ente financiero.

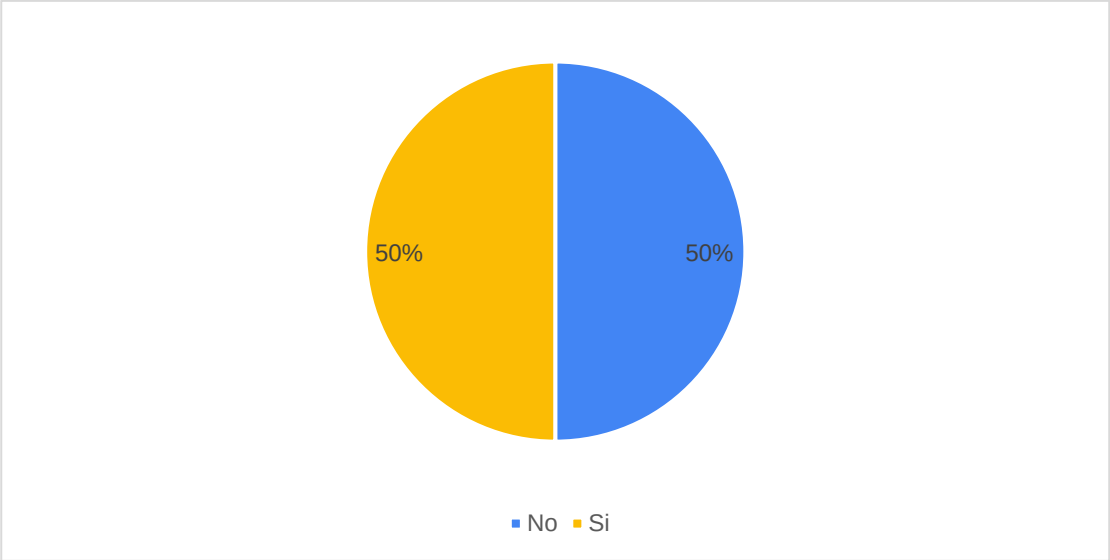

Figura 10. El Banco devolvió el dinero.

Fuente: Elaboración propia, 2024.

Tabla 11

Víctimas que interpusieron demanda judicial por estafa informática.

Respuesta	**Cantidad**	**Porcentaje**
No	11	55,00%
Sí	9	45,00%
Total de encuestados	**20**	**100%**

Fuente: Elaboración propia, 2024.

Resultados e interpretación: De las personas encuestadas que fueron víctimas de estafas informáticas 11 no interpusieron una demanda judicial a pesar de haber sufrido un daño

patrimonial, lo que representa un 55% de los damnificados. Sin embargo, 9 de las 20 víctimas de estafas si interpusieron la respectiva demanda judicial, lo que constituye un 45%.

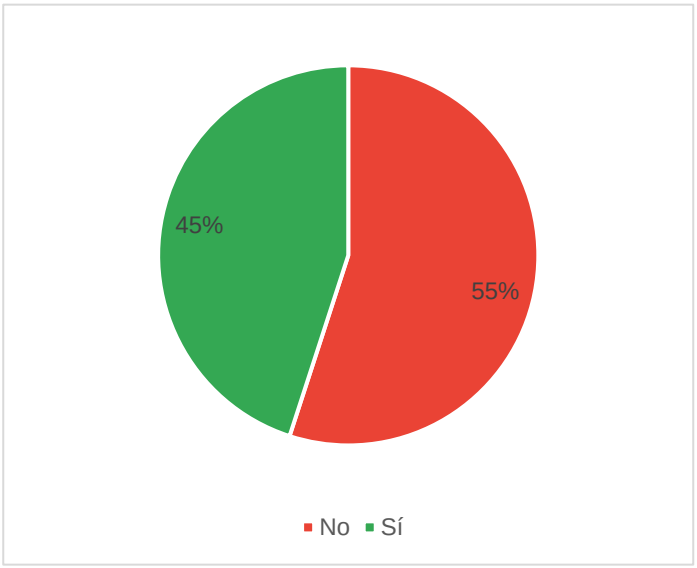

Figura 11. Víctimas que interpusieron demanda judicial por estafa informática.

Fuente: Elaboración propia, 2024.

Tabla 12

Víctimas que interpusieron reclamo administrativo por estafa informática.

Respuesta	**Cantidad**	**Porcentaje**
No	5	25,00%
Sí	15	75,00%
Total de encuestados	**20**	**100%**

Fuente: Elaboración propia, 2024.

Resultados e interpretación: Aunado a la tabla anterior, de las 20 personas que fueron víctimas de estafas informáticas, 5 de ellas no interpusieron un reclamo administrativo ante el banco donde conservan su patrimonio, equivalente a un 25% de los ofendidos. No obstante, 15

individuos si interpusieron el respectivo reclamo administrativo, lo que compone un 75%, siendo un promedio muy elevado de personas que si acuden al banco a reclamar su patrimonio.

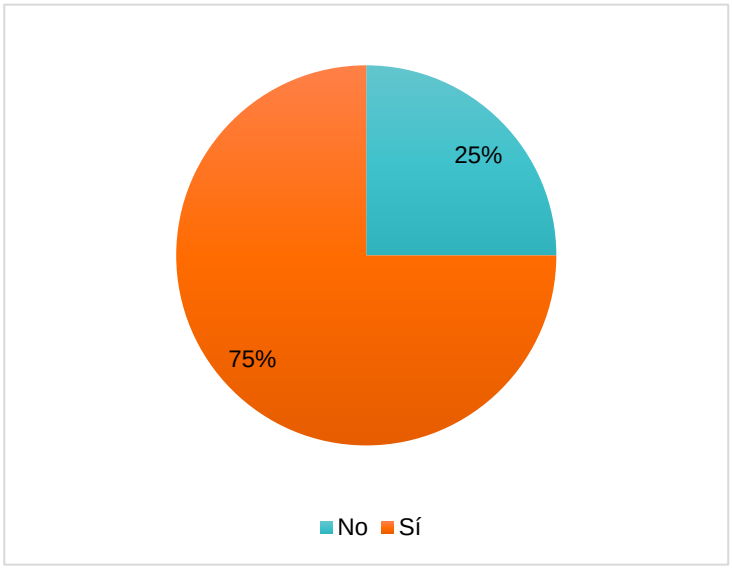

Figura 12. Víctimas que interpusieron reclamo administrativo por estafa informática.

Fuente: Elaboración propia, 2024.

Tabla 13

Facilidad para presentar el reclamo ante el Banco.

	Cantidad	Porcentaje
Muy fácil	5	25,00%
Fácil	6	30,00%
Difícil	7	35,00%
Imposible	2	10,00%
Total de encuestados	**20**	**100%**

Fuente: Elaboración propia, 2024.

Resultados e interpretación: En relación con la tabla anterior, de las víctimas de estafas informáticas, 5 consideran que fue muy fácil interponer el reclamo administrativo, con una representación del 25%, siendo muy aceptable. Por otro lado 6 personas señalaron que les fue fácil interponer la solicitud, para un 30% de satisfacción. Sin embargo, 7 personas tuvieron dificultad para presentar la gestión administrativa ante el ente financiero, con un 35%, siendo un promedio muy elevado y que recae en responsabilidad de los bancos, esto por cuanto ellos tienen el compromiso de brindar un servicio eficaz y eficiente. Peor aún 2 clientes externaron que les fue imposible interponer el reclamo administrativo, pudiendo provocar un mayor daño patrimonial, lo que representa un 10%, siendo un promedio bajo pero inaceptable en el servicio bancario que administra el patrimonio de muchas personas.

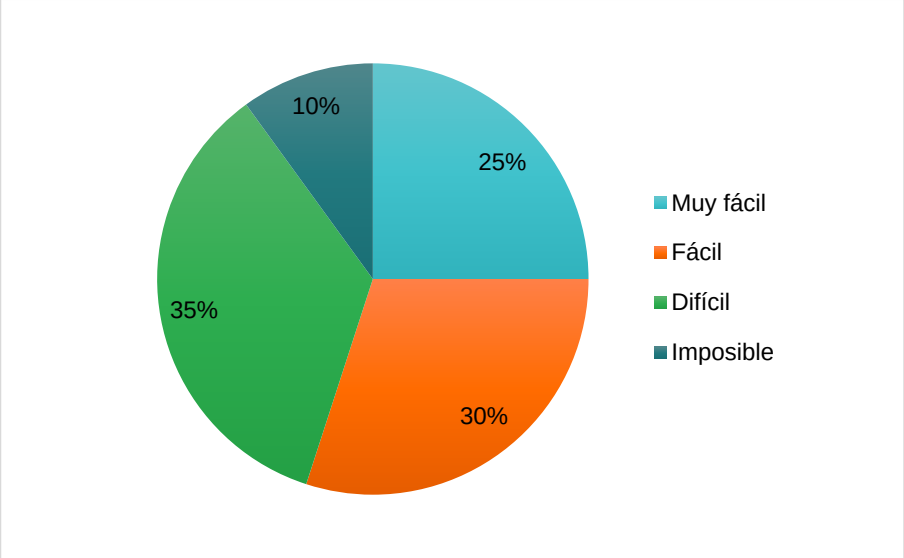

Figura 13. Facilidad para presentar el reclamo ante el Banco.

Fuente: Elaboración propia, 2024.

Tabla 14

Medios utilizados para ingresar a banca en línea o aplicación móvil.

Respuesta	Cantidad	Porcentaje
Nombre de usuario y contraseña	82	30,26%
PIN	46	16,97%
Huella dactilar	47	17,34%
Reconocimiento Facial	40	14,76%
Tarjeta dinámica	27	9,96%
Token físico	11	4,06%
Token por mensaje de texto SMS	18	6,64%
Total de formas	**271**	**100%**

Fuente: Elaboración propia, 2024.

Resultados e interpretación: De la tabla anterior se tiene los medios utilizados por las 106 personas encuestadas para el ingreso a banca en línea o aplicación móvil de los bancos, los datos no son excluyentes entre sí, pudiendo una persona utilizar varios de ellos conjuntamente, detallo: 82 personas ingresan a su información financiera mediante nombre de usuario y contraseña, equivalente a un 30,26%. Adicional, 46 personas utilizan un PIN, representado en el 16,97% del total. El reconocimiento por huella dactilar que trae incorporado algunos teléfonos inteligentes es utilizado por 47 personas para el ingreso a su información bancaria, para un porcentaje del 17,34%. Además, algunos dispositivos modernos utilizan el reconocimiento facial como método de autenticación, y de las personas encuestadas 40 lo utilizan, siendo así un 14,76%. Algunos entes financieros utilizan la tarjeta dinámica como doble factor de autenticación, dentro de los encuestados 27 clientes lo emplean, para un 9,96%. Otros métodos aplicados por los usuarios son el token físico y el token por mensaje de texto SMS, siendo 11 y 18 personas respectivamente que lo usan, consistiendo en un 4,06% y 6,64% proporcionalmente.

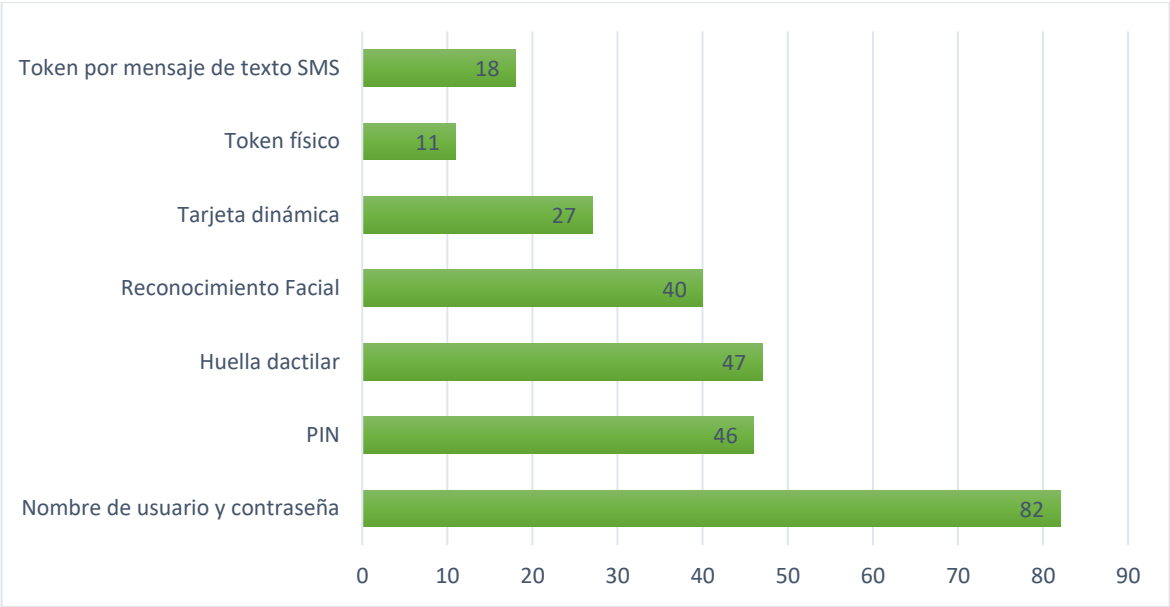

Figura 14. Medios utilizados para ingresar a banca en línea o aplicación móvil.

Fuente: Elaboración propia, 2024.

Tabla 15

Medios utilizados para ingresar a la información bancaria.

Respuesta	Cantidad	Porcentaje
Banca en línea	56	36,84%
Aplicación móvil	79	51,97%
Presencialmente en la sucursal bancaria	17	11,18%
Total de formas	**152**	**100%**

Fuente: Elaboración propia, 2024.

Resultados e interpretación: La tabla anterior expresa los medios utilizados por las 106 personas entrevistadas para ingresar a su información bancaria, las respuestas eran múltiples por lo que no son excluyentes entre sí, pudiendo una persona utilizar varios de ellos conjuntamente, puntualizo: 56 clientes bancarios ingresan a su información bancaria mediante banca en línea, lo que equivalente a un 36,84%. Sin embargo, el medio más utilizado por las personas es la aplicación móvil desde su teléfono inteligente, con 79 usuarios o el 51,97%. Por otro lado, muchos

consumidores siguen utilizando la forma presencial en la sucursal bancaria, para un total de 17 clientes, para un porcentaje del 11,18%.

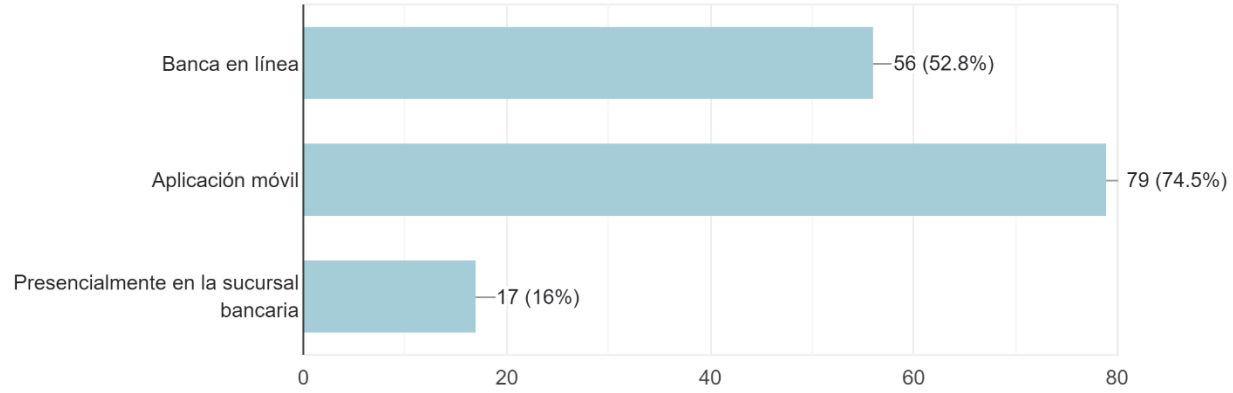

Figura 15. Medios utilizados para ingresar a la información bancaria.

Fuente: Elaboración propia, 2024.

Tabla 16

Conocimiento sobre identificación de un sitio web seguro.

Respuesta	Cantidad	Porcentaje
No	32	30,19%
Sí	74	69,81%
Total de encuestados	**106**	**100%**

Fuente: Elaboración propia, 2024.

Resultados e interpretación: De esta tabla se extrae un dato muy importante para la seguridad de los clientes bancarios, y es el conocimiento de cómo reconocer un sitio web seguro, del que las 106 personas alcanzadas 32 señalan que no conocen como identificar un sitio web seguro, para un promedio de un 30,19% preocupante, porque tienen una posibilidad en contra de ingresar a sitio plagiados de los bancos, de donde obtienen toda su información de acceso a sus cuentas bancarias. Por otro lado, un porcentaje del 69,81% o 74 usuarios, si conocen como reconocer un sitio web seguro.

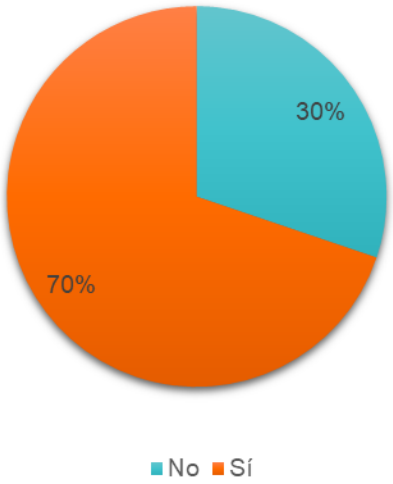

Figura 16. Conocimiento sobre identificación de un sitio web seguro.

Fuente: Elaboración propia, 2024.

Tabla 17

Utilización de redes wifi públicas para acceder a banca en línea o aplicación móvil.

Respuesta	Cantidad	Porcentaje
No	92	86,79%
Sí	14	13,21%
Total de encuestados	**106**	**100%**

Fuente: Elaboración propia, 2024.

Resultados e interpretación: La utilización de redes wifi públicas es un método por el cual los ciberdelincuentes realizan ataques informáticos para después sustraer el patrimonio de los clientes bancarios, y de los 106 encuestados 14 usuarios si utilizan dichas redes públicas, exponiendo su patrimonio y hasta información confidencial de sus dispositivos, para un 13,21%. Por otro lado, 92 encuestados si cumplen las medidas de seguridad para ingresar a banca en línea o aplicación móvil, al no utilizar las redes wifi públicas, siendo su mayoría con un 86,79%.

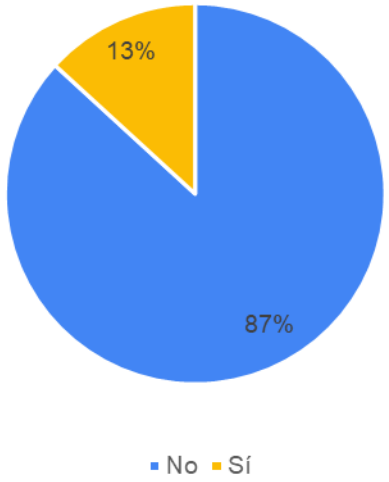

Figura 17. Utilización de redes wifi públicas para acceder a banca en línea o aplicación móvil.

Fuente: Elaboración propia, 2024.

Tabla 18

Medio por el que reciben las alertas de transacciones bancarias.

Respuesta	Cantidad	Porcentaje
Correo electrónico	96	64,43%
Mensaje de texto SMS	49	32,89%
No recibe notificación	4	2,68%
Total de medios	**149**	**100%**

Fuente: Elaboración propia, 2024.

Resultados e interpretación: De la tabla anterior se extrae el medio por el cual reciben los clientes la información de sus transacciones bancarias, la respuesta es múltiple, por lo que pudieron indicar una o varias opciones. En su mayoría o 96 usuarios reciben sus alertas bancarias mediante el correo electrónico, equivalente a un 64,43% del total de medios. Así mismo, 49 personas o un 32,89% reciben las alertas mediante un mensaje de texto SMS, pero los datos no son excluyentes entre sí, por lo que hay usuarios que lo reciben de ambas formas. Además, se obtiene el dato de que 4 personas no reciben notificaciones bancarias, siendo un 2,68%.

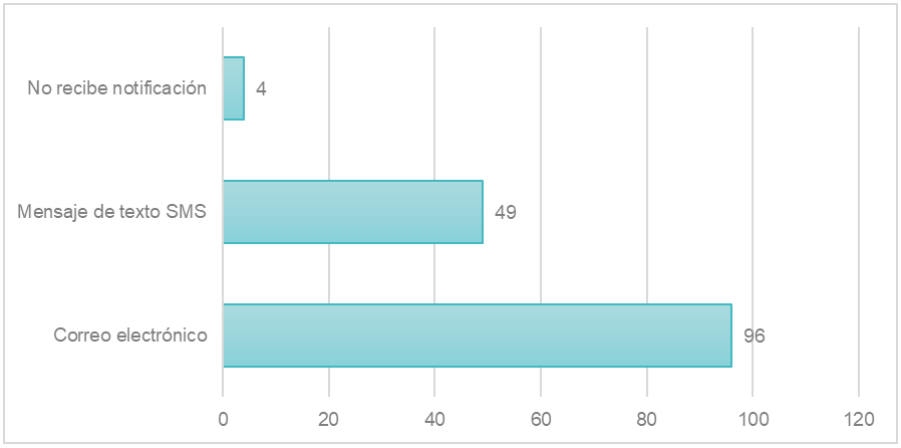

Figura 18. Medio por el que reciben las alertas de transacciones bancarias.

Fuente: Elaboración propia, 2024.

Tabla 19

Rapidez con que reciben las notificaciones bancarias.

Respuesta	Cantidad	Porcentaje
Muy rápido	42	39,62%
Rápido	46	43,40%
Con demora	12	11,32%
Con mucha demora	1	0,94%
NA	5	4,72%
Total de encuestados	**106**	**100%**

Fuente: Elaboración propia, 2024.

Resultados e interpretación: De la tabla anterior se obtiene la rapidez con que los usuarios reciben las notificaciones bancarias, para lo que 42 personas señalan que lo reciben muy rápido, representando un 39,62%. En su mayoría lo reciben rápido siendo 46 usuarios, equivalente a un 43,40% del total de personas encuestadas. Sin embargo, 12 clientes lo reciben con demora, para un 11,32%; y 1 lo recibe con mucha demora, para un 0,94%, estos con mayor dificultad para enterarse

si fueran víctimas de estafas informáticas. Así mismo, 5 personas o un 4,72% indican que no les aplica.

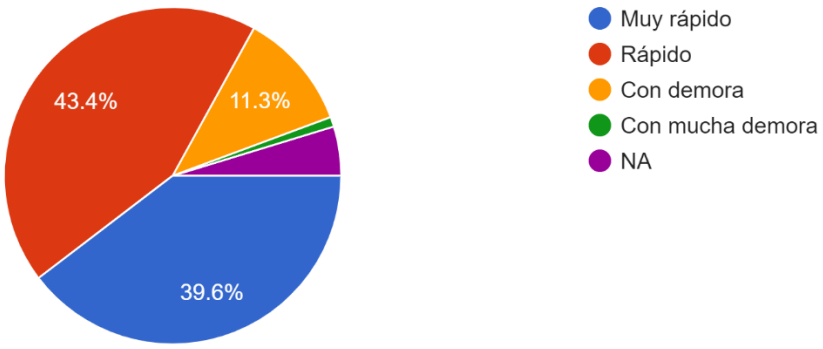

Figura 19. Rapidez con que reciben las notificaciones bancarias.

Fuente: Elaboración propia, 2024.

Tabla 20

Denuncias interpuestas en el Organismo de Investigación Judicial entre el 2019 al 2023 sobre estafas informáticas.

Delito	2019	2020	2021	2022	2023	Total general
Estafa informática	653	940	939	3129	3217	8878
Suplantación de identidad	639	797	1035	834	1125	4430
Espionaje informático	51	123	132	138	137	581
Suplantación de páginas electrónicas	33	37	107	287	67	531
Facilitación de delito informático	48	51	107	167	53	426
Instalación o propagación de programas informáticos maliciosos	8	90	76	50	17	241
Sabotaje informático	20	34	28	26	26	134
Daño informático	15	25	20	20	9	89
Total general	**1467**	**2097**	**2444**	**4651**	**4651**	**15310**

Fuente: Organismo de Investigación Judicial (2024).

Resultados e interpretación: De la tabla suministrada por el Organismo de Investigación Judicial (OIJ) donde suministran la cantidad de denuncias recibidas desde el 2019 hasta el 2023 en los delitos de: estafa informática, suplantación de identidad, espionaje informático, suplantación de páginas electrónicas, facilitación de delito informático, instalación o propagación de programas informáticos maliciosos, sabotaje y daño informáticos. En el delito tipificado como estafa informática en el historial de los últimos 5 años, tuvo un aumento paulatino, sin embargo, en los últimos 2 años el incremento en las demandas por este delito se triplicó, situación que es muy preocupante, porque significa que la población de ciberdelincuentes ha mejorado sus métodos de estafa o las personas usuarias bancarias desconfían cada vez menos, cayendo en las técnicas de los sujetos estafadores.

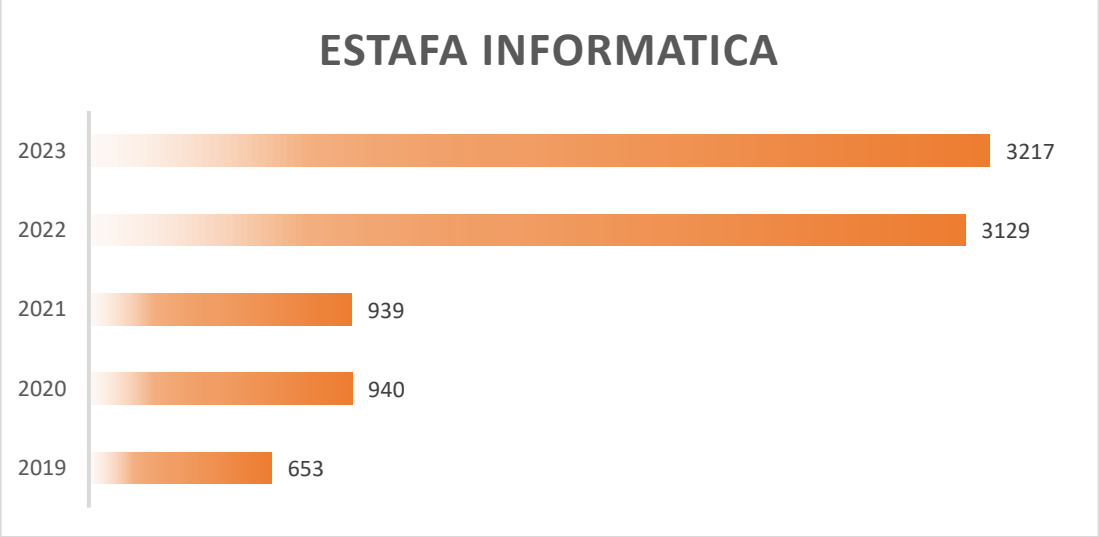

Figura 20. Estafas informaticas denunciadas ante el OIJ.

Fuente: Elaboración propia, 2024.

Por otro lado, la suplantación de identidad tuvo un comportamiento diferente ya que solo en el 2021 y 2023 presentó incrementos considerables en las denuncias, en estos delitos podría englobarse la suplantación de identidad de personas jurídicas, por ejemplo en redes sociales, engañando a usuarios y mediante ingeniería social obtener la información de acceso a las cuentas bancarias para sustraer el patrimonio de los sujetos engañados.

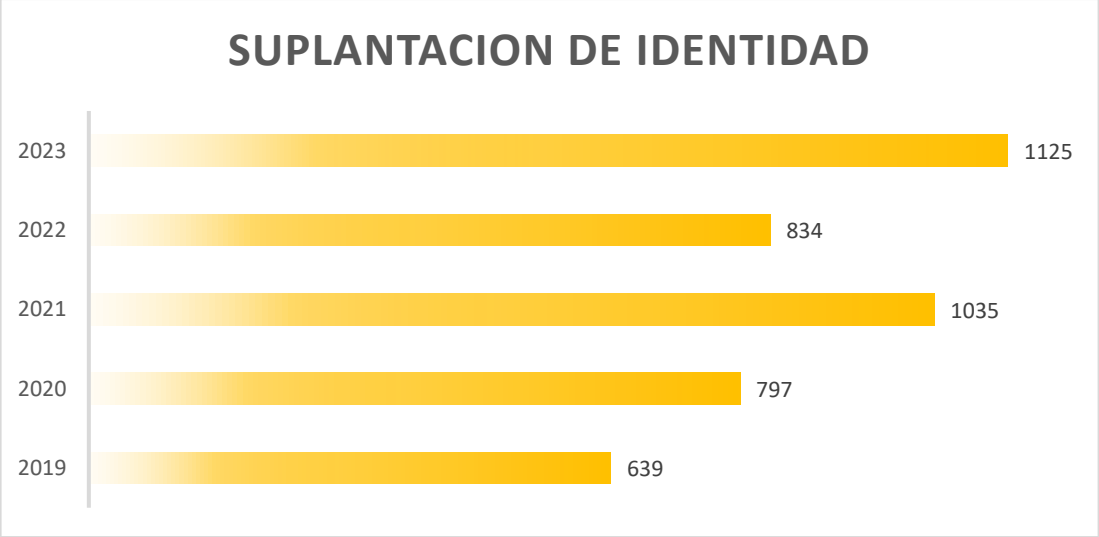

Figura 21. Denuncias por suplantación de identidad ante el OIJ.

Fuente: Elaboración propia, 2024.

Dentro del delito de espionaje informático, el cual consiste en ataques informáticos mediante diferentes técnicas invasivas como la instalación de virus maliciosos para robar la información o acceder remotamente a un ordenador, presento un aumento de más del 100% desde que inicio la pandemia por COVID-19, que provoco mayor uso de medios electrónicos para realizar las transacciones diarias.

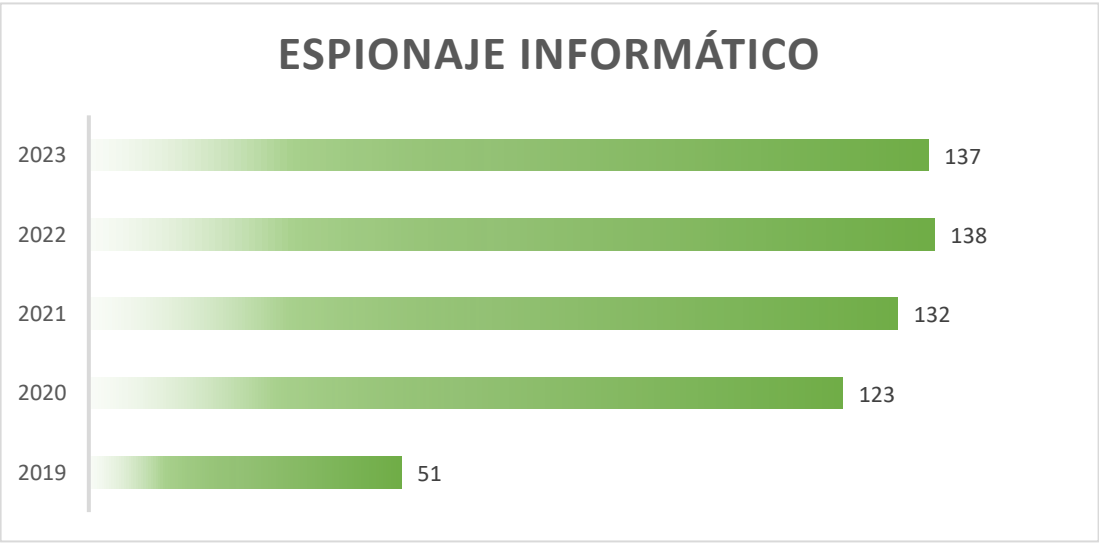

Figura 22. Denuncias por espionaje informático ante el OIJ.

Fuente: Elaboración propia, 2024.

La suplantación de páginas electrónicas fue un método cada vez más utilizado posterior a la pandemia que en nuestro país inicio en el 2020, la población de ciberdelincuentes al notar que las personas empezaron a utilizar más medios electrónicos porque no podían salir de sus casas, crearon páginas web idénticas en apariencia a las de los bancos, pero conectadas a otros servidores, forma que utilizaron para engañar usuarios y obtener la información de acceso y de autenticación de la banca en línea, y poder desalojar del patrimonio a las personas, aprovechándose del desconocimiento de los usuarios para reconocer las páginas seguras, y hasta el exceso de confianza de los clientes bancarios.

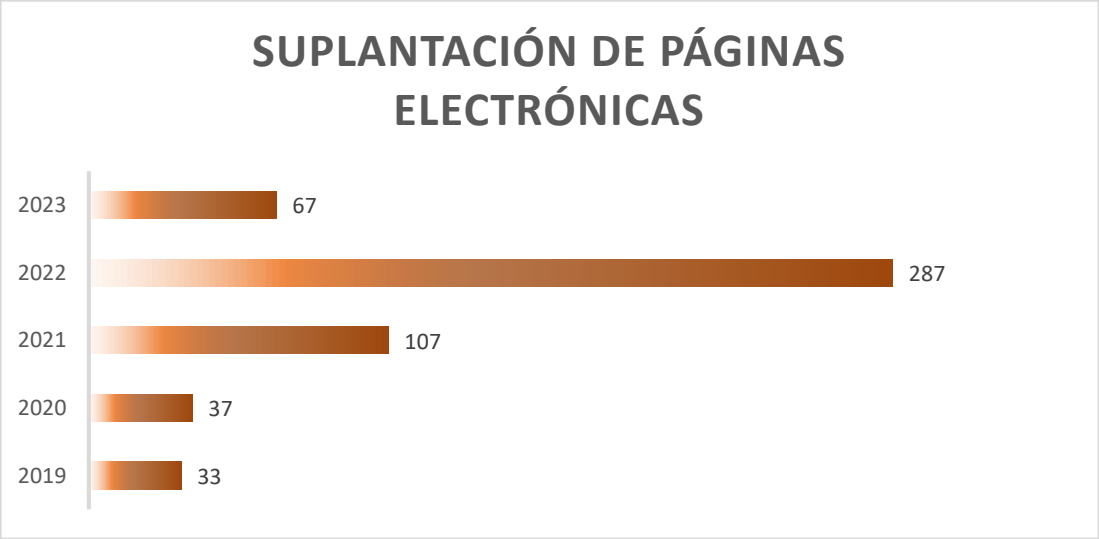

Figura 23. Denuncias por suplantación de páginas eletrónicas ante el OIJ.

Fuente: Elaboración propia, 2024.

Por último, existen otras tipificaciones muy relacionadas con las anteriores, que también presentaron aumentos significativos pero en el último año han tenido un comportamiento a la baja, y ellos son la facilitación de delito informático, instalación o propagación de programas informáticos maliciosos, sabotaje informático y daño informático, sin embargo se desconoce si esta disminución se debe a una menor incidencia de los delitos o mayor conocimiento de los métodos utilizados y por lo tanto los tipifican dentro de los que ya se mencionaron anteriormente.

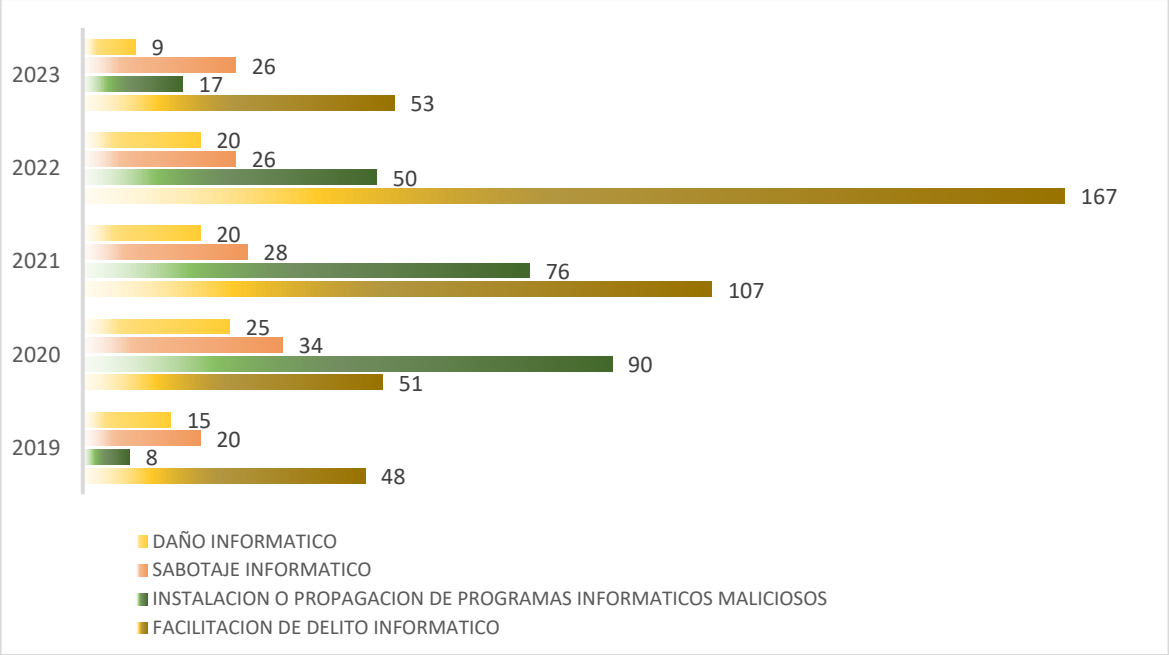

Figura 24. Denuncias varias ante el OIJ.

Fuente: Elaboración propia, 2024.

Tabla 21

Resultados obtenidos de la entrevista – No estructurada.

	Nivel de conocimiento sobre las estafas electrónicas a los clientes de la Banca Estatal		
Entrevistado	**Sustancial**	**Moderado**	**Bajo**
1	**X**		
2	**X**		
3		**X**	
4			**X**

Fuente: Elaboración propia, 2024.

Resultados e interpretación: De los datos analizados resultantes de la aplicación de la entrevista no estructurada tabulada en el cuadro anterior, se logra extraer la siguiente información: Del total de cuatro personas entrevistadas, todas ellas son profesionales en derecho. Dos de ellas

mostraron amplio conocimiento sobre las estafas informáticas realizadas a los clientes de la Banca Estatal, demostrando su ilustración en los diferentes métodos de estafas electrónicas, así como su diferenciación con los ataques informáticos, además de cuáles son las medidas de seguridad utilizadas por los entes bancarios. Expusieron su entendimiento sobre la teoría del riesgo y la responsabilidad objetiva, según el artículo 35 de la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor, así como las excepciones aplicables. Una de las personas entrevistadas mostró un moderado conocimiento sobre las estafas informáticas, esto porque conoce la diferenciación del término, no así la disimilitud con los ataques electrónicos. Sin embargo, sí conoce las medidas de seguridad utilizadas por los diferentes entes y su importancia. Ahora bien, tiene un conocimiento moderado sobre la línea jurisprudencial actual. Por último, el cuarto participante tiene un bajo conocimiento sobre los diferentes tipos de estafas electrónicas, su relación con los ataques informáticos, y desconoce la posición de los tribunales superiores en relación con la responsabilidad objetiva por parte de los entes bancarios estatales.

CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES

La sociedad mundial se encuentra en medio de una revolución tecnológica que inevitablemente ha transformado la forma de acceder a la información bancaria, dígase al patrimonio de los usuarios, especialmente como se realizan las transacciones mercantiles.

6.1 Conclusiones

Con el avance de la investigación y luego de todo lo analizado se concluye:

1. Que existe una responsabilidad objetiva de parte de los Bancos Estatales con los clientes de acuerdo con la Teoría del Riesgo contemplada en el numeral 35 de la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor.
2. Que existe un inadecuado uso de los términos correctos con relación a las estafas informáticas tanto por los Entes Bancarios como por los usuarios.
3. Hay suficiente Jurisprudencia que data de antes del 2009 con relación al tema de las estafas informáticas, en la que se valora la responsabilidad objetiva por riesgo en materia del consumidor que determina que le compete al proveedor del servicio asumir el riesgo, siempre y cuando no demuestre ajenidad al daño según las eximentes que le absuelven. Así mismo, sobre la reversión de la carga de la prueba que recae sobre el proveedor del servicio.
4. Se haya desconocimiento por parte de los usuarios sobre las medidas de seguridad que deben seguir para el uso correcto y resguardo de la información confidencial, como los datos de acceso para las plataformas bancarias.
5. Se conoce sobre las directrices internacionales sobre la protección del consumidor emanadas por la Asamblea General de la ONU, las cuales no han sido implementadas en la normativa costarricense.
6. Las medidas de seguridad de los Bancos han mejorado en acato a la Jurisprudencia, sin embargo, no existe suficiente conocimiento por los usuarios, provocando que caigan en las estafas informáticas.

Se logra constatar que existe suficiente normativa y Jurisprudencia que ahonda en el tema, tanto desde la perspectiva administrativa, civil, comercial y penal, además de recomendaciones internacionales sobre la protección al consumidor que debemos considerar en nuestro ordenamiento jurídico.

Tanto el artículo 35 de la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor, como el canon 190 de la Ley General de la Administración Pública, cobijan el

régimen de responsabilidad y sus eximentes. Además, la jurisprudencia es clara en cuanto a la responsabilidad objetiva por riesgo en materia del consumidor que le compete al proveedor del servicio asumir el riesgo, siempre y cuando no demuestre ajenidad al daño según las eximentes que le absuelven. Así mismo, sobre la reversión de la carga de la prueba que recae sobre el proveedor del servicio.

La Jurisprudencia valora la responsabilidad objetiva por riesgo en materia del consumidor como, la responsabilidad subjetiva, en la cual se requiere la concurrencia, y consecuente demostración, del dolo o culpa por parte del autor del hecho dañoso, y la objetiva que se caracteriza, en lo esencial, por prescindir de dichos elementos, siendo la imputación del daño el eje central sobre el cual se erige el deber de reparar. El comerciante, productor o proveedor, responderá por aquellos daños derivados de los bienes transados y los servicios prestados, aún y cuando en su actuar no se detecte negligencia, imprudencia, impericia o dolo.

La investigación establece que existen diversos métodos que los entes bancarios han mejorado e implementado para la seguridad de sus clientes. Si bien es cierto los entes financieros no pueden tener el control de la vida cotidiana de todos los usuarios, si es parte de su responsabilidad vigilar por la seguridad patrimonial de sus clientes, y por ello deben avanzar constantemente en los mecanismos de doble autenticación para una mayor seguridad.

Además el Estado no tiene implícito en la normativa las recomendaciones internacionales de la ONU sobre la protección y seguridad del consumidor, las cuales protegen al consumidor de asumir el riesgo creado por el proveedor del servicio, trasladándosele la responsabilidad a los Bancos, en el tema que nos ocupa, de capacitar a los consumidores para que tengan el conocimiento necesario para comprender el riesgo al que se someten al utilizar los medios digitales que le facilitan los Entes Bancarios, y de esta forma tomar la decisión de si asumen el riesgo o no utilizan el servicio.

Los proveedores deben adoptar las medidas adecuadas para garantizar la seguridad de los servicios ofrecidos a los consumidores. Esto incluye la obligación de informar de manera clara y precisa sobre los riesgos que puedan presentar los productos o servicios, así como proporcionar instrucciones de uso adecuadas.

La investigación contribuye vastamente a mejorar el desconocimiento en los usuarios sobre los tipos de ataques o estafas informáticas, así como las diferentes medidas de seguridad, que algunas de ellas son desconocidas o mal interpretadas por los usuarios, como lo es el

reconocimiento de un sitio web seguro o de una red segura, los que son muy importantes para no ser objeto de una estafa informática. Además, la importancia de incorporar las directrices internaciones a nuestro ordenamiento jurídico para aumentar el conocimiento de los usuarios y así mitigar el riesgo.

6.2 Recomendaciones

- Es de suma importancia como recomendación principal y como parte de los resultados de la investigación, que los entes bancarios estatales en obediencia a las recomendaciones señaladas en a las Directrices para la Protección del Consumidor por las Naciones Unidas sobre comercio y desarrollo, principalmente la indicada en el inciso d); elaboren, según proceda, programas y mecanismos para ayudar a los consumidores a adquirir los conocimientos y competencias necesarios para comprender los riesgos, incluidos los riesgos financieros y tomar decisiones bien fundadas. Dentro de lo que se debe instruir a los consumidores son los diferentes métodos que utilizan los usurpadores tanto en estafas como en ataques que pueden finalizar en fraudes informáticos, y el reconocimiento de los diferentes medios de seguridad para minimizar el riesgo.

- Se recomienda que en el artículo 35 de la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor se modifique la literalidad de la norma, para integrar las Directrices para la Protección del Consumidor de las Naciones Unidas sobre comercio y desarrollo, integrándolas de la siguiente manera:

> El productor, el proveedor y el comerciante deben responder concurrente e independientemente de la existencia de culpa, si el consumidor resulta perjudicado por razón del bien o el servicio, de informaciones inadecuadas o insuficientes sobre ellos o de su utilización y riesgos.
>
> Sólo se libera quien demuestre que ha sido ajeno al daño y haya implementado los mecanismos necesarios para que los consumidores adquieran el conocimiento y habilidades adecuadas para comprender los riesgos, incluidos los financieros, al tomar decisiones.
>
> Los representantes legales de los establecimientos mercantiles o, en su caso, los encargados del negocio son responsables por los actos o los hechos propios o por los de sus dependientes o auxiliares. Los técnicos, los encargados de la elaboración y el control responden solidariamente, cuando así corresponda, por las violaciones a esta Ley en

> perjuicio del consumidor". [**La negrita y cursiva es el texto por agregar].** (Artículo 35, Régimen de responsabilidad)

- Se sugiere que los Bancos Estatales inicien la implementación de mecanismos de formación para los usuarios, con el objetivo de crear conciencia sobre los riesgos asociados a la utilización de accesos digitales a sus cuentas bancarias y los posibles beneficios, con el fin de minimizar los riesgos financieros contemplados en el numeral 35 de la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor.

- Se recomienda que los Bancos Estatales desarrollen programas informativos destinados a educar a los usuarios sobre la identificación y prevención de formas de estafas y ataques informáticos. Se destaca la importancia de enfocarse en la materia de ataques informáticos, ya que suele recibir menor atención. Estos programas deberán incluir información sobre cómo reconocer medidas de seguridad efectivas para evitar ataques informáticos que puedan resultar en pérdidas patrimoniales, tales como identificar sitios web seguros, evitar el acceso a información bancaria en redes wifi-públicas, abstenerse de instalar programas desconocidos que puedan contener virus, utilizar software antivirus en todos los dispositivos electrónicos, entre otras prácticas preventivas relevantes.

- Se recomienda que los Bancos Estatales ejecuten programas o planes informativos sobre la diferenciación de las formas de estafas y ataques informáticos, esto por cuanto no se le da mucho énfasis a este último. Además de educar a los usuarios sobre el reconocimiento de las medidas de seguridad para evitar los ataques informáticos que pueden concluir en estafas patrimoniales, por ejemplo, cómo identificar un sitio web seguro, el no acceder a su información bancaria mediante redes wifi públicas, no instalar programas desconocidos que pueden contener virus, utilizar antivirus en todos sus dispositivos electrónicos, entre otras que consideren necesarias.

REFERENCIAS

Alvarado, J. (02 de mayo de 2022). Mayoría de estafadores se hacen pasar por empleados bancarios: conozca algunas pistas para reconocerlos. *El Observador*. https://observador.cr/mayoria-de-estafadores-se-hacen-pasar-por-empleados-bancarios-conozca-algunas-pistas-para-reconocerlos/

Alves, G., Ivo, P. y Moretti, D. (2022). O mɑlwɑre como meio de obtenção de prova e a sua implementação no ordenamento jurídico brasileiro. *Revista Brasileira de Direito Processual Penal, 8*(3), 1463-1500.

Anzola, A. y Oliveira, M. (2022). Regulation of Money Laundering and Corporate Criminal Responsibility in Spain: compliance as a key for Virtual Asset Service Providers. *Revista Brasileira de Direito Processual Penal, 8*(3), 1335-1370.

Banco Central de Costa Rica. (2024). Marco regulatorio de Seguridad de la Información. *Banco Central de Costa Rica*. https://www.bccr.fi.cr/transparencia-institucional/marco-regulatorio-de-seguridad-de-la-informaci%C3%B3n

Banco de Costa Rica. (2016). Reglamentos. R*eglamento para los servicios de Banca Electrónica*.https://www.bancobcr.com/wps/wcm/connect/bcr/e46dd69c-e457-4e35-bdf6-c61e7a2fae64/REG-GRE-ACE-22-04-16_V4.pdf?MOD=AJPERES

Banco Nacional de Costa Rica. (2023). Requisitos de Servicios. *Términos y condiciones de uso de Registro de dispositivos móviles en el Banco Nacional*. https://www.bncr.fi.cr/_cache_9a74/content/1609240000205802.pdf

Banco Popular y de Desarrollo Comunal. (2024). Reglamentos. *Disposiciones de uso y condiciones de los canales electrónicos*. https://www.bancopopular.fi.cr/disposiciones-de-uso-y-condiciones-de-los-canales-electronicos/

Banco Popular y de Desarrollo Comunal. (s.f.). Hablemos de ciberseguridad ¿Cómo evitar los fraudes electrónicos? [Mensaje de un blog]. https://www.bancopopular.fi.cr/hablemos-de-ciberseguridad-como-evitar-los-fraudes-electronicos/

Balmaceda, G. (2011). El delito de estafa en la jurisprudencia chilena. *Revista de Derecho (Valdivia), XXIV* (1), 59-85.

Bonilla, P. (2019). El Espectro Actual de los Delitos Informáticos. *Revista Judicial, Poder Judicial de Costa Rica, 1*(126), 220-225.

Burgos, A. (2020). El delito informático. *Acta Académica, 47*(noviembre), 175-198.

Calderón, F. (2021). *Construcción legislativa y aplicación jurisprudencial del delito de "estafa" informática en Costa Rica del año 2014 al 2019. Énfasis en el uso indebido de datos* [Tesis de Maestría, Universidad de Costa Rica]. Repositorio Kérwá-UCR. 1088. (www.kerwa.ucr.ac.cr).

Calvo, M. (2022). La responsabilidad civil de los bancos en los delitos de estafa por "phishing". *Actualidad Jurídica Iberoamericana, 1* (18), pp. 1788-1809.

Centro de Información Jurídica en Línea. (2009). *Informe de investigación sobre fraude informático.* https://cijulenlinea.ucr.ac.cr/2009/fraude-informatico/

Centro de Información Jurídica en Línea. (2009). *Informe de investigación sobre la responsabilidad objetiva de los bancos por delitos informáticos*. https://cijulenlinea.ucr.ac.cr/2009/responsabilidad-objetiva-de-los-bancos-por-delitos-informaticos/

Centro de Información Jurídica en Línea. (2023). *Informe de investigación de jurisprudencia sobre responsabilidad bancaria por el delito de estafa informática*. https://cijulenlinea.ucr.ac.cr/2023/jurisprudencia-sobre-responsabilidad-bancaria-por-el-delito-de-estafa-informatica/

Cisco. (2024). Soporte de Tecnologías. *Cisco*. https://www.cisco.com/c/es_mx/tech/voice/ip-telephony-voice-over-ip-voip/index.html

Código de Comercio [CC]. Ley 3284, 1964. Art. 613, 614 y 615. 30 de abril de 1964. (Costa Rica).

Código Penal [CP]. Ley 4573, 1970. Art. 216, 217 bis, 229 ter, 230, 231, 232 y 233. 04 de mayo de 1970. (Costa Rica).

Código Procesal Contencioso-Administrativo [CPCA]. Ley 8508, 2006. Art. 1, 2 y 139. 28 de abril de 2006. (Costa Rica).

Constitución Política de Costa Rica [Const]. Art. 24, 46, 49 y 188. 07 de noviembre de 1949 (Costa Rica).

Corte Suprema de Justicia. Sala Constitucional. Resolución 2015005615. Randall Rivera Vargas et al.: 22 de abril de 2015.

Corte Suprema de Justicia. Sala Primera. Resolución 000394-F-S1-2009. Inversiones K M K Sociedad Anónima, Banco de Costa Rica; 23 de abril del 2009.

Corte Suprema de Justicia. Sala Primera. Resolución 00300 - 2009. María de los Ángeles Arroyo Vargas, Banco de Costa Rica; 26 de marzo del 2009.

Corte Suprema de Justicia. Sala Primera. Resolución 00778 - 2012. Mario Coto Hidalgo, Banco Nacional de Costa Rica; 03 de julio del 2012.

Corte Suprema de Justicia. Sala Primera. Resolución 01431 - 2012. Emanuelle Territo, Banco Nacional de Costa Rica y Banco Popular y de Desarrollo Popular; 23 de octubre del 2012.

Corte Suprema de Justicia. Sala Primera. Resolución 01568 - 2012. Mario Alberto Odio Narvaez, Banco Nacional de Costa Rica; 29 de noviembre del 2012.

Corte Suprema de Justicia. Sala Primera. Resolución 01607 - 2012. Fabio Vargas Arias, Banco Nacional de Costa Rica; 06 de diciembre del 2012.

Corte Suprema de Justicia. Sala Primera. Resolución 00686 - 2014. Optomel Sociedad Anónima, Banco de Costa Rica; 28 de mayo del 2014.

Corte Suprema de Justicia. Sala Primera. Resolución 00385 - 2015. Karol Ulloa Mora, Banco de Costa Rica; 25 de marzo del 2015.

Corte Suprema de Justicia. Sala Primera. Resolución 00783 - 2016. Rowland Barry Lynn, Banco Nacional de Costa Rica; 21 de julio del 2016.

Corte Suprema de Justicia. Sala Primera. Resolución 01123 - 2017. Ulises Vargas Delgado, Banco de Costa Rica; 14 de setiembre del 2017.

Corte Suprema de Justicia. Sala Primera. Resolución 01289 - 2017. Laura Aguilar Masis, Banco de Costa Rica; 26 de octubre del 2017.

Corte Suprema de Justicia. Sala Primera. Resolución 00658 - 2018. Tecni Baterías Sociedad Anónima, Banco de Costa Rica; 13 de julio del 2018.

Corte Suprema de Justicia. Sala Primera. Resolución 02190 - 2020. Carlos Alberto Lobo Muñoz y Max Alberto Lobo Hernández, Banco Nacional de Costa Rica; 13 de agosto del 2020.

Corte Suprema de Justicia. Sala Primera. Resolución 02606 - 2020. Dorian Brenes Fonseca, Banco de Costa Rica y Banco Nacional de Costa Rica; 12 de noviembre del 2020.

Corte Suprema de Justicia. Sala Primera. Resolución 00604 - 2021. Carlos Luis Pérez Desanti, Banco Nacional de Costa Rica; 16 de marzo del 2021.

Corte Suprema de Justicia. Sala Primera. Resolución 02056 - 2022. Eddy David Ocampo Rodríguez, Banco Nacional de Costa Rica; 29 de setiembre del 2022.

Corte Suprema de Justicia. Sala Primera. Resolución 01116 - 2023. Carlos Roberto Serrano Pinto, Banco Nacional de Costa Rica; 05 de julio del 2023.

Corte Suprema de Justicia. Sala Primera. Resolución 01307 - 2023. Asociación Pro Defensa de Consumidores Financieros y Afines (Aprodeco), Erika Katiana Velásquez Corrales y Fabiana Gutiérrez Velásquez, Banco de Costa Rica; 27 de julio del 2023.

Devia, E. (2017). *Delito Informático: Estafa Informática del Artículo 248.2 del Código Penal*. [Tesis de Doctorado, Universidad de Sevilla]. Depósito de Investigación Universidad de Sevilla. https://hdl.handle.net/11441/75625

Digital Server. (2024). Qué es un sitio web seguro. Digital Server. https://www.digitalserver.com.mx/ordenar/knowledgebase/5/Que-es-un-sitio-web-seguro.html

ESET. (2024). Diccionario. ESET. https://www.eset.com/es/caracteristicas/antivirus-software-que-es/

Fernández, A. (2014). El concepto de responsabilidad. En J. Domínguez (Ed. 1st). *Homenaje al maestro José Barroso Figueroa por el Colegio de Profesores de Derecho Civil, Facultad de Derecho-UNAM*, pp 96-110. Castellanos Impresión, SA.

Flores, R. (2014). *Fundamentos de la metodología de la investigación*. Editorial Lulu.

Galeano, M. (2004). *Diseño de proyectos en la investigación cualitativa*. Fondo editorial Universidad EAFIT.

Gómez, M. (2006). *Introducción a la metodología de investigación científica*. Editorial Brujas.

González, N. (2021). Sistemas Jurídicos Contemporáneos: Nociones Introductorias y Familia Jurídica Romano Germánica. *Jurídica. Anuario del departamento de derecho de la universidad iberoamericana*, *1*(20), 621-672.

Google Ads. (2024). Ayuda de Google Ads. *Google Ads*. https://support.google.com/google-ads/answer/9004360?hl=es-419

Gregorio, N. (2023). *Metodologías de la investigación para anteproyectos*. Ediciones UAPA.

Gutiérrez, M. (1991). *Fraude informático y estafa.* ARTEGRAF, S.A.

Hernández, R., Baptista, M. y Fernández, C. (2014). *Metodología de la investigación.* McGraw-Hill.

Hernández, R. y Mendoza, R. (2018). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta*. McGraw-Hill.

Hierro, L. (2003). *La eficacia de las normas jurídicas*. Editorial Ariel.

Huerta, C. (2007). Sobre la validez temporal de las normas. La retroactividad y ultractividad de las normas en el sistema jurídico. *Problema: Anuario de Filosofía y Teoría del Derecho, 1*(1), 267-304.

Kelsen, H. (1949). *Teoría general del derecho y del estado.* (Trad. E. García). Imprenta Universitaria. (Trabajo original publicado en 1925).

Ley 8 de 1937. Ley Orgánica del Poder Judicial. 01 de diciembre de 1937. *La Gaceta* No. 270.

Ley 6227 de 1978. Ley General de la Administración Pública. 02 de mayo de 1978. *La Gaceta* No. 102.

Ley 7472 de 1994. Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor. 20 de diciembre de 1994. *La Gaceta* No. 14.

Ley 7558 de 1995. Ley Orgánica del Banco Central de Costa Rica. 03 de noviembre de 1995. *La Gaceta* No. 225.

Ley 8148 de 2001. Adición de los artículos 196 BIS, 217 BIS y 229 BIS al Código Penal, Ley N° 4573 para reprimir y sancionar los delitos informáticos. 09 de noviembre de 2001. *La Gaceta* No. 216.

Ley 8968 de 2011. Ley de Protección de la persona frente al tratamiento de sus datos personales. 07 de julio de 2011. *La Gaceta* No. 170.

Ley 9048 de 2012. Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal. 10 de julio de 2012. *La Gaceta* No. 214.

Ley 9605 de 2018. Fusión por absorción del Banco Crédito Agrícola de Cartago y el Banco de Costa Rica. 12 de setiembre de 2018. *La Gaceta* No. 172.

Ley 10385 de 2023. Ley para reconocer como derecho fundamental al acceso a las telecomunicaciones, tecnologías de la información y comunicaciones en todo el territorio nacional. 29 de noviembre de 2023. *La Gaceta* No. 236.

LISA Institute. (2024). Consejos Seguridad Bancaria. *LISA Institute*. https://www.lisainstitute.com/blogs/blog/consejos-seguridad-bancaria

López, R. (2017). *Fuentes de Información*. Editorial UOC.

Martínez, C. (2014). *Técnicas e instrumentos de recogida y análisis de datos*. Universidad Nacional de Educación a Distancia de Madrid.

Mayer, L. y Oliver, G. (2020). El delito de fraude informático: Concepto y delimitación. *Revista chilena de derecho y tecnología, 9*(1), 151-184.

Ministerio de Economía, Industria y Comercio. (2021). Quienes somos. *Comisión Nacional del Consumidor*.https://www.consumo.go.cr/comision_nacional_consumidor/quienes_somos.aspx.

Murcia, N. y Jaramillo L. (2000). *Investigación cualitativa: una guía para abordar estudios sociales*. Kinesis Armendia.

Naciones Unidas (2015) Directrices de las Naciones Unidas para la protección del consumidor. https://unctad.org/system/files/official-document/ares70d186_es.pdf.

Organismo de Investigación Judicial (2024). *Delitos informáticos ocurridos a nivel nacional. Periodo 2019 al 2023*. Solicitud de información 179-OPO/UAC/S-2024.

Poder Judicial. (2020). Diccionario Usual. *Poder Judicial.* https://diccionariousual.poder-judicial.go.cr/index.php/diccionario

Polaridad.es. (2024). Usuario en redes informáticas: Definición y características. Polaridad.es. https://polaridad.es/usuario-en-redes-informaticas-definicion-y-caracteristicas/?expand_article=1

Quesada, J. (12 de junio de 2023). Estos son los cuatro métodos de estafa más comunes en Costa Rica. *Calle 7 Informativo*. https://www.teletica.com/calle-7/estos-son-los-cuatro-metodos-de-estafa-mas-comunes-en-costa-rica_336708

Ramírez, N. (2018). Técnicas de la metodología cualitativa. [Mensaje en un blog]. Técnicas de la metodología cualitativa (unam.mx)

Regis, E. (26 de octubre de 2022). Tipos de fraudes por Internet: Soluciones y consejos para evitarlos [Mensaje en un blog]. https://www.conekta.com/blog/fraudes-por-internet

Rodríguez, E. (2005). *Metodología de la Investigación.* Universidad Juárez Autónoma de Tabasco.

Rojas, F. (2023). Huellas dactilares e identidad. *Revista OIJ, 1*(2). https://pjenlinea3.poder-judicial.go.cr/biblioteca/uploads/Archivos/Articulo/Huellas%20Dactilares%20e%20Identidad.pdf

Rudra, A. (5 de enero de 2023). ¿Qué es una red segura? [Mensaje en un blog]. https://powerdmarc.com/es/what-is-a-secured-network/#:~:text=Una%20red%20segura%20es%20una,como%20archivos%2C%20carpetas%20y%20aplicaciones.

Salas, D. (2010). Responsabilidad Civil Bancaria frente al cliente por Delitos Informáticos. [Tesis de licenciatura, Universidad de Costa Rica]. Repositorio SIBDI-UCR. 31126.pdf (ucr.ac.cr).

Scarfone, K. (2009). Guide to Enterprise Password Management (Draft). *National Institute of Standards and Technology, Special Publication*, *800*(118), 20899-8930.

Taylor, S. y Bodgan, R. (1984). *Introducción a los métodos cualitativos de investigación.* Editorial Paidos.

Tena, A. y Rivas, R. (1995). *Manual de investigación documental, elaboración de tesinas*. Universidad Iberoamericana.

Tribunal Contencioso Administrativo y Civil de Hacienda. Sección IV. Voto 06 - 2020. No se indica, Banco Nacional de Costa Rica; 29 de enero del 2020.

Tribunal Contencioso Administrativo y Civil de Hacienda. Sección IV. Sentencia No. 127-2020-IV. No se indica, Banco Popular y de Desarrollo Comunal; 19 de noviembre de 2020.

Tribunal Contencioso Administrativo y Civil de Hacienda. Sección I. Sentencia No. 026-2022-IX. Parménides Hungría Furcal Beriguete, Banco Popular y de Desarrollo Comunal; 30 de mayo del 2022.

Tribunal Contencioso Administrativo y Civil de Hacienda. Sección I. Resolución Nº 26 – 2023. Edwin Gerardo Lizano Arguedas, Banco Nacional de Costa Rica; 24 de marzo de 2023.

Tribunal Contencioso Administrativo y Civil de Hacienda. Sección IV. Resolución Nº 51-2023-IV. Javier Alberto Ugalde Fonseca, Banco Nacional de Costa Rica; 29 de mayo del 2023.

Tribunal Contencioso Administrativo y Civil de Hacienda. Sección III. Resolución N° 2023005234. Damaris Ruiz Valverde, Banco Nacional de Costa Rica; 08 de noviembre del 2023.

Tribunal Contencioso Administrativo y Civil de Hacienda. Resolución N° 2023006486. Annie Alicia Saborío Mora, Banco Nacional de Costa Rica; 15 de diciembre del 2023.

Tribunal de Casación Contencioso Administrativo y Civil de Hacienda. Resolución Nº 00112 - 2022. Manuel Enrique Porras Agüero, Banco Popular y de Desarrollo Comunal; 12 de mayo del 2022.

Tribunal de Casación Contencioso Administrativo y Civil de Hacienda. Resolución 128-F-TC-2023. Perménides Hungría Furcal Beriguete, Banco Popular y de Desarrollo Comunal; 13 de julio del 2023.

Visa. (2024). Notas de prensa. VISA. https://www.visa.co.cr/acerca-de-visa/sala-de-noticias/notas-de-prensa/visa-alerts.html#:~:text=El%20servicio%20de%20alertas%20ayuda,fraudulentas%20casi%20en%20tiempo%20real.

APÉNDICES

Apéndice A: Cuestionario aplicado en línea – Google Forms

Encuesta sobre Estafas Informáticas en los Bancos Estatales de Costa Rica

El objetivo de esta encuesta es conocer si los clientes de la banca estatal de Costa Rica han sufrido estafas informáticas y por qué medios. Así mismo indagar sobre las medidas de seguridad utilizadas por los bancos y sus clientes.

* Indica que la pregunta es obligatoria

1. Acepta que los datos suministrados por su persona sean utilizados en una investigación con fines académicos. *

( ) Sí

( ) No

2. Dentro de cual rango de edad se ubica. *

( ) 18 - 25 años

( ) 26 - 35 años

( ) 36 - 45 año

( ) 46 - 55 años

( ) 56 - 65 años

( ) 66 - 75 años

( ) 76 años en adelante

3. ¿Sabe usted que es una estafa informática? *

( ) Sí

( ) No

4. ¿Conoce cuáles son los Bancos Estatales de Costa Rica? *

( ) Sí

( ) No

5. ¿Ha sido víctima de estafa informática? *

Si su respuesta es No, por favor pasar a la pregunta 13

( ) Sí

( ) No

6. ¿Mediante qué medio obtuvo el estafador su información?

( ) Correo electrónico

( ) Llamada telefónica

( ) Mensaje de texto SMS

( ) Otros:_____

7. ¿En cuál Banco sufrió el daño patrimonial?

( ) Banco Nacional de Costa Rica

( ) Banco de Costa Rica

( ) Banco Popular

( ) Otro

8. ¿Considera usted que el Banco debe responder por el dinero sustraído?

( ) Sí

( ) No

9. ¿El Banco le devolvió el dinero sustraído?

( ) Si

( ) No

10. ¿Ha interpuesto una demanda judicial por ser víctima de una estafa informática?

( ) Sí

( ) No

11. ¿Ha interpuesto un reclamo administrativo por ser víctima de una estafa informática?

( ) Sí

( ) No

12. ¿Con que facilidad pudo realizar el reclamo al Banco

( ) Muy fácil

( ) Fácil

( ) Difícil

( ) Imposible

13. ¿Qué medida de seguridad implementa su Banco para el ingreso a la banca en línea o aplicación móvil? *

[ ] Nombre de usuario y contraseña

[ ] PIN

[ ] Huella dactilar

[ ] Reconocimiento Facial

[ ] Tarjeta dinámica

[ ] Token físico

[ ] Token por mensaje de texto SMS

14. ¿Mediante qué medio ingresa a su información bancaria? *

[ ] Banca en línea

[ ] Aplicación móvil

[ ] Presencialmente en la sucursal bancaria

15. ¿Conoce como identificar un sitio web seguro? *

( ) Sí

( ) No

16. ¿Utiliza las redes wifi públicas para ingresar a su aplicación móvil o banca en línea? *

( ) Sí

( ) No

17. ¿Por qué medio recibe alertas de sus transacciones bancarias? *

[ ] Correo electrónico

[ ] Mensaje de texto SMS

[ ] No recibe notificación

18. ¿Con qué rapidez recibe la notificación? *

( ) Muy rápido

( ) Rápido

( ) Con demora

( ) Con mucha demora

( ) NA

Apéndice B: Solicitud unidad de análisis criminal del OIJ

25 de enero de 2024

Licenciado
Víctor Fernández Vargas, Jefe a.i.
UNIDAD DE ANALISIS CRIMINAL
ORGANISMO DE INVESTIGACION JUDICIAL

Estimado señor:

Le agradezco interponga sus buenos oficios, a fin de que me facilite lo más pronto posible la última estadística criminal del delito de **Fraude Informático (por tipologías)** y que estén descritos por todas las provincias, todos los cantones y todos los distritos, adicionalmente si se encuentra dentro de sus posibilidades y control por institución financiera, desde enero del 2019 a diciembre del 2023. Esto con fines académicos, ya que me encuentro realizando la tesis para obtener el grado de licenciada en Derecho.

Atentamente,

Bach. Mariela Quesada Castro
Estudiante de Universidad Central

Apéndice C: Guía para la aplicación de la entrevista No estructurada a los participantes

- Conocimiento sobre el concepto básico de estafas informáticas.
- Diferencia entre estafa y ataque informático.
- Conocimiento sobre la responsabilidad objetiva de los Bancos Estatales con los clientes en estafas electrónicas.
- Conocimiento sobre las medidas de seguridad bancarias.
- Postura sobre la Teoría del Riesgo según el artículo 35 de la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor.