Universidad Internacional de las Américas

Escuela de Derecho

Trabajo Final de Graduación para optar por el grado de Licenciatura en Derecho

Análisis de los Criterios de Imputación de Responsabilidad Civil de las Entidades Bancarias Privadas en Costa Rica por Delitos de Estafas Informáticas Realizadas a Través de sus Plataformas Digitales en el período 2024.

María Milagro Hernández Rojas

Tutor:

Edwin Retana Carrera

San José

Marzo, 2026

Dedicatoria

A Dios, por sostenerme en cada momento, por darme fuerza cuando más lo necesité y por acompañarme a lo largo de este camino; y a la Virgen de la Medalla Milagrosa quien me ha cuidado y protegido desde el día de mi nacimiento.

A mis padres y mi hermano, porque entre el ruido de la vida siempre encontré calma en mi familia. Por su amor incondicional, por cada sacrificio silencioso y por ser el pilar fundamental de todo lo hoy soy. Este logro es para ustedes, por darme aliento fuerza y voluntad y sobre todo ser mi hogar en la tempestad.

A Federica, que me acompañó en silencio durante largas noches de trabajo y dudas, que con su presencia constante me enseñó el significado del amor leal, paciente y sincero.

Esta tesis está dedicada a mi Fefe, mi primer amor, quien partió mientras este trabajo aún se estaba escribiendo, pero cuya huella permanece en cada página. Su compañía fue refugio, su mirada fue consuelo y su existencia, una lección profunda de amor incondicional.

Aunque ya no esté físicamente a mi lado, sigue siendo parte de este logro, porque mucho de lo que soy y de lo que persevera en mí lo aprendí con ella.

Agradecimientos

Con profundo agradecimiento, expreso mi sincera gratitud y amor a Jafeth Villaplana, por ser mi apoyo en cada etapa de este camino, por su amor, su comprensión en los momentos difíciles. Gracias por creer en mí, incluso cuando el cansancio o las dudas aparecían.

A mi tutor, el profesor Edwin Carrera, por su paciencia infinita, su guía constante y su compromiso durante todo este proceso. Su orientación no solo enriqueció esta investigación, sino que también dejó en mí valiosas enseñanzas que trascienden lo académico.

A mis compañeros y profesores de la Universidad que formaron parte de este camino, por cada experiencia compartida, por el apoyo mutuo y por haber hecho de este recorrido académico un camino más humano, lleno de aprendizajes, risas y crecimiento.

Contenido

Índice de tablas

Introducción

En la era digital, la banca electrónica se ha consolidado como uno de los pilares fundamentales de la economía moderna, facilitando el acceso a servicios financieros mediante plataformas digitales. No obstante, este avance tecnológico ha traído consigo nuevas amenazas, entre las cuales destacan las estafas informáticas, que afectan tanto a los usuarios como a las propias entidades bancarias. En Costa Rica, el aumento de delitos informáticos ha generado una creciente preocupación sobre la responsabilidad que recae en los bancos privados cuando sus plataformas son utilizadas como medio para cometer fraudes.

Según el informe Estado de la Ciberseguridad en Costa Rica 2024, elaborado por el Laboratorio de Investigación, Desarrollo e Innovación en Ciberseguridad (LABCIBE) de la Universidad Nacional, las denuncias por delitos informáticos pasaron de 1.662 en el periodo comprendido del 01 de enero de 2018 a 6.634 en el perÍodo comprendido de 15 de octubre de 2024, lo que representa un incremento superior al 300%. Este crecimiento ha impulsado el desarrollo de un marco regulatorio más robusto, así como la necesidad de evaluar los criterios de imputación de responsabilidad civil aplicables a las entidades bancarias privadas frente a este tipo de delitos.

Por tanto, se hace necesario analizar con rigor los criterios jurídicos aplicables, tanto de naturaleza normativa nacional como derivados de principios generales del derecho civil, que permiten la imputación de responsabilidad civil a las entidades bancarias privadas en casos de fraudes informáticos.

Esta investigación se orienta particularmente a examinar dicha responsabilidad desde una perspectiva tanto contractual como extracontractual, a fin de determinar los deberes de diligencia exigibles a las instituciones financieras en el entorno digital. En este contexto, adquieren especial relevancia la protección del consumidor financiero y las garantías de seguridad en las transacciones electrónicas, elementos que configuran un nuevo paradigma en las relaciones jurídicas bancarias. Asimismo, resulta fundamental estudiar cómo la jurisprudencia costarricense ha abordado esta problemática y cuáles son los mecanismos probatorios que se han considerado idóneos para acreditar la responsabilidad en estos casos.

La presente investigación tiene como propósito analizar los criterios de imputación de responsabilidad civil en Costa Rica frente a delitos de estafas informáticas ocurridos durante el

año 2024, específicamente en el contexto de operaciones realizadas a través de plataformas digitales de entidades bancarias privadas.

Para ello, se desarrollará una revisión sistemática de fuentes normativas como el Código Civil, la legislación de protección al consumidor, la normativa penal sobre delitos informáticos y las disposiciones emitidas por la Superintendencia General de Entidades Financiera y/o el Consejo Nacional de Supervisión del Sistema Financiero, así como del desarrollo doctrinal y jurisprudencial en la materia. Este abordaje permite identificar no solo los criterios jurídicos aplicables, sino también los mecanismos probatorios que resultan determinantes para acreditar la responsabilidad en este tipo de casos.

En definitiva, este trabajo parte de una inquietud muy concreta, la cual es comprender cómo el derecho civil responde o intenta responder a un fenómeno que evoluciona rápidamente con la tecnología. Más allá del análisis teórico, la investigación busca aportar claridad en un terreno donde aún existen vacíos y tensiones, contribuyendo así a una aplicación más coherente del derecho y a una mejor protección del consumidor financiero en el entorno digital.

Capítulo I. Planteamiento del Problema

1.1 Problema

En Costa Rica, el desarrollo y expansión de las plataformas digitales utilizadas por las entidades bancarias privadas han facilitado significativamente la prestación de servicios financieros en línea, permitiendo mayor accesibilidad y eficiencia en las transacciones. Sin embargo, este avance tecnológico también ha propiciado un aumento en la comisión de delitos informáticos, especialmente aquellos relacionados con estafas electrónicas. Técnicas delictivas como el phishing, la suplantación de identidad, el uso de enlaces fraudulentos y la implementación de aplicaciones maliciosas han sido empleadas para vulnerar la seguridad de las plataformas digitales, causando perjuicios económicos a los usuarios mediante transferencias no autorizadas y apropiación indebida de fondos. En respuesta a este fenómeno, la Estrategia Nacional de Ciberseguridad Costa Rica, emitida por el Ministerio de Ciencia, Innovación y Telecomunicaciones (MICITT, 2023), como objetivo estratégico planteó la protección y resiliencia de infraestructuras críticas frente a las amenazas en ciberseguridad, estableciendo diferentes objetivos para salvaguardar los sistemas esenciales para el desempeño y conveniencia de la sociedad, entre los cuales se incluye el sector financiero privado.

En este sentido, la problemática se centra en la falta de claridad jurídica respecto a los criterios aplicables para imputar responsabilidad civil a las entidades bancarias privadas cuando estas estafas ocurren utilizando sus plataformas digitales. A pesar de que los responsables directos de las estafas suelen ser terceros ajenos a las instituciones bancarias, la relación contractual entre el banco y el cliente implica ciertos deberes de seguridad, diligencia y protección de los recursos y datos del usuario. La cuestión jurídica principal consiste en determinar si dichos deberes han sido vulnerados por acción u omisión, y si esa vulneración puede ser considerada como causal de responsabilidad civil, partiendo del régimen de responsabilidad contractual y extracontractual.

Este fenómeno ocurre en el ámbito jurídico de Costa Rica, y específicamente en el sector bancario privado, cuyas plataformas digitales son empleadas por una amplia población usuaria para realizar operaciones financieras cotidianas. Entre los actores implicados se encuentran, por un lado, los clientes bancarios, quienes resultan perjudicados por estos delitos; y por otro, las entidades bancarias privadas, responsables del diseño, gestión y supervisión de sus canales digitales. Asimismo, intervienen las autoridades judiciales y entidades reguladoras, como la

Superintendencia General de Entidades Financieras (en adelante "SUGEF"), encargadas de definir y supervisar las normas de seguridad tecnológica aplicables al sector.

El incremento de estos delitos ha sido notorio desde el año 2018, y se intensificó durante el período 2020-2024, como resultado del aumento en el uso de canales digitales debido a la pandemia por COVID-19 (MICITT, 2023). Ahora bien, de acuerdo con las cifras del OIJ en el periodo completo del 2024 se registraron 10.400 denuncias por delitos informáticos, lo que implicó un incremento del 90% más en comparación con las denuncias del periodo 2023. (Arrieta, 2025). Estas cifras incluyen tanto estafas informáticas consumadas como intentos reportados, lo que evidencia no solo la efectividad de los ciberdelincuentes, sino también una mayor conciencia y disposición de las víctimas para denunciar este tipo de hechos

Este contexto evidencia nuevas vulnerabilidades en la interacción entre los usuarios y los sistemas digitales bancarios. Según el portal de estadísticas del OIJ[1], las estafas electrónicas representan un porcentaje creciente de los delitos denunciados, y en muchos casos involucran el uso indebido de plataformas bancarias para concretar las acciones ilícitas.

La relevancia del problema radica en la necesidad de establecer un marco jurídico que permita determinar, en casos concretos, si una entidad bancaria debe asumir responsabilidad civil por los daños derivados de estas estafas. La inexistencia de criterios unificados en la legislación o en la jurisprudencia nacional genera incertidumbre para los operadores jurídicos, los usuarios afectados y las propias entidades financieras. Si el problema no se aborda, se mantiene un vacío normativo que limita el acceso efectivo a la reparación de los daños por parte de las víctimas y debilita la previsibilidad jurídica en materia de responsabilidad civil bancaria.

En cuanto a los antecedentes disponibles, se han desarrollado investigaciones que analizan los delitos informáticos desde la perspectiva penal o técnica, como lo señala Saborío (2022), quien expone los desafíos legales que implican los delitos cibernéticos en la banca digital. Sin embargo, la dimensión civil de esta problemática, y en particular la imputación de responsabilidad civil a las entidades bancarias privadas por hechos cometidos mediante sus plataformas digitales ha sido escasamente abordada en la doctrina costarricense.

Por tanto, esta investigación busca analizar los criterios legales, doctrinarios y jurisprudenciales que sustentan la posibilidad de imputar responsabilidad civil a las entidades bancarias privadas en Costa Rica frente a estafas informáticas cometidas durante el año 2024.

[1] Organismo de Investigación Judicial. (n.d.). Estadísticas policiales del OIJ. https://pjenlinea3.poder-judicial.go.cr/estadisticasoij/

Asimismo, se pretende examinar los mecanismos probatorios y jurídicos que permiten acreditar dicha responsabilidad ante los órganos jurisdiccionales. De este modo, se espera aportar a la construcción de un marco interpretativo que favorezca la aplicación coherente del derecho en esta materia, para lo cual se plantea la siguiente pregunta ¿Cuáles son los criterios jurídicos aplicables para la imputación de responsabilidad civil a las entidades bancarias privadas en Costa Rica frente a las estafas informáticas realizadas a través de sus plataformas digitales durante el período 2024?

1.2 Objetivos

1.2.1 Objetivo General

Analizar los criterios de imputación de responsabilidad civil que deben aplicarse a las entidades bancarias privadas en Costa Rica frente a los delitos de estafas informáticas realizadas a través de sus plataformas, y evaluar los mecanismos para acreditar dicha responsabilidad.

1.2.2 Objetivos Específicos

- Identificar los principales criterios legales y normativos que regulan la imputación de responsabilidad civil a las entidades bancarias privadas en Costa Rica por estafas informáticas cometidas a través de sus plataformas digitales para el período 2024.
- Examinar la jurisprudencia costarricense sobre los fallos judiciales relacionados con delitos informáticos en los que se han visto involucradas entidades bancarias privadas, con el fin de identificar patrones en la imputación de responsabilidad civil.
- Establecer el vínculo jurídico entre la responsabilidad civil de las entidades bancarias privadas y la ocurrencia de estafas informáticas, así como los mecanismos que permiten acreditar dicha responsabilidad.

1.3 Justificación

En el contexto actual de acelerada transformación digital, el uso de plataformas bancarias en línea se ha convertido en una conducta ampliamente adoptada por la gran mayoría de la población costarricense. Este fenómeno ha traído consigo múltiples beneficios en términos de eficiencia y acceso a servicios financieros.

De hecho, según las estadísticas recientes de la Superintendencia General de Entidades Financieras (SUGEF, 2023), aproximadamente el 78% de los usuarios costarricenses ha incorporado de manera regular servicios de banca digital, lo que respalda la afirmación sobre su adopción mayoritaria. Sin embargo, este avance tecnológico ha dado lugar a nuevos riesgos, siendo uno de los más significativos el aumento sostenido de las estafas informáticas.

Dicho tipo de delito representa una amenaza directa a la seguridad patrimonial de los usuarios y plantea importantes interrogantes en materia de responsabilidad jurídica: ¿hasta qué punto deben las instituciones financieras asumir responsabilidades si, a pesar de mantener elevados estándares de seguridad y diligencia, se vulneran los deberes protectores en sus plataformas digitales?

De acuerdo con el artículo 217 bis del Código Penal de Costa Rica, se establece como delito la estafa informática, sancionando con penas de hasta diez años de prisión a quienes manipulen sistemas automatizados con el fin de obtener un beneficio patrimonial indebido, especialmente cuando estos sistemas pertenecen a entidades financieras o están relacionados con operaciones bancarias (Asamblea Legislativa, 2012). Este marco legal refleja la gravedad con que se percibe este tipo de delitos, los cuales han afectado tanto a personas físicas como jurídicas. Ante este panorama, analizar los criterios jurídicos que permiten imputar responsabilidad civil a las entidades bancarias privadas por omisiones o fallas en la seguridad de sus plataformas digitales se convierte en una necesidad urgente y pertinente.

La importancia de estudiar este tema radica en la obligación que tienen las entidades bancarias de garantizar no solo la prestación del servicio, sino también la seguridad de las operaciones realizadas a través de medios digitales. Esta responsabilidad se enmarca en los principios del derecho privado y del derecho del consumidor, donde se reconoce un deber de custodia de los datos y activos de los usuarios. En este sentido, la Ley No.7472 sobre la Promoción de la Competencia y Defensa Efectiva del Consumidor, en su artículo 35, establece un régimen de

responsabilidad objetiva que obliga a los proveedores de servicios a responder por los daños causados al consumidor, salvo que prueben su ajenidad al daño:

> 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.
>
> (Así corrida su numeración por el artículo 80 de la ley de Contingencia Fiscal, No. 8343 del 18 de diciembre de 2002, que lo traspaso del antiguo artículo 32 al 35 actual). (Asamblea Legislativa, 1994. Artículo 35).

Esta norma resulta aplicable a las entidades bancarias y traslada la carga probatoria hacia ellas, reforzando su deber de diligencia frente a sus clientes.

Este trabajo resulta especialmente relevante para diversos sectores, desde una perspectiva institucional, proporciona herramientas interpretativas que pueden ser útiles para la judicatura costarricense, al enfrentar casos en los que se discute la responsabilidad civil de los bancos frente a delitos informáticos. Desde la perspectiva social, responde a la necesidad de proteger a los consumidores financieros, quienes muchas veces carecen del conocimiento técnico y jurídico para enfrentar adecuadamente estas situaciones. En el ámbito académico, el estudio contribuye al desarrollo de una línea de investigación jurídica aún naciente en Costa Rica, la cual es la responsabilidad civil derivada del uso de tecnologías en servicios bancarios.

Adicionalmente, esta investigación se apoya en la jurisprudencia nacional, como lo demuestra la sentencia No. 000248-F-S1-2011 de la Sala Primera de la Corte Suprema de Justicia, la cual expone los elementos fundamentales de la responsabilidad civil —conducta lesiva, daño, nexo de causalidad y criterio de imputación— y reconoce expresamente la existencia de supuestos de responsabilidad objetiva. En dicha resolución, la Sala establece que, en ciertos contextos, la

responsabilidad puede derivarse no de una conducta culposa, sino del riesgo creado por la actividad desarrollada, lo que resulta especialmente relevante en el ámbito bancario, donde el uso de plataformas digitales implica riesgos inherentes. Este precedente aporta una base doctrinal importante para el análisis de los casos en los que la actuación de una entidad bancaria pueda haber contribuido, por acción u omisión, a la comisión de un delito informático, incluso sin mediar culpa directa.

La investigación también pretende generar aportes prácticos. Al sistematizar los criterios legales, doctrinales y jurisprudenciales relacionados con la responsabilidad civil bancaria por estafas informáticas, se espera ofrecer un marco analítico que facilite la resolución de controversias judiciales, promueva mejores prácticas institucionales y fortalezca el diseño de políticas públicas y normativas enfocadas en la prevención y reparación del daño digital.

La pertinencia del tema en este momento obedece a que los delitos informáticos vinculados con plataformas bancarias no solo se han incrementado, sino que también presentan un reto significativo para el derecho civil, especialmente en lo que respecta a la adaptación de los principios tradicionales de la responsabilidad al entorno digital.

El no investigar este fenómeno implicaría mantener una laguna doctrinaria y normativa que podría derivar en inseguridad jurídica, desigualdad en el acceso a la justicia y desprotección del usuario financiero en un entorno cada vez más digitalizado.

De manera que, esta investigación responde a una necesidad institucional, social y académica, al abordar una problemática real y creciente que involucra derechos patrimoniales, deberes contractuales y principios de responsabilidad. Su finalidad es contribuir a la consolidación de un sistema bancario que no solo sea eficiente, sino también seguro y jurídicamente responsable frente a las amenazas que plantea el entorno tecnológico actual. En este contexto, se hace evidente la necesidad de modernizar el marco legal costarricense, a fin de que responda de manera ágil y efectiva a los desafíos que impone la transformación digital, especialmente en lo relativo a la protección de los usuarios y la imputación de responsabilidad en casos de delitos informáticos.

1.4 Antecedentes

La investigación tiene como objetivo analizar los criterios de imputación de responsabilidad civil que deben aplicarse a las entidades bancarias privadas en Costa Rica frente a los delitos de estafas informáticas realizadas a través de sus plataformas, y evaluar los mecanismos para acreditar dicha responsabilidad.

Ahora bien, la creciente digitalización de los servicios bancarios en Costa Rica ha transformado profundamente la relación entre los usuarios y las entidades financieras. Esta evolución ha facilitado el acceso a productos financieros en línea y ha incrementado la eficiencia operativa del sistema bancario. Sin embargo, también ha traído consigo nuevos riesgos, particularmente en lo que respecta a la comisión de delitos informáticos. Entre estos, las estafas electrónicas o fraudes informáticos se han convertido en una amenaza significativa tanto para los usuarios como para las propias entidades bancarias.

Según Vargas Araya (2020), la banca digital en Costa Rica ha experimentado una expansión significativa en los últimos años, impulsada en gran medida por la necesidad de adaptación frente a las restricciones derivadas de la pandemia. Esta transformación ha llevado a una mayor digitalización de procesos y a la consolidación de canales en línea, factorizando así el acceso a servicios financieros y potenciando la inclusión económica en el país.

Este fenómeno ha motivado el surgimiento de un debate jurídico relevante en torno a la imputación de responsabilidad civil a las entidades bancarias privadas por los daños ocasionados a sus usuarios a través de sus propias plataformas digitales. Dada la naturaleza técnica y la rapidez con la que ocurren estos delitos, surge la necesidad de identificar criterios claros y coherentes que permitan determinar la existencia o no de responsabilidad civil por parte de dichas entidades, así como los mecanismos idóneos para acreditar esa responsabilidad.

1.4.1 Internacionales

Desde el ámbito internacional, diversas experiencias legislativas y doctrinarias han servido como referencia para abordar la compleja relación entre los fraudes informáticos, como el phishing, y la responsabilidad civil de las entidades financieras. Un caso particularmente relevante es el estudio desarrollado por Rodríguez y Francisco (2023), titulado "*El delito de estafa informática: ¿Es posible determinar la responsabilidad civil de la entidad financiera con base en el artículo 120.3 del Código Penal como consecuencia del phishing?* " en el contexto jurídico español, donde los autores examinan detalladamente

la viabilidad de imputar responsabilidad civil a los bancos en supuestos de estafa informática, específicamente bajo la modalidad de phishing, con base en el artículo 120.3 del Código Penal de su legislación.

En su investigación, los autores sostienen que, aunque tradicionalmente la responsabilidad penal se funda en la existencia de dolo o culpa, existen supuestos en los que puede imputarse responsabilidad civil derivada de un hecho punible sin que medie culpa directa del ente financiero. Esto es posible gracias a una interpretación extensiva del artículo 120.3, que regula la responsabilidad civil subsidiaria de personas jurídicas por actos delictivos cometidos en su esfera de control o gestión, especialmente cuando se ha incumplido el deber de vigilancia, supervisión o control que razonablemente debía ejercerse.

Rodríguez y Francisco (2023) argumentan que las entidades bancarias, al operar plataformas digitales y manejar información altamente sensible de sus clientes, están sujetas a un deber de seguridad reforzado. Este deber implica no solo la implementación de medidas técnicas adecuadas, sino también la obligación de mantener actualizados los protocolos de ciberseguridad, prevenir accesos no autorizados y reaccionar de manera diligente ante posibles brechas o vulneraciones. En este sentido, cuando un banco permite —por acción u omisión— que terceros accedan de forma fraudulenta a cuentas de clientes mediante engaños como el phishing, puede considerarse que ha incumplido ese estándar de diligencia exigible, y por tanto, ser civilmente responsable.

Este enfoque doctrinal se alinea con las tendencias más modernas del derecho del consumidor y del derecho digital, que buscan trasladar parte de la carga de prevención y protección al proveedor del servicio, especialmente en contextos donde existe una evidente asimetría de información y capacidad tecnológica entre la entidad y el consumidor. En efecto, los autores subrayan que exigir al usuario bancario que pruebe las fallas de seguridad o negligencia por parte del banco es una carga probatoria desproporcionada, especialmente cuando toda la información técnica relevante está en poder de la propia institución financiera.

La propuesta de Rodríguez y Francisco ofrece, por tanto, una perspectiva normativa útil para el análisis comparado en contextos como el costarricense, donde aún se discute la posibilidad de adoptar criterios similares, como lo plantea el Proyecto de Ley No. 23.908

en Costa Rica, el cual fue aprobado por la Asamblea legislativa en segundo debate en marzo 2026, sin embargo, la misma en la redacción de este trabajo de investigación aún no ha sido dictada como ley. La idea de imputar responsabilidad civil a las entidades bancarias, incluso sin necesidad de demostrar culpa, encuentra respaldo en esta doctrina española, al considerar que la prestación de servicios financieros digitales debe ir acompañada de un estándar de seguridad proporcional al riesgo que implica.

Además, el estudio se apoya en un enfoque metodológico basado en el análisis dogmático del derecho penal y civil, combinado con el estudio de casos jurisprudenciales en los que los tribunales españoles han reconocido la responsabilidad del banco en escenarios de fraude electrónico. Esta metodología permite una valoración sistemática de la normativa vigente, sus lagunas y su aplicación práctica, aspectos que resultan también relevantes para el desarrollo de la presente investigación en el contexto costarricense.

La contribución de Rodríguez y Francisco (2023) pone de manifiesto que la responsabilidad de las entidades bancarias en fraudes informáticos no debe depender exclusivamente de la prueba de negligencia, sino que puede derivarse del incumplimiento de obligaciones de seguridad inherentes a su actividad. Este planteamiento ofrece una base teórica robusta para repensar el tratamiento jurídico del phishing y otros fraudes digitales desde una óptica más protectora del consumidor y más exigente con los proveedores de servicios financieros.

De forma similar, Anaya (2012) advierte que el aumento de transacciones electrónicas conlleva un incremento en los riesgos que deben ser gestionados por las propias entidades bancarias. El autor enfatiza que estas tienen no solo la capacidad técnica, sino también la obligación jurídica de implementar protocolos de prevención, reacción y educación al usuario para minimizar los riesgos de fraude.

En el plano penal, Lightowler-Stahlberg Juanes (2023) aborda la creciente preocupación por las estafas informáticas y la necesidad de que las entidades bancarias asuman una responsabilidad más allá de la mera diligencia contractual. En su artículo La responsabilidad civil, en el ámbito penal, de las entidades bancarias ante el auge de las estafas informáticas, el autor defiende la aplicación de una responsabilidad objetiva a las instituciones financieras, fundamentada en su posición dominante sobre los recursos tecnológicos y la información financiera de los usuarios.

Asimismo, argumenta que, dado el control que los bancos ejercen sobre los sistemas de pago y la información personal de los clientes, deben garantizar la seguridad de las transacciones y prevenir el uso fraudulento de sus plataformas. Esta perspectiva se alinea con la tendencia en la jurisprudencia española de considerar que, en actividades que implican riesgos inherentes, como la prestación de servicios financieros digitales, corresponde aplicar una responsabilidad objetiva por el peligro asociado al servicio prestado.

El autor destaca que, en muchos casos, los fraudes informáticos, como el phishing, se facilitan por la falta de controles adecuados por parte de las entidades bancarias. Además, señala que la rapidez de las transferencias electrónicas, promovida por políticas como las del Banco Central Europeo, ha incrementado las oportunidades para los ciberdelincuentes, lo que exige una respuesta más proactiva por parte de los bancos.

En este sentido, aboga por que las entidades bancarias sean responsables civilmente por los daños causados, incluso cuando el fraude haya sido cometido por un tercero, siempre que se haya producido por una omisión en la implementación de medidas de seguridad adecuadas. Esta postura se basa en el principio de que los bancos, al operar en un entorno digital, asumen el riesgo inherente a su actividad y, por lo tanto, deben responder por los perjuicios ocasionados a los usuarios.

La propuesta de Stahlberg ofrece una perspectiva valiosa para el análisis comparado en el contexto costarricense, donde aún se debate la extensión de la responsabilidad de las entidades financieras en casos de fraudes informáticos. Su enfoque destaca la necesidad de que las instituciones bancarias adopten un rol más activo en la protección de los consumidores y asuman las consecuencias de las fallas en sus sistemas de seguridad.

Por su parte, en el Reino Unido, se mantenía el Código del Modelo de Reembolso Contingente (CRM) el cual ya no está vigente, se retiró en 2018 y se reemplazó con un marco legal de reembolso. Sin embargo, en su lugar, existe un código CRM voluntario para la industria, que entró en vigor en mayo de 2019.

El Código del Modelo de Reembolso Contingente (CRM Code), implementado en 2019 por el Payment Systems Regulator (PSR). Este código establece principios para reembolsar a las víctimas de fraudes conocidos como Pagos Autorizados Push (Authorized Push Payment ‘APP’).

Este modelo ha sido considerado un referente en el ámbito internacional, al establecer una responsabilidad compartida entre banco y usuario, con énfasis en la responsabilidad proactiva de la entidad financiera. Además, pone de manifiesto que la falta de culpa directa del banco no lo exime necesariamente de responder por los daños, consolidando una visión más protectora del consumidor financiero en entornos digitales.

Finalmente, Hernández (2020) aborda la problemática de la responsabilidad de las entidades financieras en casos de fraudes electrónicos, específicamente en el contexto colombiano. La autora critica la aplicación del régimen objetivo de responsabilidad, como lo establece la Corte Suprema de Justicia en la sentencia SC18614-2016, argumentando que esta perspectiva limita los medios de defensa y excluye las causales de exoneración, además de no considerar adecuadamente la naturaleza contractual de la relación entre el banco y el cliente.

Hernández propone una interpretación integral del ordenamiento jurídico, sugiriendo que los análisis de fraudes electrónicos en el sistema financiero deben considerar la totalidad de los elementos que rodean la operación. En este sentido, aboga por una responsabilidad contractual basada en el cumplimiento de los deberes de diligencia de ambas partes, adoptando criterios subjetivos en lugar de los criterios de responsabilidad objetiva.

Esta perspectiva es relevante para el análisis comparado en el contexto costarricense, donde actualmente se debate la extensión de la responsabilidad de las entidades financieras en casos de fraudes electrónicos.

1.4.2 Nacionales

En lo que respecta a Costa Rica, el fenómeno de las estafas informáticas en el sector bancario ha experimentado un crecimiento significativo en los últimos años, reflejado tanto en el aumento de denuncias como en las pérdidas económicas asociadas.

Este contexto ha motivado el análisis y desarrollo de propuestas legales, doctrinarias y jurisprudenciales que buscan establecer con mayor claridad los criterios para la imputación de responsabilidad civil a las entidades financieras privadas.

El auge de los delitos informáticos ha generado una creciente preocupación entre las autoridades, instituciones financieras y la ciudadanía. De manera específica, el Organismo de Investigación Judicial (OIJ) ha reportado un incremento sustancial en las

denuncias por fraudes informáticos durante el año 2023. De acuerdo con los datos oficiales publicados por esta entidad, se contabilizaron más de 4.000 denuncias en ese período, lo que representa un notable crecimiento respecto a años anteriores. Estas actividades delictivas provocaron un perjuicio económico que supera los ₡85.500 millones de colones y los $53 millones de dólares, evidenciando el impacto financiero significativo que tienen este tipo de delitos sobre la economía nacional y sobre los patrimonios individuales de las personas afectadas. No obstante, el crecimiento para el periodo 2024 fue mayor ya que, de acuerdo con estadísticas del OIJ los delitos informáticos se duplicaron por día, pasando de 14 por día en 2023 a 27 por día en 2024.

El aumento de estos fraudes informáticos no ha sido fortuito, sino que obedece al perfeccionamiento de diversas modalidades criminales utilizadas por los ciberdelincuentes. Entre las prácticas más comunes se encuentran el phishing, la ingeniería social, la suplantación de identidad y el uso indebido de datos personales. Estas técnicas permiten a los estafadores engañar a los usuarios mediante la manipulación psicológica o el uso de mensajes falsos que simulan provenir de instituciones legítimas, como entidades bancarias. En muchos casos, los delincuentes logran obtener claves, números de tarjetas y otra información confidencial que les permite acceder a cuentas bancarias o realizar transferencias de fondos sin el consentimiento de los titulares.

Además, investigaciones periodísticas y reportes de seguridad digital han identificado una preocupante colaboración entre ciertos empleados bancarios y redes delictivas. De acuerdo con una investigación realizada en el periódico la República titulada "*OIJ revela tráfico de datos personales entre empleados bancarios y ciberdelincuentes"*, se han detectado casos en que funcionarios de entidades financieras han facilitado información sensible a terceros, contribuyendo directamente a la comisión de los fraudes. Este fenómeno no solo evidencia una vulnerabilidad estructural dentro del sistema financiero, sino también plantea cuestionamientos relevantes sobre los deberes de supervisión, diligencia y prevención que deben asumir las instituciones bancarias para garantizar la seguridad de las operaciones digitales. (Siles, 2022)

Frente a este panorama, se advierte que el entorno financiero costarricense se enfrenta a una amenaza que no solo compromete la confianza de los usuarios en las plataformas digitales, sino que también pone en entredicho la capacidad de los bancos para

prevenir, detectar y mitigar los riesgos tecnológicos que enfrentan. El crecimiento de las estafas digitales, como lo señala el OIJ, no es simplemente un problema de seguridad cibernética, sino también un desafío jurídico que exige una revisión crítica del marco normativo y de los criterios de imputación de responsabilidad civil que podrían aplicarse a las entidades financieras involucradas de forma directa o indirecta en estos hechos delictivos.

La integración de estos datos empíricos como lo son las estadísticas proporcionadas por el OIJ serán claves para evaluar la eficacia de los mecanismos actuales de imputación de responsabilidad civil a entidades bancarias privadas, puesto que se podrá constatar las cifras de denuncias y el impacto económico con los criterios jurídico y precedentes judiciales, logrando identificar las deficiencias y oportunidades de mejora en el marco normativo.

De esta manera, la investigación no solo se limita a un análisis teórico o doctrinal, sino que incorpora una dimensión empírica que aporta rigor y actualidad al estudio. Además, contribuye activamente a la construcción de recomendaciones normativas, orientadas a fortalecer el marco jurídico aplicable a la responsabilidad civil de las entidades bancarias privadas frente a las estafas informáticas. Esta doble perspectiva —analítica y propositiva— permite que el trabajo tenga un impacto práctico en la formulación de políticas públicas y en la mejora de los mecanismos de protección para los usuarios del sistema financiero.

Ahora bien, Espinoza (2023) propone la aplicación de la responsabilidad civil objetiva a las entidades bancarias por los fraudes cometidos a través de sus plataformas, bajo el argumento de que estas instituciones generan un riesgo inherente debido al control que ejercen sobre los sistemas y canales digitales. Esta perspectiva se sustenta en la teoría del riesgo creado, que postula que quien introduce un riesgo a la sociedad debe responder por los daños que de él se deriven, independientemente de su culpa.

A nivel legislativo, el proyecto de ley No. 23.908, actualmente aprobado por la Asamblea legislativa en segundo debate en marzo 2026, sin embargo, la misma en la redacción de este trabajo de investigación aún no ha sido dictada como ley, tiene como objetivo principal establecer un régimen de responsabilidad civil específico para las entidades financieras en casos de fraudes electrónicos y estafas informáticas que se realicen

a través de sus plataformas digitales. Esta iniciativa legislativa busca responder a la creciente preocupación por la vulnerabilidad de los usuarios ante delitos informáticos que afectan directamente su patrimonio, y que han experimentado un aumento significativo en los últimos años.

Entre las disposiciones más relevantes del proyecto destaca la inversión de la carga de la prueba, un mecanismo que propone trasladar la obligación de demostrar la diligencia debida a las instituciones bancarias. Esto significa que, en lugar de que el usuario afectado deba probar la negligencia o falta de seguridad por parte del banco, será la entidad financiera la que deberá acreditar haber implementado todas las medidas necesarias para prevenir el fraude. Esta disposición representa un cambio significativo en la dinámica procesal y en la protección del consumidor, alineándose con principios de responsabilidad objetiva aplicables en otros ámbitos del derecho del consumidor.

Asimismo, el proyecto contempla la regulación de estándares mínimos de seguridad tecnológica y protocolos de respuesta ante incidentes de fraude digital, buscando fortalecer la prevención y mitigación de riesgos en el entorno bancario digital. Se pretende además establecer mecanismos claros para la reparación integral de los daños sufridos por los usuarios, contribuyendo así a consolidar un sistema financiero más seguro y confiable.

En este contexto, la iniciativa legislativa No. 23.908 refleja un esfuerzo legislativo por actualizar y complementar el marco jurídico costarricense frente a las nuevas modalidades delictivas en el ámbito digital, adaptando las normas a los desafíos tecnológicos actuales. Su análisis es fundamental para comprender las tendencias y debates normativos que influyen en la imputación de responsabilidad civil a las entidades bancarias privadas, y para identificar posibles líneas de mejora en la protección de los consumidores financieros.

Además, esta propuesta legislativa contribuye al fortalecimiento de la confianza pública en la banca digital, al establecer mecanismos más claros y eficaces para la defensa de los derechos de los usuarios frente a fraudes electrónicos, lo que resulta esencial en un entorno donde la seguridad y la transparencia son pilares de la relación entre las entidades financieras y sus clientes.

Sin embargo, este proyecto ha generado reacciones contrastantes. La Asociación Bancaria Costarricense (ABC) ha expresado su preocupación, argumentando que la

aprobación del texto podría incentivar el fraude y trasladar injustamente la carga de la responsabilidad a las entidades financieras. En contraposición, diversas organizaciones ciudadanas y defensores de los derechos de los consumidores han manifestado su respaldo al proyecto, al considerar que existe una clara asimetría informativa y tecnológica entre los usuarios y los bancos, lo que dificulta que los primeros puedan probar fallas o negligencias en la seguridad digital. (Calderón, 2025)

En esta investigación el análisis del Proyecto de Ley No. 23.908 es fundamental para comprender las tendencias y debates normativos que influyen en la imputación de responsabilidad civil a las entidades bancarias privadas, y para identificar posibles líneas de mejora en la protección de los consumidores financieros.

Ahora bien, uno de los desafíos más relevantes en el tratamiento jurídico de las estafas informáticas en Costa Rica es la evidente falta de claridad normativa respecto a la imputación de responsabilidad civil a las entidades bancarias privadas. Esta ambigüedad se manifiesta tanto en la legislación sustantiva como en la normativa sectorial que regula la relación entre los bancos y sus clientes en entornos digitales. Aunque el ordenamiento jurídico costarricense contempla normas generales en materia penal y de protección al consumidor, como el artículo 217 bis del Código Penal, el artículo 35 de la Ley No. 7472 o el Acuerdo SUGEF 10-07, no existe un marco legal integral ni específico que regule de forma detallada las obligaciones de seguridad digital de las entidades financieras, ni los criterios aplicables para atribuirles responsabilidad civil en casos de fraude electrónico.

La legislación vigente presenta vacíos importantes frente a los nuevos escenarios delictivos digitales, muchos de los cuales no estaban contemplados cuando se redactaron las normas actuales. Por ejemplo, el delito de estafa informática fue incorporado recientemente mediante reformas al Código Penal, pero su formulación general dificulta su aplicación directa a situaciones complejas como el phishing, el smishing o la suplantación de identidad en entornos bancarios virtuales. Además, no existe una regulación específica que determine con precisión los estándares de diligencia exigibles a las entidades bancarias en términos de ciberseguridad, ni los deberes concretos de prevención, monitoreo, notificación o reparación ante incidentes informáticos.

Esta situación normativa deja a los consumidores financieros en una posición desventajosa, ya que, ante la inexistencia de reglas claras, las entidades financieras pueden

eludir con mayor facilidad la responsabilidad civil alegando falta de negligencia o desconocimiento de la causa del daño. Como lo destaca Anaya (2012), uno de los principales problemas de las transacciones electrónicas bancarias es precisamente la dificultad de los usuarios para demostrar que el banco incurrió en una omisión de seguridad, debido a que la mayoría de la información técnica relevante está en manos de la propia entidad, lo que genera una notoria asimetría informativa.

El problema se agrava por la ausencia de jurisprudencia uniforme en la materia. Si bien existen algunas resoluciones judiciales, como la sentencia No. 000248-F-S1-2011 de la Sala Primera de la Corte Suprema de Justicia, que sientan criterios sobre responsabilidad objetiva y los elementos necesarios para imputar civilmente a un agente económico, estas decisiones no abordan de forma específica el entorno de fraudes informáticos bancarios, ni generan una doctrina clara aplicable a estos casos. La dispersión de criterios y la falta de precedentes consolidados contribuyen a la incertidumbre jurídica tanto para las víctimas como para las instituciones financieras.

En este contexto, la falta de claridad normativa representa una barrera para la protección efectiva de los derechos de los consumidores y para la generación de confianza en los servicios financieros digitales. Tal como lo señala Rodríguez y Francisco (2023), en su estudio sobre la posibilidad de atribuir responsabilidad civil a las entidades financieras en casos de phishing, el marco normativo debe evolucionar para reconocer la naturaleza cambiante de los delitos cibernéticos y garantizar un equilibrio adecuado entre los derechos del usuario y los deberes del proveedor del servicio.

Frente a este panorama, la presente investigación busca contribuir al debate académico y legislativo sobre la necesidad de establecer un marco normativo claro, actualizado y funcional que regule de manera específica la responsabilidad civil de las entidades bancarias privadas en relación con las estafas informáticas.

Capítulo II. Marco Teórico

El análisis de la responsabilidad civil de las entidades bancarias frente a estafas informáticas no puede abordarse sin antes construir una base teórica sólida que permita entender cómo operan, en conjunto, las categorías clásicas del derecho civil y los nuevos desafíos del entorno digital. Precisamente por eso, este capítulo no se limita a exponer conceptos, sino que busca ordenar y conectar aquellos elementos que resultan indispensables para interpretar el problema desde una perspectiva jurídica coherente.

En primer lugar, se retoman los fundamentos de la responsabilidad civil, no como una revisión meramente doctrinal, sino como un punto de partida necesario para comprender cómo se configuran sus elementos —daño, nexo causal, hecho generador y criterio de imputación— en escenarios donde intervienen tecnologías digitales. A partir de ahí, se incorporan las principales teorías contemporáneas de imputación, especialmente aquellas que han cobrado mayor relevancia en contextos de riesgo tecnológico, como la teoría del riesgo creado, el deber de seguridad y los enfoques relacionados con la distribución de la carga de la prueba.

Sobre esa base, el análisis se traslada al ámbito bancario, donde la relación entre entidad financiera y usuario presenta características particulares. No se trata de una relación simétrica, debido a que el banco concentra el control técnico, la información y la gestión de los sistemas, mientras que el usuario actúa en una posición claramente más vulnerable. Esta realidad obliga a reflexionar cómo se aplican las reglas tradicionales de responsabilidad civil en un contexto donde los riesgos no siempre son visibles ni fácilmente controlables por quien utiliza el servicio.

Por último, el capítulo incorpora el estudio de las estafas informáticas y del riesgo tecnológico asociado a las plataformas digitales bancarias. Aquí el interés no es solo describir las modalidades de fraude, sino entender cómo estas interactúan con los deberes jurídicos de las entidades financieras y cómo inciden en la determinación de su eventual responsabilidad. De esta manera, el marco teórico no solo aporta definiciones, sino que construye una guía interpretativa que servirá de base para el análisis posterior.

En conjunto, este capítulo permite situar el problema en su dimensión real, no como un conflicto aislado, sino como el resultado de la tensión entre un derecho civil construido sobre bases tradicionales y un entorno tecnológico que evoluciona constantemente.

1. Fundamentos de la Responsabilidad Civil

1.1 Concepto y función de la responsabilidad civil

La responsabilidad civil constituye uno de los pilares fundamentales del Derecho Privado, al establecer el deber de reparar el daño causado a otro por una conducta antijurídica. Se trata de un mecanismo de protección jurídica que impone consecuencias legales a quien lesiona injustamente un derecho o interés legítimo de otra persona. Según Mosset Iturraspe (2004), la responsabilidad civil trata de la obligación legal que recae sobre una persona para reparar o compensar el perjuicio ocasionado a otra, ya sea por actos propios, por hechos de terceros bajo su responsabilidad o por el uso o posesión de bienes.

Es importante destacar que Pérez (1994), define como responsabilidad:

> Situación por la cual se realiza la atribución de un efecto jurídico "de necesidad" (de un resarcimiento), sea como consecuencia de una culpabilidad o de un riesgo creado en la hipótesis de responsabilidad extracontractual o de la violación de un vínculo preexistente en los casos de responsabilidad contractual (p.384). [2]

Por otro lado, Hernández (2018), señala que la responsabilidad civil implica el deber legal de asumir las consecuencias económicas derivadas de las actuaciones propias o de aquellas realizadas por personas por las que se deba responder, cuando estas ocasionen un daño a un tercero, ya sea individual o colectivo. Desde la perspectiva procesal, esta figura se concreta en la obligación de restituir el bien afectado, reparar el daño ocasionado y compensar los perjuicios que se hayan generado a raíz de un hecho ilícito. [3]

Ahora bien, normativamente la tutela de los daños y perjuicios en Costa Rica constitucionalmente se encuentra regulado bajo el artículo 41 de la Constitución Política, el cual señala: "ARTÍCULO 41.- Ocurriendo a las leyes, todos han de encontrar reparación para las injurias o daños que hayan recibido en su persona, propiedad o intereses morales. Debe hacérseles justicia pronta, cumplida, sin denegación y en estricta conformidad con las leyes" (Constitución Política, 1949, art.41).

Por otro lado, el Código Civil, regula el tema bajo el artículo 1045, que corresponde a: "ARTÍCULO 1045.- Todo aquel que por dolo, falta, negligencia o imprudencia, causa a otro un

---

[2] PÉREZ VARGAS, Víctor (1994). Derecho Privado. San José, Costa Rica. Tercera Edición. Litografía e Imprenta LIL, S.A. p.384

[3] Hernández, P. P. (2018). Responsabilidad civil: (ed.). Santiago de los Caballeros, Universidad Abierta para Adultos (UAPA). Recuperado de https://elibro.net/es/ereader/bibliouia/175610?page=21.

daño, está obligado a repararlo junto con los perjuicios" (Código Civil de Costa Rica, 1885, artículo 1045).

En virtud de lo anterior, esta figura no se limita a establecer el deber de resarcir el daño, sino que también determina la forma en que el sistema jurídico asigna y distribuye los riesgos sociales que surgen como consecuencia de la generación de perjuicios.

Más allá de su carácter estrictamente indemnizatorio, la responsabilidad civil cumple otras funciones que amplían su alcance dentro del ordenamiento jurídico moderno. Se reconoce que la responsabilidad civil mantiene una función resarcitoria, pero no solo se aplica desde dicha perspectiva, sino que también, se da desde un punto preventivo y desde su función distributiva del riesgo.

La función resarcitoria desde su concepción clásica es la de reparación o indemnización de daños y perjuicios. Básicamente, la idea que la sostiene es que quien causa un daño debe asumir las consecuencias económicas que de él se derivan, procurando que el afectado quede en la medida posible en una situación equivalente a la que habría tenido si el hecho dañoso no hubiese ocurrido. En material patrimonial, el objetivo resulta alcanzable, pues el menoscabo se traduce en aspectos económicos, por lo cual se puede compensar desde una indemnización, por lo cual, desde esta perspectiva, el centro del sistema es la protección del interés lesionado.

Por otro lado, la responsabilidad civil, ha dejado de responder únicamente como un mecanismo destinado a reparar lo ya ocurrido y funge desde una función preventiva, en cuanto influye en el comportamiento de quienes desarrollan actividades que pueden generar daños. La posibilidad de tener que asumir las consecuencias económicas de un perjuicio actúa como un incentivo para actuar con mayor cuidado y adoptar medidas razonables de prevención.

"Pugliatti, desde hace mucho, había hecho notar que la lesión a los intereses se produce no solamente con el daño actual, sino también con el potencial o peligro" (Pérez Vargas, 2016, como se citó en Vindas Castiglioni p. 64).

De forma tal que la función preventiva actúa *ex ante* de la causa del daño, de tal manera, que la idea señala que en un sistema indemnizatorio resulta más económico optar por la prevención que por la reparación de este, ya que tiene como propósito no cargar sino anticipar y reducir la probabilidad de que el perjuicio ocurra.

Asimismo, se incorporó una visión distributiva, bajo la cual, hace ver que la responsabilidad civil no solo repara, sino que distribuye los riesgos inherentes a determinadas

actividades. Esta función se centra en situaciones en las que, por razones de interés social, se establece como una regla de responsabilidad objetiva. Donde se trata de actividades que, aunque implican cierto riesgo, resultan necesarias o beneficiosas para la sociedad; por ello, los riesgos que generan se distribuyen entre distintos agentes, buscando equilibrar la protección de los afectados con la continuidad de dichas actividades.

Como señala Pantaleón (1991), en sociedades tecnológicamente avanzadas resulta inevitable que ciertas actividades generen riesgos estructurales; el problema jurídico consiste en determinar quién debe soportarlos. Esta lógica es especialmente relevante en contextos donde la actividad profesional crea riesgos que exceden el control del consumidor promedio.

En virtud de lo anterior, se puede definir que las funciones de la responsabilidad civil sean: resarcitoria, preventiva y distributiva, no operan de manera aislada, sino que se entrelazan y se complementan, proporcionando un marco completo y coherente que refleja la responsabilidad civil en su dimensión moderna.

1.2 Elementos estructurales de la responsabilidad civil

La responsabilidad civil no es un concepto abstracto, se configura a partir de elementos concretos que permiten determinar cuándo una conducta obliga a reparar un daño. La doctrina, tanto clásica como moderna, reconoce cuatro componentes esenciales: el hecho generador, el daño, el nexo causal y el factor de atribución.

El Tribunal Segundo Civil mediante la resolución 089-2010 del 17 de marzo de 2010, ha señalado que para que se dé la responsabilidad civil deben cumplirse con los cuatro requisitos:

> Cabe señalar, desde ahora, que la responsabilidad civil consta de cuatro elementos fundamentales:1- El hecho que la generaría; 2- El daño producido; 3- El nexo de causalidad entre el hecho y el daño; 4- El criterio jurídico de imputación del deber resarcitorio, a cargo de un sujeto distinto de quien fue lesionado en sus bienes jurídicos materiales o inmateriales. En la responsabilidad subjetiva, este criterio jurídico de imputación radica en el dolo o la culpa en el actuar del obligado; mientras que en la objetiva se prescinde del dolo o la culpa, para imputar legalmente el deber resarcitorio a sujetos vinculados al hecho generador del daño, por aspectos de justicia o equidad relevantes para el legislador, tales como el riesgo creado o el principio según el cual quien obtiene un lucro de una actividad debe asumir los daños que esta produce (aunque no sea un riesgo grave el generado por ella), entre otros. En cuanto a la carga de la prueba,

> en ambos tipos de responsabilidad quien reclama el resarcimiento debe demostrar el hecho generador, el daño producido y la necesaria vinculación causal entre ambos. En la responsabilidad subjetiva ha de demostrar, además, que el daño se produjo por dolo o culpa de quien es llamado a responder, pero en la objetiva no es necesario probar estos aspectos, bastando entonces con la prueba de los tres primeros elementos señalados. Eso sí, conforme a la doctrina más relevante en este campo, la parte demandada podría exonerarse de la responsabilidad objetiva si acredita que el daño es producto de fuerza mayor, caso fortuito o culpa de la víctima o de un tercero" (Tribunal Segundo Civil, Sección Segunda, resolución 089-2010, de las trece horas diez minutos del diecisiete de marzo de dos mil diez).

En virtud, se denota que cada uno cumple un rol específico en la estructura de la responsabilidad, y su análisis resulta clave para entender cómo se aplican los criterios de imputación.

1.2.1. Hecho generador.

El hecho generador es la acción u omisión de un sujeto, y dependiendo del análisis de atribución fáctica y jurídica, del cual se determinará si ocasionó un daño (Reglero Campos, 2006). Es decir, es aquel que constituye la conducta o situación de la que emana el daño, puede ser un acto positivo, como la realización de un fraude informático o de una omisión, como la falta de medidas de seguridad en la plataforma digital, de un banco que incumple un deber legal o contractual.

Para el objeto de esta investigación, en la banca digital, el hecho generador puede implicar tanto la acción de un tercero que ejecute el fraude como la omisión de la entidad bancaria que permite que la conducta perjudicial tenga efectos. Por ejemplo, un sistema de autenticación insuficiente, un monitoreo deficiente o alguna falla en el proceso de seguridad de la plataforma, que puede facilitar el daño al cliente. En este sentido, la responsabilidad civil, no solo analiza la conducta directa del sujeto causante, sino también las condiciones que la hicieron posible.

1.2.2. Daño.

Los sistemas abiertos, naturalmente, definen el daño de modo amplio a partir de la pérdida o la disminución que sufre la víctima en sus bienes u otros intereses no reñidos con la ley (Alessandri Rodríguez, 2005, p. 153).

Según, Henao (2015), el daño se conceptualiza como:

> El daño es toda afrenta a los intereses lícitos de una persona, trátese de derechos pecuniarios o de no pecuniarios, de derechos individuales o colectivos, que se presenta como lesión definitiva de un derecho o como alteración de su goce pacífico y que, gracias a la posibilidad de accionar judicialmente, es objeto de reparación si los otros requisitos de la responsabilidad –imputación y fundamento del deber de reparar- se encuentran reunidos. (pp. 280 - 285)

Por otro lado, para Díez Picazo (1999) la definición del daño conlleva una dificultada dado que debe ser abarcado de manera total para que pueda satisfacer los problemas, de forma que lo define como el menoscabo ocurrido en intereses patrimoniales o extrapatrimoniales.

En virtud de lo anterior, se puede identificar que el daño corresponde al perjuicio que sufre la víctima. Este daño puede ser patrimonial que implica la pérdida o detrimento económico que puede cuantificarse en términos pecuniarios, tal como el robo de fondos a través de la plataforma digital, y por otro lado, el extrapatrimonial que corresponde a aquellas afectaciones a bienes inmateriales, para ejemplo práctico de la investigación puede ser la reputación, tranquilidad o estrés generado por el fraude ocasionado.

De forma que la identificación y cuantificación del daño es esencial para la función resarcitoria de la responsabilidad civil, ya que sirve para determinar la magnitud o medidas preventivas necesarias.

1.2.3. Nexo Causal.

Implica que exista un vínculo directo entre la conducta del autor y el daño producido. Esta relación puede determinarse conforme a la teoría de la causalidad adecuada, es decir, que el hecho haya sido apto, según el curso normal de las cosas, para producir el daño (De Ángel Yagüez, 2001).

Patiño (2008), describe le nexo causal como:

> La relación necesaria y eficiente entre el hecho generador del daño y el daño probado. La jurisprudencia y la doctrina indican que para poder atribuir un resultado a una persona y declararla responsable como consecuencia de su acción u omisión, es indispensable definir si aquel aparece ligado a esta por una relación de causa-efecto. Si no es posible encontrar esa relación mencionada, no tendrá sentido alguno continuar el juicio de responsabilidad. (p.193)

Ahora bien, la teoría denominada *conditio sine qua non* o teoría de la equivalencia de las condiciones, atribuida a Von Buri, parte de la idea básica de que cuando ocurre un daño,

normalmente no existe una sola causa, sino varias condiciones que contribuyen al resultado, es decir, sostiene que toda condición sin la cual el resultado no se habría producido debe considerarse causa del daño (De Cuevillas, 2000).

Por otro lado, existe la teoría de la causalidad próxima, esta pretende identificar la causa temporal más cercana al daño, en otras palabras, se considera casusa aquella que esté más cerca en el tiempo (Yzquierdo, 2001).

También se desarrollaron las teorías de la causa preponderante y de la causa eficiente, vinculadas a Biding, Oertmann y Birkmeyer, que procuran determinar cuál antecedente contribuyó en mayor medida o con mayor eficacia al resultado (Bustamante, 2003).

No obstante, estas propuestas tampoco eliminan la dificultad central: ¿cómo medir esa "preponderancia" o esa "eficacia"? En escenarios donde confluyen múltiples factores como ocurre frecuentemente en entornos tecnológicos, la decisión termina dependiendo de valoraciones que el operador jurídico debe realizar, aun cuando se invoquen criterios aparentemente objetivos.

Por su parte, Von Kries, a quien se le asocia con la teoría de la causalidad adecuada, introdujo un enfoque probabilístico, sosteniendo que solo deben considerarse causas aquellas condiciones que, según el curso normal de los acontecimientos, eran idóneas para producir el daño (Díez Picazo, 1999).

Y recientemente la teoría de imputación objetiva, que señala que no basta con constatar una relación fáctica entre conducta y daño, sino que es necesario que el sujeto haya creado un riesgo jurídicamente desaprobado y que ese riesgo se haya materializado en el resultado (Díez-Picazo, 1999).

1.2.4. Factor de atribución.

El Factor de atribución se refiere a la manera en que el ordenamiento jurídico asigna la responsabilidad, lo que permite definir si la responsabilidad se fundamenta en la culpa, en el riesgo creado, en el incumplimiento de un deber de seguridad o en otro criterio normativo. Ahora bien, bajo una teoría clásica, la responsabilidad se ha relacionado con la culpa o el dolo. Sin embargo, la doctrina contemporánea ha abierto la puerta a la responsabilidad objetiva, donde no se requiere demostrar intención o negligencia, basta con que exista un riesgo reconocido socialmente y un vínculo claro entre el sujeto y el daño causado.

García de Enterría (2003) sostiene que "En tal caso, la imputación de responsabilidad, en cuanto fenómeno jurídico, se produce automáticamente una vez que se prueba la relación de

causalidad existente entre la actividad del sujeto productor del daño y el perjuicio producido" (p. 386).

Esta distinción es esencial, pues permite apartar la causalidad física, que se limita únicamente a establecer la conexión entre hecho y resultado, de la responsabilidad civil, que se centra en la asignación de obligaciones reparadoras a un patrimonio en específico.

Asimismo, se reconoce la diferencia entre causalidad fáctica que es la cuestión de hecho y la causalidad jurídica que se refiere a la cuestión jurídica, la primera recae sobre quien materialmente provocó el daño y la segunda, en cambio, reconoce a quien debe responder económicamente, ya sea directamente o como responsable subsidiario, como sucede en los casos de responsabilidad por el hecho ajeno. Este enfoque es particularmente relevante en escenarios complejos, como los fraudes a través de plataformas bancarias digitales, donde la acción directa de un tercero puede coexistir con fallas en los sistemas del banco o negligencia en los protocolos de seguridad, generando situaciones de concurrencia de responsabilidades.

Sumado a lo anterior, el análisis del factor de atribución no se completa sin considerar las causales exonerativas, que son las circunstancias normadas que anulan la culpabilidad o el nexo causal y que permiten confirmar o desvirtuar la responsabilidad asignada. Entre estas se encuentran la fuerza mayor, el caso fortuito, el hecho de un tercero y la conducta de la víctima. Estas causales funcionan como límites al alcance de la imputación, evitando que se traslade injustamente la obligación de reparación, y establecen criterios claros para determinar cuándo la persona o entidad identificada como responsable realmente debe asumir las consecuencias del daño.

1.3 Responsabilidad subjetiva y objetiva

La sentencia No. 002273F-S1-2023 de Sala Primera de la Corte Suprema de Justicia en Costa Rica, del 06 de diciembre de 2023, se ha pronunciado sobre estas dos vertientes:

> IV. Del régimen de responsabilidad aplicable al caso concreto. Sobre el particular esta Sala desde vieja data ha indicado, que mediante la responsabilidad civil se atribuye a un sujeto la obligación de reparar, indemnizar o compensar un daño infringido a la esfera jurídica de otro sujeto, como consecuencia de un acto o una actividad realizada por aquél. Esta responsabilidad se divide en subjetiva y objetiva, de acuerdo con el criterio de imputación que se utiliza en cada caso: en el primero, la voluntad del obligado, quien actúa en forma culpable; en el segundo, criterios objetivos tales como el riesgo, expresamente establecidos por la ley. Desde esa óptica, en la subjetiva, se requiere la concurrencia, y consecuente

demostración del daño, el dolo o culpa por parte del autor del hecho dañoso y la relación de causalidad entre la conducta que lo produce y el menoscabo, mientras la objetiva se caracteriza, en lo esencial, por prescindir de los elementos subjetivos de imputación, siendo suficiente –en tesis de principio- se demuestre el daño y la relación de causalidad para atribuir responsabilidad a los sujetos quienes objetivamente deben responder. También suele ser dividida en contractual y extracontractual, según provenga del incumplimiento de una obligación convenida libremente por las partes, o del incumplimiento del deber general de no causar daño a los demás.

La responsabilidad civil puede configurarse bajo dos enfoques: 1) Subjetiva 2) Objetiva. Estos determinan la manera en que se le aplica la obligación de reparar el daño. Debe tenerse en cuenta, que la primera se basa en la existencia de un elemento negligente o volitivo por parte de quien cause el daño, por otro lado, la segunda se basa en resultados y riesgos generados, independiente del dolo o culpa del sujeto. A partir de esta distinción, resulta pertinente analizar de manera individual las características y elementos de cada uno de estos regímenes de responsabilidad.

1.3.1 Responsabilidad subjetiva.

En este enfoque hay una atribución propia de responsabilidad por la conducta antijurídica imputable al sujeto que comete el daño, es decir, este actúa desde el dolo o la culpa. De forma que para que este tipo de responsabilidad se dé, se necesita que existan tres elementos, siendo: Culpabilidad, antijuridicidad y causalidad entre la conducta y el daño.

En este contexto, la responsabilidad subjetiva puede presentarse bajo dos modalidades, como lo es la responsabilidad directa por hecho propio, que se configura cuando la obligación de reparar el daño recae sobre quien realizó la conducta generadora del perjuicio y por otro lado, la responsabilidad indirecta por hecho ajeno, la cual surge cuando el deber de resarcimiento se atribuye a una persona distinta de quien ejecutó materialmente el hecho dañoso, en virtud de una relación jurídica que justifica dicha imputación.

Uno de los elementos que pueden fundamentar la responsabilidad subjetiva es el dolo. En términos generales, el dolo se entiende como la actuación consciente y voluntaria dirigida a producir un resultado dañoso o, al menos, realizada con conocimiento de que dicho resultado puede producirse como consecuencia de la conducta desplegada. En este sentido, el dolo implica

un grado elevado de reprochabilidad, ya que el agente actúa con intención o plena conciencia del daño que su comportamiento puede generar. (Tamayo Jaramillo, 2015)

Por otro lado, se encuentra la culpa que representa otro de los fundamentos clásicos de la responsabilidad subjetiva. La culpa no implica la intención de causar un daño, sino la realización de una conducta negligente, imprudente o carente de la diligencia que razonablemente se espera en determinadas situaciones. De forma que, la culpa se configura cuando el sujeto omite las precauciones necesarias o actúa de manera descuidada, generando con ello un perjuicio a otra persona. (De Ángel Yagüez, 1993)

Como lo señala Encinar (2000) "Si la responsabilidad civil subjetiva, aunque de forma muy tenue, manifiesta un reproche, habrá de exigírsele la culpabilidad, como consecuencia de la agencia moral del individuo, presupuesto éste absolutamente necesario para la imputación de la responsabilidad". Por lo cual, en el ámbito de la responsabilidad subjetiva, el daño se fundamenta en la valoración de la conducta del sujeto, de forma que solo resulta procedente cuando existe un grado de reproche atribuible al individuo.

Dentro del análisis de la imputación subjetiva, adquieren relevancia las figuras de la "culpa in vigilando" y la "culpa in eligendo". La culpa in vigilando se configura cuando un sujeto no ejerce una supervisión adecuada sobre quienes actúan bajo su dependencia o responsabilidad, permitiendo con su omisión la producción del daño. La culpa in eligendo, por su parte, se refiere a la falta de diligencia en la elección de las personas o mecanismos tecnológicos que colaboran o ejecutan actividades esenciales dentro de la estructura del obligado. (De Ángel Yagüez, 2001)

En el contexto de las plataformas digitales bancarias, estas formas de culpa pueden manifestarse, por ejemplo, en la contratación de proveedores tecnológicos inseguros *in eligendo* o en la falta de monitoreo efectivo de actividades sospechosas dentro del sistema informático del banco *in vigilando*. En ambos casos, la negligencia en el cumplimiento de estos deberes puede dar lugar a una imputación válida de responsabilidad civil por parte de la entidad bancaria, al no haber actuado con la diligencia esperada en su función de garante de la seguridad digital.

1.3.2 Responsabilidad objetiva.

Para este enfoque de responsabilidad el requisito de infracción se prescinde, de forma que no se solicita como criterio de imputación los elementos de dolo o culpa, sino que su fundamento reside en el principio de riesgo, que corresponde cuando el sujeto (persona o entidad) desarrolla

una actividad legal pero esencialmente peligrosa, de forma que debe responder por los daños que esta puede ocasionar a terceros.

Una de sus principales características radica en que se aplica a actividades plenamente legales, bajo dicho contexto, cualquier daño derivado de dichas actividades puede ser considerado indemnizable, incluso cuando el acto que lo provoca se encuentra dentro de los límites de la legalidad. Por otro lado, otra característica esencial de este enfoque es su simplicidad en cuanto a los requisitos para la imputación, ya que basta con que exista una relación de causalidad entre el hecho y el perjuicio, así como que se den las condiciones de imputación objetiva. En este sentido, se impone la obligación de reparar los daños que se generan como consecuencias de determinadas actividades. (Encinar, 2000)

Al respecto el jurista costarricense Pérez (1998), como se citó en CIJUL (2008) p.27, señaló:

> La responsabilidad objetiva se resume en una ventaja a favor del lesionado que significa una parcial inversión de la prueba, en el sentido de que ésta queda exonerado de la carga de probar la culpa (culpa o dolo) del causante del daño y vano sería el intento de éste de probar su falta de culpa.

En otro punto, los criterios doctrinales para establecer la imputación objetiva en este contexto comprenden elementos como:

- El riesgo general: Se reconoce como aquellas situaciones que, por su propia naturaleza, implican una posibilidad de causar daño, pero que la sociedad acepta como necesarias para el desarrollo de ciertas actividades, siempre que los beneficios superen los riesgos. Para que un riesgo sea socialmente aceptado se deben a dos condiciones: 1) Que la actividad genere un beneficio importante para la sociedad mientras el riesgo que conlleva sea reducido. 2) Que las personas que podrían resultar afectadas por ese riesgo residual no sean identificables de manera específica. (Arburola, 2010) De forma que la imputación solo procedería si el agente ha creado un peligro no cubierto por el riesgo permitido y este se materializa en un daño.
- La prohibición de regreso: Este criterio impide que, una vez comprobada la existencia del daño, el responsable se exonere alegando la eventual ausencia de conducta culposa. (Reglero, 2014, como se citó en Casal, 2016, p.126), señala sobre este criterio:

De acuerdo con el jurista español, Don Luis Fernando Reglero Campos, “en cuanto a la denominada prohibición de regreso (en alemán, “Regreβverbot”), por la que se impide retroceder

en la cadena causal desde que se verificó una intervención dolosa o gravemente negligente de un tercero, estamos ante la irrupción de un nuevo curso causal (una conducta humana) en el ya iniciado por la conducta del eventual responsable (o en el seno de su actividad), que da lugar a un resultado que con aquella conducta o esta actividad no se hubiera alcanzado o bien hubiera sido diferente al finalmente acaecido.

- El incremento del riesgo: El criterio del incremento del riesgo parte de la idea de que no todo daño que tenga una relación causal con una conducta puede atribuirse jurídicamente a quien la realizó. Para que exista imputación objetiva, es necesario que la actuación del agente haya creado o aumentado un riesgo que el ordenamiento jurídico considera no permitido, y que precisamente ese riesgo sea el que se materializa en el resultado dañoso.

En este sentido, el daño solo puede imputarse cuando la conducta del agente genera una situación de peligro o agrava un riesgo existente, y ese peligro termina concretándose en el resultado que se pretende reparar. Sin embargo, incluso si el riesgo se materializa, la imputación puede excluirse cuando la norma que fundamenta la responsabilidad no tenía como finalidad evitar ese tipo específico de resultado, lo que exige analizar también el ámbito de protección de la norma.

- La adecuación de la conducta: También se le conoce como teoría de la causalidad adecuada, básicamente se refiere a que un hecho es causal cuando es favorable para producir una violación del bien jurídico. De forma que permite analizar si un resultado dañoso puede atribuirse a un agente, no solo por la existencia de un nexo causal, sino considerando si su conducta era social y jurídicamente aceptable dentro de las circunstancias del caso.

- La eventual provocación: Es criterio se aplica para determinar cuándo un daño puede atribuirse a un agente considerando la intervención o conducta del propio afectado. Este criterio surge para atender situaciones donde la víctima o un tercero contribuye, de manera indirecta, a la concreción del daño, ya sea por su reacción ante un riesgo o por la forma en que enfrenta la situación creada por el agente. Se puede analizar bajo dos escenarios:

    i. Casos de provocación o desafío: Aquí la víctima participa de manera activa en un evento de riesgo. En estas circunstancias, el resultado lesivo puede ser parcialmente atribuido a la conducta de la víctima, porque su acción interviene en la cadena causal iniciada por el agente, modificando la forma en que se produce el daño.

ii. Casos de auxilio necesario: En este tipo de situaciones, la persona afectada asume un riesgo, frente a un peligro generado culpablemente por el agente. Aunque el daño se materialice durante el intento de auxilio, la imputación al agente original se mantiene, aunque se reconoce que la acción de la víctima contribuyó al desenlace.

De manera que este criterio busca matizar la imputación objetiva, evaluando no solo la conducta del agente, sino también la interacción de la víctima con el riesgo creado. Permite diferenciar cuándo la acción del agente es la causa principal del daño y cuándo la conducta de la víctima o de un tercero influyó significativamente en el resultado final, evitando atribuciones automáticas que no reflejarían adecuadamente la dinámica de los hechos.

De esta manera, tales elementos contribuyen a fundamentar la atribución de responsabilidad cuando el daño se materializa como consecuencia de un riesgo jurídicamente relevante asociado a la actividad desarrollada, lo que en determinados supuestos permite prescindir de la demostración directa de culpa y centrar el análisis en la creación o gestión del riesgo.

Por su parte Torrealba (2011) señala que "se considera que quién obtiene beneficios de una actividad lícita pero riesgosa, debe asumir por su propia cuenta los daños que dicha actividad provoque en perjuicio de terceros" (p. 106).

De forma que la responsabilidad objetiva se distingue de la responsabilidad subjetiva porque no requiere evaluar la intención o culpa del agente, sino que se centra en el riesgo generado por la actividad realizada. En este sentido, el factor principal para atribuir responsabilidad es la existencia de un riesgo que pueda producir un daño a terceros. Así, la imputación no depende de la conducta negligente o dolosa del sujeto, sino de la relación causal entre el riesgo creado y el perjuicio efectivamente causado.

Resulta fundamental definir con precisión qué se entiende por riesgo y determinar cuándo el riesgo creado por una conducta es suficiente para generar responsabilidad. No todo riesgo conduce automáticamente a la imputación de responsabilidad: debe ser un riesgo jurídicamente relevante, vinculado de manera directa con la actividad realizada y con el daño producido. De esta manera, la responsabilidad objetiva se configura como un mecanismo preventivo y reparador, asegurando que quienes desarrollan actividades potencialmente peligrosas asuman los efectos de los daños que puedan derivarse de las mismas. (Acosta, 2014)

Sobre lo anterior, Cubides (2012), señala “la responsabilidad derivada del riesgo no depende del dolo o la culpa del agente, sino que se origina en la mera ocurrencia del daño consecuente de la actividad peligrosa” (p.270).

Referente a la responsabilidad objetiva, concretamente de las entidades bancarias con respecto al criterio de imputación, Jiménez (2025) señala que,

> El riesgo creado por la actividad bancaria, sin necesidad de probar culpa o negligencia. Este criterio se basa en el hecho de que las entidades financieras, al realizar actividades peligrosas por la naturaleza de los servicios electrónicos, deben asumir los riesgos inherentes a esas actividades (p. 134).

De forma que el riesgo inherente a la actividad bancaria puede constituir un criterio relevante para la imputación de responsabilidad en el marco de la responsabilidad civil objetiva.

1.4 Responsabilidad contractual y extracontractual

La responsabilidad civil se configura como un mecanismo para garantizar la reparación de los daños ocasionados a terceros, ya sea que deriven del incumplimiento de obligaciones contractuales o de actos ilícitos extracontractuales. La distinción entre ambos tipos de responsabilidad radica principalmente en la existencia o no de un vínculo jurídico previo, en los elementos necesarios para la imputación y en la carga de la prueba exigida para la procedencia de la indemnización.

1.4.1 Responsabilidad contractual.

La responsabilidad contractual se configura cuando existe previamente una obligación jurídica específica a cargo de una persona determinada, cuyo incumplimiento ocasiona un daño a quien es titular del derecho correlativo. Es decir, se da cuando proviene el incumplimiento de una obligación convenida libremente por las partes.

Asimismo, esta forma de responsabilidad no se limita únicamente a las obligaciones derivadas de un contrato, sino que puede originarse en cualquier otra fuente de obligaciones reconocida por el ordenamiento jurídico, siempre que la conducta exigida pueda ser reclamada de manera coercitiva por el titular del derecho frente al obligado.

En Costa Rica, el fundamento legal de la responsabilidad contractual se deriva del Código Civil:

> ARTÍCULO 702.- El deudor que falte al cumplimiento de su obligación, sea en la sustancia, sea en el modo, será responsable por el mismo hecho de los daños y perjuicios

> que ocasione a su acreedor, a no ser que la falta provenga de hecho de éste, fuerza mayor o caso fortuito (Código Civil,1885, art. 702).

Bajo lo anterior, se identifica entonces que, en caso de incumplir una obligación se debe reparar el daño. En estos casos, el perjudicado no es quien tiene la obligación de demostrar que el incumplimiento se originó de una conducta culposa, sino que basta con acreditar la existencia del incumplimiento, el daño que se deriva de este y la relación de causalidad entre ambos para que surja la obligación de reparar.

No obstante, se puede intentar desvirtuar dicha relación causal demostrando la concurrencia de circunstancias que excluyan su responsabilidad, tales como el hecho de la víctima, la intervención de un tercero, el caso fortuito o la fuerza mayor.

Ahora bien, en las obligaciones de medios, en las que no se garantiza un resultado específico sino la realización de una actividad diligente, resulta necesario acreditar que el sujeto actuó con culpa o negligencia, lo cual implica demostrar que no desplegó el nivel de diligencia que razonablemente se esperaba para intentar alcanzar el resultado previsto. En cambio, en las obligaciones de resultado basta con comprobar que la prestación pactada no se cumplió, generando un daño al acreedor, para configurar la responsabilidad.

Por otro lado, además de las obligaciones principales derivadas del contrato, la doctrina reconoce la existencia de deberes accesorios, que obligan a la parte contratante a actuar conforme a los principios de buena fe y diligencia.

Al respecto Cerutti (2015), analizó este concepto relacionado a la obligación de seguridad e indicó:

> Con cita de Mazeaud -Tunc y Honorat, como: "Obligación de restituir al otro contratante, o sus bienes, sanos y salvos a la expiración del contrato", o "la obligación accesoria, en virtud de la cual el deudor debe, además de la prestación principal prevista en el contrato, velar que no recaiga ningún daño a la persona o eventualmente a los bienes de su cocontratante". Entiende que la obligación de seguridad es un típico deber de garantía, que se presenta en los supuestos específicos, y de un modo análogo a aquellas situaciones en las que una obligación suplementaria acompaña a la principal. Señala que "Ese deber de garantía se manifiesta en la protección de la persona del cocontratante, es decir que es un deber de protección, integrando esa categoría que se denomina como deberes accesorios que acompañan al cumplimiento" y que "En realidad, esta obligación no resulta sino una

especie de la más general que impone la relación contractual, en el sentido de que cada parte tiene —debe— que salvaguardar en su integridad la esfera de intereses propia de la otra parte.

Bajo el contexto bancario, este deber se traduce en la obligación de garantizar la seguridad de los fondos y de las operaciones electrónicas, implementando sistemas de protección, autenticación y monitoreo de transacciones. La omisión en estas medidas puede constituir un incumplimiento contractual, incluso cuando no exista dolo o culpa directa, especialmente en contratos de prestación de servicios financieros digitales.

1.4.2 Responsabilidad extracontractual.

La responsabilidad extracontractual se configura cuando una persona violenta la esfera jurídica de otra sin que haya entre ellas una relación jurídica o si existiendo ésta no tiene nada que ver con la actuación que produjo el daño. Es decir, que no es necesario que exista un vínculo previo o relación existente, sino que alude al deber general que prohíbe lesionar la esfera jurídica de otro.

Por su parte la Sala Primera de la Corte Suprema de Justicia en Costa Rica, mediante la sentencia No. 00589 – 1999 del 01 de octubre de 1999, ha indicado:

> Por su parte, la responsabilidad extracontractual recae sobre quien, fuera de toda relación contractual previa, ha causado un daño en la esfera jurídica de otro sujeto, por culpa, o a través de la puesta en marcha de una actividad riesgosa o creación de un riesgo social. Esta responsabilidad no nace del incumplimiento de un vínculo determinado, sino de la violación del deber general de no dañar a los otros. Su régimen está basado en los artículos 1045, 1046, 1047 y 1048 del Código Civil. El primero de ellos dispone que: "Todo aquel que por dolo, falta, negligencia o imprudencia causa a otro un daño, está obligado a repararlo junto con los perjuicios".- Principio que es fundamento de toda responsabilidad civil." (Resolución número 320 de las 14:20 Hrs. del 9 de noviembre de 1990). Tocante a la carga de la prueba, en materia de responsabilidad civil extracontractual, esta Sala ha indicado: "VII.- Una de las diferencias fundamentales entre la responsabilidad civil contractual y extracontractual, radica en la carga de la prueba, pues en la responsabilidad derivada de un contrato el acreedor no está obligado a demostrar la culpa del deudor, ya que ésta se presume en tanto el segundo no demuestre que su incumplimiento o el atraso no le son imputables, como el caso fortuito o la fuerza mayor; en cambio, en la responsabilidad extracontractual o

> aquiliana le compete al damnificado demostrar la culpabilidad del autor del acto ilícito. Así el artículo 317, inciso 1), del Código Procesal Civil, dispone que a quien formule una pretensión le incumbe la carga de la prueba respecto de los hechos constitutivos de su derecho. Por otra parte, uno de los elementos configurantes de la responsabilidad extracontractual subjetiva, lo constituye la relación de causalidad directa o eficiente que debe existir entre el comportamiento o conducta antijurídica y el daño, siendo este último el presupuesto de cualquier tipo de responsabilidad extracontractual por lo que su demostración también constituye un requisito sine quo non para que prospere la pretensión resarcitoria...". (Sentencia número 17 de las 15 Hrs. del 29 de enero de 1992)

Tal como se puede observar, esta responsabilidad se fundamenta en la violación del deber general de no causar perjuicios a otros, ya sea por culpa, dolo o por el riesgo creado por determinadas actividades. En el ámbito bancario, las actividades de prestación de servicios digitales generan riesgos inherentes, de manera que la falta de medidas de seguridad que ocasionen un perjuicio a los usuarios podría dar lugar a responsabilidad extracontractual, incluso frente a quienes no mantienen una relación contractual directa con la entidad financiera.

En la responsabilidad extracontractual corresponde al afectado demostrar la conducta antijurídica, el daño y la relación causal. Según lo establecido por la jurisprudencia costarricense, la responsabilidad puede surgir tanto por culpa o dolo, como por la creación de un riesgo especial derivado de actividades peligrosas o socialmente relevantes, caso en el cual se analiza la imputación objetiva.

2. Teorías Contemporáneas de Imputación

2.1 Teoría del riesgo creado

La teoría del riesgo creado surge frente a las limitaciones del modelo clásico de responsabilidad basado exclusivamente en la culpa. Su desarrollo suele atribuirse a los juristas franceses Raymond Saleilles y Louis Josserand, quienes plantearon que la responsabilidad no debía depender únicamente de demostrar una conducta culposa, sino también del hecho de haber generado un riesgo que pudiera afectar a otros. Desde esta perspectiva, quien desarrolla una actividad que introduce un peligro en la esfera social debe asumir las consecuencias de los daños que eventualmente se produzcan como resultado de ese riesgo, aun cuando no se logre acreditar una falta o negligencia en su comportamiento. (Hernández, 2018)

Raymond Saleilles (1897), sustenta esta teoría de la siguiente manera "El que crea una fuente de daño, así el que explota una fábrica, debe reparación si los riesgos se concretan. El exclusivo hecho del perjuicio compromete su responsabilidad; en la contrapartida de los beneficios que obtiene de la empresa" (p.87).

El voto número 655 de las 15 horas 05 minutos del 19 de setiembre de 2007, emitido por la Sala Primera de la Corte Suprema de Justicia, dispuso:

> "(…) Esta concepción, surge porque el modelo de la culpa era insuficiente para dar respuesta a la multiplicación de los peligros y daños propios de la vida moderna. La teoría del riesgo, entendida en el sentido de que, quien ejerce o se aprovecha de una actividad con elementos potencialmente peligrosos para los demás, debe también soportar sus inconvenientes, vino a cambiar la mayor parte de las legislaciones. También se le denomina teoría del daño creado, cuyo paradigma de imputación radica en atribuir el daño a todo el que introduce en la sociedad un elemento virtual de producirlo, debiendo prescindirse de la subjetividad del agente, y centrarse en el problema de la reparación y sus límites en torno de la causalidad material. Solo interesa indagar cual hecho fue la causa del efecto para imputarlo, dado que es suficiente la producción del resultado dañoso, siendo innecesaria la configuración de un acto ilícito a través de los elementos tradicionales. Como corolario de lo expuesto, la culpa, negligencia, imprudencia o impericia del agente, no son los elementos esenciales para dar nacimiento a la obligación dentro de los parámetros de la responsabilidad objetiva. De allí que, no tiene ninguna importancia, para desvirtuarla, que se logre demostrar que no incurrió en alguno de ellos. En este mismo sentido, puede verse la sentencia no. 61 de las 14 horas 50 minutos del 19 de junio de 1997, de esta Sala. Por tal razón, la noción de riesgo sustituye los conceptos de culpa y antijuricidad, prescindiéndose como criterios de imputación. Se enfoca en una conducta o actividad de un sujeto físico o jurídico, caracterizada por la puesta en marcha de una prestación peligrosa, o la mera tenencia de un objeto de peligro. Por ende, el elemento a considerar es el riesgo creado. Sobre el tema en particular, puede consultarse la sentencia no. 376 de las 14 horas 40 minutos del 9 de julio de 1999, de este órgano colegiado. Debe agregarse, que se parte del supuesto de que el origen de las obligaciones es el uso lícito de cosas peligrosas, y que al provocar daño, exigen al que se sirve de ellas, a resarcirlo. Para la configuración de este tipo de responsabilidad deben darse los siguientes componentes: a) el empleo de cosas que

> conlleven peligro o riesgo; b) causar un daño; y c) la relación o nexo de causa efecto entre el hecho y el daño. Finalmente, es importante mencionar que, dentro de esta temática, opera una parcial inversión de la prueba, en el sentido de que el lesionado queda exonerado de la carga de probar la culpa o dolo de quien provocó el daño. En consecuencia, le atañe a la persona física o jurídica a quien se le atribuye la responsabilidad, demostrar que los daños se produjeron por fuerza mayor o por culpa de la víctima. Doctrina que informan los numerales 35 párrafo segundo de la Ley No.7472 y el 1048 párrafo quinto del Código Civil." (Igualmente, puede verse la resolución No. 646-F-2001 de las 16 horas 45 minutos del 22 de agosto de 2001, de la Sala Primera de la Corte Suprema de Justicia).

En este sentido, el fundamento de esta teoría se apoya en la idea de una justicia distributiva, ya que si un sujeto obtiene algún tipo de beneficio mediante una actividad que implica riesgos para terceros, resulta razonable que soporte las consecuencias cuando ese riesgo se materializa en un daño.

De ahí a que la doctrina haya distinguido dos aproximaciones dentro de esta concepción, tal como lo señala Hernandez (2018):

> De ahí las dos vertientes de la teoría del riesgo: la del riesgo provecho que exige del hombre un provecho pecuniario; y la del Riesgo Creado que exige un provecho cualquiera aunque no sea pecuniario. Conforme a la Teoría del Riesgo el juez no tiene que examinar la conducta del autor del daño ni el carácter licito del acto imputable al pretendido responsable. Esta teoría ha sido calificada con justicia como Teoría Objetiva. (p. 29)

Bajo este marco, el análisis de la responsabilidad se desplaza desde la valoración subjetiva de la conducta del agente hacia la identificación del riesgo generado por la actividad que desarrolla. Así, el juez no necesita concentrarse en determinar si el autor actuó con culpa o si su conducta fue ilícita en sentido estricto, sino en establecer si el daño guarda relación con el riesgo introducido por dicha actividad. Este enfoque, por tanto, se vincula con una concepción objetiva de la responsabilidad.

Respecto a la teoría del riesgo o el daño creado, el Tribunal Contencioso Administrativo Sección IV en fecha 03 de noviembre de 2014, mediante la resolución No.94-2014, señala:

> Para la tutela efectiva de estos derechos, el legislador adoptó un sistema de responsabilidad objetiva, con el claro interés de evitar que por dificultades probatorias prácticamente insalvables puedan quedar desamparadas las víctimas de las actividades empresariales de

fabricación y comercio, actividades per se generadoras de riesgos para la integridad física o el patrimonio ajenos: “ 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. Solo se libera quien demuestra que ha sido ajeno al daño. Los representantes legales de los establecimientos mercantiles o, en su caso, lo 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”. (Artículo 32, Ley No. 7472 citada). VII.- La responsabilidad objetiva, ha dicho esta Sala: “ Es el resultado de una revisión del instituto de la responsabilidad que vino a ser necesaria cuando se tomó conciencia que el molde de la culpa era estrecho para contener las aspiraciones de justicia que clamaban en un mundo cada vez más complejo. Exigencias de la realidad, la multiplicación de los peligros y daños propios de la vida moderna, justificaron que en determinadas situaciones la responsabilidad fuese tratada como un crédito de la víctima que el demandado debía desvirtuar. La teoría del riesgo, según la cual quien ejerce o se aprovecha de una actividad con elementos potencialmente peligrosos para los demás, debe también soportar sus inconveniencias, permeó la mayor parte de las legislaciones y en el caso de Costa Rica origina el párrafo V de comentario. Esta teoría es también denominada del daño creado, cuyo paradigma de imputación, según lo refiere el Profesor Nombre 40083, "...estriba en atribuir el daño a todo el que introduce en la sociedad un elemento virtual de producirlo...ella, agrega, "...prescinde de la subjetividad del agente, y centra el problema de la reparación y sus límites en torno de la causalidad material, investigando tan solo cual hecho fue, materialmente, causa del efecto, para atribuírselo sin más. Le basta la producción del resultado dañoso, no exige la configuración de un acto ilícito a través de los elementos tradicionales...". (Nombre40083, Nombre40084. Responsabilidad Civil, Abeledo Perrot, III Edic., Buenos Aires, 1987, p. 106)

La teoría del riesgo se distingue por permitir una identificación más amplia de los sujetos que pueden resultar responsables por un daño. En este enfoque, no solo se considera al autor material que ejecuta el hecho dañino, sino también a aquellas personas que se encuentran

vinculadas con la actividad generadora del riesgo y que, directa o indirectamente, obtienen algún beneficio de su desarrollo. En consecuencia, la responsabilidad puede extenderse a quienes participan en la creación, control o aprovechamiento de la fuente de peligro.

Desde una perspectiva procesal, esta concepción modifica el punto de partida del análisis de la responsabilidad. En lugar de centrarse exclusivamente en determinar quién fue el autor físico del daño, el examen se dirige a establecer qué sujetos participaron en la generación del riesgo que finalmente se materializó en el perjuicio. De esta manera, el eje de la imputación se traslada desde la conducta individual hacia la estructura de la actividad que introduce el riesgo en la sociedad.

Bajo este modelo, la responsabilidad no se determina preguntando únicamente quién ejecutó el acto que produjo el daño, sino quién o quiénes crearon, controlaron o se beneficiaron del riesgo que permitió su materialización.

Dentro de la evolución doctrinal surgió también el concepto de riesgo profesional, desarrollado inicialmente en el ámbito de los accidentes laborales. Esta teoría sostiene que los daños sufridos por los trabajadores en el ejercicio de sus funciones no deben atribuirse exclusivamente a la culpa del empleador, sino al riesgo inherente a la actividad productiva organizada por la empresa.

A su vez, dentro de la evolución doctrinal, surge el riesgo profesional, el cual se fundamenta en la idea de que quien organiza una actividad económica y obtiene beneficios de ella debe asumir también los riesgos que dicha actividad genera para quienes participan en su desarrollo. En consecuencia, los accidentes de trabajo comenzaron a ser considerados como una manifestación normal del funcionamiento de la empresa, lo que justificó la adopción de sistemas de responsabilidad objetiva y de seguridad social para garantizar la reparación de los daños. (García, 2004)

Aunque esta figura surgió en el ámbito laboral, su lógica ha influido profundamente en el desarrollo de la responsabilidad civil moderna, extendiéndose a otros sectores en los que determinadas actividades generan riesgos estructurales para terceros, como el transporte, la industria, los servicios públicos y las actividades financieras.

Sobre la teoría del riesgo profesional Padilla, Rueda y Zafra (2014), sugieren que,

> La teoría del riesgo profesional, la cual consiste en una modalidad de la teoría del riesgo provecho, que pone especial atención en la responsabilidad por accidentes de trabajo. Se diferencia de esta, y de ahí su autonomía, pues no solo se requiere un beneficio económico,

sino que es además necesaria la existencia de una actividad calificada como especializada o técnica, es decir, se tiene en cuenta el concepto de profesionalismo. (p. 134)

Otro ámbito relevante de aplicación de la teoría del riesgo creado es el de las actividades peligrosas, entendidas como aquellas que, por su naturaleza o por los medios empleados para su ejecución, implican una probabilidad significativa de causar daños a terceros.

La doctrina ha señalado que el carácter peligroso de una actividad no depende necesariamente de la existencia de una conducta ilícita, sino de la potencialidad dañosa inherente a la actividad misma. En consecuencia, quien desarrolla una actividad que introduce un factor de riesgo en la sociedad debe responder por los daños que se produzcan como consecuencia de su realización.

En el contexto actual, las actividades que utilizan tecnologías digitales también pueden generar riesgos significativos para los usuarios. El funcionamiento de plataformas electrónicas de pago, sistemas de banca en línea o aplicaciones financieras implica el manejo de información sensible, transacciones económicas y sistemas informáticos susceptibles de ataques o manipulaciones fraudulentas. Por ello, cuando se materializan daños derivados de estos riesgos, tal como ocurre en los casos de estafas informáticas, surge el debate jurídico sobre la responsabilidad de las entidades que administran dichas plataformas.

Un elemento central de la teoría del riesgo creado es la distribución del riesgo dentro de la sociedad. La finalidad de este enfoque no es únicamente identificar al responsable del daño, sino asignar los costos derivados de las actividades riesgosas a quien se encuentra en mejores condiciones de prevenirlos o asumirlos.

Desde esta perspectiva, la responsabilidad objetiva cumple una función preventiva y distributiva. Preventiva, porque incentiva a quienes desarrollan actividades riesgosas a adoptar medidas de seguridad más rigurosas; y distributiva, porque evita que el peso del daño recaiga exclusivamente sobre la víctima.

En el ámbito financiero y tecnológico, este criterio adquiere especial relevancia, ya que, las entidades bancarias poseen el control de las plataformas digitales, diseñan los sistemas de seguridad, administran la infraestructura informática y obtienen beneficios económicos de la prestación de estos servicios.

2.2 Teoría del deber de seguridad

La teoría del deber de seguridad constituye una de las construcciones doctrinales más relevantes dentro de la evolución contemporánea de la responsabilidad civil. Su desarrollo responde a la necesidad de garantizar una mayor protección a las personas frente a los riesgos derivados de determinadas relaciones jurídicas, particularmente aquellas en las que una de las partes se encuentra en posición de organizar o controlar una actividad que puede generar daños a terceros.

En términos generales, el deber de seguridad se refiere a la obligación que tiene una persona, en virtud de una relación jurídica previa o del ejercicio de una actividad determinada, de adoptar las medidas necesarias para evitar que se produzcan daños a quienes participan en dicha relación o se encuentran dentro del ámbito de riesgo de la actividad. De esta manera, el ordenamiento jurídico impone al sujeto responsable no solo el cumplimiento de la prestación principal del contrato o de la actividad desarrollada, sino también la obligación adicional de preservar la integridad física, patrimonial o moral de quienes puedan verse afectados por ella.

Tal como se desarrolla en CIJUL (2010):

> Uno de los principales derechos o bienes jurídicos tutelados por el legislador, al promulgar la Ley LPCDEC, ha sido la seguridad y la salud de los consumidores. Para ello, las soluciones que brindaba el derecho tradicional eran insuficientes, pues como se ha establecido y la jurisprudencia nacional lo ha confirmado, la culpa como factor de atribución resulta en muchos de los casos indemostrable.
>
> A tal efecto, este deber de seguridad implica una responsabilidad de los elaboradores y de todos aquellos que se encuentren en una posición de demanda o sean los causantes de tales actividades lícitas pero riesgosas, y por ende, asuman las consecuencias de éstas; en otras palabras, la responsabilidad del fabricante o productor tiene carácter objetivo, solo podrá eximirse de dicha responsabilidad cuando demuestre ser ajeno a la causa productora del daño. (p.6)

Desde la perspectiva doctrinal, el deber de seguridad suele ser entendido como una obligación accesoria o implícita dentro de determinadas relaciones jurídicas. En efecto, la doctrina ha señalado que esta obligación surge cuando, además de la prestación principal del contrato, existe el deber de garantizar que la ejecución de dicha prestación no genere daños a la otra parte o a terceros. En este sentido, se ha definido la obligación de seguridad como aquella en virtud de la

cual el deudor debe velar por que durante la ejecución del contrato no se produzcan daños a la persona o a los bienes del cocontratante.

Bajo esta concepción, el vínculo jurídico entre las partes no se limita únicamente al cumplimiento de la prestación pactada, sino que incorpora también un deber de protección que busca evitar la producción de daños durante el desarrollo de la actividad o del servicio prestado.

Ahora bien, uno de los principales debates doctrinales en torno al deber de seguridad se refiere a su naturaleza jurídica. En términos generales, la doctrina ha identificado dos grandes corrientes interpretativas.

La primera de ellas sostiene que el deber de seguridad tiene naturaleza contractual, al considerarlo como una obligación accesoria que se integra de manera implícita dentro del contenido de determinados contratos. Bajo esta concepción, el incumplimiento del deber de seguridad constituye una forma de incumplimiento contractual que puede generar responsabilidad civil por los daños ocasionados.

Por otra parte, una segunda posición doctrinal considera que el deber de seguridad puede operar también en el ámbito extracontractual, especialmente cuando los riesgos derivados de una actividad afectan a personas que no se encuentran vinculadas mediante un contrato con el sujeto responsable. En estos casos, la obligación de seguridad surge de la aplicación del principio general *alterum non laedere*, referente a no dañar a otro, lo que permite exigir la reparación de los daños ocasionados cuando se demuestra que el sujeto responsable no adoptó las medidas necesarias para prevenirlos.

En este sentido, Goldenberg (1984) sostiene que el deber de seguridad puede manifestarse tanto en el ámbito contractual como en el extracontractual, dependiendo de la naturaleza de la relación jurídica existente entre las partes y de las circunstancias en las que se produce el daño.

Asimismo, es necesario diferenciar la obligación de seguridad, entendida como una manifestación específica, del deber general de seguridad o previsibilidad que le sirve de fundamento. Este último se vincula con el principio jurídico tradicional de no causar daño a otros *alterum non laedere*, el cual establece el deber básico de evitar perjudicar a terceros.

De forma que esta teoría reconoce su génesis en el deber genérico de no dañar tanto de forma contractual como extracontractual. Al respecto (Wayar, 1986, como se citó en Alferillo, 1999), señala “el deber de seguridad es un principio jurídico superior. Tiene la misma jerarquía

que el deber general de no dañar (neminen laedere) y su observancia es obligatoria e inexcusable para todo aquel que aprovecha el trabajo ajeno…".

Es por ello, que en entornos donde la actividad desplegada implica el uso de tecnologías complejas, el deber de seguridad exige un nivel de diligencia superior al que se observa en actividades ordinarias. Este estándar intensificado responde a la naturaleza del servicio, al grado de exposición al riesgo y a la posición de control que posee quien organiza la actividad.

En virtud de lo anterior y bajo el contexto de esta investigación, la Sala Primera en la Resolución 135-2022 emitida el 15 de febrero de 2011, sostuvo que,

> A la fecha de los hechos el Banco contaba con una serie de medidas con el propósito de minimizar los riesgos de la Internet. Sin embargo, para este Órgano Colegiado, también es cierto que, dicho medio continuaba siendo riesgoso. Según lo señaló el Tribunal, era responsabilidad del demandado dotar a dicho sistema de la seguridad idónea, con el propósito de garantizar que las transacciones eran efectuadas por su usuario y no por personas ajenas que tuvieran a disposición datos sensibles del cliente. Es claro, en materia de seguridad bancaria en medios electrónicos los esfuerzos deben ser continuos y acordes con los más altos estándares. En ese sentido, luego de analizada la prueba aportada, se tiene que la seguridad con que dispone el Banco resulta adecuada solo para proteger la integridad de la base de datos y la plataforma transaccional a lo interno. Pero, no debe dejarse de lado que teniendo en cuenta que su función esencial es la intermediación financiera, que incluye la captación de capitales provenientes del público, lleva implícita su custodia, tanto desde el punto de vista físico, como del registro electrónico correspondiente. No cabe duda que está obligada a garantizar la seguridad de las operaciones realizadas, ya sea en ventanilla o en cualquier otro medio puesto a disposición de los clientes, la cual debe abarcar, necesariamente, el uso de todos aquellos mecanismos a su disposición que le permitan contar con un mayor grado de certeza en cuanto a la identificación de las personas que están facultadas para realizar transacciones electrónicas desde las cuentas, -como el uso del teclado virtual y el token, no implementados al momento de los hechos que dieron lugar a esta demanda.

Este pronunciamiento establece que la obligación de seguridad no se agota en medidas mínimas, sino que requiere un nivel de protección tecnológica acorde con el riesgo asociado al servicio. La referencia a "los más altos estándares" representa una manifestación del estándar

profesional agravado, dado que implica que la entidad debe implementar medidas de seguridad alineadas con las prácticas recomendadas en el sector, incluyendo sistemas de autenticación confiables y mecanismos de prevención y supervisión continuos.

Se puede entender que los bancos, al ofrecer servicios digitales, adquieren una obligación de resultado respecto a la seguridad informática, en tanto que el cliente deposita su confianza en la plataforma para realizar operaciones financieras (SUGEF, 2021). La falta de medidas adecuadas que permitan prevenir o mitigar los fraudes puede constituir una vulneración del deber de garantía, dando lugar a la responsabilidad civil. (González, 2022)

De forma que, en el ámbito de los servicios financieros digitales, la responsabilidad civil trasciende la reparación de daños patrimoniales e incluye un deber de custodia tecnológica. Esto implica que la entidad responsable de administrar sistemas electrónicos de pago o plataformas de banca en línea debe implementar mecanismos de seguridad destinados a minimizar el riesgo de fraudes y accesos no autorizados.

2.3 Teoría del nexo causal y ruptura por culpa de la víctima

2.3.1 Teoría del nexo causal.

La teoría del nexo causal tiene sus raíces principalmente en el derecho penal alemán del Siglo XIX, estar teoría establece que para que una conducta pueda considerarse causa de un resultado punible, debe existir un vínculo directo y efectivo entre la acción u omisión del sujeto y el resultado producido. En otras palabras: no basta con que alguien haya realizado un acto; es necesario que dicho acto haya sido determinante en la producción del daño o resultado ilícito.

De la misma forma, la teoría del nexo causal constituye un pilar esencial en la imputación de responsabilidad civil, tanto en su modalidad contractual como extracontractual. Su importancia radica en que es el fundamento de toda atribución de efectos jurídicos a una conducta, pues no puede imputarse jurídicamente un resultado dañoso a un sujeto sin que previamente se haya demostrado que su conducta fue causalmente determinante para la producción de ese resultado.

Se entiende que el nexo causal es uno de los requisitos constitutivos de la responsabilidad civil, la cual se refiere al vínculo que debe darse entre la violación del bien jurídico o el daño con la conducta activa u omisiva efectuada.

La teoría del nexo causal, en la doctrina alemana, se abarca desde dos perspectivas, la primera que corresponde a causalidad que da origen a la obligación de responder *(haftungsbegründende Kausalität)* se analiza principalmente en el contexto del supuesto de hecho

de la responsabilidad civil extracontractual. Por otro lado, la causalidad que determina la extensión de la obligación de indemnizar *(haftungsausfüllende Kausalität)* se centra más en el ámbito de las consecuencias jurídicas, es decir, en la eficacia reparadora del daño causado a los derechos del afectado. (López, 2019)

Por su parte Bonasi Benucci, se refiere a que el nexo causal no simboliza un solo problema para el derecho, dado que se trata de un problema metajurídico, dado que la existencia de una relación causal suele establecerse mediante la observación empírica, es decir, cuando la experiencia demuestra que a un determinado hecho antecedente suele seguirle una consecuencia específica. Sin embargo, este criterio se basa en probabilidades, puesto que no permite explicar completamente los casos de causalidad atípica, donde un hecho produce efectos que no son los comúnmente esperados. Además, resulta complejo diferenciar con precisión entre probabilidad y generalidad. (Bonasi 2019)

Asimismo, (Carnelutti, 1915, como se citó en Bonasi, 2019), indica que "la probabilidad es la limitada medida en que la causalidad puede ser captada por la inteligencia humana" (p.81).

Históricamente, el estudio de la causalidad ha evolucionado desde enfoques puramente empíricos hacia modelos que incorporan criterios normativos. Las teorías clásicas —como la equivalencia de las condiciones o conditio sine qua non— buscaban identificar si un hecho constituía una condición necesaria para la producción del daño. No obstante, la complejidad de los eventos dañosos evidenció la necesidad de integrar criterios jurídicos adicionales que permitieran delimitar qué causas resultan relevantes para efectos de imputación, dando lugar a desarrollos como la teoría de la causa adecuada y la imputación objetiva.

En virtud de ello, se procede a ampliar dichas teorías:

i) La equivalencia de las condiciones *"conditio sine qua non"*: De fines del Siglo XIX fue atribuida al alemán Von Buri, y se refiere a que un hecho puede ser considerado causa de otro que ocurre posteriormente cuando, de no haberse producido el primero, el segundo tampoco habría tenido lugar. Desde esta perspectiva, la relación causal se determina mediante un análisis hipotético: si al suprimir mentalmente el hecho antecedente el daño deja de producirse, entonces dicho antecedente puede ser reconocido como causa del resultado. (De Cuevillas Marozzi, 2000) Bajo este criterio, todos los hechos previos que hayan contribuido de esa manera a la producción del daño adquieren relevancia causal. Por ello, cuando existen varios antecedentes que cumplen

con esa condición, no resulta sencillo privilegiar uno sobre los demás ni excluirlos, ya que la ausencia de cualquiera de ellos habría impedido la ocurrencia del perjuicio.

No obstante, esta forma de entender la causalidad ha sido objeto de críticas. Se ha señalado que tiende a ampliar de manera excesiva el concepto de causa, pues puede llevar a incluir una cadena indefinida de antecedentes, abarcando incluso las causas de las causas. En la práctica, esto provoca que también se consideren dentro de la causalidad elementos que, más que verdaderas causas del daño, funcionan únicamente como condiciones que hicieron posible su aparición. (Bonasi 2019)

ii) La causa próxima: Es teoría surge como un intento de poner límites al análisis de la cadena causal dentro del derecho de daños. Su planteamiento parte de la idea de que no todos los antecedentes que preceden a un daño deben considerarse jurídicamente relevantes, pues si se aceptara cada uno de ellos como causa, la explicación causal podría extenderse indefinidamente hasta abarcar las llamadas "causas de las causas". Para evitar esa expansión ilimitada, esta postura sostiene que debe atenderse únicamente al antecedente que se encuentre más cercano al resultado lesivo.

Este enfoque se vincula con las reflexiones atribuidas a Francis Bacon jurista francés del siglo XVI, quien propuso identificar el hecho que, desde el punto de vista temporal, se ubica inmediatamente antes del daño y que, por tanto, puede considerarse su causa directa o inmediata. Bajo esta lógica, las causas más remotas quedarían desplazadas por la proximidad de aquella que precede de manera más inmediata al resultado.

Sin embargo, esta teoría también ha sido objeto de críticas. La cercanía temporal entre un hecho y el daño no siempre garantiza que dicho hecho sea el verdadero responsable de su producción. En muchos casos, el acontecimiento más próximo puede ser simplemente el efecto de otros factores anteriores que, aunque más lejanos en el tiempo, explican de manera más adecuada el origen del daño. Por esta razón, se ha señalado que limitar el análisis únicamente a la causa inmediata puede conducir a conclusiones incompletas o incluso equivocadas sobre la verdadera relación causal. (Bonasi, 2019)

iii) La causa adecuada: Tiene sus bases en la doctrina alemana y francesa, específicamente bajo las ideas del fisiólogo alemán Ohannes Von Kries. Esta teoría solo reconoce relevancia a aquellos hechos que, según un criterio de probabilidad o regularidad, podrían razonablemente generar el resultado dañino en un determinado período de tiempo.

Bajo este enfoque, la probabilidad se entiende como la frecuencia con que se observa la relación entre dos tipos de eventos, en algunos casos, esta relación se da de manera necesaria, como ocurre con las leyes naturales, mientras que en otros solo puede determinarse a partir de un análisis estadístico (Díez-Picazo, 2000).

En consecuencia, para establecer si un hecho constituye la causa de un daño, es necesario evaluar si existe una relación suficiente entre ese antecedente y el perjuicio producido, considerando la regularidad con la que un evento conduce a otro. Solo los hechos que cumplan este criterio de probabilidad pueden ser imputados como causales, mientras que aquellos cuya influencia sobre el daño es meramente circunstancial o excepcional quedan excluidos de la atribución de responsabilidad.

iv) Teoría de la imputación objetiva: En el ámbito del derecho penal, se desarrolló la teoría de la imputación objetiva, cuya finalidad es delimitar cuándo un resultado puede atribuírsele a una persona. Siguiendo las ideas de Roxin y Jakobs, se plantea que un hecho solo puede imputarse a alguien si esa persona ha generado un peligro concreto sobre un bien jurídico que no estaba protegido por un riesgo permitido, y si dicho peligro efectivamente se materializa en el resultado.

Jakobs complementa esta perspectiva mediante varios criterios que permiten precisar los límites de la imputación: el riesgo permitido, que delimita los peligros aceptables; el principio de confianza, que protege la expectativa de comportamiento normal de terceros; la prohibición de regreso, que evita atribuir consecuencias a conductas que se interrumpen por hechos posteriores ajenos; y la competencia de la víctima, que considera situaciones en las que la víctima contribuye de manera significativa al resultado. En conjunto, estos principios ayudan a determinar con mayor precisión cuándo un evento puede ser jurídicamente imputado a un sujeto determinado. (Díez-Picazo, 2000)

2.3.2 Ruptura por culpa de la víctima.

Dentro del análisis de la teoría del nexo causal, la figura de la ruptura por culpa de la víctima adquiere especial relevancia para delimitar los alcances de la imputación de un daño. Esta doctrina reconoce que, aunque exista una conducta originaria que genere un riesgo o contribuya a la producción del resultado lesivo, la intervención de la propia víctima puede modificar o incluso extinguir la relación causal. De forma que se complementa las teorías de la causa adecuada y de la imputación objetiva, pues permite integrar criterios normativos para evaluar si un resultado dañoso

puede atribuirse jurídicamente al agente o si, por el contrario, la acción de la víctima rompe la cadena causal previamente establecida.

En términos operativos, la culpa exclusiva de la víctima ocurre cuando su comportamiento descuidado, imprudente o contrario a normas de cuidado previsibles se convierte en la causa determinante del daño, desplazando la imputación del autor inicial. Es decir, se configura cuando el daño resulta únicamente de un comportamiento negligente o imprudente de la propia víctima, eximiendo al agente causante de la obligación de resarcirlo. (Escobar, 2000) Este principio reconoce que, aunque exista una conducta inicial que genere riesgo, la intervención de la víctima puede modificar la cadena causal hasta el punto de que el autor original no sea responsable.

Al respecto, la Sala Primera de la Corte Suprema de Justicia, ha analizado este término, señalando en la resolución 002606-F-S1-2020 emitida a las quince horas veintidós minutos del doce de noviembre de dos mil veinte:

> 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. Al entenderlo de esa forma los Juzgadores de instancia, estima esta Cámara que la valoración probatoria y la aplicación normativa efectuada en el fallo impugnado resultan conforme a derecho, ergo, los reparos endilgados deberán ser rechazados. *(lo resaltado no pertenece al original)*

De forma que se puede observar como la Sala Primera de la Corte Suprema de Justicia, aborda el tema de que cuando el daño se produce como consecuencia exclusiva de la imprudencia o falta de diligencia de la víctima, se configura un elemento de ruptura del nexo causal que exime al agente de responsabilidad civil.

Por otro lado, la culpa concurrente ocurre cuando tanto el agente como la víctima participan con un grado de imprudencia que contribuye al resultado dañoso. En estos casos, la determinación de la responsabilidad depende de la intensidad relativa de las culpas y del deber de diligencia de cada parte (Montero, 1999).

La intervención de terceros constituye otra forma de ruptura del nexo causal. Cuando un tercero actúa de manera exclusiva y produce el daño, la responsabilidad civil se desplaza hacia este último, considerándose el hecho como un caso fortuito o de fuerza mayor respecto del agente inicial, salvo que exista participación culposa de este último (Abeliuk, 2001).

Finalmente, la previsibilidad del daño es un criterio clave para evaluar la imputación de responsabilidad, ya que, un hecho se considera imputable cuando el resultado era previsible y podía haberse evitado mediante la debida diligencia; en contraste, eventos imprevisibles o irresistibles excluyen la responsabilidad, consolidando el límite jurídico de la imputación en función de la capacidad de control del agente sobre el resultado. (Escobar, 2000)

De esta forma y bajo el contexto de estafas informáticas a través de plataformas bancarias, la teoría del nexo causal y las figuras de culpa y previsibilidad permiten analizar si la entrega voluntaria de claves por parte del cliente rompe la cadena causal y exime a la entidad bancaria de responsabilidad civil, o si su deber de seguridad digital limita esta exoneración.

2.4. Carga de la prueba en responsabilidad civil

El principio general que rige la distribución de la carga de la prueba se expresa en el aforismo latino affirmanti incumbit probatio, según el cual corresponde probar a quien afirma un hecho en el que funda su pretensión. Este principio constituye la regla tradicional del derecho procesal civil y responde a la lógica según la cual la parte que invoca una situación jurídica determinada debe aportar los medios probatorios que permitan acreditarla ante el órgano jurisdiccional.

Desde la perspectiva doctrinal, la carga de la prueba se concibe como una regla de juicio dirigida al juez, destinada a resolver los casos en los que los hechos relevantes no han sido suficientemente acreditados durante el proceso. En tal sentido, no se trata de una obligación jurídica en sentido estricto, sino de una regla procesal que establece cuál de las partes asume el riesgo de que un hecho permanezca incierto. (Taruffo, 2008) De esta forma, la carga probatoria se vincula estrechamente con el principio dispositivo que rige el proceso civil, en virtud del cual son las partes quienes deben aportar los hechos y los medios de prueba necesarios para sustentar sus pretensiones.

Al respecto el Tribunal Segundo Civil Sección Extraordinaria mediante la Resolución No. 00783 – 2017 del veintisiete de noviembre de dos mil diecisiete, señala:

> Antes de entrar a analizar las inconformidades de la apelante, es menester recordar que los hechos que conforman la causa de pedir y la resistencia de la parte demandada, solamente precisan de prueba cuando resultan ser controvertidos. Por ello, el numeral 317 del Código Procesal Civil establece que la carga de la prueba incumbe a quien formula una pretensión, respecto a las afirmaciones de los hechos constitutivos de su derecho y a quien se oponga a una pretensión, en cuanto a las afirmaciones de hechos impeditivos, modificativos o extintivos del derecho del actor. Sobre el tema, la Sección Segunda de este Tribunal ha indicado que: "IV) Al establecer una demanda judicial, las partes se encuentran obligadas, bajo el principio de la carga probatoria, a brindarle al juez todos los elementos de prueba que tengan a mano para demostrar los hechos que se alegan como fundamento de su demanda o de su defensa. En este sentido, es importante recordar que la labor del Juez se parece mucho a la de un historiador, que reconstruye los hechos con base en las huellas que éstos han dejado".

De lo anterior, se puede observar como a nivel de Tribunales se identifica este principio bajo el cual se demuestra la obligación procesal de demostrar un hecho. Ahora bien, en Costa Rica, dada la reforma del Código Procesal Civil, la carga de la prueba se regula a la luz del artículo 41, la cual dispone:

> ARTÍCULO 41.- Disposiciones generales sobre prueba
>
> 41.1 Carga de la prueba. Incumbe la carga de la prueba:
>
> 1. A quien formule una pretensión, respecto de los hechos constitutivos de su derecho.
>
> 2. A quien se oponga a una pretensión, en cuanto a los hechos impeditivos, modificativos o extintivos del derecho del actor.
>
> Para la aplicación de lo dispuesto en los incisos anteriores de este artículo, se deberá tener presente la disponibilidad y facilidad probatoria que corresponde a cada una de las partes, de acuerdo con la naturaleza de lo debatido.
>
> Las normas precedentes se aplicarán siempre que una disposición legal expresa no distribuya con criterios especiales la carga de la prueba. (Código Procesal Civil, Ley 9342, 2016, artículo 41)

Como puede observarse la normativa señala que quien exige el cumplimiento de una obligación debe demostrar su existencia; mientras que la segunda parte del artículo establece que quien afirma estar exento de ella debe justificar la razón que lo libera de dicha obligación, de forma

que conforme el principio incumbit probatio, quien alega y quien se defiende debe aportar la prueba.

Ahora bien, para los juristas, ha sido un desafío encontrar una regla general y universal que establezca cómo se distribuye la carga de la prueba de acuerdo con el principio de justicia distributiva y el principio de igualdad. La dificultad de diseñar esta norma radica en que la prueba puede resultar extremadamente difícil o inaccesible, lo cual plantea la pregunta de qué sentido tiene establecer derechos y facultades si, al momento de hacerlos valer en los tribunales, probar su existencia es casi imposible. (Ormazabal, 2017)

Con el propósito de superar las limitaciones derivadas de la aplicación estricta del principio tradicional, la doctrina y la jurisprudencia han desarrollado mecanismos de redistribución de la carga de la prueba, entre los cuales destaca la denominada inversión de la carga probatoria.

La inversión de la carga de la prueba implica que, en determinadas circunstancias, corresponde al demandado demostrar que su conducta fue diligente o que el daño no le es imputable, en lugar de exigir al demandante que pruebe completamente la culpa o negligencia del responsable. Este fenómeno se justifica principalmente cuando existe una asimetría de información entre las partes, es decir, cuando una de ellas dispone de mayores posibilidades técnicas o documentales para acreditar los hechos discutidos en el proceso.

En este sentido, la doctrina ha desarrollado el concepto de cargas probatorias dinámicas, según el cual la carga de la prueba debe recaer en la parte que se encuentra en mejores condiciones de aportar los elementos probatorios necesarios para esclarecer los hechos. Como señala Peyrano (2004), la distribución dinámica de la carga de la prueba busca evitar decisiones injustas derivadas de la imposibilidad material de una de las partes para acreditar determinados hechos.

En la responsabilidad objetiva, la imputación recae sobre quien genera el riesgo; por lo tanto, solo podrá liberarse de dicha responsabilidad si logra demostrar la existencia de alguna causa eximente aplicable al caso. Pérez (1994) señala que,

> La responsabilidad objetiva se resume en una ventaja a favor del lesionado, que significa una parcial inversión de la carga de la prueba, en el sentido de que éste queda exonerado de la carga de probar la culpa (culpa o dolo) del causante del daño y vano sería el intento de probar su falta de culpa, a diferencia de lo que ocurre en los supuestos de responsabilidad subjetiva (p.417).

Ahora bien, este criterio resulta particularmente relevante en el ámbito de los servicios bancarios digitales, donde las entidades financieras poseen el control de los sistemas informáticos, los registros de transacciones, los protocolos de seguridad y la información técnica necesaria para determinar cómo se produjo una operación fraudulenta. En tales casos, exigir al usuario afectado que pruebe de manera directa la falla del sistema o la negligencia del banco puede resultar excesivamente gravoso o incluso imposible.

En la misma línea, el Tribunal Contencioso Administrativo Sección IV mediante la resolución No. 00054 – 2012 del veintiocho de mayo del dos mil doce, indica:

> Precisamente, producto de este criterio que proviene del artículo 35 tantas veces aludido, la reiterada jurisprudencia de la Sala Primera de la Corte Suprema (de cual se hace cita en considerandos posteriores) ha definido que, desde el punto de vista procesal, le corresponde al demandado probar que es ajeno a la producción del daño que la parte actora alega haber sufrido como consecuencia de la utilización de los servicios riesgosos. De acuerdo con la Sala Primera de la Corte Suprema de Justicia, este mecanismo se sustenta en el principio de que la carga probatoria corresponde a la parte que se encuentre en mejores condiciones para aportar la prueba al proceso. (…) El numeral 35 de la Ley 7472 ya citado establece que en relaciones de consumo de ésta naturaleza la carga de la prueba se traslada a quien tenga mejor posición en la relación, en este caso la parte débil lo es el usuario, por lo que le corresponde dicha carga probatoria a la institución bancaria, y con la traída al proceso, no ha lograrlo acreditar la ajenidad del daño, pues a quedado expuesto claramente las omisiones en que ha incurrido el banco en protección de las cuentas bancarias y dineros de sus usuarios.

Uno de los aspectos centrales en la imputación de responsabilidad civil a las entidades bancarias en relación con las estafas informáticas es la prueba del incumplimiento del deber de seguridad. Este deber constituye una obligación jurídica que recae sobre los proveedores de servicios financieros y tecnológicos, consistente en adoptar medidas razonables para proteger a los usuarios frente a riesgos previsibles derivados del uso de plataformas digitales.

Desde la perspectiva doctrinal, el deber de seguridad se entiende como una obligación de protección que exige al proveedor garantizar que los servicios ofrecidos no generen daños injustificados a los usuarios. En el ámbito contractual, esta obligación puede considerarse una

manifestación del principio de buena fe y de la obligación de diligencia que debe observar el prestador del servicio. (Díez-Picazo, 2011)

Sobre este punto se trae a colación lo señalado por el Tribunal Contencioso Administrativo Sección IV mediante la resolución No. 00054 – 2012 del veintiocho de mayo del dos mil doce, donde manifiesta:

> Le corresponde dicha carga probatoria a la institución bancaria, y con la traída al proceso, no ha lograrlo acreditar la ajenidad del daño, pues a quedado expuesto claramente las omisiones en que ha incurrido el banco en protección de las cuentas bancarias y dineros de sus usuarios. Se alega por el banco el eximente de responsabilidad de la culpa de la víctima, pero no hizo llegar al proceso elementos de los cuales se pueda extraer que la señora Nombre3516 proporcionó su información bancaria a terceros, máxime que no era costumbre de la actora realizar transferencias por esos montos, y alterar los límites diario de transferencias en su cuenta, lo que efectivamente revela un comportamiento anormal de esa cuenta, lo cual pudo haberse prevenido si el banco contara con medidas tecnológicas para detener movimientos no comunes dentro de las cuentas bancarias de acuerdo al perfil de su cliente, lo cual se enmarca dentro de su obligación de tener a disposición de su cliente, toda la sofisticación requerida en la suficiencia informática actualizada de orden preventivo en materia de seguridad por medio de la detección y alarma de movimientos ajenos a la normalidad en la relación Banco-Cliente, ya que se trata de elementos propios integrantes de la ciencia y técnica de la ingeniería informática, que el Banco accionado puedo haber tenido a disposición y utilización dentro de sus sistemas para evitar el daño acaecido.

En este sentido, el deber de seguridad se traduce en la implementación de medidas tecnológicas destinadas a prevenir accesos no autorizados, fraudes electrónicos o manipulación de datos. Entre estas medidas pueden incluirse sistemas de autenticación multifactor, protocolos de cifrado, monitoreo de transacciones sospechosas, alertas de seguridad y mecanismos de verificación de identidad.

Ahora bien, la acreditación del incumplimiento de este deber dentro de un proceso judicial suele realizarse mediante diversos mecanismos probatorios, tales como:

- Registros de transacciones electrónicas.
- Informes periciales informáticos.
- Auditorías de seguridad de los sistemas bancarios.

- Protocolos internos de prevención de fraude.
- Comunicaciones entre el banco y el usuario afectado.
- Reportes de incidentes de seguridad.

En muchos casos, la prueba directa del incumplimiento resulta compleja para el usuario afectado, ya que la información relevante se encuentra bajo el control de la entidad bancaria. Por ello, la jurisprudencia ha reconocido que la ocurrencia de un fraude informático dentro de la plataforma digital puede constituir un indicio relevante de una posible falla en el sistema de seguridad, lo que justifica exigir a la entidad financiera que demuestre la adecuación de sus mecanismos de protección.

Al respecto, el Tribunal Contencioso Administrativo, en la sentencia no 743-08 de las 14:10 horas del 26 de setiembre del 2008, señala lo siguiente:

> Es importante señalar que en este tipo de responsabilidad no se puede imputar la carga probatoria a la parte más débil, en este caso al actor. De hacerse así, sería negar la posibilidad de que esta parte pueda ser efectivamente reparada. De tal suerte, que se ha utilizado el criterio tradicional de inversión de la carga de la prueba. Sin embargo, la Sala I recientemente ha adoptado otra posición, argumentando que en realidad lo que se tiene que hacer es hacer una justa dimensión del artículo 317 del Código Procesal Civil y establecer que en realidad tiene que probar quien está en mayores posibilidades de hacerlo porque la prueba está a su disposición. Hace entonces la Sala I una correcta interpretación del artículo 317 del Código Procesal Civil, argumentando que la carga de la prueba se traslada a quien con motivo de su situación procesal se haya en mejores condiciones para acercar las probanzas al proceso. Lo anterior, se puede corroborar en la sentencia de la Sala I número 212-FS12008.

De tal modo que la carga de la prueba se encuentra estrechamente vinculada con los mecanismos de acreditación de la responsabilidad civil, ya que la distribución de la carga probatoria determina qué tipo de pruebas deben aportarse en el proceso para demostrar la existencia del daño, el incumplimiento del deber de seguridad y la relación causal entre ambos elementos. En los casos de estafas informáticas realizadas a través de plataformas bancarias, la acreditación de la responsabilidad requiere generalmente el análisis técnico de los sistemas informáticos utilizados por la entidad financiera, así como la evaluación de las medidas de seguridad implementadas para prevenir fraudes electrónicos.

2.4.1 In dubio pro consumptore con relación a la carga de la prueba.

En materia de consumo, el principio In dubio pro consumptore favorece la protección del usuario, especialmente en escenarios de asimetría informativa y técnica, como es el caso de los servicios bancarios digitales (De la Vega, 2019). Este principio se refleja en la carga dinámica de la prueba, mecanismo procesal que permite flexibilizar la distribución probatoria en favor del consumidor, quien, por su parte, suele tener menor acceso a la evidencia técnica necesaria para demostrar la responsabilidad del banco.

Al respecto la Sala Constitucional de la Corte Suprema de Justicia mediante la resolución No.202101158, emitida el veinte de enero de dos mil veintiuno, señala:

> Igualmente, en lo referente a los derechos de los consumidores y usuarios, este Tribunal Constitucional, adoptando como marco de referencia el último párrafo del artículo 46 de la Constitución Política, ha perfilado un nuevo principio, "in dubio pro consumptore", a favor de consumidores y usuarios toda vez que los considera la parte más débil de la cadena productiva, requiriendo por ello de una especial protección del Estado frente a los productores y proveedores. En ese sentido, se ha señalado que principios de orden público social justifican el amplio desarrollo que se promueve en torno a la protección de los derechos de los consumidores, disponiéndose además que "...es notorio que el consumidor se encuentra en el extremo de la cadena formada por la producción, distribución y comercialización de los bienes de consumo que requiere adquirir para su satisfacción personal, y su participación en ese proceso, no responde a razones técnicas ni profesionales, sino en la celebración constante de contratos a título personal. Por ello la relación en esa secuencia comercial es de inferioridad y requiere de una especial protección frente a los proveedores de los bienes y servicios, a los efectos de que previo a externar su consentimiento contractual cuente con todos los elementos de juicio necesarios, que le permitan expresarlo con toda libertad y ello implica el conocimiento cabal de los bienes y servicios ofrecidos. Van incluidos por los expresados, en una mezcla armónica, varios principios constitucionales, como la preocupación estatal a favor de los más amplios sectores de la población cuando actúan como consumidores, la reafirmación de la libertad individual al facilitar a los particulares la libre disposición del patrimonio con el concurso del mayor posible conocimiento del bien o servicio a adquirir, la protección de la salud cuando esté involucrada, el ordenamiento y la sistematización de las relaciones recíprocas

entre los interesados, la homologación de las prácticas comerciales internacionales al sistema interno y en fin, la mayor protección del funcionamiento del habitante en los medios de subsistencia" (ver sentencia número 1441-92 de las 13 horas 45 minutos del 2 de junio de l992 y número 4463-96 de las 9 horas 45 minutos del 30 de agosto de 1996). -ver también No. 2022006669 del veinticinco de marzo de dos mil veintidós-

Como se desprende la Sala Constitucional, desarrolla este principio refiriéndose a que la carga de la prueba corresponde a quien esté en las mejores condiciones.

En casos de fraude digital, esta carga dinámica implica que la entidad bancaria debe demostrar que cumplió con los estándares de seguridad y que no existió negligencia en la protección de sus sistemas, lo que puede traducirse en una inversión de la carga probatoria en favor del usuario afectado (Salas Peña, 2010). Este enfoque contribuye a equilibrar la relación jurídica y facilita el acceso efectivo a la reparación para las víctimas de estafas informáticas

3. Responsabilidad Civil en el Ámbito Bancario

3.1 Naturaleza jurídica de las entidades bancarias privadas

El análisis de la responsabilidad civil de las entidades bancarias privadas frente a las estafas informáticas realizadas mediante plataformas digitales exige comprender previamente la naturaleza jurídica de estas instituciones dentro del sistema financiero.

Las entidades bancarias no constituyen simples intermediarios comerciales, sino que son organizaciones especializadas que desempeñan una función esencial dentro de la economía moderna, caracterizada por la administración de recursos ajenos, la intermediación financiera y la prestación de servicios altamente tecnificados.

De acuerdo con la Ley Orgánica del Sistema Bancario Nacional, el sistema bancario costarricense se encuentra integrado por:

Artículo 1- El Sistema Bancario Nacional estará integrado por:

1) El Banco Central de Costa Rica.

2) El Banco Nacional de Costa Rica.

3) El Banco de Costa Rica.

4) (Derogado por el artículo 1 de la Ley de Disolución del Banco Anglo Costarricense N.º 7471, de 20 de diciembre de 1994).

5) (Derogado por el artículo 13 de la Ley No. 9605, de 12 de setiembre de 2018, Fusión por absorción del Banco Crédito Agrícola de Cartago y el Banco de Costa Rica).

6) Cualquier otro banco del Estado que en el futuro llegara a crearse.

7) Los bancos comerciales privados, establecidos y administrados conforme con lo prescrito en el título VI de esta ley.

8) La sucursal bancaria domiciliada en Costa Rica de un banco extranjero.

El Sistema se regirá por la presente ley, la Ley Orgánica del Banco Central de Costa Rica y las demás leyes aplicables, así como por los respectivos reglamentos. (Ley 1644, 1953, art. 1) *(Lo resaltado no pertenece al original)*

Bajo lo anterior, las entidades bancarias privadas desarrollan una actividad económica vinculada a la intermediación financiera. Esta actividad comprende la captación de recursos del público y su posterior colocación mediante operaciones crediticias u otros instrumentos financieros. El ejercicio de estas funciones implica la utilización de conocimientos técnicos, infraestructura tecnológica y el cumplimiento de marcos regulatorios específicos que rigen el funcionamiento del sistema financiero.

En el ámbito jurídico, la doctrina ha señalado que las actividades profesionales especializadas generan un deber de diligencia reforzado, ya que quienes las ejercen poseen conocimientos técnicos superiores respecto de los usuarios o consumidores de los servicios ofrecidos. Es por ello, que cuando una actividad se realiza de forma profesional y organizada, el nivel de diligencia exigible al prestador del servicio se eleva, pues se presume que este dispone de los conocimientos y medios necesarios para evitar la producción de daños. (Díez Picazo,1999).

En este sentido, la Sala Primera de la Corte Suprema de Justicia, mediante la resolución No. 0000233-F-S1-2017 del nueve de marzo de dos mil diecisiete, y hace referencia que la actividad financiera concretamente la bancaria por su naturaleza debe fortalecer sus sistemas:

> Sin duda la actividad financiera, más concretamente la bancaria, produce un elevado nivel de riesgo, el cual se incrementa por la internet, que impone al Banco el fortalecimiento de los dispositivos de seguridad en todos los niveles, tanto en relación a las actividades realizadas por sus funcionarios o contratistas, como en lo pertinente a los medios que sus clientes se ven compelidos a usar para acceder y recibir el servicio ofrecido, el cual, además, se desarrolla, establece, implementa y promociona por el ente bancario también para su beneficio. Así las cosas, no solo ha de responder por la fortaleza de sus sistemas internos, sino también por la seguridad de quienes al accesarlos se valen de los únicos canales que la propia institución reconoce y admite como riesgosos.

Asimismo, la Ley Orgánica del Sistema Bancario Nacional, a la luz del artículo 3) inciso 3) señala que es una función esencial de la entidad bancaria custodiar y administrar los depósitos bancarios de la colectividad, aclarando que para entidades bancarias privadas se debe cumplir ciertos requisitos.

De forma que se desprende, que otro elemento de la naturaleza jurídica de las entidades bancarias privadas es la existencia de deberes fiduciarios derivados de la administración de recursos de terceros, ya que entre la relación banco – cliente existe un alto grado de confianza, lo que implica que la entidad financiera debe actuar con lealtad, transparencia y diligencia en la gestión de los intereses de sus usuarios.

En este sentido y desde la perspectiva de la responsabilidad civil, el deber fiduciario se traduce en la obligación de proteger los intereses patrimoniales del cliente y prevenir riesgos previsibles asociados al servicio prestado. En concordancia y desde la perspectiva de la responsabilidad civil, cuando una relación contractual se basa en un grado particular de confianza, se espera que quien presta el servicio actúe con una diligencia mayor a la común. Esto se debe a que la otra parte coloca en él la salvaguarda de sus intereses, confiando en su actuación profesional y en el cuidado con el que desempeñe sus funciones.

Finalmente, la naturaleza jurídica de las entidades bancarias también implica la aplicación de un estándar técnico elevado en el desarrollo y operación de sus sistemas financieros y ahora con la era digital, los sistemas tecnológicos. Este estándar deriva de la complejidad de las operaciones bancarias y del impacto que estas tienen en la estabilidad económica y en la protección del patrimonio de los clientes.

3.1.2 Banca electrónica.

El desarrollo tecnológico ha influido de manera significativa en la evolución de los servicios financieros, particularmente en la forma en que las entidades bancarias realizan operaciones con sus clientes. En este contexto surge la denominada banca electrónica, la cual permite la realización de operaciones financieras mediante sistemas informáticos y redes de comunicación sin que sea necesaria la presencia física del cliente en una sucursal bancaria.

Desde una perspectiva conceptual, la banca electrónica puede entenderse como un sistema que permite la comunicación e interacción entre el cliente y la entidad bancaria mediante la transmisión de datos a través de medios electrónicos. Este modelo facilita la ejecución de diversas operaciones financieras, tales como transferencias de fondos, consultas de saldo, pagos

electrónicos y otras gestiones relacionadas con la administración de cuentas bancarias. Dichas operaciones se realizan mediante plataformas tecnológicas que procesan información financiera y permiten la interacción remota entre las partes. (Sala Peña, 2010)

Al respecto, Sergio Rodríguez Azuero, señala:

> Se utiliza la expresión "electrónica" pues ha sido la más extendida en el lenguaje del sector. En estricto rigor, sin embargo, esta nueva banca se soporta en los importantes desarrollos de la electrónica, incluidos los microcircuitos, con su capacidad lógica de proceso y de almacenamiento de información; pero así mismo, en el desarrollo de las comunicaciones que ha permitido construir distintos tipos de redes, y para ellos diferentes protocolos; y desde luego, el desarrollo de la informática, como tal, pues los programas o aplicativos han obtenido niveles que contribuyen con los dos factores anteriores a la transformación global. (p.197)

De forma tal que en un sentido más amplio, la banca electrónica también comprende el conjunto de procesos de automatización aplicados al funcionamiento interno de las entidades bancarias. Esto incluye el uso de sistemas informáticos destinados al procesamiento de datos, la gestión de transacciones financieras y la interconexión con otras instituciones del sistema financiero. Por esta razón, la banca electrónica se vincula con los procesos de informatización y modernización de las operaciones bancarias.

La utilización de medios electrónicos en la prestación de servicios financieros ha permitido ampliar el acceso a las operaciones bancarias y modificar los mecanismos tradicionales de interacción entre las entidades financieras y los usuarios. No obstante, la incorporación de tecnologías digitales también ha sido asociada con la aparición de nuevas modalidades de fraude que utilizan medios informáticos para realizar operaciones financieras no autorizadas.

Estas conductas pueden manifestarse mediante diversas formas de manipulación tecnológica o engaño dirigido a los usuarios, las cuales serán abarcadas más adelante. Sin embargo, la ocurrencia de este tipo de conductas ha generado la necesidad de implementar mecanismos tecnológicos destinados a la protección de las operaciones realizadas mediante plataformas digitales.

Lo que ha llevado a que las entidades bancarias utilicen distintos mecanismos de seguridad informática orientados a la protección de los sistemas que permiten la realización de operaciones

electrónicas. La implementación de estos mecanismos forma parte del funcionamiento de los sistemas utilizados en la prestación de servicios bancarios digitales.

Bajo este marco, el estudio de la banca electrónica permite comprender el entorno tecnológico en el que se desarrollan las operaciones financieras mediante plataformas digitales, así como los elementos que pueden considerarse al analizar la posible responsabilidad civil de las entidades financieras en casos relacionados con estafas informáticas.

3.2 Derecho del consumidor financiero

Antes de abordar el derecho del consumidor financiero, es menester delimitar el concepto de "consumidor", el cual se encuentra definido en la Ley No.7472 denominada "Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor". Dicha normativa estable que "Toda persona física o entidad de hecho o de derecho, que, como destinatario final, adquiere, disfruta o utiliza los bienes o los servicios, o bien, recibe información o propuestas para ello. También se considera consumidor al pequeño industrial o al artesano -en los términos definidos en el Reglamento de esta Ley- que adquiera productos terminados o insumos para integrarlos en los procesos para producir, transformar, comercializar o prestar servicios a terceros". (Ley No.7472, 1994, art.2)

Asimismo, la jurisprudencia constitucional ha desarrollado el alcance del derecho del consumidor dentro del ordenamiento jurídico costarricense. En este sentido, la Sala Constitucional de la Corte Suprema de Justicia de Costa Rica, mediante la resolución No. 2006-017747 del 11 de diciembre de 2006, señaló que el derecho del consumidor se encuentra conformado por un conjunto de normas, principios e instituciones orientadas a garantizar una posición de equilibrio entre los consumidores y los demás agentes económicos que participan en el mercado.

En dicha resolución se destaca que el fundamento constitucional de esta protección se encuentra en el artículo 46 de la Constitución Política de Costa Rica, el cual reconoce el derecho de los consumidores y usuarios a la protección de sus intereses económicos y al acceso a información adecuada y veraz sobre los bienes y servicios ofrecidos en el mercado. Asimismo, la disposición constitucional establece que el Estado debe apoyar las organizaciones destinadas a la defensa de los derechos de los consumidores.

De esta forma, el derecho del consumidor se configura como un conjunto de mecanismos jurídicos orientados a equilibrar la relación entre proveedores y consumidores dentro del mercado, particularmente en aquellos ámbitos donde pueden existir asimetrías de información o de poder

económico entre las partes. Esta protección resulta especialmente relevante en el ámbito de los servicios financieros, en el cual los usuarios de servicios bancarios participan en relaciones contractuales con entidades que cuentan con mayor capacidad técnica y organizativa en la prestación de dichos servicios.

Ahora bien, el consumidor financiero puede entenderse desde múltiples dimensiones. En el ámbito cotidiano, es la persona que utiliza los servicios bancarios para gestionar sus operaciones diarias. Desde la perspectiva económica, se trata de un actor cuya actividad origina ingresos y gastos que afectan directamente a las instituciones supervisadas. Comercialmente, constituye uno de los activos más relevantes para estas entidades, dado que su participación y confianza sostienen buena parte del negocio financiero y desde la perspectiva jurídica, sujeto que conviene contratos con las entidades financieras. (Chaves, 2021)

Por su lado Chacón y Mora (2015), señalan que,

> La conexión entre las entidades financieras y los consumidores se da precisamente por medio de la prestación de un servicio financiero, por medio de la venta de un producto financiero, o bien, por el simple ofrecimiento de ambos. Desde las tratativas preliminares de la relación, o desde el ofrecimiento público de los servicios o productos, debe existir claridad en el tipo de servicio o producto ofrecido; sin embargo, esta situación no se da en muchas ocasiones, porque la mayoría de los consumidores no saben diferenciar unos de otros. (p. 66)

Por su lado, a nivel constitucional, el marco normativo que protege al consumidor financiero en Costa Rica se sustenta en principios fundamentales que orientan tanto la regulación como la supervisión de las instituciones financieras.

Entre estos principios, la libertad contractual destaca por garantizar a los individuos “la plena libertad de contratar o no hacerlo, de escoger la materia del contrato, de determinar con quién se contratará, es decir, fijar con toda amplitud el contenido del contrato” (Baudrit, 1991, p. 66). Este principio asegura que los consumidores puedan participar activamente en las relaciones contractuales, reconociendo su capacidad de decisión y negociación. Por otra parte, la libertad de empresa protege el desarrollo de la actividad económica desde su planificación, organización y ejecución hasta la generación de utilidades, asegurando que las entidades financieras puedan operar dentro de un marco que fomente la iniciativa privada y el emprendimiento. (Hernández, 2008) Finalmente, el principio de legalidad establece que todas las actuaciones de las autoridades

y entidades públicas deben sujetarse estrictamente al ordenamiento jurídico vigente, de modo que cualquier acción esté previamente autorizada y regulada expresamente por la ley (Chacón y Mora, 2015, p. 150).

Uno de los aspectos centrales en el derecho del consumidor financiero es la asimetría informativa, entendida como la diferencia en el nivel de conocimiento y acceso a información entre la entidad financiera y el usuario. Las entidades bancarias, debido a la especialización de sus operaciones, disponen de información técnica detallada sobre los productos y servicios que ofrecen, así como sobre los riesgos asociados a las transacciones digitales. Los usuarios, en cambio, poseen un acceso más limitado a este tipo de información y a los recursos técnicos necesarios para interpretarla. (CIJUL, 2013)

Esta desigualdad de información puede colocar al usuario en una posición de mayor vulnerabilidad, al no poder evaluar de manera completa los riesgos de sus decisiones ni identificar posibles fallas en los sistemas bancarios. Por ello, la legislación y la regulación financiera buscan garantizar transparencia y acceso a información clara y suficiente, con el fin de mitigar los efectos de esta asimetría en la relación contractual.

Por otro lado, se ha explorada la figura del "consumidor hipervulnerable" que como se ha citado en López (2022):

> Consumidor hipervulnerable, es decir, de aquel que presenta una capa adicional de vulnerabilidad a aquella que es estructural o inherente a su calidad de consumidor, la que ha concitado la atención de la dogmática comparada más reciente. Y es que como acertadamente precisa Barocelli la presunción homogeneizadora del consumidor medio invisibiliza las diferencias, particularidades y situaciones en que se encuentran algunos consumidores, perjudicando especialmente a los más vulnerables, obligándolos a demostrar esa situación en todos los casos y dejando su estimación a criterio del juzgador, esfuerzo del que se puede prescindir si se admite la categoría de consumidor hipervulnerable. (p.340)

Ahora bien, la asimetría informativa y el carácter especializado de la actividad bancaria hacen que sea necesario otorgar al consumidor financiero una protección reforzada. La Procuraduría General de la República mediante el dictamen C-015-2015 de fecha 03 de febrero de 2015, señala que deben existir mecanismos institucionales para asegurar una aplicación

exhaustiva, objetiva, optima y justa de las reglas con relación a la protección del consumidor financiero:

> La necesidad de protección al consumidor de servicios financieros ha sido puesta en evidencia por instancias internacionales como el Banco Mundial. Las Buenas Prácticas para la Protección al Consumidor Financiero (emitidas por el Banco en junio de 2012) (http://siteresources.worldbank.org/EXTFINANCIALSECTOR/Resources/282884-1339624653091/8703882-1339624678024/8703850-1340026711043/8710076-1340026729001/FinConsumerProtection_GoodPractices_SPANISH_FINAL), postulan la existencia de normas, de rango legal, relativas a la protección al consumidor con respecto de los productos y servicios financieros, que comprendan mecanismos institucionales necesarios para asegurar una aplicación exhaustiva, objetiva, oportuna y justa de las reglas. (Magda Rojas Chaves, Procuradora General Adjunta, 2015)

Ahora bien, dicha protección se traduce en obligaciones adicionales para las instituciones financieras, como, por ejemplo:

- Proporcionar información clara, veraz y comprensible sobre productos y servicios.
- Implementar protocolos de seguridad y prevención de fraudes que reduzcan el riesgo de pérdidas patrimoniales.
- Facilitar mecanismos efectivos para presentar reclamaciones y acceder a la justicia en caso de daños derivados de fallas en la prestación del servicio.

Otro aspecto relevante del derecho del consumidor financiero es la vulnerabilidad técnica, entendida como la exposición del usuario a riesgos derivados de la complejidad de los sistemas informáticos y la infraestructura tecnológica utilizada por las entidades bancarias. La banca electrónica, al operar mediante plataformas digitales y sistemas automatizados, exige al usuario una comprensión técnica que generalmente excede su capacidad, generando dependencia del correcto funcionamiento de los sistemas y de las medidas de seguridad implementadas por la entidad. (Sala Peña, 2010)

La vulnerabilidad técnica implica que el usuario no puede identificar ni corregir fallas en los sistemas de manera directa, lo que refuerza la necesidad de que la entidad financiera asuma la carga de implementar y demostrar medidas de seguridad adecuadas, así como de responder por los daños ocasionados por fallas en sus sistemas. Este concepto es especialmente relevante para la imputación de responsabilidad civil en casos de estafas informáticas o fraudes electrónicos, ya que

la falla de un sistema o la ausencia de controles tecnológicos puede constituir un elemento central para establecer negligencia o incumplimiento del deber de seguridad.

3.3 Marco normativo costarricense aplicable

El análisis de la responsabilidad civil de las entidades bancarias privadas frente a estafas informáticas realizadas a través de plataformas digitales requiere examinar el marco normativo costarricense que regula el funcionamiento del sistema financiero, la protección del consumidor y la tipificación de los delitos informáticos. En Costa Rica, estas disposiciones se encuentran distribuidas en normas de rango constitucional, legislación ordinaria y normativa prudencial emitida por los órganos de supervisión financiera.

Este conjunto normativo establece obligaciones relacionadas con la transparencia en la información, la gestión de riesgos tecnológicos, la seguridad de los sistemas financieros y la protección de los usuarios, elementos que resultan relevantes al analizar la eventual imputación de responsabilidad civil de las entidades bancarias cuando se producen estafas informáticas mediante plataformas digitales.

En materia de protección al consumidor su fundamento constitucional se encuentra a la luz del artículo 46 de la Constitución Política de Costa Rica, la cual reconoce expresamente el derecho de los consumidores y usuarios a la protección de sus intereses económicos y a recibir información adecuada y veraz sobre los bienes y servicios que se ofrecen en el mercado.

Este reconocimiento constitucional establece la obligación del Estado de promover mecanismos que garanticen condiciones de equilibrio entre los consumidores y los agentes económicos que participan en el mercado. En el ámbito de los servicios financieros, esta protección adquiere particular relevancia debido a la complejidad técnica de los productos financieros y a la creciente utilización de plataformas digitales para la realización de transacciones económicas.

Por otro lado, la Ley No. 7472: Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor establece el marco general de protección de los consumidores en Costa Rica. Esta normativa regula las relaciones entre proveedores y consumidores, estableciendo principios orientados a garantizar transparencia, seguridad y responsabilidad en la prestación de bienes y servicios.

Dentro de esta ley, resultan particularmente relevantes los artículos 32, 34, 35 y 72, los cuales establecen obligaciones específicas para los proveedores y mecanismos de responsabilidad frente a daños ocasionados a los consumidores.

El artículo 32 reconoce el derecho del consumidor a recibir información veraz, clara y suficiente sobre los bienes y servicios ofrecidos en el mercado. En el ámbito financiero, esta disposición implica que las entidades bancarias deben proporcionar información adecuada sobre las características, condiciones y riesgos asociados a los servicios que ofrecen, incluidos aquellos que se prestan mediante canales digitales. Asimismo, como puntos esenciales, dicha ley establece como derecho fundamental e irrenunciable del consumidor la protección de sus legítimos intereses económicos y sociales y mecanismos efectivos de acceso para la tutela administrativa y judicial de sus derechos e intereses legítimos, que conduzcan a prevenir adecuadamente, sancionar y reparar con prontitud la lesión de estos, según corresponda. (Ley 7472, 1994).

Por su parte, el artículo 34 establece las obligaciones del comerciante, para el contexto de esta investigación analógicamente -el banco-; en este articulado se establece:

> (…) d) Suministrar, a los consumidores, las instrucciones para utilizar adecuadamente los artículos e informar sobre los riesgos que entrañe el uso al que se destinan o el normalmente previsible para su salud, su seguridad y el medio ambiente. (…)
>
> i) Resolver el contrato bajo su responsabilidad, cuando tenga la obligación de reparar el bien y no la satisfaga en un tiempo razonable.
>
> j) Fijar plazos prudenciales para formular reclamos. (…)
>
> m) Cumplir con lo dispuesto en las normas de calidad y las reglamentaciones técnicas de acatamiento obligatorio. (…)
>
> El incumplimiento de alguna de las obligaciones enumeradas en este artículo, faculta al interesado para acudir a la Comisión nacional del consumidor creada en esta Ley, o a los órganos jurisdiccionales competentes y para hacer valer sus derechos, en los términos que señala el artículo (*)43 de la presente Ley. (*)(Actualmente corresponde al 46). (Ley 7472, 1994, art.34)

En este sentido, la responsabilidad del proveedor frente a daños ocasionados al consumidor como consecuencia de defectos en los bienes o servicios suministrados, en el incumplimiento de medidas, en el deber de garantizar la seguridad y posibilidad de reclamos. De forma, que esta disposición introduce un criterio de responsabilidad que puede resultar aplicable cuando el daño deriva de fallas en los sistemas tecnológicos utilizados para la prestación de servicios financieros.

De manera más específica, el artículo 35 establece un régimen de responsabilidad objetiva para los productores, proveedores y comerciantes cuando se produzcan daños derivados del uso

de bienes o servicios, de información insuficiente o de riesgos asociados a su utilización. Bajo este régimen, el proveedor responde por el daño ocasionado salvo que logre demostrar que el mismo se produjo por causa ajena, como fuerza mayor o culpa de la víctima:

> 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.
>
> (Así corrida su numeración por el artículo 80 de la ley de Contingencia Fiscal, No. 8343 del 18 de diciembre de 2002, que lo traspaso del antiguo artículo 32 al 35 actual) (Ley 7472, 1994, art.35) [4]

Este principio resulta relevante en el contexto de los servicios financieros digitales, donde el uso de plataformas tecnológicas puede generar riesgos para los usuarios, especialmente cuando se producen accesos no autorizados o estafas informáticas.

Finalmente, el artículo 72 de la ley supra señalada, refuerza el carácter de orden público e irrenunciable de la ley, lo cual impide que cláusulas contractuales limiten derechos mínimos del consumidor.

Otra normativa relevante dentro del ordenamiento jurídico costarricense en materia de seguridad de la información es la Ley No. 8968: Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales, la cual establece el marco jurídico para la protección de los datos personales que son recolectados, almacenados y procesados por entidades públicas y privadas.

[4] Corresponde a la versión vigente de la norma, la reforma del proyecto de Ley 23.908 , al momento de realizar la investigación no ha sido publicada, dado que el proyecto se encontraba en trámite.

En particular, el artículo 4 de esta ley consagra el principio de seguridad de los datos, el cual establece la obligación de los responsables de bases de datos de adoptar las medidas técnicas, administrativas y organizativas necesarias para garantizar la protección de la información frente a accesos no autorizados, alteraciones, pérdidas o cualquier forma de tratamiento indebido.

Este principio adquiere especial relevancia en el ámbito del sistema financiero, dado que las entidades bancarias administran grandes volúmenes de información personal y financiera de los usuarios, tales como datos de identificación, registros de transacciones, credenciales de acceso y perfiles transaccionales. En este contexto, la normativa impone a las instituciones financieras el deber de implementar mecanismos adecuados de seguridad informática y de gestión de la información para prevenir accesos indebidos o vulneraciones que puedan facilitar la comisión de fraudes informáticos.

Ahora bien, desde la perspectiva de la responsabilidad civil, el incumplimiento de estas obligaciones de seguridad en el tratamiento de datos personales podría constituir un elemento relevante para determinar la existencia de negligencia en la gestión de los sistemas tecnológicos utilizados por las entidades bancarias. En consecuencia, esta normativa refuerza el deber de seguridad tecnológica que recae sobre las entidades financieras en la protección de la información de sus clientes dentro del entorno digital.

De la misma manera, es importante entender que la supervisión del sistema financiero costarricense se encuentra a cargo de diversas entidades regulatorias, entre ellas la Superintendencia General de Entidades Financieras (en adelante “SUGEF”), cuya función consiste en supervisar y fiscalizar el funcionamiento de las entidades financieras.

Por otro lado, el Consejo Nacional de Supervisión del Sistema Financiero (CONASSIF) posee la facultad de aprobar la normativa aplicable a las entidades supervisadas. Esta competencia se encuentra establecida en el artículo 171 inciso b) de la Ley Reguladora del Mercado de Valores (Ley No. 7732), el cual faculta a dicho órgano para aprobar las normas necesarias para la regulación y supervisión del sistema financiero.

Asimismo, el artículo 131 inciso c) de la Ley Orgánica del Banco Central de Costa Rica (Ley No. 7558) establece que el Superintendente General de Entidades Financieras puede proponer al CONASSIF las normas que considere necesarias para el desarrollo de las labores de supervisión y fiscalización del sistema financiero.

Dentro de este marco regulatorio, el Acuerdo 10-7, denominado “Reglamento sobre la Transparencia ante el Usuario Financiero en la Prestación de Productos y Servicios por parte de Entidades Supervisadas por SUGEF”. En el período 2024 y dada la necesidad creciente de establecer lineamentos que regularan el problema de estafas informáticas, se adiciona a la norma Acuerdo 10-7 el capítulo III correspondiente a “Aspectos mínimos de control para prevenir y mitigar la ocurrencia de estafas informáticas en contra de los usuarios financieros”

Este reglamento busca garantizar estrategias de mitigación y educación en ciber higiene digital, así como regular la responsabilidad de la entidad supervisada, lo cual resulta especialmente relevante en el entorno de los servicios prestados mediante plataformas digitales. (SUGEF, 2024)

Siguiendo en la misma línea, el Consejo Nacional de Supervisión del Sistema Financiero (en adelante “CONASSIF”) aprobó el Reglamento General de Gestión de la Tecnología de Información, Acuerdo CONASSIF 5-17 (anteriormente conocido como Acuerdo SUGEF 14-17), el cual determina los requerimientos mínimos para la gestión de la tecnología de información (TI) que deben acatar las entidades y empresas supervisadas del sistema financiero costarricense incluida la banca privada. Sin embargo, debido a una serie de reforzamientos, este fue modificado integralmente, para lo cual se dispuso el Acuerdo CONASSIF 5-24, publicado en fecha 22 de julio de 2024. (CONASSIF, 2024)

En este sentido, el Acuerdo CONASSIF 5-24, denominado Reglamento General de Gobierno y Gestión de la Tecnología de Información, junto con sus respectivos lineamientos, tiene como propósito establecer las directrices que orientan el adecuado gobierno y la administración de las tecnologías de información, así como la gestión de los riesgos asociados a su utilización.

Bajo el contexto de la presente investigación, este marco regulatorio adquiere particular relevancia en el funcionamiento de las entidades bancarias privadas, dado el papel central que la tecnología desempeña en la prestación de sus servicios financieros. Entre las obligaciones establecidas por esta regulación se incluyen la gestión de riesgos tecnológicos, la implementación de controles de seguridad informática y la adopción de medidas destinadas a prevenir incidentes que puedan afectar la integridad de los sistemas financieros.

Ahora bien, en los últimos años, el incremento de las estafas informáticas y de los fraudes electrónicos asociados al uso de plataformas digitales ha generado un debate jurídico sobre la responsabilidad de las entidades financieras en la custodia de los fondos de sus clientes. Como respuesta a esta problemática, la Asamblea Legislativa de Costa Rica aprobó en marzo 2026, el

Proyecto de Ley No. 23.908, denominado “Protección a las personas consumidoras en la custodia de su dinero que administra cualquier entidad financiera en Costa Rica, ya sea pública o privada, autorizada para este fin”, el cual se encuentra a la espera de la firma del Poder Ejecutivo para su promulgación y posterior entrada en vigencia. (Asamblea Legislativa de Costa Rica, 2026)

Esta reforma introduce modificaciones relevantes al régimen jurídico aplicable a los servicios financieros, particularmente en lo relativo a la responsabilidad de las entidades financieras frente a la sustracción de fondos derivada de fraudes electrónicos o estafas informáticas. La normativa se orienta a fortalecer la protección del consumidor financiero y a establecer procedimientos claros para la atención de reclamaciones relacionadas con operaciones no autorizadas.

Uno de los aspectos más relevantes de la reforma consiste en la modificación del artículo 35 de la Ley No. 7472, Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor, que regula el régimen de responsabilidad de los proveedores frente a daños ocasionados a los consumidores.

La reforma reafirma el principio de responsabilidad objetiva, al establecer que los productores, proveedores y comerciantes responden por los daños ocasionados al consumidor con independencia de la existencia de culpa, siempre que el perjuicio se derive del bien o servicio ofrecido o de la información proporcionada sobre este.

En el caso específico del sistema financiero, la reforma introduce una disposición expresa según la cual las entidades financieras, públicas o privadas, que ofrezcan servicios de intermediación financiera deberán responder por los daños ocasionados por la sustracción de dinero o del patrimonio de las cuentas de los usuarios, cuando dicha sustracción sea realizada por un tercero no autorizado por el titular de la cuenta.

Esta disposición representa un avance significativo en la regulación del consumidor financiero, ya que establece de manera explícita la responsabilidad de las entidades financieras en casos de fraude electrónico o estafa informática, independientemente del mecanismo utilizado para la sustracción de los fondos. No obstante, la norma también contempla la posibilidad de que las entidades financieras se liberen de responsabilidad cuando logren demostrar la existencia de alguna de las eximentes previstas en la legislación vigente.

Desde una perspectiva doctrinal, esta regulación se vincula con la teoría de la responsabilidad por riesgo creado, según la cual quien desarrolla una actividad que implica riesgos para terceros debe asumir las consecuencias de los daños que se deriven de dicha actividad.

La reforma también establece un procedimiento específico que deben seguir los usuarios financieros cuando consideren que han sido víctimas de estafas informáticas, fraudes electrónicos o transacciones no autorizadas.

De acuerdo con la normativa aprobada, el usuario financiero dispone de un plazo de treinta días naturales para presentar su reclamo ante la entidad financiera correspondiente. Este reclamo debe formalizarse mediante un formulario dispuesto por la entidad y debe acompañarse de una denuncia presentada ante el Organismo de Investigación Judicial.

Una vez recibido el reclamo, la entidad financiera dispone de un plazo máximo de treinta días naturales para investigar los hechos y determinar si el reclamo es procedente. Este plazo puede ampliarse, por una única vez, hasta por diez días hábiles adicionales, siempre que dicha ampliación sea comunicada oportunamente al usuario.

Durante la investigación, la entidad financiera deberá demostrar que cumple con los controles preventivos, detectivos y correctivos exigidos por la normativa emitida por la SUGEF, particularmente en lo relativo a la protección de la información y de las cuentas de los usuarios.

Asimismo, la entidad deberá acreditar que sus sistemas informáticos no fueron vulnerados y que se implementaron mecanismos adecuados para prevenir o detectar operaciones atípicas, tales como el análisis de patrones transaccionales, el monitoreo de dispositivos utilizados por el usuario y la verificación de los mecanismos de autenticación empleados en las transacciones.

En caso de que la entidad financiera determine que el reclamo es procedente, deberá restituir los fondos sustraídos en un plazo máximo de diez días naturales, así como eliminar cualquier cargo o interés aplicado como consecuencia de la estafa.

Otro aspecto relevante de la reforma consiste en la intervención de la SUGEF como órgano supervisor en los casos en que las entidades financieras rechacen un reclamo presentado por un usuario.

Cuando una entidad financiera determine que el reclamo no procede, deberá remitir a la SUGEF y al Organismo de Investigación Judicial un informe que contenga las evidencias técnicas y los incidentes de seguridad detectados durante la investigación, incluyendo análisis forenses o bitácoras de los sistemas informáticos.

Posteriormente, la SUGEF dispone de un plazo de diez días hábiles para validar si la decisión adoptada por la entidad financiera se encuentra debidamente fundamentada en las pruebas aportadas. En caso de que el supervisor no ratifique la decisión de la entidad, esta deberá proceder con la restitución de los fondos al usuario afectado.

Este mecanismo introduce un control administrativo adicional, orientado a garantizar que las entidades financieras no rechacen de manera arbitraria las reclamaciones presentadas por los usuarios.

La reforma también incorpora modificaciones a la Ley General de la Administración Pública y al Código Procesal Civil, con el propósito de establecer la inversión de la carga de la prueba en favor de los consumidores en casos relacionados con fraudes electrónicos o conflictos derivados de servicios financieros.

De acuerdo con esta disposición, tanto en sede administrativa como judicial corresponderá a las entidades financieras demostrar que actuaron conforme a los estándares de seguridad y diligencia exigidos por la normativa aplicable. Esta medida responde a la existencia de una asimetría probatoria, ya que las entidades financieras poseen mayor acceso a la información técnica relacionada con las operaciones electrónicas y con el funcionamiento de los sistemas informáticos utilizados para la prestación del servicio.

La doctrina ha señalado que la inversión de la carga de la prueba constituye un instrumento jurídico destinado a equilibrar las relaciones entre consumidores y proveedores cuando existe una desigualdad estructural en el acceso a la información o a los medios probatorios (Lorenzetti, 2006).

La reforma también impone nuevas obligaciones a las entidades financieras y a los órganos supervisores del sistema financiero.

Entre estas obligaciones se encuentra la necesidad de que las entidades financieras implementen protocolos de atención inmediata para víctimas de estafas, los cuales deben ser aprobados por la SUGEF y aplicados por el personal de las entidades cuando un usuario informe que ha sido víctima de fraude.

Asimismo, se establece la obligación de que las entidades financieras proporcionen información clara y actualizada a los usuarios sobre las medidas de seguridad disponibles y sobre las prácticas recomendadas para prevenir fraudes electrónicos.

Por otra parte, la normativa dispone que la SUGEF deberá emitir regulaciones específicas destinadas a prevenir, reducir y erradicar las estafas informáticas en el sistema financiero, las

cuales deberán actualizarse periódicamente para incorporar estándares internacionales en materia de seguridad digital.

Estas medidas reflejan una tendencia regulatoria orientada a fortalecer la confianza en el sistema financiero digital y a reforzar la protección del consumidor financiero, particularmente en un contexto donde el uso de canales electrónicos para la realización de transacciones financieras continúa en expansión.

Desde la perspectiva del presente estudio, la aprobación del proyecto de ley No. 23.908 resulta particularmente relevante, ya que introduce criterios normativos que inciden directamente en la determinación de la responsabilidad civil de las entidades bancarias frente a estafas informáticas.

La reforma consolida tres elementos jurídicos fundamentales para el análisis de la imputación de responsabilidad:

- El reconocimiento expreso de la responsabilidad de las entidades financieras en la custodia de los fondos de los usuarios.
- La inversión de la carga de la prueba en favor del consumidor financiero, lo que implica que la entidad bancaria debe demostrar que adoptó las medidas de seguridad adecuadas.
- La obligación de implementar mecanismos de prevención, monitoreo y autenticación robusta, cuyo incumplimiento podría constituir un elemento relevante para determinar la existencia de negligencia o incumplimiento del deber de seguridad.

Esta reforma normativa constituye un elemento central para el análisis de los criterios de imputación de responsabilidad civil de las entidades bancarias en Costa Rica, especialmente en los casos relacionados con estafas informáticas realizadas a través de plataformas digitales.

Finalmente, en el ámbito penal, el ordenamiento jurídico costarricense ha incorporado disposiciones destinadas a sancionar las conductas ilícitas relacionadas con el uso indebido de sistemas informáticos.

Inicialmente, la Ley No. 8148 de 2001 introdujo al Código Penal diversas figuras delictivas relacionadas con la informática, entre ellas la violación de comunicaciones electrónicas, el fraude informático y la alteración de datos o sabotaje informático.

Posteriormente, la Ley No. 9048 de 2012 reformó diversos artículos del Código Penal e incorporó nuevas figuras delictivas relacionadas con el uso de tecnologías digitales, tales como la estafa informática, el daño informático, la violación de datos personales y la suplantación de

identidad digital. El artículo 217 bis del Código Penal sanciona el fraude informático, definido como "el uso de medios informáticos, electrónicos o telemáticos, para ejecutar maniobras fraudulentas que induzcan en error a una persona o sistema, y con ello se obtenga un beneficio patrimonial indebido" (Asamblea Legislativa de Costa Rica, 2012).

3.4 Vías de reclamación para los consumidores financieros en Costa Rica frente a operaciones bancarias no autorizadas

El desarrollo de servicios financieros mediante plataformas digitales ha ampliado el acceso a productos bancarios, pero también ha incrementado la exposición de los usuarios a riesgos asociados con fraudes electrónicos, estafas informáticas y transacciones no autorizadas. En este contexto, el ordenamiento jurídico costarricense reconoce distintos mecanismos administrativos, institucionales y judiciales mediante los cuales los consumidores financieros pueden presentar denuncias o reclamos frente a las entidades financieras cuando consideran que sus derechos han sido vulnerados.

Estas vías de reclamación se fundamentan en el marco normativo compuesto por la Constitución Política de Costa Rica, la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor No. 7472, la normativa emitida por SUGEF, CONASSIF y normativa interna de cada entidad bancaria privada.

La primera vía de reclamación disponible para el consumidor financiero consiste en la presentación de un reclamo directo ante la entidad bancaria privada que presta el servicio financiero.

En particular, las entidades financieras supervisadas deben contar con mecanismos internos destinados a la recepción y gestión de reclamos relacionados con la prestación de sus servicios. Estos mecanismos incluyen plataformas digitales, centros de atención al cliente y oficinas físicas donde los usuarios pueden presentar denuncias por transacciones no autorizadas, errores en operaciones bancarias o posibles fraudes electrónicos.

Ahora bien, la obligación de las entidades financieras de recibir y tramitar este tipo de reclamos se vincula con los principios de información, seguridad y responsabilidad del proveedor, establecidos en la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor No. 7472, particularmente en lo relativo a la responsabilidad del proveedor frente a daños ocasionados al consumidor por la prestación del servicio o por información insuficiente sobre su uso y riesgos.

Asimismo, la normativa prudencial emitida por SUGEF exige que las entidades supervisadas dispongan de mecanismos adecuados para la atención de quejas y reclamaciones de los usuarios, especialmente en relación con servicios financieros prestados mediante canales digitales.

De acuerdo con disposiciones regulatorias recientes incorporadas al Reglamento sobre divulgación de información y publicidad de productos y servicios financieros Acuerdo SUGEF 10-07, las entidades financieras deben establecer procedimientos para la recepción y resolución de quejas o reclamos relacionados con fraudes electrónicos o transacciones no autorizadas, garantizando que los usuarios puedan acceder a estos mecanismos de manera clara y oportuna. (SUGEF, 2024)

Es importante, tener en cuenta que cuando el consumidor financiero considera que la entidad bancaria no ha atendido adecuadamente su reclamo o que existe una irregularidad en el funcionamiento del servicio financiero, puede presentar una queja o denuncia ante SUGEF. Sin embargo, la SUGEF no actúa como un tribunal encargado de resolver conflictos individuales entre clientes y entidades financieras, es decir, no es un órgano especializado para ver situaciones micro, dado que su función consiste en analizar posibles incumplimientos regulatorios y adoptar medidas de supervisión o sanción cuando corresponda, lo cual puede incidir indirectamente en la protección de los consumidores financieros.

Otra vía relevante para los consumidores financieros es la Oficina del Consumidor Financiero (en adelante "OCF"), una instancia privada creada con el objetivo de atender consultas, quejas y reclamaciones relacionadas con servicios financieros. (Oficina del Consumidor, 2025)

La OCF actúa como un mecanismo alternativo de resolución de conflictos entre los consumidores financieros y las entidades que se encuentran afiliadas a esta oficina, como lo son: DAVIBANK, Banco Promerica, DAVIVIENDA, Banco Improsa, Banco LAFISE, BAC, Banco Cathay y Banco BCT S.A.[5] Entre sus funciones principales se encuentra la orientación al consumidor sobre sus derechos, la recepción de reclamaciones y la mediación entre el cliente y la entidad financiera involucrada.

Aunque las resoluciones de esta oficina no tienen carácter jurisdiccional, su intervención puede contribuir a facilitar la solución de controversias entre las partes, evitando la necesidad de acudir a procesos judiciales más complejos. Bajo esta modalidad, los consumidores han sido

[5] Recopilado de la página web sobre afiliados de la Oficina del Consumidor Financiero https://www.ocf.fi.cr/

indemnizados en su totalidad o en un cincuenta por ciento, ya que muchas veces se encuentra en una “responsabilidad compartida”. (Solano, 2026)

Por otro lado, cuando el consumidor financiero considera que ha sido víctima de un delito, como una estafa informática, fraude electrónico o suplantación de identidad, puede presentar una denuncia penal ante el Organismo de Investigación Judicial.

La denuncia ante el OIJ tiene como finalidad iniciar una investigación penal destinada a identificar a los responsables del delito y determinar la eventual responsabilidad penal de los autores. Este procedimiento es independiente de las reclamaciones administrativas o civiles que el consumidor pueda interponer contra la entidad financiera. Sin embargo, en este punto se puede configurar la figura de la acción civil resarcitoria, a la luz del Código Procesal Penal señala:

Artículo 40- Carácter accesorio. En el procedimiento penal, la acción civil resarcitoria solo podrá ser ejercida mientras esté pendiente la persecución penal. Sobreseído provisionalmente el imputado o suspendido el procedimiento, de conformidad con las previsiones de ley, el ejercicio de la acción civil se suspenderá hasta que la persecución penal continúe y quedará a salvo el derecho de interponer la demanda ante los tribunales competentes.

El Tribunal Penal deberá pronunciarse sobre el fondo de la acción civil resarcitoria válidamente ejercida, aún y cuando se haya dictado sentencia absolutoria o de sobreseimiento definitivo en la fase de juicio (Código Procesal Penal, 1996, art. 40).

De forma que el Código Procesal Penal permite que la víctima se constituya como actor civil dentro del proceso penal, lo cual le permite solicitar al juez la reparación de los daños ocasionados por el delito. De esta forma, en caso de que el tribunal determine la existencia del delito y la responsabilidad del imputado, también puede ordenar el pago de una indemnización a favor de la persona afectada.

Finalmente, el consumidor financiero puede acudir a la vía judicial cuando considera que ha sufrido un daño patrimonial como consecuencia de la actuación de la entidad financiera o de fallas en la prestación del servicio.

En estos casos, es posible interponer acciones civiles de responsabilidad destinadas a obtener la reparación del daño sufrido. Para el contexto de la investigación, debido a que son entidades bancarias privadas, estas acciones se fundamentan en la interposición de un proceso sumario civil, así como en el régimen de responsabilidad establecido en la Ley No. 7472,

particularmente en lo relativo a la responsabilidad objetiva de los proveedores frente a daños ocasionados al consumidor.

Adicionalmente, las reformas legislativas recientes relacionadas con fraudes electrónicos han reforzado la protección del consumidor financiero al introducir mecanismos como la inversión de la carga de la prueba en casos relacionados con fraudes electrónicos o servicios financieros, lo cual implica que la entidad financiera puede verse obligada a demostrar que actuó conforme a los estándares de seguridad y diligencia exigidos por la normativa aplicable.

4. Estafas Informáticas y Riesgo Tecnológico

4.1 Estafas Informáticas

En la era digital, los delitos informáticos representan uno de los principales desafíos jurídicos, tanto por su rápida evolución como por la complejidad técnica que implican. En Costa Rica, estos delitos han experimentado un crecimiento acelerado, en particular aquellos relacionados con fraudes financieros mediante el uso de plataformas digitales bancarias.

Sobre este punto de acuerdo con el informe Estado de la Ciberseguridad en Costa Rica 2024, elaborado por el Laboratorio de Investigación, Desarrollo e Innovación en Ciberseguridad (LABCIBE) de la Universidad Nacional, las denuncias por delitos informáticos tuvieron un aumento significativo para el período 2024 (período comprendido hasta el 15 de octubre de 2024) (p.11):

Tabla 1. Cantidad de denuncias por Delitos Informáticos, según año, período comprendido del 01/01/2018 hasta el 15/10/2024

Año	Totales
2018	1662
2019	2116
2020	2403
2021	2884
2022	5170
2023	5273
2024*	6634
Total:	26142

Fuente: Unidad de Análisis Criminal OIJ 2024

Gráfico 1. Denuncias por Delitos Informáticos, según año. Período comprendido del 1/01/2018 hasta 15/10/2024

Fuente: Unidad de Análisis Criminal OIJ 2024 [6]

De forma que los delitos informáticos que afectan al sector bancario adoptan diversas modalidades, muchas de ellas centradas en el engaño o manipulación de los usuarios para obtener

[6] Tomado del Informe Estado de la Ciberseguridad en Costa Rica 2024, elaborado por el Laboratorio de Investigación, Desarrollo e Innovación en Ciberseguridad (LABCIBE) de la Universidad Nacional (p.11).

acceso a información confidencial o ejecutar transferencias fraudulentas. Entre las formas más comunes destacan:

- Phishing: Técnica que simula comunicaciones oficiales del banco (correos electrónicos, SMS, sitios web falsos) para obtener credenciales de acceso del usuario (MICITT, 2023).
- El Pharming: Trata del desvío del tráfico de internet de un sitio web hacia otro de aspecto similar, con el fin de obtener información personal (nombre, contraseñas, etc.) que el usuario incorpora a la página falsa y que se registra ahí, lo que hacen es que posterior al registro pueden robar los datos de autenticación y suplantar la identidad del usuario (Salas, 2010).
- Smishing: Variante del phishing realizada por mensajes de texto (SMS) que inducen al usuario a proporcionar información personal o hacer clic en enlaces maliciosos.
- Spoofing: Suplantación de identidad digital mediante la falsificación de direcciones de correo, números telefónicos o sitios web, con el fin de ganarse la confianza del usuario.
- Ingeniería social: Manipulación psicológica del usuario para que voluntariamente revele datos sensibles o realice acciones riesgosas, aprovechando la confianza o el desconocimiento.
- Malware: Programas maliciosos que se instalan en el dispositivo del usuario para capturar información, registrar pulsaciones del teclado (keyloggers) o redirigir conexiones a sitios fraudulentos.

Estas estafas se caracterizan por explotar vulnerabilidades humanas y técnicas, combinando herramientas tecnológicas con tácticas de persuasión o engaño. Los delitos informáticos, por su naturaleza compleja y dinámica, presentan desafíos significativos para su prevención, detección y sanción efectiva.

En primer lugar, son altamente transnacionales, lo que complica la trazabilidad de los hechos y la identificación de los responsables. En segundo lugar, el uso de tecnologías como redes privadas virtuales (VPN), proxies, direcciones IP dinámicas y cifrado dificultan el rastreo de las conexiones utilizadas por los ciberdelincuentes (UCR, 2023).

Además, muchas de estas estafas ocurren en tiempos muy breves, donde las transferencias se ejecutan de forma inmediata, dejando poco margen para su reversión. Otra dificultad clave radica en que, en varios casos, la víctima autoriza involuntariamente la transacción, ya sea al

proporcionar sus claves o al ingresar a enlaces maliciosos, lo cual complica la atribución de responsabilidad y la recuperación de los fondos perdidos.

El componente de ingeniería social hace que estos delitos no dependan exclusivamente de fallas tecnológicas, sino también de fallos humanos, lo que obliga a los bancos a implementar mecanismos de control más robustos y adaptados al comportamiento del usuario (Rodríguez Bonilla, 2022).

4.2 Riesgo tecnológico en plataformas digitales bancarias

Las plataformas digitales bancarias constituyen el canal principal a través del cual las entidades financieras ofrecen servicios electrónicos a sus clientes, permitiendo la realización de operaciones financieras en línea de manera rápida y eficiente. Estas plataformas comprenden diversos componentes tecnológicos, entre los que se incluyen aplicaciones móviles (apps), servicios de banca en línea, sistemas de autenticación multifactorial y dispositivos de seguridad como tokens.

Este proceso de digitalización ha generado importantes beneficios en términos de eficiencia, accesibilidad y rapidez en la prestación de servicios financieros; sin embargo, también ha incrementado la exposición de las entidades bancarias a diversos riesgos tecnológicos, los cuales pueden materializarse en pérdidas económicas para los usuarios y generar potenciales responsabilidades para las instituciones financieras.

Ahora bien, las aplicaciones móviles y los sistemas de banca en línea constituyen interfaces tecnológicas que permiten a los usuarios acceder a sus cuentas bancarias y realizar operaciones financieras mediante dispositivos conectados a internet. Estos sistemas se apoyan en protocolos de seguridad como el cifrado criptográfico SSL/TLS, cuyo objetivo es proteger la transmisión de datos y evitar su interceptación por terceros no autorizados. (González, 2022)

El uso de tokens —dispositivos físicos o aplicaciones que generan códigos temporales— es común para la autenticación multifactorial, añadiendo una capa adicional de seguridad que complementa la contraseña tradicional. La autenticación multifactorial requiere que el usuario demuestre su identidad mediante al menos dos factores distintos: algo que sabe (contraseña), algo que tiene (token o dispositivo móvil) o algo que es (datos biométricos). (SUGEF, 2021)

Estos sistemas están diseñados para minimizar el riesgo de accesos no autorizados, garantizando la integridad, confidencialidad y disponibilidad de los servicios financieros.

Por su lado, la seguridad de la información se entiende como el conjunto de medidas preventivas orientadas a resguardar tanto los datos como los recursos asociados a ellos. Su propósito es reducir los riesgos frente a posibles amenazas y evitar que terceros puedan aprovechar debilidades o vulnerabilidades existentes en los sistemas (Maiwald, 2005).

Dentro de este marco, los sistemas de autenticación desempeñan un papel central en la prevención del fraude digital. La literatura especializada señala que la autenticación multifactorial representa uno de los mecanismos más eficaces para reducir el riesgo de accesos fraudulentos, especialmente en servicios financieros en línea (Bonneau et al., 2012). Sin embargo, estos sistemas deben complementarse con otras medidas de seguridad, como la gestión adecuada de credenciales, la detección de anomalías en el comportamiento del usuario y la actualización constante de los protocolos de seguridad.

Desde la perspectiva de la responsabilidad civil, la implementación adecuada de estos sistemas puede constituir un elemento relevante para determinar si la entidad bancaria ha cumplido con su deber de diligencia en la protección de los activos y datos de sus clientes.

Otro componente esencial de la gestión del riesgo tecnológico en la banca digital es el monitoreo antifraude, que consiste en el uso de herramientas tecnológicas para detectar patrones sospechosos en las transacciones financieras. Estas herramientas emplean técnicas de análisis de datos y aprendizaje automático para identificar comportamientos anómalos que podrían indicar la existencia de fraude. (SUGEF, 2024)

4.3. Riesgos y Vulnerabilidades Asociados

Pese a las medidas tecnológicas implementadas, las plataformas digitales bancarias presentan vulnerabilidades inherentes a su naturaleza conectada y a la interacción humana. Entre los riesgos más significativos se encuentran:

- Ataques cibernéticos como el phishing, malware, y ataques de intermediario (man-in-the-middle), que buscan interceptar o manipular la información financiera (MICITT, 2023).
- Fallas en la seguridad de software o hardware, incluyendo errores de programación, vulnerabilidades en sistemas operativos y aplicaciones, que pueden ser explotadas por ciberdelincuentes (Rodríguez Bonilla, 2022).
- Riesgos asociados a la gestión del acceso y control de usuarios, donde la debilidad en los mecanismos de autenticación o la falta de actualización constante puede facilitar accesos indebidos (González, 2022).

- Factores humanos, tales como la falta de capacitación de los usuarios, errores en el manejo de credenciales y la susceptibilidad a la ingeniería social, que disminuyen la eficacia de las barreras técnicas (UCR, 2023).

La conjunción de estos factores hace que, aunque las plataformas digitales sean herramientas eficientes, no sean infalibles frente a las amenazas digitales. En este sentido, las entidades bancarias deben mantener una política de seguridad dinámica y continua, actualizando sus protocolos y fortaleciendo la cultura de seguridad tanto interna como externa.

4.4.Estándares técnicos razonables en la seguridad bancaria digital

Desde la perspectiva jurídica, la determinación de la responsabilidad civil en casos de fraude digital suele implicar la evaluación de si la entidad bancaria ha adoptado estándares técnicos razonables de seguridad. Estos estándares se refieren a las prácticas generalmente aceptadas en la industria financiera para proteger los sistemas informáticos y prevenir accesos no autorizados.

Entre dichas prácticas se incluyen la autenticación multifactorial, el cifrado de datos, la monitorización de transacciones, la gestión de incidentes de seguridad y la actualización constante de los sistemas informáticos (Bonneau et al., 2012).

La adopción de estos mecanismos contribuye a reducir la probabilidad de fraudes y permite demostrar que la entidad ha actuado con la diligencia exigible en la prestación de servicios financieros digitales.

En este sentido, el análisis del riesgo tecnológico en plataformas bancarias no solo constituye un aspecto técnico, sino también un elemento relevante para determinar la existencia de un eventual incumplimiento del deber de seguridad, aspecto que puede incidir directamente en la imputación de responsabilidad civil frente a los daños ocasionados por estafas informáticas.

Capítulo III. Marco Metodológico

La presente investigación se desarrolla bajo un enfoque cualitativo bajo el paradigma jurídico - doctrinal, orientado al análisis e interpretación del fenómeno jurídico relacionado con la imputación de responsabilidad civil a las entidades bancarias privadas en Costa Rica frente a delitos de estafas informáticas cometidos a través de sus plataformas digitales durante el período 2024.

El enfoque cualitativo permite comprender fenómenos jurídicos mediante la interpretación de normas, doctrinas y decisiones judiciales, lo cual resulta particularmente pertinente en investigaciones del ámbito del derecho, donde el objeto de estudio se centra en el análisis de criterios normativos y jurisprudenciales (Hernández et al., 2014).

En este sentido, la investigación se fundamenta principalmente en la revisión sistemática de fuentes documentales, tales como legislación nacional, doctrina jurídica especializada y jurisprudencia emitida por los órganos jurisdiccionales costarricenses. A partir de este análisis, se busca identificar los criterios jurídicos aplicables para la imputación de responsabilidad civil a las entidades bancarias privadas cuando se producen fraudes informáticos a través de sus plataformas digitales.

El estudio presenta un alcance descriptivo y explicativo. Por un lado, describe los principales criterios legales y jurisprudenciales que regulan la responsabilidad civil de las entidades bancarias privadas frente a delitos informáticos. Por otro lado, analiza y explica la relación jurídica existente entre el deber de seguridad de las entidades financieras y los daños patrimoniales ocasionados a los usuarios del sistema bancario digital.

El diseño metodológico corresponde a una investigación documental con análisis jurídico sistemático, mediante la cual se examinan las fuentes normativas y jurisprudenciales para identificar patrones interpretativos utilizados por los operadores jurídicos en la determinación de la responsabilidad civil en el contexto de fraudes informáticos.

3.1 Tipo de Investigación

La presente investigación es de tipo aplicada, dado que su propósito consiste en analizar un problema jurídico concreto y contemporáneo relacionado con la imputación de responsabilidad civil a las entidades bancarias privadas frente a delitos de estafa informática cometidos mediante sus plataformas digitales.

La investigación aplicada recibe el nombre de “investigación práctica o empírica”, que se caracteriza porque busca la aplicación o utilización de los conocimientos adquiridos, a la vez que se adquieren otros, después de implementar y sistematizar la práctica basada en investigación. El uso del conocimiento y los resultados de investigación que da como resultado una forma rigurosa, organizada y sistemática de conocer la realidad. (Murillo, 2008)

En este caso, el estudio busca aportar elementos de análisis jurídico que permitan comprender los criterios de imputación de responsabilidad civil en el contexto del sistema bancario digital costarricense.

El desarrollo de la banca electrónica y de los servicios financieros digitales ha generado nuevas formas de fraude informático que plantean desafíos significativos para el derecho civil y el derecho bancario. En consecuencia, resulta necesario examinar cómo el ordenamiento jurídico costarricense aborda la responsabilidad de las entidades financieras frente a los daños ocasionados a los usuarios mediante estas nuevas modalidades delictivas.

En este sentido, la investigación aplicada permite analizar el marco normativo vigente, la doctrina jurídica especializada y la jurisprudencia nacional, con el objetivo de identificar criterios interpretativos que contribuyan a fortalecer la seguridad jurídica y la protección de los usuarios del sistema financiero.

3.2 Alcance de la Investigación

El alcance de la presente investigación es descriptivo y explicativo. Ya que, desde una perspectiva descriptiva, el estudio pretende identificar y sistematizar los principales criterios legales, doctrinales y jurisprudenciales relacionados con la imputación de responsabilidad civil a las entidades bancarias privadas en Costa Rica cuando se producen fraudes informáticos a través de sus plataformas digitales.

Los estudios descriptivos buscan especificar las características, propiedades y elementos que componen un fenómeno determinado, permitiendo comprender su estructura y funcionamiento dentro de un contexto específico (Hernández et al., 2014). En este caso, la investigación describe el marco jurídico aplicable a la responsabilidad civil bancaria en el contexto de delitos informáticos.

Por otra parte, desde una perspectiva explicativa, la investigación busca analizar las relaciones jurídicas existentes entre el deber de seguridad de las entidades bancarias, el riesgo

tecnológico asociado al uso de plataformas digitales y la producción de daños patrimoniales a los usuarios del sistema financiero.

Este enfoque explicativo permite examinar cómo los órganos jurisdiccionales interpretan los elementos configurativos de la responsabilidad civil —tales como el daño, la culpa, el nexo causal y la carga probatoria— al resolver casos relacionados con fraudes informáticos en el ámbito bancario.

De esta manera, el estudio no solo describe el marco jurídico vigente, sino que también analiza los fundamentos jurídicos que permiten establecer la responsabilidad civil de las entidades financieras en el entorno digital.

3.3 Enfoque de la Investigación

El enfoque de la investigación es cualitativo, dado que se orienta a la interpretación y análisis del fenómeno jurídico relacionado con la responsabilidad civil de las entidades bancarias privadas frente a delitos de estafa informática.

Como menciona Cerda (1994), el enfoque cualitativo "hace referencia a caracteres, atributos, esencia, totalidad o propiedades no cuantificables, que … podían describir, comprender y explicar mejor los fenómenos, acontecimientos y acciones del grupo social o del ser humano" (como se citó en Ñaupas et al., 2018, p.141).

Asimismo, Villabela (2020) indica:

La investigación cualitativa se inspira en un paradigma emergente, alternativo, naturalista, humanista, constructivista, interpretativo o fenomenológico, que aborda problemáticas condicionadas histórica y culturalmente en las cuales el hombre está insertado y cuyo propósito es la descripción de los objetos que estudia, la interpretación y la comprensión. De esta forma, la investigación responde a las preguntas ¿qué es? y ¿cómo es?; y tiende a precisar la cualidad, la manera de ser, lo que distingue y caracteriza. (164)

En el ámbito del derecho, el enfoque cualitativo resulta particularmente pertinente porque permite examinar de manera detallada el contenido de normas jurídicas, doctrinas y decisiones judiciales, identificando los criterios interpretativos utilizados por los operadores jurídicos.

En la presente investigación, el enfoque cualitativo se manifiesta a través del análisis interpretativo de:

- Legislación nacional relacionada con responsabilidad civil, delitos informáticos y regulación bancaria.

- Jurisprudencia emitida por los órganos jurisdiccionales costarricenses en casos relacionados con fraudes informáticos.

Este enfoque permite comprender cómo se construyen los criterios jurídicos utilizados para determinar la responsabilidad civil de las entidades bancarias privadas frente a los daños ocasionados por estafas informáticas en el contexto de la banca digital.

3.4 Método de Investigación

Debido al enfoque cualitativo y al carácter analítico del problema jurídico, el diseño de investigación adoptado es hermenéutico. Según García y Rosas (2019), el diseño hermenéutico se centra en la interpretación de textos jurídicos, normativos y jurisprudenciales, buscando comprender su significado en contextos específicos y su aplicación práctica.

De acuerdo con Monroy y Navas, al método hermenéutico, se refiere a:

> Se dice que la hermenéutica es el arte de interpretar textos, principalmente los de tipo religioso o filosófico. Este método implica que cualquier cosa puede ser comprensible a partir de métodos que lleven el pensamiento a la interpretación. Parte de la premisa de que el ser humano es por naturaleza interpretativo. La interpretación funciona en dos sentidos: de lo general a lo particular y en sentido inverso, de lo particular a lo general. El que interpreta un texto debe desprenderse de sus prejuicios para lograr un entendimiento, tanto de la temporalidad del texto como del autor, comprendiendo el contexto temporal y espacial de cada uno. La hermenéutica intenta descifrar el significado de las palabras. (p.98)

Por lo que, este diseño es adecuado para estudiar la responsabilidad civil de las entidades bancarias frente a estafas informáticas, ya que permite examinar las leyes, reglamentos, fallos judiciales y doctrinas relevantes, interpretando cómo se articulan en la práctica judicial y cómo se acreditan los elementos de la responsabilidad civil.

En el desarrollo de la presente investigación, este método se aplicará mediante:

- El análisis normativo, para examinar las disposiciones legales relacionadas con la responsabilidad civil y los delitos informáticos.
- El análisis jurisprudencial, para examinar los criterios utilizados por los órganos jurisdiccionales al resolver casos relacionados con fraudes informáticos en el ámbito bancario.

Este enfoque metodológico permite construir una interpretación sistemática de los criterios jurídicos que sustentan la imputación de responsabilidad civil a las entidades bancarias privadas en Costa Rica.

Asimismo, es menester señalar que en la presente investigación no se incorporó la técnica de entrevista como instrumento de recolección de información, en virtud de la naturaleza del problema en estudio, el enfoque cualitativo y el método hermenéutico que dirige el diseño metodológico.

El estudio se centra en examinar e interpretar normas jurídicas, criterios doctrinales y resoluciones judiciales relacionadas con la responsabilidad civil de las entidades bancarias frente a estafas informáticas. Por ello, el interés no está puesto en las opiniones o experiencias de actores específicos, sino en comprender cómo el derecho regula este fenómeno a partir de sus propias fuentes formales.

Desde esta lógica, el método hermenéutico exige un trabajo enfocado en la lectura, análisis e interpretación de textos jurídicos dentro de su contexto. En ese sentido, recurrir a entrevistas —ya sea a jueces, funcionarios bancarios o usuarios— podría aportar información interesante, pero no resulta necesario para responder la pregunta de investigación, que está orientada a identificar y explicar los criterios jurídicos aplicables, más que a recoger percepciones o prácticas.

Además, incorporar entrevistas habría implicado introducir un componente subjetivo que no es central para este tipo de estudio, cuyo eje es el análisis dogmático del derecho. Por esta razón, se optó por trabajar con técnicas de análisis documental, como el análisis normativo y jurisprudencial, que permiten abordar el problema con mayor precisión y coherencia metodológica.

En consecuencia, la decisión de no utilizar entrevistas no debe entenderse como una limitación, sino como una elección metodológica acorde con el tipo de investigación realizada y con los objetivos planteados.

3.5 Tipo de Muestreo

La presente investigación utiliza un muestreo no probabilístico de tipo intencional o por criterios, el cual resulta adecuado para estudios cualitativos de carácter jurídico, en los que la selección de las unidades de análisis se realiza en función de su relevancia para los objetivos de estudio.

Según Ñaupas et al., (2018), el muestreo intencional es común en investigaciones cualitativas porque permite seleccionar unidades de análisis que aporten información relevante para la comprensión del fenómeno estudiado, privilegiando la profundidad analítica sobre la representatividad estadística.

Para la selección de las sentencias que conforman la muestra jurisprudencial se consideraron los siguientes criterios de inclusión:

- Resoluciones judiciales emitidas por tribunales costarricenses, especialmente por la Sala Primera de la Corte Suprema de Justicia y tribunales contencioso-administrativos.
- Casos relacionados con fraudes informáticos, transferencias electrónicas no autorizadas, estafas digitales o vulneraciones en servicios de banca electrónica.
- Sentencias que analicen la imputación de responsabilidad civil de entidades bancarias o financieras frente a los daños ocasionados a los usuarios.

Es importante señalar que para la población que se utilizará relacionada a la jurisprudencia en órganos jurisdicciones, se debe hacer la salvedad que, aunque el objeto de estudio de la presente investigación se centra en la responsabilidad civil de las entidades bancarias privadas, una parte significativa de la jurisprudencia costarricense relacionada con fraudes informáticos en servicios bancarios digitales se ha desarrollado en casos que involucran entidades bancarias de naturaleza pública.

Ahora bien, esta circunstancia no impide trasladar los criterios construidos por los tribunales hacia el ámbito de la banca privada. Desde el punto de vista jurídico, existe una base suficientemente sólida que permite esa extrapolación.

Por un lado, los elementos clásicos de la responsabilidad civil —hecho generador, daño, nexo causal y factor de atribución— no varían según la naturaleza de la entidad bancaria. Se trata de categorías propias del derecho civil que resultan aplicables tanto a bancos públicos como privados.

Por otro lado, y esto resulta especialmente relevante para este estudio, el artículo 35 de la Ley No. 7472 establece un régimen de responsabilidad objetiva para todos los proveedores de servicios, sin hacer distinción alguna entre entidades públicas o privadas. En ese sentido, los bancos, independientemente de su naturaleza, quedan sometidos a un mismo estándar jurídico en su relación con el consumidor financiero.

Esto implica que la responsabilidad no se construye únicamente a partir de la culpa, sino del riesgo que genera la propia actividad. A su vez, la carga de la prueba se desplaza hacia el proveedor del servicio, quien solo puede liberarse si logra demostrar que el daño le es completamente ajeno.

Bajo esta lógica, el análisis jurisprudencial desarrollado en esta investigación no se limita a revisar casos aislados, sino que busca identificar criterios interpretativos que trascienden el caso concreto y que, dentro del marco del derecho del consumidor, resultan plenamente aplicables a la banca privada.

De ahí que la utilización de jurisprudencia relacionada con entidades bancarias públicas no solo es válida, sino metodológicamente necesaria, en la medida en que permite construir una visión más integrada y coherente sobre la imputación de la responsabilidad civil bancaria.

Además, estas resoluciones resultan particularmente valiosas, ya que los tribunales, al analizar estos casos, recurren a principios generales del derecho civil que son comunes a todo el sistema, como: el deber de seguridad en la prestación del servicio, la relación causal entre la actuación de la entidad financiera y el daño sufrido por el usuario, y la forma en que se distribuye la carga de la prueba.

En consecuencia, el examen de dichas resoluciones permitirá identificar patrones interpretativos aplicables al sistema bancario en general, independientemente de la naturaleza pública o privada de la entidad financiera involucrada, lo cual contribuye a comprender los criterios jurídicos que podrían aplicarse a las entidades bancarias privadas frente a casos de estafas informáticas realizadas mediante plataformas digitales.

3.6 Técnicas e instrumentos de recolección y análisis de la información

El análisis de los datos en la presente investigación se desarrollará siguiendo un enfoque cualitativo, orientado a la interpretación sistemática de la normativa, doctrina y jurisprudencia relacionadas con la imputación de responsabilidad civil de las entidades bancarias privadas frente a delitos de estafas informáticas en Costa Rica durante 2024.

Para la recolección y análisis de la información se emplearán por diversas estrategias de interpretación jurídica, relacionadas a la investigación documental:

3.6.1 Análisis de contenido jurídico

Esta técnica permitirá identificar, clasificar y organizar la información contenida en las normas, resoluciones judiciales y textos doctrinales. Se aplicará un procedimiento sistemático de

codificación de contenidos, orientado a extraer categorías jurídicas relevantes para la investigación, tales como:

- Factor de atribución: culpa, riesgo o garantía.
- Nexo causal: relación entre la actuación de la entidad bancaria y el daño causado.
- Carga de la prueba: obligaciones probatorias de las partes involucradas.
- Deber de seguridad tecnológica: estándares y obligaciones que deben cumplir las entidades financieras para proteger a sus clientes frente a fraudes informáticos.

Este análisis permitirá identificar los elementos recurrentes en la interpretación de los órganos jurisdiccionales y en la aplicación de la normativa, así como las posibles divergencias o vacíos en la regulación vigente.

3.6.2 Análisis comparativo

Se efectuará un análisis comparativo de los criterios interpretativos presentes en la jurisprudencia y la doctrina especializada. Esta estrategia permitirá:

- Detectar patrones en la forma en que los órganos jurisdiccionales costarricenses atribuyen responsabilidad civil en casos de estafas informáticas.
- Contrastar la aplicación de normas y principios generales del derecho con las decisiones judiciales.
- Establecer posibles líneas de evolución jurisprudencial o divergencias interpretativas que requieran clarificación doctrinal o normativa.

3.6.3 Sistematización dogmática

Los hallazgos obtenidos se integrarán en una estructura coherente y organizada, con el objetivo de:

- Explicar cómo se articulan los criterios normativos, jurisprudenciales y doctrinales para la imputación de responsabilidad civil.
- Comprender cómo los órganos jurisdiccionales interpretan el deber de seguridad de las entidades financieras en el contexto digital.
- Identificar mecanismos prácticos para acreditar la responsabilidad civil de los bancos frente a fraudes informáticos.

Como parte de la recolección, para la para la organización y sistematización de la información, que permitirán un análisis detallado, se usarán instrumentos como:

- Fichas de análisis normativo, destinadas a registrar de manera ordenada artículos, leyes y reglamentos pertinentes al estudio.
- Matrices de análisis jurisprudencial, diseñadas para identificar los criterios de imputación aplicados por los órganos jurisdiccionales, los nexos causales establecidos y la implementación de los deberes de seguridad.
- Cuadros comparativos de criterios de imputación, que faciliten la comparación y contraste entre distintos casos judiciales y las disposiciones normativas correspondientes.
- Guías de categorización temática, utilizadas para clasificar y organizar los hallazgos según categorías relevantes para la investigación, como culpa, riesgo, deber de seguridad y carga de la prueba.

3.6.4 Procedimiento de codificación y categorización

El proceso de análisis cualitativo incluirá las siguientes etapas:

a) Familiarización con los datos: lectura detallada de normas, sentencias y doctrinas seleccionadas para comprender su contenido general.

b) Codificación inicial: identificación y clasificación de fragmentos relevantes de las normas, resoluciones judiciales y textos doctrinales, los cuales serán organizados en categorías jurídicas previamente definidas, tales como culpa, riesgo creado, nexo causal y carga de la prueba.

c) Agrupamiento y formación de categorías: los códigos se organizarán en categorías amplias que respondan a los objetivos específicos de la investigación.

d) Revisión y refinamiento de categorías: verificación de coherencia y pertinencia de las categorías, ajustando o subdividiendo según sea necesario.

e) Definición y denominación de categorías: cada categoría recibirá un nombre claro y descriptivo, con una definición precisa que delimite su contenido y alcance.

3.6.5Análisis interpretativo y crítico

El análisis interpretativo y crítico se enfocará en examinar sistemáticamente los criterios jurídicos utilizados para imputar responsabilidad civil a las entidades bancarias privadas en Costa Rica frente a estafas informáticas cometidas a través de sus plataformas digitales durante el período 2024.

Se empleará un enfoque cualitativo basado en la interpretación jurídica de normas, doctrinas y decisiones judiciales, con el objetivo de identificar cómo los operadores del derecho

construyen y aplican los criterios de imputación de responsabilidad civil en casos concretos. Este análisis permitirá:

- Describir y sistematizar los criterios legales y normativos aplicables a la responsabilidad civil de las entidades bancarias privadas frente a delitos informáticos, atendiendo a principios como la culpa, el riesgo y el deber de seguridad tecnológica.
- Examinar la jurisprudencia costarricense para identificar patrones interpretativos, nexos causales establecidos y mecanismos probatorios utilizados por los órganos jurisdiccionales al determinar la responsabilidad civil.
- Establecer el vínculo jurídico entre el deber de seguridad de las entidades financieras y los daños ocasionados a los usuarios mediante fraudes informáticos, incorporando la interpretación de la doctrina y las resoluciones judiciales para explicar cómo se acredita la responsabilidad civil.

3.6.6. Presentación de resultados

Los resultados se presentarán de forma temática y argumentativa, estructurados de acuerdo con los objetivos específicos de la investigación. Cada tema incluirá:

- Descripción general del criterio identificado.
- Ejemplos extraídos de la normativa, doctrina y jurisprudencia.
- Interpretación crítica que relacione los hallazgos con el contexto jurídico nacional y la protección de los usuarios de plataformas digitales.

Este procedimiento garantiza un análisis riguroso, sistemático y confiable, propio de la investigación cualitativa en el ámbito jurídico, permitiendo comprender cómo se configuran los criterios de imputación de responsabilidad civil de las entidades bancarias privadas frente a delitos de estafas informáticas en Costa Rica.

3.7 Operacionalización de Variables

La operacionalización de variables es un proceso metodológico esencial en la investigación cualitativa, ya que permite traducir conceptos abstractos en dimensiones, indicadores e instrumentos observables y medibles. Esta transformación facilita el análisis empírico de fenómenos complejos, como la responsabilidad civil de las entidades bancarias frente a delitos informáticos, al establecer criterios concretos para su estudio. A través de este proceso, se garantiza que las variables seleccionadas no solo estén teóricamente fundamentadas, sino también empíricamente verificables.

En investigaciones jurídicas de enfoque cualitativo documental, la operacionalización se realiza mediante categorías de análisis, las cuales permiten examinar de manera sistemática las fuentes normativas, doctrinales y jurisprudenciales relacionadas con el fenómeno estudiado.

En esta investigación, se identificaron:

3.7.1. Imputación de responsabilidad civil a entidades bancarias privadas

La primera variable se refiere a la imputación de responsabilidad civil de las entidades bancarias privadas cuando se producen daños patrimoniales a los usuarios del sistema financiero como consecuencia de estafas informáticas cometidas mediante el uso de plataformas digitales bancarias. Esta categoría engloba el conjunto de criterios jurídicos que permiten determinar cuándo una entidad bancaria puede ser considerada civilmente responsable por los perjuicios ocasionados a los clientes en el contexto de operaciones financieras realizadas a través de medios electrónicos.

En este sentido, la variable se centra en el análisis de los elementos jurídicos que integran la responsabilidad civil dentro del ordenamiento jurídico costarricense, tales como el factor de atribución, el nexo causal y el daño indemnizable, los cuales constituyen componentes fundamentales para establecer la obligación de reparar los daños ocasionados. A través del estudio de estos elementos se busca comprender cómo los órganos jurisdiccionales costarricenses determinan la responsabilidad de las entidades bancarias frente a fraudes informáticos que afectan las cuentas o transacciones de los usuarios.

Esta variable permite examinar, por ejemplo, los distintos criterios utilizados por los operadores jurídicos para atribuir responsabilidad a las instituciones financieras, tales como la aplicación de la culpa en la prestación del servicio bancario, la teoría del riesgo creado derivado del uso de plataformas tecnológicas y la posible aplicación de regímenes de responsabilidad objetiva o subjetiva. Asimismo, permite analizar el modo en que los órganos jurisdiccionales establecen el nexo causal entre el funcionamiento de los sistemas digitales del banco y el daño sufrido por el usuario, así como los supuestos en los que dicho vínculo puede verse interrumpido por conductas atribuibles al propio cliente.

Del mismo modo, esta variable incluye el estudio del daño indemnizable, particularmente en lo relativo a los perjuicios patrimoniales ocasionados por la sustracción de fondos mediante mecanismos de fraude informático. En este contexto, se analizan aspectos como la restitución de los montos sustraídos, la posible indemnización por daño moral y los criterios utilizados por los órganos jurisdiccionales para determinar el alcance de la reparación civil.

En consecuencia, el análisis de esta variable permite comprender cómo el derecho civil costarricense responde a los nuevos desafíos planteados por la digitalización del sistema financiero y por el incremento de los delitos informáticos que afectan a los usuarios de los servicios bancarios electrónicos.

3.7.2. Criterios legales y normativos aplicables a la responsabilidad civil bancaria

La segunda variable corresponde al conjunto de normas jurídicas que regulan la responsabilidad civil de las entidades bancarias privadas en Costa Rica frente a los daños ocasionados por estafas informáticas realizadas mediante plataformas digitales. Esta variable incluye el análisis del marco normativo civil y de la regulación bancaria vigente, con el propósito de identificar los criterios legales que permiten atribuir responsabilidad a las instituciones financieras en el contexto de los servicios bancarios electrónicos.

En primer lugar, esta variable comprende el estudio de las normas contenidas en el ordenamiento jurídico civil, particularmente aquellas relacionadas con la responsabilidad contractual y extracontractual. A partir de estas disposiciones se examinan los principios que rigen la obligación de reparar daños, los presupuestos jurídicos necesarios para configurar la responsabilidad civil y los criterios utilizados para determinar la culpa o negligencia en la prestación de servicios.

Asimismo, la variable incorpora el análisis de la regulación bancaria y financiera aplicable a las entidades bancarias privadas, la cual establece las obligaciones que deben cumplir dichas instituciones en la prestación de servicios financieros a través de medios digitales. En este ámbito se examinan disposiciones relacionadas con el deber de seguridad en las operaciones bancarias electrónicas, las obligaciones de custodia tecnológica, los mecanismos de autenticación de usuarios y los estándares de protección de la información financiera.

El análisis de esta variable permite evaluar el grado en que el marco normativo costarricense establece obligaciones claras para las entidades financieras en relación con la prevención de fraudes informáticos y la protección de los usuarios del sistema bancario digital. De igual forma, permite identificar si las normas existentes resultan suficientes para enfrentar los riesgos tecnológicos asociados al uso de plataformas electrónicas en la prestación de servicios financieros.

3.7.3. Jurisprudencia costarricense sobre fraudes informáticos en el ámbito bancario

La tercera variable corresponde al análisis de la jurisprudencia costarricense relacionada con casos de fraudes informáticos que han involucrado a entidades bancarias. Esta variable se orienta a identificar los criterios interpretativos desarrollados por los órganos jurisdiccionales nacionales al resolver controversias relacionadas con la responsabilidad civil derivada de delitos informáticos en el ámbito financiero.

En este contexto, el análisis se centra en las tendencias interpretativas presentes en las resoluciones judiciales, particularmente en lo relativo a la forma en que los jueces aplican los principios de responsabilidad civil a los casos de estafas informáticas cometidas mediante plataformas bancarias digitales. Entre los aspectos que se examinan se encuentran la reiteración de determinados criterios jurisprudenciales, la aplicación del deber de seguridad bancaria y el reconocimiento de la posición de garante de las entidades financieras frente a los usuarios del sistema bancario digital.

Asimismo, el estudio de esta variable permite identificar patrones en la argumentación judicial, así como los fundamentos jurídicos utilizados para determinar si la entidad bancaria debe asumir la responsabilidad por los daños ocasionados a los clientes. De esta manera, el análisis jurisprudencial contribuye a comprender cómo el derecho se aplica en la práctica judicial frente a los nuevos desafíos que plantea la digitalización de los servicios financieros.

3.7.4. Riesgo tecnológico y deber de seguridad en la banca digital

La cuarta variable se refiere al riesgo tecnológico asociado al uso de plataformas digitales en la prestación de servicios financieros y al deber de seguridad que recae sobre las entidades bancarias en la gestión de dichos sistemas. Esta variable parte del reconocimiento de que la digitalización del sistema bancario ha generado nuevas oportunidades para la prestación de servicios financieros, pero también ha incrementado los riesgos relacionados con la seguridad informática y la protección de los datos de los usuarios.

En este sentido, la variable analiza los elementos que contribuyen a la creación de riesgo tecnológico, tales como el uso de plataformas digitales para la realización de transacciones bancarias, los sistemas de autenticación y verificación de identidad utilizados por las entidades financieras, así como los protocolos de seguridad informática destinados a prevenir accesos no autorizados o fraudes electrónicos.

Asimismo, esta variable incluye el estudio del deber profesional reforzado que recae sobre las entidades bancarias, el cual se fundamenta en la especial posición de confianza que dichas instituciones ocupan dentro del sistema financiero. En este contexto se examinan aspectos como el estándar de diligencia exigido a las entidades financieras en la protección de los fondos de los clientes y la asimetría técnica existente entre el banco y el usuario en el manejo de sistemas tecnológicos complejos.

El análisis de esta variable permite comprender cómo el derecho aborda los riesgos derivados de la utilización de tecnologías digitales en el ámbito bancario y cuáles son las obligaciones que deben asumir las entidades financieras para garantizar la seguridad de las operaciones electrónicas.

3.7.5. Mecanismos de acreditación de la responsabilidad civil

La quinta variable corresponde a los mecanismos jurídicos que permiten acreditar la responsabilidad civil de las entidades bancarias privadas en los procesos judiciales relacionados con fraudes informáticos. Esta variable se centra principalmente en el análisis de los medios probatorios utilizados para demostrar la existencia del daño, la relación causal entre el funcionamiento de la plataforma digital y el perjuicio sufrido por el usuario, así como la eventual responsabilidad de la entidad financiera.

Dentro de esta variable se examina particularmente la dimensión relacionada con la carga de la prueba, la cual resulta fundamental para determinar cuál de las partes debe demostrar los hechos relevantes dentro del proceso judicial. En este contexto se analizan situaciones como la posible inversión de la carga probatoria en casos donde existe una evidente asimetría técnica entre el banco y el cliente, así como la utilización de pruebas periciales tecnológicas, registros electrónicos de transacciones y documentos bancarios que permitan reconstruir los hechos que dieron origen al fraude informático.

El análisis de esta variable permite comprender los criterios utilizados por los órganos jurisdiccionales para valorar la prueba en este tipo de casos y determinar si la entidad bancaria ha incumplido su deber de seguridad en la prestación de servicios financieros digitales.

En conjunto, la operacionalización de estas variables permite estructurar de manera sistemática el análisis del fenómeno jurídico objeto de estudio, facilitando la identificación de los criterios legales, doctrinales y jurisprudenciales que intervienen en la imputación de

responsabilidad civil a las entidades bancarias privadas en Costa Rica frente a delitos de estafas informáticas realizadas mediante sus plataformas digitales.

Tabla 1. Operalización De Variable

Variable	Tipo de variable	Dimensión	Indicadores	Técnica	Instrumento
Imputación de responsabilidad civil a entidades bancarias privadas	Dependiente	Factor de atribución	-Aplicación de culpa -Aplicación del riesgo creado -Responsabilidad objetiva o subjetiva	Análisis jurisprudencial	Matriz de análisis jurisprudencial con reconstrucción del caso y codificación de criterios de imputación utilizados por la Sala Primera (culpa, riesgo creado, objetividad)
		Nexo causal	- Identificación del hecho generador - Relación entre falla del sistema y daño sufrido por el usuario - Ruptura del nexo causal por conducta del usuario	Análisis jurisprudencial	Matriz de análisis jurisprudencial orientada a la reconstrucción del camino del fraude y la identificación de la ruptura del nexo causal (conducta del usuario, hecho de tercero, ajenidad del daño)
		Daño indemnizable	-Daño patrimonial -Daño moral -Restitución de fondos sustraídos	Análisis jurisprundencial	Matriz de análisis de resoluciones enfocada en la determinación del daño indemnizable, modalidades de reparación (restitución, intereses) y criterios de reconocimiento del daño moral
Criterios legales y normativos aplicables	Independiente	Marco normativo civil	-Normas sobre responsabilidad contractual	Análisis normativo	Matriz de análisis normativo con interpretación

Variable	Tipo de variable	Dimensión	Indicadores	Técnica	Instrumento
			-Normas sobre responsabilidad extracontractual		jurídica de normas civiles y de consumo aplicables a la imputación de responsabilidad bancaria
		Regulación bancaria	-Deber de seguridad en servicios financieros digitales -Normativa de supervisión financiera -Obligaciones de custodia tecnológica de las entidades bancarias	Análisis normativo	Matriz normativa orientada a identificar estándares de seguridad tecnológica y deberes regulatorios exigibles a las entidades bancarias.
Jurisprudencia costarricense sobre fraudes informáticos	Independiente	Tendencias interpretativas	- Reiteración de criterios jurisprudenciales - Aplicación del deber de seguridad bancaria - Posición de garante de la entidad financiera	Análisis jurisprudencial	Matriz de categorización jurisprudencial con identificación de patrones interpretativos y evolución del criterio de la Sala Primera en materia de fraude bancario digital
Riesgo tecnológico y deber de seguridad	Independiente	Creación de riesgo tecnológico	- Uso de plataformas digitales bancarias - Sistemas de autenticación y verificación - Protocolos de seguridad informática	Revisión documental y normativo	Matriz normativa orientada a la caracterización del riesgo tecnológico inherente a la banca digital
		Deber profesional reforzado	- Estándar de diligencia bancaria - Asimetría técnica entre cliente y banco	Análisis sistemático	Cuadro de análisis integrador sobre estándares de diligencia profesional y deber de seguridad

Variable	Tipo de variable	Dimensión	Indicadores	Técnica	Instrumento
					reforzado en servicios financieros digitales
Mecanismos de acreditación de la responsabilidad civil	Independiente	Carga de la prueba	- Inversión de la carga probatoria - Prueba pericial tecnológica - Prueba documental bancaria	Análisis jurisprudencial	Matriz de análisis probatorio basada en jurisprudencia, orientada a la valoración de prueba tecnológica (registros, IP, transacciones) y a la distribución dinámica de la carga de la prueba

3.8 Consideraciones Éticas

La presente investigación se desarrolla respetando los principios éticos aplicables a la investigación académica. Dado que el estudio se basa exclusivamente en fuentes documentales de acceso público, tales como legislación, doctrina y jurisprudencia, no se involucran participantes humanos ni se recopilan datos personales.

Asimismo, se garantizará el uso responsable de la información, citando adecuadamente las fuentes utilizadas y respetando los principios de integridad académica y propiedad intelectual.

Capítulo IV. Análisis de Datos

El presente capítulo desarrolla el análisis de la información obtenida a partir de la revisión sistemática de fuentes normativas, doctrinales y jurisprudenciales vinculadas con la responsabilidad civil de las entidades bancarias frente a estafas informáticas cometidas mediante plataformas digitales. En concordancia con el enfoque cualitativo y con el método hermenéutico definidos en el capítulo metodológico, el estudio no se orientó a una medición cuantitativa del fenómeno, sino a la identificación e interpretación de los criterios jurídicos que actualmente permiten explicar cómo se atribuye, limita o excluye la responsabilidad civil bancaria en este tipo de conflictos.

Las fuentes examinadas fueron seleccionadas por su relación directa con la responsabilidad civil bancaria, la protección del consumidor financiero, la seguridad del servicio digital y la jurisprudencia costarricense relevante sobre fraudes informáticos bancarios.

Posteriormente, la información fue organizada mediante una ficha de análisis normativo y una matriz de análisis jurisprudencial. A partir de dichos instrumentos fue posible clasificar los hallazgos en torno a cuatro categorías centrales:

- El factor de atribución de responsabilidad civil.
- El nexo causal entre el funcionamiento de las plataformas bancarias y el daño sufrido por el usuario.
- El deber de seguridad tecnológica de las entidades financieras.
- Los mecanismos probatorios utilizados para acreditar la responsabilidad civil bancaria.

Esta organización permitió advertir no solo coincidencias entre normas y resoluciones judiciales, sino también tensiones interpretativas relevantes, especialmente en lo relativo a la aplicación del artículo 35 de la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor, al alcance del deber de seguridad bancaria y al tratamiento de la conducta del usuario como posible causa de ruptura del nexo causal.

El análisis mostró, además, que la responsabilidad civil de las entidades bancarias en el entorno digital no puede comprenderse desde una única lógica. En algunos supuestos predomina una lectura basada en el incumplimiento del deber de diligencia o seguridad; en otros, el razonamiento judicial se aproxima a esquemas de responsabilidad objetiva o de riesgo creado; y, en no pocos casos, la discusión se desplaza hacia la ajenidad del daño y la conducta de la víctima.

Precisamente por ello, los resultados se presentan de forma temática, siguiendo la lógica de los objetivos específicos de la investigación y buscando responder, de manera articulada, a la pregunta central sobre cuáles son los criterios jurídicos aplicables para imputar responsabilidad civil a las entidades bancarias privadas en Costa Rica frente a las estafas informáticas realizadas a través de sus plataformas digitales.

4.1. Criterios legales y normativos aplicables a la responsabilidad civil bancaria

4.1.1. Fundamento constitucional y civil de la tutela del usuario financiero

Uno de los primeros resultados que arroja el análisis normativo es que la imputación de responsabilidad civil a las entidades bancarias no descansa en una única disposición, sino en un entramado normativo de distinta jerarquía. En la base constitucional se encuentra el artículo 46 de la Constitución Política, que reconoce el derecho de los consumidores y usuarios a la protección de sus intereses económicos y a recibir información adecuada y veraz. Aunque se trata de una cláusula general, su importancia en el ámbito financiero es evidente: la actividad bancaria se desarrolla en un espacio marcado por la confianza, la complejidad técnica y una clara asimetría entre quien presta el servicio y quien lo utiliza. Desde esa perspectiva, la protección constitucional del consumidor no se agota en la publicidad o en el deber de información, sino que se proyecta también sobre la seguridad del servicio prestado.

A ello se suma el régimen general de responsabilidad civil previsto en el Código Civil costarricense, particularmente en su artículo 1045, que establece la obligación de reparar el daño causado por dolo, culpa, negligencia o imprudencia. Aunque esta norma responde a la estructura clásica de la responsabilidad civil subjetiva, sigue siendo relevante en materia bancaria porque permite valorar si la entidad incurrió en una conducta negligente al diseñar, operar o supervisar sus plataformas digitales. En otras palabras, incluso cuando el fraude es materialmente ejecutado por un tercero, la discusión civil puede orientarse a determinar si el banco omitió medidas razonables de seguridad o si actuó por debajo del estándar de diligencia exigible a un operador profesional.

En este punto resulta importante destacar que la actividad bancaria, por su propia naturaleza, no puede equipararse a cualquier otra actividad económica. La entidad financiera administra recursos ajenos, opera mediante sistemas altamente tecnificados y presta un servicio cuya falla puede producir efectos patrimoniales inmediatos y severos en la esfera del usuario. Por ello, la exigencia de diligencia no puede medirse con el patrón ordinario del buen padre de familia,

sino con uno agravado o profesional, acorde con el nivel de especialización de la actividad. Esta idea se encuentra ampliamente respaldada en la doctrina contemporánea sobre responsabilidad profesional y servicios financieros, la cual subraya que, cuando una organización desarrolla actividades complejas y obtiene beneficio económico de ellas, asume también deberes reforzados de prevención y control del riesgo. (Díez-Picazo, 1999) (Pantaleón, 1991)

4.1.2. La protección del consumidor financiero como eje del análisis

La segunda línea normativa que emerge con claridad en el estudio corresponde al derecho del consumidor. La Ley No. 7472 permite ubicar al usuario de servicios bancarios dentro de la categoría de consumidor financiero, lo cual tiene consecuencias jurídicas decisivas. El artículo 32 reconoce derechos fundamentales e irrenunciables del consumidor; el artículo 34 impone deberes concretos al proveedor, especialmente en materia de información, advertencia y cumplimiento de estándares técnicos; el artículo 35 regula el régimen de responsabilidad por daños derivados del bien o servicio; y el artículo 72 refuerza el carácter de orden público de la ley, impidiendo que cláusulas contractuales, reglamentos internos o condiciones de uso desplacen la protección mínima legal.

Este hallazgo tiene especial importancia para la presente investigación, porque permite analizar los fraudes informáticos bancarios no solo desde la óptica del incumplimiento contractual o del ilícito civil clásico, sino también desde la lógica protectora del derecho del consumo. En otras palabras, el banco deja de aparecer únicamente como deudor de una prestación financiera y pasa a ser examinado como proveedor de un servicio que debe reunir condiciones de seguridad, información suficiente y mecanismos adecuados de atención al usuario. Esto modifica de manera sensible la estructura del análisis, pues desplaza el centro de gravedad desde la culpa individual del banco hacia la evaluación del servicio que la entidad ha puesto en circulación y de los riesgos que ese servicio genera para sus usuarios.

En este marco, el artículo 35 de la Ley 7472 adquiere una relevancia particular. El texto legal establece que el productor, proveedor y comerciante deben responder concurrente e independientemente de la existencia de culpa cuando el consumidor resulte perjudicado por razón del bien o servicio, por informaciones inadecuadas o insuficientes sobre ellos o por su utilización y riesgos, liberándose únicamente quien logre demostrar que ha sido ajeno al daño. Esta formulación ha servido a la jurisprudencia costarricense como punto de apoyo para construir un régimen de imputación más cercano al riesgo del servicio que al modelo clásico de culpa probada.

No obstante, como se verá más adelante, la práctica judicial no ha sido uniforme: en algunos casos la Sala Primera ha enfatizado el riesgo creado y la posición técnica del banco; en otros, ha puesto el acento en la conducta del usuario y en la ruptura del nexo causal.

Conviene subrayar, además, que la lectura del artículo 35 no puede hacerse de manera aislada. Su sentido se ve reforzado por el artículo 34, que exige al proveedor informar adecuadamente sobre el uso y riesgos del servicio, y por el artículo 72, que impide relativizar esas obligaciones mediante cláusulas contractuales predispuestas. Por ello, en el ámbito de la banca digital, la obligación de seguridad no se limita a disponer de una plataforma funcional; también comprende el deber de educar al usuario, advertirle sobre riesgos previsibles y facilitar vías oportunas de reclamo cuando se produce un incidente. Desde una mirada metodológica, esta conclusión es relevante porque muestra que el análisis de la responsabilidad bancaria no debe limitarse al momento del daño, sino abarcar también el diseño preventivo del servicio.

4.1.3. Regulación prudencial y seguridad de datos

El estudio normativo también permitió identificar un tercer bloque de regulación, integrado por normas prudenciales y técnicas que, aunque no pertenecen al derecho civil en sentido estricto, sí resultan indispensables para definir el estándar de conducta exigible a las entidades bancarias. En este punto cobran especial importancia la Ley Reguladora del Mercado de Valores y la Ley Orgánica del Banco Central, en cuanto atribuyen al CONASSIF y a la SUGEF competencias para dictar normativa aplicable a las entidades supervisadas. Esto significa que las obligaciones de gobierno tecnológico, control de riesgos y transparencia frente al usuario financiero no son simples recomendaciones operativas, sino parámetros jurídicamente relevantes en la evaluación de la diligencia bancaria.

Dentro de este bloque, el Acuerdo SUGEF 10-07 adquiere especial importancia por cuanto incorpora reglas orientadas a prevenir y mitigar estafas informáticas contra usuarios financieros. Su capítulo III introduce, precisamente, aspectos mínimos de control vinculados con información al usuario, medidas de prevención, atención de reclamos y gestión del riesgo de fraude. Por su parte, el Acuerdo CONASSIF 5-24 establece lineamientos de gobierno y gestión de tecnología de información, lo que incluye la administración de riesgos tecnológicos y la implementación de controles de seguridad. En conjunto, ambas normas permiten concretar el contenido del deber de seguridad tecnológica que, de otro modo, podría quedar formulado de manera demasiado abierta o abstracta.

En una línea complementaria, la Ley N°8968, relativa a la protección de datos personales, también aporta un elemento relevante al análisis. Si bien no fue concebida específicamente para el sector bancario, su principio de seguridad obliga a quienes administran bases de datos a adoptar medidas técnicas y organizativas destinadas a impedir accesos no autorizados, alteraciones o pérdidas de información. Dado que las entidades financieras gestionan datos personales, financieros y transaccionales de alta sensibilidad, esta ley refuerza la idea de que la seguridad informática forma parte del contenido jurídico de la actividad bancaria y no constituye un aspecto meramente accesorio.

Finalmente, el análisis normativo permitió advertir que muchas de las estafas informáticas estudiadas se materializan mediante transferencias electrónicas y otros movimientos procesados a través del sistema nacional de pagos. Por ello, más que hablar de una ley aislada del sistema de pagos, resulta más preciso referirse al marco regulatorio integrado por la Ley Orgánica del Banco Central y el Reglamento del Sistema de Pagos. Este marco confirma que el sistema debe operar bajo parámetros de seguridad, eficiencia y confiabilidad, lo que vuelve jurídicamente relevante cualquier discusión sobre trazabilidad de transferencias, monitoreo de operaciones y prevención de movimientos atípicos.

4.1.4. La dimensión penal del fenómeno y la evolución normativa posterior

El análisis de la normativa no estaría completo sin la dimensión penal del fenómeno. El artículo 217 bis del Código Penal tipifica la estafa informática y permite delimitar el hecho ilícito generador del daño patrimonial que luego da lugar a la discusión civil. En esa misma dirección, la Ley No. 9048 reforzó la protección penal frente al uso indebido de tecnologías digitales para la realización de fraudes, daños informáticos y otras conductas relacionadas. Este componente es importante porque muestra que el ordenamiento costarricense reconoce la especificidad del fraude cometido mediante medios tecnológicos y, por tanto, la necesidad de abordarlo con herramientas jurídicas diferenciadas.

En este sentido, el estudio identificó una evolución normativa posterior especialmente significativa en el expediente legislativo No. 23.908, relativo a la protección de las personas consumidoras en la custodia de su dinero. Aunque este proyecto no forma parte del derecho vigente aplicable al período 2024, su contenido es útil como elemento de contexto porque revela una tendencia clara hacia el reforzamiento de la responsabilidad de las entidades financieras, la inversión de la carga de la prueba en ciertos conflictos y la exigencia de protocolos más estrictos

de prevención y restitución. Metodológicamente, sin embargo, debe ser tratado como referente de evolución normativa posterior, no como base directa del análisis del período de estudio.

4.1.5. Daño indemnizable en casos de fraude informático bancario

Otro aspecto que debe incorporarse dentro del análisis normativo de la responsabilidad civil bancaria es el relativo al daño indemnizable, en tanto constituye uno de los elementos esenciales de toda pretensión resarcitoria. En los casos de estafas informáticas cometidas a través de plataformas bancarias digitales, el daño que con mayor frecuencia se presenta es de naturaleza patrimonial, pues se manifiesta en la sustracción de fondos, la realización de transferencias no autorizadas, la disposición ilegítima de recursos depositados en cuenta o la generación de cargos derivados de operaciones fraudulentas.

Desde esta perspectiva, la consecuencia jurídica más inmediata, cuando se acredita la responsabilidad de la entidad bancaria, consiste en la restitución de los montos sustraídos, junto con los intereses correspondientes. Esta forma de reparación responde a la lógica de la reparación integral del daño, en virtud de la cual se procura restablecer la situación patrimonial del usuario al estado en que se encontraba antes de la ocurrencia del hecho dañoso. En la jurisprudencia analizada, este criterio se refleja con claridad, como puede observarse en el apéndice C., resoluciones como la sentencia 01477-2011 en la cual se ordenó el reintegro de los fondos debitados indebidamente, la sentencia 01701-2025, donde además de la restitución del monto sustraído se reconocieron intereses y otros rubros resarcitorios y en la sentencia 00778-2012 donde se reconoce la restitución, intereses y costas.

Ahora bien, junto al daño patrimonial, también es posible advertir la eventual existencia de daño moral, aunque su reconocimiento en este tipo de procesos no resulta frecuente. Ello obedece a que los tribunales costarricenses suelen exigir una acreditación específica de la afectación extrapatrimonial sufrida por la víctima, de manera que no basta con afirmar la existencia de angustia, preocupación o inseguridad derivadas del fraude, sino que es necesario demostrar la entidad real del perjuicio. Por esta razón, el daño moral mantiene un carácter más restringido dentro de la práctica judicial, aunque no queda excluido de manera absoluta. La sentencia 01701-2025 constituye un ejemplo relevante, en tanto evidencia que este rubro puede ser reconocido cuando las circunstancias del caso y la prueba aportada permiten justificarlo.

En cuanto a los criterios de cuantificación del daño, se observa que los tribunales recurren principalmente a elementos objetivos derivados de la prueba documental y tecnológica, tales como

estados de cuenta, registros de transacciones, comprobantes de transferencias y demás documentos bancarios que permitan establecer con precisión el monto de la pérdida sufrida. De este modo, la cuantificación del daño patrimonial tiende a apoyarse en parámetros verificables y concretos. En cambio, cuando se analiza el daño moral, la determinación del monto indemnizable depende de una valoración prudencial del juzgador, quien debe atender las particularidades del caso, la intensidad de la afectación y la suficiencia de la prueba rendida.

Por otra parte, también debe señalarse que, cuando no se logra establecer la responsabilidad civil de la entidad bancaria —ya sea por ruptura del nexo causal, por culpa de la víctima o por acreditación de ajenidad del daño— no procede el reconocimiento de indemnización, como se puede desprender de la sentencia 0460-2017 y 00040-2025, donde no se reconoce indemnización alguna, al considerarse que el daño no es imputable al banco.

Ahora bien, lo anterior, pone de manifiesto que el análisis del daño indemnizable no puede separarse de la imputación jurídica del hecho, pues la reparación solo resulta procedente cuando el perjuicio puede atribuirse válidamente a la conducta, al riesgo o al incumplimiento imputable a la entidad financiera.

En consecuencia, el estudio del daño indemnizable permite advertir que la discusión sobre responsabilidad civil bancaria frente a estafas informáticas no se limita a determinar quién debe responder, sino que también exige precisar cómo debe repararse el perjuicio ocasionado. En este ámbito, la restitución de fondos constituye la manifestación más frecuente del resarcimiento, mientras que el daño moral mantiene una aplicación más excepcional y sujeta a una acreditación rigurosa dentro del proceso judicial.

Por otro lado, a partir de los elementos normativos expuestos, se sistematiza seguidamente el marco jurídico aplicable mediante la siguiente matriz de análisis normativo.

Tabla 2. Matriz de normativa

Nombre de la norma	**Artículo**	**Contenido relevante**	**Interpretación jurídica**	**Relación con la responsabilidad bancaria**	**Observaciones**
Constitución Política de Costa Rica	Artículo 46	Reconoce el derecho de los consumidores y usuarios a la	Constituye el fundamento constitucional de la protección	En el ámbito bancario, este artículo respalda la exigencia de	Funciona como base constitucional para interpretar

Nombre de la norma	Artículo	Contenido relevante	Interpretación jurídica	Relación con la responsabilidad bancaria	Observaciones
		protección de sus intereses económicos y a recibir información adecuada y veraz sobre los bienes y servicios que se ofrecen en el mercado.	al consumidor en Costa Rica y establece el deber del Estado de garantizar condiciones de equilibrio entre consumidores y proveedores.	que las entidades financieras brinden servicios seguros, transparentes y con información clara sobre los riesgos asociados al uso de plataformas digitales.	la responsabilidad civil bancaria desde la protección del consumidor financiero.
Código Civil de Costa Rica	Artículo 1045	Establece que toda persona que cause daño a otra por dolo, culpa o negligencia está obligada a repararlo. Este artículo constituye la base del régimen general de responsabilidad civil extracontractual	Consagra el principio general de responsabilidad civil, según el cual la producción de un daño antijurídico genera la obligación de indemnizar cuando exista culpa, negligencia o	Permite analizar si la entidad bancaria incurrió en negligencia o incumplimiento del deber de diligencia en la gestión de sus plataformas digitales, lo que podría generar responsabilidad civil frente a los usuarios afectados por	Es la norma base para analizar los elementos clásicos de la responsabilidad civil: daño, culpa, nexo causal y obligación de reparar.

Nombre de la norma	Artículo	Contenido relevante	Interpretación jurídica	Relación con la responsabilidad bancaria	Observaciones
		en el ordenamiento jurídico costarricense.	dolo por parte del responsable.	estafas informáticas.	
Código Civil de Costa Rica	Art. 702	Reconoce la responsabilidad contractual, por el incumplimiento de la obligación existe el deber de responder por los daños y perjuicios, salvo que la falta provenga del acreedor, fuerza mayor o caso fortuito.	Establece un régimen de responsabilidad contractual basado en el incumplimiento, donde surge la obligación de indemnizar siempre que exista daño y nexo causal, salvo que el deudor pruebe una causa eximente.	En el ámbito bancario, el banco actúa como deudor de una obligación de custodia y seguridad sobre los fondos del cliente. Su responsabilidad surge cuando se acredita un incumplimiento de ese deber (por ejemplo, fallas en seguridad), pero puede exonerarse si demuestra culpa del usuario, hecho de tercero o ajenidad del daño.	Este artículo se articula con la lógica jurisprudencial analizada, donde la Sala Primera exige la prueba del nexo causal y admite eximentes como la culpa de la víctima o el hecho de tercero. Aunque el régimen bancario tiende hacia la objetivación (art. 35 Ley del Consumidor), el 702 sigue siendo base para entender la imputación y las

Nombre de la norma	Artículo	Contenido relevante	Interpretación jurídica	Relación con la responsabilidad bancaria	Observaciones
					causas de exclusión de responsabilidad.
Ley No. 7472: Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor	Artículo 32	Reconoce derechos fundamentales e irrenunciables del consumidor, incluyendo la protección de sus intereses económicos y el acceso a mecanismos de tutela administrativa y judicial para la defensa de sus derechos.	Define al consumidor como sujeto protegido dentro de las relaciones de mercado, estableciendo garantías frente a posibles abusos o desequilibrios en la relación con los proveedores.	Permite considerar al usuario de servicios bancarios como consumidor financiero, lo que habilita la aplicación del régimen de protección al consumidor frente a fraudes en plataformas digitales.	Refuerza la posibilidad de analizar los conflictos derivados de estafas informáticas desde la perspectiva del derecho del consumidor.
Ley No. 7472	Artículo 34	Establece las obligaciones del comerciante o proveedor, incluyendo el deber de suministrar información adecuada sobre	Impone deberes de información, advertencia y seguridad en la prestación de servicios, particularmente cuando el uso del producto o	En el ámbito financiero digital, implica que las entidades bancarias deben informar a los usuarios sobre los riesgos asociados al uso	Permite vincular el deber de seguridad bancaria con la obligación de informar adecuadamente

Nombre de la norma	Artículo	Contenido relevante	Interpretación jurídica	Relación con la responsabilidad bancaria	Observaciones
		el uso de los bienes o servicios, advertir sobre riesgos previsibles y cumplir normas técnicas y de calidad.	servicio pueda generar riesgos para el consumidor.	de plataformas electrónicas y adoptar medidas para prevenir fraudes informáticos.	sobre riesgos tecnológicos.
Ley No. 7472	Artículo 35	Establece un régimen de responsabilidad para productores, proveedores y comerciantes por los daños ocasionados al consumidor derivados del bien o servicio ofrecido o de la información proporcionada. Solo se libera quien demuestre ser ajeno al daño.	Introduce un régimen de responsabilidad que puede interpretarse bajo criterios de responsabilidad objetiva o responsabilidad basada en el riesgo creado en las relaciones de consumo.	Constituye la principal base normativa para analizar la responsabilidad civil de las entidades bancarias cuando se producen daños derivados del uso de plataformas digitales o de fallas en la prestación del servicio financiero.	Es la norma central para el análisis de imputación de responsabilidad civil en servicios bancarios digitales.

Nombre de la norma	Artículo	Contenido relevante	Interpretación jurídica	Relación con la responsabilidad bancaria	Observaciones
Ley No. 7472	Artículo 72	Establece que las disposiciones de esta ley son de orden público y prevalecen sobre prácticas comerciales o cláusulas contractuales en contrario.	Impide que los proveedores limiten o excluyan los derechos del consumidor mediante contratos de adhesión o reglamentos internos.	En materia bancaria, evita que cláusulas contractuales o condiciones de uso de plataformas digitales excluyan la responsabilidad del banco frente a daños ocasionados a los usuarios.	Refuerza el carácter imperativo de la protección del consumidor financiero.
Ley Reguladora del Mercado de Valores No. 7732	Artículo 171 inciso b	Establece que el Consejo Nacional de Supervisión del Sistema Financiero (CONASSIF) tiene la facultad de aprobar las normas necesarias para la regulación, supervisión y fiscalización de	Reconoce la potestad normativa del CONASSIF para emitir regulaciones que orienten el funcionamiento del sistema financiero y la supervisión de las entidades financieras.	Permite justificar la obligatoriedad de las normas prudenciales emitidas por el CONASSIF y la SUGEF en materia de gestión de riesgos tecnológicos y seguridad informática.	Vincula la regulación prudencial con la evaluación del deber de diligencia de las entidades bancarias.

Nombre de la norma	Artículo	Contenido relevante	Interpretación jurídica	Relación con la responsabilidad bancaria	Observaciones
		las entidades financieras.			
Ley Orgánica del Banco Central de Costa Rica No. 7558	Artículo 131 inciso c	Establece que el Superintendente General de Entidades Financieras puede proponer al CONASSIF las normas necesarias para la supervisión del sistema financiero.	Define el marco institucional para la emisión de normativa técnica orientada a garantizar la estabilidad y seguridad del sistema financiero.	Refuerza la importancia de las regulaciones técnicas emitidas por la SUGEF en materia de seguridad informática y gestión de riesgos tecnológicos.	Complementa la base jurídica del sistema de supervisión financiera en Costa Rica.
Ley No. 8968: Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales	Artículo 4	Establece el principio de seguridad de los datos personales, obligando a los responsables de bases de datos a adoptar medidas técnicas y organizativas que garanticen la protección de la información	Impone a las entidades que administran información personal el deber de implementar medidas de seguridad adecuadas para proteger los datos que gestionan.	En el ámbito bancario, esta norma resulta relevante porque las entidades financieras administran grandes volúmenes de datos personales y financieros de los usuarios, por lo que la falta de medidas de	Refuerza el deber de seguridad tecnológica de las entidades bancarias y su responsabilidad en la protección de la información de los clientes.

Nombre de la norma	Artículo	Contenido relevante	Interpretación jurídica	Relación con la responsabilidad bancaria	Observaciones
		frente a accesos no autorizados, alteraciones o pérdidas.		seguridad adecuadas podría facilitar fraudes informáticos o accesos no autorizados a cuentas bancarias.	
Acuerdo SUGEF 10-07: Reglamento sobre la Transparencia ante el Usuario Financiero	Capítulo III	Establece aspectos mínimos de control para prevenir y mitigar estafas informáticas contra los usuarios financieros, incluyendo mecanismos de información, prevención y atención de reclamos.	Introduce obligaciones regulatorias específicas relacionadas con la prevención de fraudes digitales y la protección del usuario financiero.	Permite evaluar si las entidades bancarias cumplen con controles preventivos, detectivos y correctivos para evitar estafas informáticas en plataformas digitales.	Es una norma clave para el análisis del deber de seguridad tecnológica en el sistema financiero.
Acuerdo CONASSIF 5-24:	Reglamento general	Establece lineamientos para el gobierno	Define estándares mínimos de	Permite determinar si la entidad bancaria	Refuerza la relación entre riesgo

Nombre de la norma	Artículo	Contenido relevante	Interpretación jurídica	Relación con la responsabilidad bancaria	Observaciones
Reglamento General de Gobierno y Gestión de la Tecnología de Información		y la gestión de la tecnología de información y la administración de riesgos tecnológicos en entidades financieras supervisadas.	gestión tecnológica, control de riesgos y seguridad informática dentro del sistema financiero costarricense.	implementó controles tecnológicos adecuados para prevenir accesos no autorizados o fraudes informáticos.	tecnológico y responsabilidad civil bancaria.
Código Penal de Costa Rica	Artículo 217 bis	Tipifica la estafa informática, sancionando el uso de medios informáticos o telemáticos para ejecutar maniobras fraudulentas que produzcan un beneficio patrimonial indebido.	Define jurídicamente el fenómeno del fraude informático y establece su tratamiento penal dentro del ordenamiento jurídico costarricense.	Permite identificar el hecho ilícito que origina el daño patrimonial al usuario bancario y que puede generar responsabilidad civil.	Conecta la dimensión penal del fraude con la responsabilidad civil derivada del daño.
Ley No. 9048 (Reforma de delitos informáticos)	Reformas al Código Penal	Introduce y actualiza los delitos informáticos en	Refuerza la protección penal frente al uso indebido de	Permite contextualizar jurídicamente el aumento de	

Nombre de la norma	Artículo	Contenido relevante	Interpretación jurídica	Relación con la responsabilidad bancaria	Observaciones
		el Código Penal costarricense, incluyendo fraude informático, suplantación de identidad digital y daño informático.	tecnologías digitales para cometer fraudes o estafas.	delitos informáticos vinculados a servicios financieros digitales.	
Proyecto de Ley No. 23.908: Protección a las personas consumidoras en la custodia de su dinero	Proyecto legislativo	Propone fortalecer la responsabilidad de las entidades financieras frente a la sustracción de fondos derivada de fraudes electrónicos y establecer procedimientos claros para la atención de reclamaciones.	Refleja una tendencia legislativa hacia una mayor protección del consumidor financiero y hacia la inversión de la carga de la prueba en conflictos derivados de fraudes electrónicos.	Refuerza el principio de responsabilidad de las entidades financieras en la custodia del dinero de los usuarios y establece mecanismos de restitución de fondos.	No forma parte del derecho vigente para el período 2024, pero es relevante como evolución normativa.

Nota: Hernández, 2026

4.2. Análisis jurisprudencial sobre fraudes informáticos en el ámbito bancario

De acuerdo con la sistematización realizada en la matriz jurisprudencial apéndice A y B, se evidenció que la construcción judicial de la responsabilidad civil bancaria ha sido progresiva y,

a la vez, oscilante. Las primeras resoluciones analizadas, particularmente 01477-2011 y 00778-2012 emitidas por la Sala Primera de la Corte Suprema de Justicia, reflejan una línea favorable a una comprensión intensa del riesgo creado por la banca electrónica. En estos casos, la Sala Primera consideró que la entidad financiera debía responder cuando no lograba acreditar suficientemente que el daño había sido producido por una causa enteramente ajena a su esfera de control. Se trataba de supuestos en los que la operación fraudulenta ocurría dentro del canal digital ofrecido por el banco, sin que este pudiera demostrar, con la claridad exigida, una eximente suficiente.

Estas resoluciones permiten identificar dos ideas de fondo. La primera, que la actividad bancaria digital genera un riesgo que no puede trasladarse íntegramente al usuario. La segunda, que la entidad financiera, por su posición técnica y organizativa, está en mejores condiciones para explicar cómo ocurrió la operación fraudulenta, cuáles controles existían y si el sistema presentaba o no vulnerabilidades relevantes.

En esa línea, la sentencia No. 00778-2012 resulta particularmente relevante, ya que establece que la actividad bancaria, como actividad lucrativa, implica la asunción de riesgos, introduciendo además la lógica de la carga dinámica de la prueba, lo que obliga al banco a demostrar la ajenidad del daño, al igual que en la sentencia No. 01477-2011, la Sala atribuye responsabilidad al banco por fallas en sus protocolos de seguridad, configurando un supuesto claro de responsabilidad por incumplimiento del deber de seguridad. Asimismo, en la sentencia No. 00970-2014 se consolida el criterio de imputación por riesgo tecnológico, reconociendo que la entidad asume los riesgos derivados del uso de plataformas digitales, incluso cuando no ejerce un control absoluto sobre el canal de acceso. En ese sentido, estas decisiones no solo desarrollan una lectura del riesgo creado, sino también una aproximación a la carga dinámica de la prueba. Sin embargo, del análisis de la matriz jurisprudencial se evidencia que el régimen de responsabilidad objetiva no se aplica de manera automática, sino que se encuentra condicionado al examen del caso en concreto.

En efecto, a partir de las sentencias posteriores, como 00686-2014, 00970-2014, 00460-2017, 02190-2020 y 02056-2022, se observa un giro interpretativo importante. En ellas, la Sala Primera empezó a otorgar un peso decisivo a la conducta del usuario (culpa de la víctima), especialmente cuando este revelaba claves, tokens, códigos dinámicos o cualquier otra información sensible a terceros.

Ahora bien, este criterio que recurre a la culpa de la víctima como fundamento para romper el nexo causal, permite observar que, a partir, del análisis de la matriz jurisprudencial apéndice A y B, la Sala Primera, al examinar la conducta del usuario, parte de un estándar de diligencia media, que supone un nivel general de conocimiento, atención y cuidado por parte del consumidor financiero.

Lo cual se refleja en diferentes sentencias en las que la entrega de credenciales o el acceso a entornos fraudulentos se consideran suficientes para atribuir el daño al propio usuario. Como por ejemplo, en la sentencia No. 00686-2014, donde el ingreso a una página web falsa fue determinante para excluir la responsabilidad del banco, y en la sentencia No. 00460-2017, en la que se atribuye el resultado a una deficiente custodia de las credenciales. En la misma línea, la sentencia No. 02190-2020 establece que la entrega de claves, aun mediando engaño, constituye una conducta imputable al cliente. Asimismo, la sentencia No. 00040-2025 mantiene este enfoque al señalar que, cuando el fraude se realiza con datos legítimos obtenidos mediante ingeniería social, el daño se considera ajeno a la esfera de control del banco.

Sin embargo, el análisis de los casos también muestra que los fraudes informáticos actuales no siempre responden a descuidos simples. Con frecuencia intervienen técnicas de ingeniería social más elaboradas, que incluyen la simulación de comunicaciones oficiales, la creación de situaciones de urgencia o la construcción de escenarios diseñados para inducir confianza en el usuario. Esto se aprecia, por ejemplo, en la sentencia No. 01493-2025, donde el fraude se ejecuta mediante acceso remoto tras un proceso de manipulación, o en la sentencia No. 01456-2025, en la que el usuario es inducido a error a través de correos electrónicos que replican comunicaciones del banco.

Bajo este contexto, en la doctrina se ha incorporado la figura del consumidor hipervulnerable para describir situaciones en las que el usuario, aun siendo jurídicamente capaz, enfrenta riesgos tecnológicos que lo colocan en una posición de desventaja frente a esquemas de fraude cada vez más complejos. Esta situación se relaciona con la asimetría técnica y cognitiva entre el consumidor y los sistemas digitales, así como con la evolución de las estrategias utilizadas para obtener acceso indebido a la información.

Desde esta perspectiva, el estándar de diligencia media no puede aplicarse de forma uniforme sin atender a las circunstancias concretas en que ocurre el fraude. En particular, cuando intervienen técnicas de ingeniería social avanzadas, la valoración de la conducta del usuario

requiere considerar el contexto en el que se produjo la interacción y las características del mecanismo de engaño utilizado.

Esta aproximación más contextual ya se refleja en algunas resoluciones en las que, pese a la intervención de terceros, la Sala opta por mantener el nexo causal. En la sentencia No. 01307-2023, por ejemplo, se valora que la conducta del usuario era consistente con su patrón habitual, desplazando el análisis hacia la capacidad del banco para detectar operaciones atípicas. De manera similar, en la sentencia No. 01701-2025, las transferencias realizadas desde una dirección IP extranjera sin la activación de alertas o controles reforzados, evidencian una deficiencia en la gestión del riesgo por parte del banco.

Este tipo de situaciones pone de manifiesto que la intervención de un tercero no basta, por sí sola, para excluir la responsabilidad bancaria; lo determinante es establecer si dicho hecho puede considerarse verdaderamente ajeno al riesgo propio del servicio o si, por el contrario, se inscribe dentro del ámbito de riesgo que la propia actividad bancaria digital introduce y debe gestionar. Asimismo, en la resolución No. 01477-2011, la existencia de fallas en los protocolos de seguridad fundamenta la imputación de responsabilidad al banco.

En ese sentido, el análisis de la matriz jurisprudencial derivada del apéndice b, permite identificar que la determinación del nexo causal no se agota en verificar si el usuario proporcionó información sensible. Resulta necesario examinar las condiciones en que dicha información fue obtenida, distinguiendo entre supuestos de descuido evidente y situaciones en las que la conducta del usuario se produce en un contexto de manipulación que forma parte del riesgo propio del servicio digital.

De forma que la jurisprudencia más reciente revela una evolución hacia criterios menos lineales y más atenta a las particularidades de cada caso. Las resoluciones 01307-2023, 01892-2023, 00926-2024, 00040-2025, 01456-2025 y 01493-2025 ya no se limitan a afirmar o negar la responsabilidad objetiva en abstracto, sino que examinan con mayor detalle la secuencia del fraude, la forma en que el tercero obtuvo acceso, la existencia de patrones transaccionales atípicos, la reacción del banco y la prueba tecnológica disponible. En estas decisiones, la Sala parece abandonar cualquier automatismo y prefiere resolver a partir de una ponderación concreta entre la gestión del riesgo por parte del banco y la conducta desplegada por el usuario.

En ese contexto, se trae de nuevo a colación la resolución 00040-2025 que resulta particularmente ilustrativa porque explicita que la Sala se ha orientado hacia un análisis del caso

concreto y de la prueba, más que hacia una aplicación tajante de la responsabilidad objetiva en relaciones de consumo financiero. Esto no equivale a negar el valor del artículo 35 de la Ley 7472, sino a admitir que su aplicación exige valorar si la entidad realmente puede ser considerada jurídicamente vinculada al daño producido, o si, por el contrario, la prueba demuestra que el daño provino de una actuación ajena y decisiva del propio usuario o de un tercero.

De forma global, el análisis jurisprudencial permite identificar tres patrones interpretativos. El primero es la existencia de una base judicial que reconoce la relevancia del riesgo creado y del deber reforzado de seguridad bancaria. El segundo es la consolidación de la culpa de la víctima como causal de ruptura del nexo causal en supuestos de revelación de credenciales o uso imprudente de los canales digitales. El tercero, más reciente, es una tendencia casuística y probatoria, en la que la responsabilidad ya no se decide desde fórmulas abstractas, sino a partir de la reconstrucción precisa del hecho fraudulento y de la valoración del cumplimiento o incumplimiento de deberes concretos por parte del banco.

Tabla 3. Matriz de categorización jurisprudencial

Sentencia	Tribunal	Año	Hechos relevantes	Tipo de fraude	Factor de atribución	Nexo causal	Daño indemnizable	Criterio jurídico aplicado	Deber de seguridad y riesgo tecnológico	Criterio de responsabilidad	Prueba valorada	Decisión	Observaciones
01477-2011	Sala Primera Corte Suprema de Justicia	2011	Empresa demandó al banco por débitos no autorizados en cuentas empresariales debido a fallas en el protocolo de seguridad bancaria.	Fraude electrónico mediante operaciones no autorizadas	Responsabilidad objetiva bancaria, con apoyo en la teoría del riesgo creado	Se estableció vínculo entre fallas del sistema de seguridad y la sustracción de fondos	Restitución de fondos sustraídos	Deber de seguridad bancaria y responsabilidad por riesgo creado	Se reconoce un deber reforzado de seguridad en servicios bancarios digitales, dada la posición técnica y organizativa superior del banco frente al cliente.	Responsabilidad objetiva bancaria	Documentación bancaria y registros de transacciones	Se declara con lugar la demanda y se ordena reintegro de fondos	Reconoce deber reforzado de seguridad en servicios bancarios
00778-2012	Sala Primera Corte Suprema de Justicia	2012	Cliente sufrió ocho transferencias no autorizadas desde su cuenta mediante internet banking desde una dirección IP extranjera.	Fraude electrónico en banca en línea	Responsabilidad objetiva con redistribución de la carga probatoria	El tribunal consideró que la actividad bancaria crea un riesgo para los usuarios y que el banco debía demostrar su ajenidad al daño.	Restitución e intereses	Art. 35 Ley de Protección al Consumidor	El banco aparece como garante de un sistema seguro y de controles eficaces frente a operaciones atípicas o riesgos previsibles.	Responsabilidad objetiva con redistribución de carga probatoria	Informes bancarios y registros del sistema	Se condenó al banco a reintegrar las sumas sustraídas e intereses.	Sentencia relevante sobre carga probatoria en fraude bancario

Sentencia	Tribunal	Año	Hechos relevantes	Tipo de fraude	Factor de atribución	Nexo causal	Daño indemnizable	Criterio jurídico aplicado	Deber de seguridad y riesgo tecnológico	Criterio de responsabilidad	Prueba valorada	Decisión	Observaciones
00686-2014	Sala Primera Corte Suprema de Justicia	2014	Cliente del Banco de Costa Rica sufrió transferencias electrónicas no autorizadas por aproximadamente ₡3.700.000 tras ingresar a una página falsa del banco donde introdujo todos los datos de su clave dinámica.	Phishing / pharming	Régimen objetivo en la relación de consumo, pero con eximente por culpa de la víctima	Se determinó que el usuario ingresó voluntariamente sus datos en una página fraudulenta, lo que constituye culpa de la víctima y hecho de tercero, rompiendo el nexo causal.	No se reconoció indemnización	Responsabilidad objetiva del proveedor en relación de consumo	El deber de seguridad del banco no se consideró infringido porque no se acreditó vulneración del sistema, sino un engaño exitoso al usuario.	Culpa de la víctima como eximente	Registros de navegación y sistema de seguridad bancaria	Se rechaza la responsabilidad del banco al acreditarse eximente de responsabilidad por culpa del usuario.	Caso paradigmático sobre ruptura del nexo causal por conducta del usuario
00970-2014	Sala Primera Corte Suprema de Justicia	2014	Empresa cliente denunció transferencias electrónicas no autorizadas desde su cuenta bancaria mediante internet banking por un monto cercano a ₡3.652.000. Alegó posible suplantación de identidad mediante phishing	Phishing o suplantación de identidad en banca electrónica	Responsabilidad objetiva en servicios financieros, pero con análisis de conducta del usuario y suficiencia probatoria	El tribunal consideró que las transacciones se realizaron con las credenciales correctas y que no se probó una falla del sistema del banco.	No se reconoció indemnización	Análisis de responsabilidad objetiva por riesgo creado en servicios de banca electrónica y valoración de la prueba técnica sobre la seguridad del sistema.	El análisis se centró en si existía vulnerabilidad tecnológica atribuible al banco; al no probarse, prevaleció la idea de custodia de credenciales por el usuario.	Responsabilidad objetiva en servicios financieros	Pericia técnica y testimonio experto	Se rechazó la responsabilidad del banco al considerarse posible negligencia del usuario en la	Importante sobre vulnerabilidad del acceso a internet banking

Sentencia	Tribunal	Año	Hechos relevantes	Tipo de fraude	Factor de atribución	Nexo causal	Daño indemnizable	Criterio jurídico aplicado	Deber de seguridad y riesgo tecnológico	Criterio de responsabilidad	Prueba valorada	Decisión	Observaciones
			u otros métodos informáticos.									custodia de sus credenciales.	
00460-2017	Sala Primera Corte Suprema de Justicia	2017	Empresa cliente denunció sustracción de dinero mediante transferencias electrónicas realizadas desde su cuenta bancaria sin autorización. Se comprobó que otras personas también tenían acceso a las cuentas.	Fraude informático en banca electrónica	Responsabilidad objetiva con eximente	El tribunal determinó que el acceso a la información confidencial del sistema provino del propio cliente o de terceros con acceso autorizado, lo que constituye culpa de la víctima.	No se reconoció indemnización	Análisis del artículo 35 de la Ley de Protección al Consumidor, teoría del riesgo creado y redistribución de la carga de la prueba.	La seguridad del banco no se tuvo por deficiente, pues el problema se vinculó al manejo interno de credenciales y accesos por parte del cliente.	Responsabilidad objetiva con eximente	Informes bancarios y correos electrónicos	Se rechaza la responsabilidad del banco al no acreditarse falla en el sistema de seguridad.	Destaca importancia del manejo confidencial de credenciales

Sentencia	Tribunal	Año	Hechos relevantes	Tipo de fraude	Factor de atribución	Nexo causal	Daño indemnizable	Criterio jurídico aplicado	Deber de seguridad y riesgo tecnológico	Criterio de responsabilidad	Prueba valorada	Decisión	Observaciones
02190-2020	Sala Primera Corte Suprema de Justicia	2020	Usuarios de banca telefónica fueron víctimas de estafa tras recibir una llamada fraudulenta ("llamada millonaria") y posteriormente se realizaron transferencias desde sus cuentas sin autorización.	Ingeniería social / Estafa telefónica	Responsabilidad objetiva con eximente por culpa de la víctima	Se determinó que el usuario entregó información confidencial (clave del servicio), lo que constituye culpa de la víctima y rompe el nexo causal.	No se reconoció indemnización	Teoría del riesgo creado	La Sala refuerza que, aunque el servicio bancario genera riesgo, el deber de seguridad no convierte al banco en asegurador universal frente a cualquier engaño externo exitoso.	Responsabilidad objetiva con eximente de culpa de la víctima	Testimonio de funcionario bancario y registros de transacciones	Se rechaza la demanda y se absuelve al banco de responsabilidad.	Refuerza doctrina de ruptura del nexo causal por imprudencia del usuario.
02056-2022	Sala Primera Corte Suprema de Justicia	2022	Cliente denunció transferencias electrónicas realizadas desde su cuenta mediante internet banking y retiros posteriores en cajeros automáticos.	Fraude electrónico	Responsabilidad objetiva con análisis de ajenidad del daño	El banco demostró que las transacciones se realizaron utilizando datos confidenciales del cliente y que no existió falla del sistema. Por lo que se determinó que el banco demostró ser ajeno al daño	No se reconoció indemnización	Régimen de responsabilidad objetiva en servicios bancarios	Se examina el alcance del deber de seguridad en clave tecnológica, concluyendo que no se incumple si el banco demuestra funcionamiento regular de sus sistemas.	Responsabilidad objetiva con análisis de ajenidad del daño	Registros de autenticación y transacciones	Se declaró sin lugar el recurso y se confirmó que el banco no era responsable del daño.	Importante para determinar ajenidad del daño en fraude electrónico

Sentencia	Tribunal	Año	Hechos relevantes	Tipo de fraude	Factor de atribución	Nexo causal	Daño indemnizable	Criterio jurídico aplicado	Deber de seguridad y riesgo tecnológico	Criterio de responsabilidad	Prueba valorada	Decisión	Observaciones
01307-2023	Sala Primera Corte Suprema de Justicia	2023	Cliente del Banco de Costa Rica sufrió múltiples transferencias electrónicas fraudulentas tras recibir una llamada de un estafador que se hizo pasar por funcionario del banco y solicitó datos de la clave dinámica. El fraude generó pérdidas superiores a ₡10 millones y USD $2.790.	Ingeniería social / Fraude telefónico	Debate entre responsabilidad objetiva y culpa del usuario	El tribunal evaluó si la entrega voluntaria de datos por parte del cliente rompía el nexo causal entre el sistema del banco y el daño.	No se reconoció indemnización	Responsabilidad bancaria en relación de consumo	Aunque se discute el deber de seguridad bancaria, la decisión privilegia la custodia de credenciales por parte del usuario como elemento decisivo.	Debate entre responsabilidad objetiva y culpa del usuario	Registros de transacciones y reclamo bancario	Se rechazó la pretensión indemnizatoria al considerar que el fraude se facilitó por la entrega de credenciales al tercero.	Caso relevante sobre información personal obtenida por estafadores. Adicional, examina deber de seguridad bancaria

Sentencia	Tribunal	Año	Hechos relevantes	Tipo de fraude	Factor de atribución	Nexo causal	Daño indemnizable	Criterio jurídico aplicado	Deber de seguridad y riesgo tecnológico	Criterio de responsabilidad	Prueba valorada	Decisión	Observaciones
01892-2023	Sala Primera Corte Suprema de Justicia	2023	Cliente del banco (adulta mayor) fue víctima de transacciones electrónicas no autorizadas tras recibir una llamada telefónica de un supuesto funcionario bancario que obtuvo sus datos personales y logró acceder a su banca en línea, efectuando varias transferencias desde sus cuentas.	Ingeniería social / fraude electrónico	Responsabilidad objetiva bancaria discutida bajo la previsibilidad del fraude y el deber de vigilancia	Discusión sobre si el banco debió detectar transacciones inusuales. El tribunal consideró que el daño se produjo porque la información confidencial fue facilitada a terceros, sin demostrarse vulneración del sistema bancario.	No se reconoció indemnización	Responsabilidad objetiva bancaria	La decisión reconoce la existencia de operaciones atípicas como tema relevante, pero no suficiente por sí solo si no se acredita un defecto concreto en el sistema de control del banco.	Debate sobre deber de seguridad y previsibilidad del fraude	Historial de transacciones y denuncia ante OIJ	Se rechaza la demanda y se confirma la inexistencia de responsabilidad del banco.	Destaca deber de vigilancia ante operaciones atípicas

Sentencia	Tribunal	Año	Hechos relevantes	Tipo de fraude	Factor de atribución	Nexo causal	Daño indemnizable	Criterio jurídico aplicado	Deber de seguridad y riesgo tecnológico	Criterio de responsabilidad	Prueba valorada	Decisión	Observaciones
00926-2024	Sala Primera Corte Suprema de Justicia	2024	La cliente del Banco facilitó códigos de verificación y datos del token durante una llamada telefónica en la que los estafadores se hicieron pasar por funcionarios bancarios. Posteriormente se realizaron múltiples transferencias electrónicas y un extrafinanciamiento con su tarjeta de crédito.	Ingeniería social (estafa electronica)	Responsabilidad bancaria en consumo con énfasis en custodia de credenciales	Se determinó que las transacciones se realizaron utilizando credenciales válidas del cliente, por lo que no se acreditó vulneración del sistema bancario.	No se reconoció indemnización	Responsabilidad bancaria en consumo	El caso pone en el centro el token, OTP y contraseñas como mecanismos de seguridad cuya eficacia se presume si no se demuestra una falla técnica atribuible al banco.	Se analizó la responsabilidad bancaria frente al fraude electrónico y la eficacia de los sistemas de autenticación (token, OTP, contraseñas). El tribunal valoró la custodia de credenciales por parte del usuario.	Estados de cuenta y registros de transferencias	Se rechazó el reclamo del cliente y no se atribuyó responsabilidad al banco.	Caso representativo de fraude telefónico en banca digital
00040-2025	Sala Primera Corte Suprema de Justicia	2025	Cliente engañada mediante llamada para actualizar datos, lo que permitió acceder a su correo y luego a su banca en línea.	Ingeniería social / phishing	Responsabilidad objetiva con análisis de ajenidad del daño	Se rompe el nexo causal porque el usuario proporcionó información confidencial	No se reconoció indemnización	Art. 35 Ley del Consumidor	El riesgo tecnológico no conduce automáticamente a responsabilizar al banco; la sentencia matiza la aplicación automática del régimen objetivo.	Responsabilidad objetiva con análisis de ajenidad del daño	Registros de transacciones y comunicaciones electrónicas	Demanda rechazada	La Sala matiza la aplicación automática de responsabilidad objetiva

Sentencia	Tribunal	Año	Hechos relevantes	Tipo de fraude	Factor de atribución	Nexo causal	Daño indemnizable	Criterio jurídico aplicado	Deber de seguridad y riesgo tecnológico	Criterio de responsabilidad	Prueba valorada	Decisión	Observaciones
01456-2025	Sala Primera Corte Suprema de Justicia	2025	Cliente del Banco sufrió fraude cibernético luego de recibir una llamada de un supuesto funcionario que obtuvo información y acceso a su correo electrónico asociado a la banca en línea.	Ingeniería social / phishing	Responsabilidad bancaria en servicios digitales con análisis de ajenidad del daño	El tribunal concluyó que el fraude ocurrió porque la víctima entregó información confidencial que permitió acceder a su correo y posteriormente a su cuenta bancaria.	No se reconoció indemnización	Responsabilidad bancaria en servicios digitales	Se reconoce la importancia de las medidas de seguridad digital, pero se niega la imputación cuando el banco acredita que el acceso se produjo por información suministrada por la propia víctima.	Discusión sobre riesgo tecnológico y medidas de seguridad	Comunicaciones electrónicas y movimientos bancarios	Se declara sin lugar la demanda, al acreditarse ajenidad del banco respecto al daño.	Relevante para análisis de seguridad digital bancaria
01493-2025	Sala Primera Corte Suprema de Justicia	2025	Consumidora fue víctima de fraude mediante acceso remoto (AnyDesk) tras llamada de un supuesto funcionario que la convenció de instalar software y realizar gestiones en línea; se realizaron múltiples transferencias por	Ingeniería social con acceso remoto	Responsabilidad objetiva bancaria, con discusión sobre la ruptura del nexo causal	Discusión sobre si la conducta del usuario rompe el nexo causal. El tribunal concluyó que las operaciones se realizaron utilizando credenciales válidas del cliente,	No se reconoció indemnización	Responsabilidad objetiva bancaria	El caso muestra una modalidad más sofisticada de fraude, pero la Sala mantiene el énfasis en la conducta del usuario cuando esta facilita el acceso remoto al sistema.	Debate sobre riesgo tecnológico y deber de seguridad	Registros de transacciones y reclamos bancarios	Se rechaza la demanda al estimarse falta de responsabilidad del banco.	Caso complejo sobre fraude mediante software remoto

Sentencia	Tribunal	Año	Hechos relevantes	Tipo de fraude	Factor de atribución	Nexo causal	Daño indemnizable	Criterio jurídico aplicado	Deber de seguridad y riesgo tecnológico	Criterio de responsabilidad	Prueba valorada	Decisión	Observaciones
			aproximadamente $30.000.			obtenidas mediante engaño de terceros.							
01701-2025	Sala Primera Corte Suprema de Justicia	2025	Usuaria sufrió transferencias electrónicas no autorizadas desde su cuenta bancaria por ₡4.400.000 realizadas desde una dirección IP en el extranjero.	Fraude informático	Responsabilidad objetiva bancaria	Discusión sobre control de seguridad bancaria. El tribunal consideró que no se acreditó negligencia de la víctima ni causa externa suficiente para romper el nexo causal.	Restitución del monto sustraído, intereses y daño moral	Teoría del riesgo creado	La sentencia revaloriza el deber de control y seguridad del banco frente a operaciones anómalas, especialmente cuando existen indicios de vulnerabilidad tecnológica.	Responsabilidad objetiva bancaria	Registros de IP, transacciones y expediente penal	Se declara con lugar la demanda, condenando al banco a pagar el monto sustraído, intereses y daño moral.	Relevante para análisis de vulnerabilidades tecnológicas

Nota: Hernández, 2026.

4.3. Riesgo tecnológico y deber de seguridad en la banca digital

Uno de los hallazgos más consistentes del estudio es que el fraude informático en el ámbito bancario no puede analizarse únicamente como un problema de engaño individual, sino también como una manifestación del riesgo tecnológico propio de la banca digital. Las plataformas bancarias modernas operan sobre entornos conectados, administran credenciales, datos sensibles y operaciones patrimoniales en tiempo real, y se encuentran expuestas de manera permanente a ataques de phishing, ingeniería social, malware, accesos remotos y otras formas de manipulación. En ese contexto, el riesgo no es extraordinario ni marginal, sino que forma parte de la estructura misma del servicio.

Este dato resulta particularmente importante desde la teoría de la imputación. Si la actividad desarrollada introduce un riesgo específico en la esfera social, y si además genera provecho económico para quien la organiza, entonces no parece jurídicamente razonable exigir a la víctima que soporte por sí sola las consecuencias de la materialización de ese riesgo. Esta es, precisamente, la lógica que subyace a la teoría del riesgo creado y que, aunque no siempre sea aplicada con la misma intensidad por la jurisprudencia costarricense, sigue estando presente como trasfondo argumentativo de muchos de los fallos analizados.

Ahora bien, el reconocimiento del riesgo tecnológico no conduce necesariamente a una responsabilidad automática. Lo que sí produce es una elevación del estándar de diligencia exigible al banco. La entidad financiera no solo debe mantener operativa una plataforma, sino que debe diseñarla, administrarla y supervisarla con criterios de seguridad razonables y actualizados. Esto incluye autenticación multifactorial, monitoreo antifraude, análisis de patrones de comportamiento, protección de datos, canales de alerta, respuesta oportuna ante incidentes y educación continua al usuario. La regulación prudencial costarricense va precisamente en esa dirección, al exigir controles mínimos de prevención y una gestión integral del riesgo tecnológico.

Desde esta perspectiva, el deber de seguridad bancaria adquiere una naturaleza compleja. Por un lado, funciona como deber accesorio dentro de la relación contractual entre banco y cliente, y por otro, puede proyectarse como deber general de protección, especialmente cuando el daño deriva del funcionamiento del servicio o de la ausencia de controles adecuados. En ambos planos, lo relevante es que la seguridad deja de ser un aspecto puramente técnico para convertirse en un parámetro jurídico de imputación. De la matriz jurisprudencial derivado del apéndice F se logra identificar que de acuerdo con la sentencia No. 01701-2025, la falta de monitoreo frente a

transacciones inusuales configura responsabilidad. Asimismo, la sentencia 01493-2025 evidencia la necesidad de adaptación frente a nuevas modalidades de fraude como el acceso remoto, concluyendo en este sentido que el deber de seguridad es dinámico y evoluciona con la tecnología.

Ahora bien, la doctrina contemporánea sobre responsabilidad civil ha insistido en que la seguridad, particularmente en actividades profesionalizadas, no puede medirse desde la simple evitación del daño consumado, sino desde la razonabilidad de las medidas implementadas para prevenirlo. En otras palabras, lo decisivo no es si el banco logró impedir todo fraude imaginable, sino si actuó conforme a un estándar profesional acorde con los riesgos previsibles del entorno digital. De ahí que, en la valoración judicial, tengan tanta importancia los mecanismos de autenticación, el monitoreo de movimientos atípicos y la capacidad de detección temprana de operaciones incompatibles con el perfil histórico del cliente.

4.4. Mecanismos de acreditación de la responsabilidad civil bancaria

En los casos de fraude informático bancario, la cuestión probatoria ocupa un lugar central. El análisis de las sentencias estudiadas demuestra que la discusión sobre responsabilidad no se resuelve únicamente mediante la invocación abstracta de normas civiles o de consumo, sino a partir de la capacidad de las partes para acreditar cómo se produjo el daño, qué información fue utilizada, qué controles existían y si el sistema presentó señales de vulneración o funcionamiento anormal. Por ello, la prueba tecnológica emerge como uno de los ejes más importantes de la imputación civil bancaria.

Entre los medios probatorios más relevantes identificados en la matriz jurisprudencial conforme el apéndice F, se encuentran los registros de autenticación, los estados de cuenta, las bitácoras de acceso, las direcciones IP, las comunicaciones electrónicas, los informes internos del banco, la denuncia penal ante el OIJ y, en ciertos casos, la prueba pericial técnica. Estos elementos no se valoran de manera aislada; su función consiste en reconstruir la secuencia del fraude y en determinar si la entidad actuó conforme a los estándares de seguridad que le eran exigibles.

Ahora bien, del análisis comparado de los casos, se permite identificar que la acreditación de la responsabilidad civil bancaria no depende exclusivamente de la existencia del fraude, sino de la capacidad del material probatorio para explicar de forma coherente el origen del daño.

Así, cuando la prueba tecnológica logra demostrar que el acceso a la cuenta se produjo mediante el uso de credenciales legítimas obtenidas a través de engaño al usuario, la Sala tiende a considerar acreditada la ajenidad del daño y, en consecuencia, a excluir la responsabilidad del

banco. Este criterio se observa, por ejemplo, en la sentencia No. 00040-2025, en la que se determinó que las transacciones se realizaron con los datos de la propia titular, obtenidos mediante ingeniería social, sin evidencia de vulneración del sistema bancario. De forma concordante, en resoluciones como la No. 00686-2014 y la No 02190-2020, la entrega de información confidencial por parte del usuario fue considerada suficiente para romper el nexo causal, al tratarse de conductas que escapan del control de la entidad financiera

En estos supuestos, los registros del sistema, las trazas de autenticación y la secuencia de transacciones permiten al banco reconstruir el iter del fraude y demostrar que la operación se ejecutó conforme a los mecanismos ordinarios de validación, lo que conduce a un resultado probatorio orientado a la exoneración de responsabilidad. De este modo, la prueba tecnológica no solo cumple una función descriptiva, sino también exonerativa, en tanto permite acreditar la ruptura del nexo causal mediante figuras como la culpa de la víctima o la ajenidad del daño.

Por otro lado, la sentencia No. 00970-2014 deja ver la importancia de la prueba pericial para evidenciar las limitaciones del control bancario sobre el canal de acceso a internet, destacando que el riesgo tecnológico forma parte del servicio ofrecido por la entidad. Asimismo, en la sentencia No. 01477-2011, la acreditación de fallas en los protocolos de seguridad permitió vincular el daño con un incumplimiento del deber de seguridad del banco.

Algo similar ocurre en las sentencias No. 01701-2025, donde se realizaron transferencias desde una dirección IP extranjera, lo cual evidencio una operación que, por su localización y características, podía ser calificada como inusual y merecedora de control reforzado. En la N°01892-2023, la multiplicidad de transacciones atípicas y el cambio de patrón de comportamiento del cliente adquirieron valor probatorio para cuestionar la suficiencia del monitoreo bancario. De forma parecida, la sentencia No. 01307-2023 incorpora la idea de valorar el patrón histórico de uso del cliente como elemento útil para determinar si la entidad debió detectar y bloquear operaciones incompatibles con la conducta habitual del usuario.

De estos casos se desprende que uno de los mecanismos contemporáneos más relevantes de acreditación de la responsabilidad bancaria es la comparación entre la operación fraudulenta y el comportamiento transaccional ordinario del cliente. Cuando el banco no logra justificar por qué una operación manifiestamente inusual no fue detectada, bloqueada o sometida a verificación adicional, la valoración probatoria tiende a inclinarse hacia la responsabilidad de la entidad.

No obstante, también existen supuestos intermedios en los que la prueba no permite una conclusión completamente cerrada. Así se aprecia en las sentencias No. 01456-2025 y N°01493-2025, donde la información disponible genera dudas sobre la suficiencia de las medidas de seguridad, pero no siempre alcanza para acreditar de forma plena una falla técnica específica o una imputación directa e incontrovertible.

Ahora bien, la asimetría técnica entre banco y cliente resulta aquí decisiva. El usuario, por regla general, no tiene acceso a la arquitectura interna del sistema, a las bitácoras completas de sesión, a los algoritmos de detección de anomalías ni a los parámetros de autenticación utilizados por la entidad. El banco, en cambio, dispone de toda esa información y se encuentra, por tanto, en mejor posición para explicar si la operación cuestionada fue normal, irregular, vulnerable o compatible con el comportamiento histórico del cliente. Esta realidad explica que tanto la doctrina como la jurisprudencia costarricense hayan aceptado, en distintos grados, la idea de una carga probatoria dinámica o de una redistribución de la carga de la prueba en favor del usuario.

Lo anterior no significa que el cliente quede dispensado de toda carga probatoria. Debe acreditar, al menos, la existencia del daño y la ocurrencia de la operación no autorizada. Sin embargo, una vez constatado ese daño dentro del canal digital provisto por el banco, el peso de la prueba tiende a desplazarse hacia la entidad financiera, particularmente en lo relativo a la ajenidad del daño, a la seguridad del sistema y a la suficiencia de sus controles. Este desplazamiento encuentra justificación no solo en la lógica del artículo 35 de la Ley 7472, sino también en el principio de tutela efectiva del consumidor y en la imposibilidad material del usuario de demostrar hechos que solo el banco puede conocer y documentar con precisión.

De forma que con la sistematización realizada en la matriz jurisprudencial se identificaron tres ejes fundamentales, el primero es la reconstrucción técnica del fraude, mediante registros, correos, tokens, direcciones IP y trazas de autenticación, el segundo es la redistribución de la carga de la prueba, especialmente en razón de la asimetría técnica entre banco y usuario y el tercero es la valoración del estándar de seguridad y monitoreo exigible a la entidad financiera, a partir del comportamiento transaccional del cliente y de la capacidad del banco para detectar operaciones anómalas.

Desde esta perspectiva, la acreditación de la responsabilidad civil bancaria exige un análisis integral de la prueba. No basta con constatar que el usuario fue víctima de fraude; tampoco basta con que el banco afirme que el sistema no fue vulnerado. Lo jurídicamente relevante es determinar,

a partir del conjunto probatorio, si la entidad gestionó de manera adecuada el riesgo del servicio y si el daño puede vincularse, de forma jurídicamente relevante, a una falla, insuficiencia o ausencia de medidas razonables de seguridad.

4.5. Integración de los criterios de imputación de responsabilidad civil bancaria

La integración de los hallazgos normativos, doctrinales y jurisprudenciales permite afirmar que la imputación de responsabilidad civil a las entidades bancarias privadas frente a estafas informáticas en Costa Rica se construye sobre una base plural y no sobre una regla única. En primer término, aparece el deber de seguridad tecnológica, que se desprende del derecho del consumidor, de la protección de datos y de la regulación prudencial del sistema financiero. Este deber exige a la entidad bancaria implementar controles preventivos, detectivos y correctivos razonables en la operación de sus plataformas digitales.

En segundo lugar, se identifica la teoría del riesgo creado como criterio particularmente útil para comprender por qué la actividad bancaria digital no puede tratarse como una actividad neutral desde el punto de vista de la imputación. El banco organiza, controla y explota económicamente un servicio que introduce riesgos específicos para el patrimonio del usuario. En esa medida, no resulta extraño que el ordenamiento y la jurisprudencia le impongan una carga reforzada de prevención y de explicación cuando el daño se produce dentro de ese entorno de riesgo.

En tercer lugar, el nexo causal aparece como criterio delimitador. La responsabilidad bancaria no se deriva de cualquier daño sufrido por el usuario, sino solo de aquel que pueda vincularse jurídicamente al riesgo del servicio o al incumplimiento del deber de seguridad. De allí que la jurisprudencia preste tanta atención a la culpa de la víctima, al hecho de tercero y a la ajenidad del daño. No se trata de categorías accesorias, sino que son mecanismos que permiten decidir cuándo el daño debe atribuirse al banco y cuándo, por el contrario, la cadena causal ha sido desplazada por una conducta ajena.

En cuarto lugar, el análisis confirma la importancia de la protección reforzada del consumidor financiero, especialmente por la asimetría informativa y técnica que caracteriza la relación banco-cliente. Finalmente, en quinto lugar, la carga dinámica de la prueba se muestra como un criterio transversal, indispensable para que la tutela del usuario no se convierta en una protección puramente formal e ilusoria.

Vistas en conjunto, estas categorías permiten comprender que la responsabilidad civil bancaria en fraudes informáticos no se decide mediante una simple oposición entre culpa y objetividad. En realidad, lo que se observa es una estructura de imputación más compleja, en la que convergen elementos de responsabilidad por riesgo, deberes profesionales de seguridad, valoración del comportamiento del usuario y reglas probatorias adaptadas a un entorno tecnológicamente asimétrico.

4.6. Discusión de resultados

A la luz de la pregunta de investigación, los resultados permiten sostener que los criterios jurídicos aplicables para la imputación de responsabilidad civil a las entidades bancarias privadas en Costa Rica frente a estafas informáticas realizadas a través de sus plataformas digitales se configuran a partir de una relación dinámica entre norma, riesgo, causalidad y prueba.

En el plano normativo, el ordenamiento costarricense ya contaba en 2024 con bases suficientes para abordar este tipo de conflictos, como lo eran: la Constitución Política, el Código Civil, la Ley 7472, la Ley 8968, la normativa prudencial emitida por SUGEF y CONASSIF, y la legislación penal sobre fraude informático. En el plano jurisprudencial, sin embargo, la construcción de la responsabilidad no ha sido uniforme. La Sala Primera ha oscilado entre una comprensión más intensa del riesgo creado y otra más restrictiva, centrada en la ajenidad del daño y en la conducta del usuario.

Esta oscilación no debe entenderse como incoherencia absoluta, sino como expresión de la dificultad jurídica propia del fenómeno. El fraude bancario digital se sitúa en una zona de intersección entre el engaño del tercero, la conducta del usuario y la gestión técnica del servicio. Por ello, la imputación no puede resolverse de manera automática ni exclusivamente desde una categoría dogmática. Requiere valorar, caso por caso, si la entidad financiera adoptó las medidas que razonablemente podían esperarse de ella, si el daño se produjo dentro del riesgo propio del servicio ofrecido y si existe prueba suficiente para atribuírselo jurídicamente.

En consecuencia, este trabajo de investigación permite concluir que la responsabilidad civil bancaria frente a estafas informáticas no puede reducirse a la sola ocurrencia del fraude ni a la mera constatación de que el usuario proporcionó información sensible. Lo decisivo es determinar si, a la luz del marco normativo vigente y de la prueba producida, el banco gestionó adecuadamente el riesgo tecnológico inherente al servicio digital que puso en circulación. Esa es, en última

instancia, la clave con la que el derecho costarricense ha comenzado a construir los criterios de imputación en esta materia.

Capítulo V. Conclusiones y Recomendaciones

5.1. Conclusiones

La presente investigación tuvo como propósito analizar los criterios de imputación de responsabilidad civil aplicables a las entidades bancarias privadas en Costa Rica frente a delitos de estafas informáticas cometidos a través de sus plataformas digitales, así como los mecanismos jurídicos que permiten acreditar dicha responsabilidad. A partir del análisis normativo, doctrinal y jurisprudencial desarrollado, se establecen las siguientes conclusiones con relación a los objetivos de la presente investigación:

En cuanto al primer objetivo específico referente a identificar los criterios legales y normativos aplicables, el análisis permite advertir que el ordenamiento jurídico costarricense vigente para el período 2024 ofrece un conjunto de normas relevantes para abordar la responsabilidad civil bancaria en casos de fraude informático, aunque no de manera completamente sistemática. Este marco se compone de disposiciones constitucionales, civiles, de protección al consumidor, de protección de datos personales, así como de normativa prudencial y penal. Sin embargo, en la práctica surgen dificultades interpretativas importantes, sobre todo en lo que respecta al alcance del deber de seguridad tecnológica y a la determinación de cuándo el daño puede considerarse ajeno al banco, lo que evidencia la falta de una regulación específica y clara en esta materia.

Por otra parte, en relación con el segundo objetivo específico dirigido al examen de la jurisprudencia costarricense, se observa que no existe una línea uniforme en la forma en que se imputa la responsabilidad civil a las entidades bancarias en casos de estafas informáticas. Más bien, la jurisprudencia ha ido evolucionando. En un inicio, la Sala Primera tendía a destacar el riesgo propio de la actividad bancaria digital y el deber reforzado de seguridad; posteriormente, comenzó a dar mayor peso a la conducta del usuario, especialmente cuando este facilitaba información sensible; y, en resoluciones más recientes, se aprecia un enfoque más casuístico, en el que cada asunto se analiza a partir de sus particularidades y de la prueba disponible.

En lo que respecta al tercer objetivo específico sobre establecer el vínculo jurídico entre la responsabilidad civil bancaria y la ocurrencia de estafas informáticas, así como los mecanismos para acreditarla, se concluye que dicho vínculo no opera de forma automática. Por el contrario, depende de la interacción de varios elementos, como lo son: el riesgo tecnológico propio de la banca digital, el deber de seguridad y custodia que recae sobre la entidad financiera, la existencia

de un daño patrimonial, el nexo causal y, por supuesto, la conducta del usuario. En este contexto, el hecho de que el cliente haya entregado voluntariamente sus credenciales puede influir en la ruptura del nexo causal, pero no basta por sí solo para excluir la responsabilidad del banco; es necesario valorar si el daño se mantiene dentro del riesgo que implica el servicio ofrecido.

En esta misma línea, la acreditación de la responsabilidad civil en estos casos se da en gran medida en la prueba tecnológica y documental, como lo pueden ser los registros de autenticación, historiales de transacciones, direcciones IP, bitácoras del sistema o comunicaciones electrónicas. Aquí resulta evidente la desventaja en la que se encuentra el usuario frente al banco, lo que justifica la aplicación de criterios como la carga dinámica de la prueba, especialmente cuando se trata de demostrar si el daño es ajeno a la entidad o si esta cumplió con los estándares de seguridad exigibles.

De manera global, el estudio también permite indicar que las entidades bancarias privadas, por la propia naturaleza tecnológica de los servicios que ofrecen, asumen un deber de seguridad reforzado. Este no se limita a garantizar el funcionamiento del servicio, sino que implica adoptar medidas razonables de prevención, monitoreo y respuesta frente a riesgos informáticos previsibles. Este deber cobra especial importancia en un contexto donde existe una clara asimetría técnica, informativa y probatoria entre el banco y el usuario.

Finalmente, en relación con el objetivo general de la investigación, se concluye que la imputación de responsabilidad civil a las entidades bancarias privadas frente a estafas informáticas en Costa Rica no responde a una regla única. Más bien, exige una valoración conjunta de distintos factores, como el riesgo generado por la actividad digital, el cumplimiento del deber de seguridad, la existencia o ruptura del nexo causal, la conducta del usuario y la calidad de la prueba aportada. En consecuencia, cada caso debe analizarse en función de sus propias circunstancias, evitando soluciones automáticas que no reflejan la complejidad real de este tipo de situaciones.

5.2. Recomendaciones

Con fundamento en los resultados obtenidos en la presente investigación, y con el propósito de contribuir al fortalecimiento de la seguridad en el sistema financiero digital, así como a una tutela más efectiva del consumidor financiero, se plantean diversas recomendaciones orientadas a distintos actores del sistema.

En relación con el primer objetivo referente al análisis de los criterios legales y normativos aplicables, se recomienda que las entidades bancarias privadas fortalezcan sus sistemas de gestión

del riesgo tecnológico. Esto implica no solo incorporar mecanismos como la autenticación multifactorial, el monitoreo constante de transacciones o herramientas que permitan detectar operaciones inusuales a tiempo, sino también asegurarse de que estos sistemas se mantengan actualizados frente a la evolución constante de las modalidades de fraude. De manera que no solo se reduzca el riesgo de operaciones no autorizadas, sino que también se mejore la trazabilidad de los incidentes, lo cual resulta clave en caso de conflicto.

Asimismo, se recomienda que las entidades bancarias refuercen sus protocolos internos de atención de incidentes de seguridad y de gestión de reclamaciones relacionadas con fraudes informáticos, mediante procedimientos claros, estandarizados, auditables y accesibles para las personas usuarias. En esta línea, resulta pertinente promover el uso de mecanismos alternativos de resolución de conflictos, particularmente a través de instancias como la Oficina del Consumidor Financiero, con el fin de brindar soluciones más ágiles, técnicas y menos onerosas, evitando en la medida de lo posible la judicialización de estos casos.

Por otra parte, a la luz del segundo objetivo vinculado al análisis del marco normativo, desde la perspectiva regulatoria, si bien existen disposiciones emitidas por la Superintendencia General de Entidades Financieras y el Consejo Nacional de Supervisión del Sistema Financiero en materia de gestión de riesgos y seguridad tecnológica, se considera necesario avanzar hacia una mayor precisión operativa de estos estándares en el contexto específico del fraude informático bancario. En particular, resulta conveniente desarrollar lineamientos más detallados en aspectos como la trazabilidad de las operaciones, la documentación y conservación de la evidencia digital, así como los mecanismos de registro y reporte de incidentes de fraude, lo que permitiría facilitar su valoración en sede judicial y reducir las dificultades interpretativas identificadas en la práctica.

En cuanto al tercer objetivo vinculado al análisis jurisprudencial, se recomienda que los operadores jurídicos, especialmente jueces, litigantes y peritos, adopten un enfoque integral en el estudio de los casos de fraude informático bancario. Este análisis no debería centrarse exclusivamente en la conducta del usuario, sino que debe incorporar también la valoración del riesgo inherente al servicio digital, la gestión del riesgo por parte de la entidad financiera, la previsibilidad del daño, la suficiencia de las medidas de seguridad implementadas y la capacidad del banco para acreditar la ajenidad del daño. La adopción de este enfoque contribuirá a decisiones más acordes con la complejidad del fenómeno, así como a la construcción de criterios más uniformes en la jurisprudencia y al fortalecimiento de la seguridad jurídica.

En cuanto a los mecanismos de acreditación de la responsabilidad civil, se recomienda promover el acceso a prueba pericial especializada en materia de seguridad informática dentro de los procesos judiciales. Dada la asimetría técnica y económica existente entre el usuario financiero y la entidad bancaria, resulta pertinente valorar alternativas como la disponibilidad de peritos oficiales, el apoyo de órganos auxiliares del sistema judicial o la suscripción de convenios con universidades u otras entidades técnicas o la creación de mecanismos institucionales que faciliten el acceso a este tipo de prueba. Esto permitiría garantizar una mayor igualdad de condiciones procesales y una mejor reconstrucción de los hechos.

Asimismo, se recomienda fortalecer los procesos de capacitación de los operadores jurídicos en materia de prueba digital, fraude informático, seguridad tecnológica y responsabilidad civil en entornos financieros digitales, con el fin de mejorar la calidad de las decisiones judiciales y contribuir a una mayor consistencia en los criterios aplicados.

De igual manera, se sugiere que las entidades bancarias desarrollen programas permanentes de educación financiera digital dirigidos a los usuarios, orientados a la prevención de fraudes como phishing, smishing, spoofing e ingeniería social. Estas iniciativas deben implementarse de forma continua y adaptarse a los distintos perfiles de usuarios y a las modalidades de fraude más frecuentes, sin que ello implique trasladar al usuario la responsabilidad principal en la prevención del daño.

Por otro lado, en atención al objetivo general de esta investigación, se recomienda que tanto los operadores jurídicos como las entidades financieras adopten un enfoque integral en el análisis y gestión de los casos de fraude informático bancario, que considere de manera conjunta el marco normativo aplicable, el riesgo tecnológico, el deber de seguridad, el nexo causal, la conducta del usuario y la prueba aportada. Este enfoque permitirá decisiones más coherentes con la complejidad técnica y jurídica del fenómeno, contribuirá a la protección efectiva del consumidor financiero y favorecerá la consolidación de criterios más claros y uniformes en la imputación de la responsabilidad civil en el entorno digital.

Finalmente, se estima pertinente fomentar investigaciones jurídicas futuras orientadas al análisis de la aplicación e impacto del Proyecto de Ley No. 23.908, relativo a la protección de las personas consumidoras en la custodia de su dinero administrado por entidades financieras, una vez que entre en vigencia.

En particular, resultará relevante examinar si la eventual incorporación de criterios más intensos de tutela al consumidor financiero, así como posibles modificaciones en la distribución de la carga de la prueba y en los estándares de responsabilidad de las entidades bancarias, produce variaciones en el comportamiento de los órganos jurisdiccionales. De esta manera, este tipo de estudios permitirá valorar si se generan cambios en los patrones jurisprudenciales actuales, especialmente en lo referente a la imputación de responsabilidad civil, a la interpretación del riesgo tecnológico y a la tutela efectiva de las personas usuarias frente a estafas informáticas en el sistema bancario digital.

Bibliografía

Abeliuk Manasevich, R. (2001). *Las obligaciones* (4.ª ed.). Editorial Jurídica de Chile.

Acosta Betancourt, S. (2014). *Responsabilidad objetiva-una propuesta de modernización legislativa al régimen de responsabilidad civil por actividades peligrosas.* [Trabajo de Grado Universidad de los Andes]. https://repositorio.uniandes.edu.co/server/api/core/bitstreams/098661a4-b2ad-4ca0-b729-bdf006143b0f/content

Acuerdo CONASSIF 5-24 [CONASSIF]. *Reglamento General de Gobierno y Gestión de la Tecnología de Información*. 22 de julio 2024. https://www.sugef.fi.cr/normativa/normativa_transversal/documentos/CONASSIF%205-24%20(v01%205%20agosto%202024).pdf

Acuerdo SUGEF 10-7 [SUGEF]. *Reglamento sobre la transparencia ante el usuario financiero en la prestación de productos y servicios por parte de entidades supervisadas por SUGEF*. 27 de junio 2007 https://www.sugef.fi.cr/normativa/normativa_vigente/SUGEF%2010-07%20(v5%2001%20junio%202025).pdf

Alessandri Rodríguez, A. (2005). De *la responsabilidad extracontractual en el derecho civil chileno*. Santiago de Chile: Editorial Jurídica de Chile.

Alferillo, P. E. (1999). *Reflexiones sobre la obligación de seguridad en el Derecho de Daños.* La Voz del Foro, 4(30), 19. https://www.acaderc.org.ar/wp-content/blogs.dir/55/files/sites/55/2021/04/seguridaddanos.pdf

Anaya, C. (2012). *Riesgos en las transacciones electrónicas bancarias: Una carga que debe ser asumida por la banca*. Revista e-Mercatoria, 11(1), 287–331. https://bdigital.uexternado.edu.co/entities/publication/0c935a9c-6db4-4a9f-89ac-5265d6055d7c

Arburola Valverde, A. (2010). *La teoría de la imputación objetiva en el derecho penal.* Revista Judicial de Costa Rica, (95), 147–167.

Arrieta E. (2025) *Bancos advierten de más estafas electrónicas si se aprueba proyecto impulsado por el PLN para responsabilizar a entidades financieras.* La República https://www.larepublica.net/noticia/bancos-advierten-de-mas-estafas-electronicas-si-se-aprueba-proyecto-impulsado-por-el-pln-para-responsabilizar-a-entidades-financieras

Arrieta, M. (2023). *La responsabilidad de las entidades bancarias frente a los fraudes informáticos en Costa Rica.* Editorial Jurídica Centroamericana.

Asamblea Legislativa de Costa Rica. (1995). *Ley Orgánica del Banco Central de Costa Rica*, Ley No. 7558. Costa Rica.

Asamblea Legislativa de Costa Rica. (2012). *Código Penal*. Ley N.º 4573. http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=5027

Asamblea Legislativa de la República de Costa Rica. (1994). Ley No. 7472. *Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor.* http://www.pgrweb.go.cr/scij/busqueda/normativa/normas/nrm_texto_completo.aspx?nValor1=1&nValor2=26481

Asamblea Legislativa de la República de Costa Rica. (1996). *Código Procesal Penal,* Ley No. 7594 del 4 de junio de 1996. https://pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=41297&nValor3=0&strTipM=TC

Asamblea Legislativa de la República de Costa Rica. (2012). Ley N.º 9048. *Reforma del Código Penal para la tipificación de delitos informáticos y conexos*. http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=73583

Asamblea Legislativa. (2023). *Expediente legislativo No. 23.908: Proyecto de ley sobre responsabilidad bancaria en fraudes electrónicos. San José, Costa Rica.*

Baudrit, D. (1991). *El principio general de la libertad de contratar*. Revista de Derecho Constitucional, 2.

Bonasi Benucci, E. (2019). *La responsabilidad civil* (1 ed.). Santiago de Chile, Ediciones Olejnik. https://elibro.net/es/ereader/bibliouia/239587?page=81.

Bonneau, J., Herley, C., Van Oorschot, P., & Stajano, F. (2012). *The quest to replace passwords: A framework for comparative evaluation of web authentication schemes.* University of Cambridge. https://www.cl.cam.ac.uk/~fms27/papers/2012-BonneauHerOorSta-password.pdf

Bustamante Alsina, J. (1997). *Teoría general de la responsabilidad civil.* Abeledo Perrot.

Calderón G. (2025). *Bancos advierten sobre efectos de proyecto que tramita Congreso ante estafas telefónicas.* Teletica. https://www.teletica.com/politica/bancos-advierten-sobre-efectos-de-proyecto-que-tramita-congreso-ante-estafas-telefonicas_382112

Centro de Información Jurídica en Línea. (2008). *Caso fortuito y fuerza mayor en accidentes de tránsito.* *https://cijulenlinea.ucr.ac.cr/?s=CASO+FORTUITO+Y+FUERZA+MAYOR+EN+ACCIDENTES+DE+TR%C3%81NSITO*

Centro de Información Jurídica en Línea. (2010). *Responsabilidad civil objetiva prevista en la normativa de defensa del consumidor*. https://cijulenlinea.ucr.ac.cr/?s=RESPONSABILIDAD+CIVIL+OBJETIVA+PREVISTA+EN+LA+NORMATIVA+DE+DEFENSA+DEL+CONSUMIDOR

Centro de Información Jurídica en Línea. (2013). *El Deber De Brindar Información Veraz Al Consumidor*. https://cijulenlinea.ucr.ac.cr/?s=EL+DEBER+DE+BRINDAR+INFORMACI%C3%93N+VERAZ+AL+CONSUMIDOR

Cerutti, M. D. (2015). *La obligación de seguridad y su aplicación en el Código Civil y Comercial.* Revista de responsabilidad civil y seguros, 129-154.

Chacón, N., & Mora, D. (2015). *Los derechos del consumidor financiero en la Nueva Arquitectura Financiera Internacional: su aplicación en Costa Rica.* Universidad de Costa Rica. https://repositorio.sibdi.ucr.ac.cr/items/e70ffa1c-4b7a-46d6-b266-dec6a623fa87

Corte Suprema de Justicia, Sala Primera. (2011). Sentencia No. 000248-F-S1-2011 del 10 de marzo de 2011.

Cubides Camacho, J. (2012). *Obligaciones* (7.ª ed.). Grupo Editorial Ibáñez.

De Ángel Yagüez, J. (2001). *Responsabilidad civil: fundamentos y evolución doctrinal.* Civitas.

De Ángel Yagüez, R. (1993). *Tratado de responsabilidad civil.* Civitas.

De Cuevillas Matozzi, I. (2000). *La relación de causalidad en la órbita del derecho de daños.* Tirant lo Blanch.

De la Vega, R. (2019). *Principios de protección al consumidor y su impacto en la responsabilidad civil*. Revista Derecho y Sociedad, 45(2), 112-130.

Delfino.cr. (2023). *Asamblea: Expediente 23908.* https://delfino.cr/asamblea/proyecto/23908

Díez-Picazo, L. (1999). *Derecho de daños* (1.ª ed., p. 307). Civitas Ediciones.

Encinar, A. S. (2000). *El concepto jurídico de responsabilidad en la teoría general del derecho.* Anuario de la Facultad de derecho de la Universidad Autónoma de Madrid,(4), 27-56.

Escobar Fornos, I. (2000). *Derecho de obligaciones* (2.ª ed.). Editorial Hispamer.

Espinoza Cerdas, S. K. (2023). *Responsabilidad civil objetiva de la actividad bancaria frente al fraude informático (phishing).* Derecho en Sociedad, 16(2), 28–52. https://revistas.ulacit.ac.cr/index.php/derecho-en-sociedad/article/view/37

Ferrara, L. (2010). L*a responsabilidad civil: teoría y práctica*. Abeledo Perrot.

García de Enterría, E. (2003). *Curso de derecho administrativo* (Vol. II, reimp.). Civitas.

García, S. U. (2004). *La responsabilidad por riesgo*. Revista Ratio Juris, 1(1), 29-50.

Goldenberg, I. (1984). *La relación de la causalidad en la responsabilidad civil.* Editorial Astrea.

González, M. (2022). *Seguridad en plataformas digitales bancarias: protocolos y desafíos*. Revista Tecnología y Finanzas, 15(3), 45-60.

Henao, J. (2015). *Las formas de reparación en la responsabilidad del Estado: hacia su unificación sustancial en todas las acciones contra el Estado.* Revista de Derecho Privado, 227 - 266.

Hernández Botero, J. (2020). *La responsabilidad de las entidades financieras por fraudes electrónicos* [Trabajo de grado, Universidad Pontificia Bolivariana]. Recuperado de https://repository.upb.edu.co/bitstream/handle/20.500.11912/6161/La%20responsabilidad%20de%20las%20entidades%20financieras%20por%20fraudes%20electr%C3%B3nicos.pdf?sequence=1&isAllowed=y

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). Metodología de la investigación (6.ª ed.). McGraw-Hill España. https://apiperiodico.jalisco.gob.mx/api/sites/periodicooficial.jalisco.gob.mx/files/metodologia_de_la_investigacion_-_roberto_hernandez_sampieri.pdf

Hernández, P. P. (2018). *Responsabilidad civil.* Universidad Abierta para Adultos (UAPA). https://elibro.net/es/ereader/bibliouia/175610?page=31

Hernández, R. (2008). *Constitución Política de la República de Costa Rica: comentada, anotada y con citas de jurisprudencia*. Juricentro.

Hernández, R., Fernández, C., & Baptista, P. (2014). *Metodología de la investigación* (6.ª ed.). McGraw-Hill Education.

Jiménez Gil, W. (2025). *La responsabilidad objetiva de los bancos en los casos de fraude electrónico en Colombia*. Revista Misión Jurídica, 18 (28), 127 -153.

Ley No. 7558, Ley Orgánica del Banco Central de Costa Rica. 3 de noviembre de 1995. Diario Oficial La Gaceta N.º 225.

Ley No. 7732, Ley Reguladora del Mercado de Valores. 17 de diciembre de 1997. Diario Oficial La Gaceta N.º 18.

Lightowler-Stahlberg Juanes, P. (2023). *La responsabilidad civil, en el ámbito penal, de las entidades bancarias ante el auge de las estafas informáticas.* Oliva-Ayala Abogados. https://www.oliva-ayala.es/la-responsabilidad-civil-en-el-ambito-penal-de-las-entidades-bancarias-ante-el-auge-de-las-estafas-informaticas

López Casal, Y. (2009). *El nexo causal en la responsabilidad civil extracontractual.* Revista Judicial de Costa Rica, (90). 119-152.

López Casal, Y. (2016). *La imputación objetiva y sus criterios en el derecho de daños costarricense.* Revista Judicial de Costa Rica, (119). 108-124.

López Díaz, Patricia Verónica. (2022). El consumidor hipervulnerable como débil jurídico en el derecho chileno: una taxonomía y alcance de la tutela aplicable. *Latin american legal studies*, *10*(2), 340-415. https://dx.doi.org/10.15691/0719-9112vol10n2a7

López Martínez, F. (2017). *El deber de garantía en la responsabilidad civil*. Revista de Derecho Privado, 30(1), 78-95.

Lorenzetti, R. L. (2006). *Responsabilidad civil: fundamentos para un nuevo paradigma.* Rubinzal-Culzoni.

Maiwald, Eric (2005). *Fundamentos de Seguridad de Redes.* (2.ª ed.). Mc Graw-Hill Interamericana Editores, S.A.

Mazeaud, H., Mazeaud, L., & Tunc, A. (1963). *Tratado teórico y práctico de la responsabilidad civil* (Tomo I, Vol. I). Ediciones Jurídicas Europa-América.

MICITT. (2023). *Estrategia Nacional de Ciberseguridad Costa Rica 2023–2027.* Ministerio de Ciencia, Innovación y Telecomunicaciones. Recuperado de https://www.micitt.go.cr/sites/default/files/2023-06/Estrategia-Nacional-de-Ciberseguridad-MICITT-2023-2027.pdf

MICITT. (2023). Informe nacional sobre ciberseguridad 2022–2023. Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones.

Monroy Mejía, M. D. L. Á. y Nava Sánchez llanes, N. (2018). *Metodología de la investigación.* Grupo Editorial Éxodo. https://elibro.net/es/ereader/bibliouia/172512?page=99.

Montero Piña, F. (1999). *Obligaciones* (5.ª ed.). Premiá Editores.

Mora S. (2025). *Defensoría urge la aprobación de proyecto de ley para proteger a consumidores frente a fraudes electrónicos.* Delfino https://delfino.cr/2025/04/defensoria-urge-la-aprobacion-de-proyecto-de-ley-para-proteger-a-consumidores-frente-a-fraudes-electronicos

Mosset Iturraspe, J. (2004). *Responsabilidad por daños* (T. I). Rubinzal-Culzoni.

Murillo E. (2025) *Denuncias por delitos informáticos crecieron 300% en seis años.* CR HOY https://www.crhoy.com/denuncias-por-delitos-informaticos-crecieron-300-en-seis-anos/

Ñaupas Paitán, H., Valdivia Dueñas, M. R., Palacios Vilela, J., & Romero Delgado, H. E. (2018). *Metodología de la investigación cuantitativa-cualitativa y redacción de la tesis* (5.ª ed.). Ediciones de la U.

OFC. (2025) Sobre la Oficina al Consumidor y sus servicios. https://www.ocf.fi.cr/

Organismo de Investigación Judicial. (2024). *Denuncias relacionadas con delitos informáticos*. Sección de Delitos Informáticos.

Ormazabal, G. (2017). *Discriminación y carga de la prueba en el proceso civil.* Marcial.

Padilla, J., Rueda, N., & Zafra Sierra. (2014). *Labor creadora de la jurisprudencia de la "Corte de Oro": Los ejemplos de la causa del contrato, el error de derecho y la responsabilidad por actividades peligrosas*. Revista de Derecho Privado, (26), 105–156.

Pantaleón, F. (1991). *Responsabilidad civil: función y fundamentos.* Anuario de Derecho Civil, 44(2), 345–378.

Patiño, H. (2008). *Responsabilidad extracontractual y causales de exoneración aproximación a la jurisprudencia del consejo de estado colombiano.* Revista de Derecho Privado, N°14. https://revistas.uexternado.edu.co/index.php/derpri/article/view/555/525

Pérez, V. (1994). *Derecho privado* (3.ª ed.). Litografía e Imprenta LIL, S.A.

Pérez, L. (1994). *Teoría general de la responsabilidad civil.* Editorial Dykinson.

Pizarro, R. D., & Vallespinos, C. G. (2009). *Instituciones de Derecho Privado – Obligaciones* (2ª ed.). Hammurabi.

Procuraduría General de la República. (2015, 3 de febrero). Dictamen C-015-2015. Sistema Costarricense de Información Jurídica (SCIJ).

https://pgrweb.go.cr/scij/Busqueda/Normativa/pronunciamiento/pro_ficha.aspx?param1=PRD&param6=1&nDictamen=18687&strTipM=T

Reglero Campos, F. (2006). Tratado de Responsabilidad Civil (Tercera ed.). Navarra: Arazandi, S.A.

Rodríguez Azuero, Sergio (2002). *Contratos Bancarios: su significación en América Latina. Colombia.* (5.ª ed.). Legis Editores S.A.

Rodríguez Bonilla, J. A. (2022). *Estafas mediante sistemas informáticos de entes financieros.* IURITec. https://iuritec.com/jurisis-notas/estafas-mediante-sistemas-informaticos-de-entes-financieros/

Rodríguez, A., & Francisco, J. (2023). *El delito de estafa informática: ¿Es posible determinar la responsabilidad civil de la entidad financiera en base al artículo 120.3 del Código Penal como consecuencia del phishing?* Revista de Derecho Penal y Criminología, 30(3), 273–304. https://hdl.handle.net/10481/101164

Saborío, M. (2022). *Ciberdelitos y la banca digital: Desafíos legales en Costa Rica.* Revista Costarricense de Derecho Público, 27(2), 105–127.

Sala Primera de la Corte Suprema de Justicia. (2011). Resolución No. 01477-2011, expediente 09-002692-1027-CA (8 de diciembre de 2011).

Sala Primera de la Corte Suprema de Justicia. (2011). Sentencia No. 000248-F-S1-2011. San José, Costa Rica.

Sala Primera de la Corte Suprema de Justicia. (2012). Resolución No. 00778-2012, expediente 10-003907-1027-CA (3 de julio de 2012).

Sala Primera de la Corte Suprema de Justicia. (2014). Resolución No. 00686-2014, expediente 11-005470-1027-CA (28 de mayo de 2014).

Sala Primera de la Corte Suprema de Justicia. (2014). Resolución No. 00970-2014, expediente 10-002417-1027-CA (24 de julio de 2014).

Sala Primera de la Corte Suprema de Justicia. (2017). Resolución No. 00460-2017, expediente 13-003350-1027-CA (4 de mayo de 2017).

Sala Primera de la Corte Suprema de Justicia. (2020). Resolución No. 02190-2020, expediente 13-007991-1027-CA (13 de agosto de 2020).

Sala Primera de la Corte Suprema de Justicia. (2022). Resolución No. 02056-2022, expediente 15-009564-1027-CA (29 de septiembre de 2022).

Sala Primera de la Corte Suprema de Justicia. (2023). Resolución No. 01307-2023, expediente 19-004967-1027-CA (27 de julio de 2023).

Sala Primera de la Corte Suprema de Justicia. (2023). Resolución No. 01892-2023, expediente 20-002416-1027-CA (2 de noviembre de 2023).

Sala Primera de la Corte Suprema de Justicia. (2024). Resolución No. 00926-2024, expediente 19-006604-1027-CA (10 de julio de 2024).

Sala Primera de la Corte Suprema de Justicia. (2025). Resolución No. 00040-2025, expediente 20-004415-1027-CA (16 de enero de 2025).

Sala Primera de la Corte Suprema de Justicia. (2025). Resolución No. 01456-2025, expediente 21-005915-1027-CA (9 de octubre de 2025).

Sala Primera de la Corte Suprema de Justicia. (2025). Resolución No. 01493-2025, expediente 19-004932-1027-CA (14 de octubre de 2025).

Sala Primera de la Corte Suprema de Justicia. (2025). Resolución No. 01701-2025, expediente 19-003908-1027-CA (18 de noviembre de 2025).

Salas Peña, D. (2010). *Responsabilidad civil bancaria frente al cliente por delitos informáticos* [Tesis de licenciatura, Universidad de Costa Rica]. http://iij.ucr.ac.cr/wp-content/uploads/bsk-pdf-manager/2017/06/Tesis-Daniela-Salas.pdf

Siles A. (2022). *OIJ revela tráfico de datos personales entre empleados bancarios y ciberdelincuentes*. La República. https://www.larepublica.net/noticia/oij-revela-trafico-de-datos-personales-entre-empleados-bancarios-y-ciberdelincuentes

Superintendencia General de Entidades Financieras (SUGEF). (2021). Reglamento sobre Seguridad de la Información para Entidades Financieras.

Superintendencia General de Entidades Financieras (SUGEF). (2023). Indicadores financieros. https://www.sugef.fi.cr/servicios/reportes/IndicadoresFinancieros.aspx

Tamayo Jaramillo, J. (2007). *Tratado de responsabilidad civil* (t. I). Legis Editores S. A.

Taruffo, M. (2008). *La prueba de los hechos.* Trotta.

Telediario Costa Rica. (2023). *Ladrones informáticos han robado más de ₡53 mil millones en 2023*. https://www.telediario.cr/en-alerta/ladrones-informaticos-robado-53-mil-millones-2023

Torrealba, F. (2011). *Responsabilidad civil.* Editorial Juricentro.

Universidad de Costa Rica (UCR). (2023). *Con una mejor cultura digital disminuyen los riesgos de una estafa informática.* UCR Noticias. https://www.ucr.ac.cr/noticias/2023/11/08/con-una-mejor-cultura-digital-disminuyen-los-riesgos-de-una-estafa-informatica.html

Ureña J. (2024). *OIJ recibió más de 4 mil denuncias por fraudes informáticos en el 2023*. Teletica. https://www.teletica.com/nacional/oij-recibio-mas-de-4-mil-denuncias-por-fraudes-informaticos-en-el-2023_359775

Vargas Araya, J. P. (2020). *La importancia de la banca digital en Costa Rica y su aceleración como resultado de la pandemia del COVID-19* [Tesis de grado, Universidad Latinoamericana de Ciencia y Tecnología]. Repositorio ULACIT. https://repositorio.ulacit.ac.cr/bitstream/handle/20.500.14230/10799/REF-1614117157-1.pdf?sequence=1

Vega Briceño, E., Lemaitre Picado, R., Villegas Carranza, A., & Solís Cordoncillo, C. M. (2025). *Estado de la ciberseguridad en Costa Rica 2024.* Universidad Nacional, Sede Regional Chorotega. https://repositorio.una.ac.cr/server/api/core/bitstreams/4853e1b3-c476-4932-9452-252a257c7d4e/content

Villabela Armengol C. (2020) *Pasos hacia una revolución en la enseñanza del derecho en el sistema romano – germánico.* Universidad Nacional Autónoma de Mexico. https://archivos.juridicas.unam.mx/www/bjv/libros/13/6226/22a.pdf

Vindas Castiglioni, J. E. (2022). *Criterios para indemnización de daños y perjuicios conforme con los artículos 40 y 40 bis de la Ley 8039.* Revista Tribuna Libre, 9(1), 61–75. https://revista.uescuelalibre.cr/index.php/tribunalibre/article/view/15/14

Vives M. (2023). *Tres fracciones apoyan proyecto para proteger a costarricenses de estafas bancarias.* Semanario Universidad. https://semanariouniversidad.com/pais/tres-fracciones-apoyan-proyecto-para-proteger-a-costarricenses-de-estafas-bancarias/

Yzquierdo Tolsada, M. (2001). *Sistema de responsabilidad civil contractual y extracontractual.* Dykinson.

Apéndice A. Matriz de análisis jurisprudencial (factor de atribución)

Codificación

CUL	culpa
RC	riesgo creado
OBJ	responsabilidad objetiva
NC+	Nexo causal existe
NC-	Nexo Causal no existe
CV	culpa de la víctima
HT	hecho de tercero
AJ	ajenidad

Nº	**Sentencia**	**Reconstrucción del caso**	**Tipo de fraude**	**Conducta del usuario**	**Conducta del banco**	**Factor**	**Tipo resp.**	**Nexo**	**Ruptura**	**Criterio de la Sala**
1	00040-2025	Llamada fraudulenta, entrega datos, acceso a correo y cuenta	Phishing	Entrega información	Sin falla técnica	OBJ	Objetiva	NC-	CV/AJ	No hay responsabilidad por ajenidad
2	00460-2017	Sustracción con accesos compartidos	Credenciales	Mala custodia	Sistema correcto	OBJ	Objetiva	NC-	CV	Culpa del usuario excluye
3	00686-2014	Ingreso a página falsa	Phishing	Error al ingresar datos	Sin vulneración	OBJ/RC	Objetiva	NC-	CV	Riesgo no cubre negligencia
4	00778-2012	Transferencias no autorizadas	Indeterminado	No probada culpa	No prueba ajenidad	OBJ	Objetiva	NC+	—	Carga dinámica de prueba
5	00926-2024	Entrega de tokens por llamada	Phishing	Facilita claves	Sistema funcional	OBJ	Objetiva	NC-	CV	No hay falla bancaria
6	00970-2014	Fraude vía internet sin entrega probada	Phishing	Niega conducta	No controla canal	RC	Riesgo	NC+	—	Riesgo tecnológico
7	01307-2023	Uso habitual y fraude posterior	Ingeniería social	Conducta diligente	Duda control	OBJ	Objetiva	NC+	—	Valoración del patrón
8	01456-2025	Correos falsos simulando banco	Phishing	Inducido	Posible debilidad	RC	Riesgo	NC+	—	Mayor deber de seguridad

Nº	Sentencia	Reconstrucción del caso	Tipo de fraude	Conducta del usuario	Conducta del banco	Factor	Tipo resp.	Nexo	Ruptura	Criterio de la Sala
9	01477-2011	Débitos por fallas de seguridad	Sistema	Correcta	Incumple protocolos	RC	Riesgo	NC+	—	Responsabilidad bancaria
10	01493-2025	Acceso remoto con AnyDesk	Ingeniería social	Manipulado	Falta prevención	RC	Riesgo	NC+	—	Nuevas modalidades
11	01701-2025	Transferencias desde IP extranjera	Acceso indebido	No participa	No detecta anomalía	RC	Riesgo	NC+	—	Falta de monitoreo
12	01892-2023	Múltiples transacciones inusuales	Ingeniería social	No habitual	Sin control	OBJ	Objetiva	NC+	—	Deber reforzado
13	02056-2022	Uso correcto de credenciales	Acceso válido	Indeterminado	Sistema correcto	OBJ	Objetiva	NC-	AJ	No imputación
14	02190-2020	Usuario entrega clave telefónica	Ingeniería social	Imprudente	Sistema correcto	OBJ	Objetiva	NC-	CV	Culpa de la víctima

Apéndice B. Matriz de análisis jurisprudencial (nexo causal)

Codificación

CI	Contacto inicial
EM	Engaño / manipulación (Estrategia de ingeniería social)
OD	Obtención de datos (Captura de credenciales, OTP, claves)
AS	Acceso al sistema
ET	Ejecución de transacciones
EU	Entrega de información
NC	Negligencia en custodia (Falta de cuidado en credenciales)
ID	Inducido al error
CD	Conducta diligente
NP	No probada
IN	Indeterminada
TF	Tercero Fraudulento
SD	Suplantación digital
AR	Acceso remote
AE	Acceso externo
NA	No acreditado
SB	Sistema adecuado
FS	Falla del Sistema
FM	Falla del monitoreo
DP	Duda probatoria
NCB	No controla canal externo
CV	Culpa de la victima
AJ	Ajenidad del daño
CV/AJ	Culpa + ajenidad
-	No ruptura
RCN	Ruptura del nexo causal (No hay responsabilidad bancaria)
RB	Responsabilidad Bancaria (Se imputa responsabilidad al banco)
MN	Mantenimiento del nexo (No se rompe la relación causal)
DR	Deber reforzado (se exige estándar elevado al banco)
RT	Riesgo tecnológico (se reconoce riesgo inherente)
AN	Análisis Abierto (la sala no define claramente)

Nº	**Sentencia**	**Iter del fraude (reconstrucción)**	**Conducta del usuario**	**Intervención de terceros**	**Conducta del banco**	**Ruptura del nexo causal**	**Criterio de la Sala**
1	00040-2025	CI: llamada → EM: engaño → OD: entrega datos → AS: acceso correo → ET: transferencias	Entrega información confidencial	Delincuentes acceden a correo y cuenta	Sistema sin vulneración	CV / AJ	Se rompe el nexo, banco no responde
2	00460-2017	CI: acceso indebido → OD: credenciales → AS → ET	Falta de custodia de datos	Terceros con acceso posible	Sistema adecuado	CV	Culpa del usuario excluye

Nº	Sentencia	Iter del fraude (reconstrucción)	Conducta del usuario	Intervención de terceros	Conducta del banco	Ruptura del nexo causal	Criterio de la Sala
3	00686-2014	CI: acceso web falsa → EM: phishing → OD → AS → ET	Ingresa datos en sitio falso	Página fraudulenta	Sin falla técnica	CV	Riesgo no cubre negligencia
4	00778-2012	AS → ET (no se acredita iter completo)	No probada	No clara	No prueba ajenidad	—	Se mantiene nexo
5	00926-2024	CI: llamada → EM → OD: tokens → AS → ET	Facilita claves dinámicas	Delincuentes ejecutan fraude	Sistema correcto	CV	Ruptura por conducta del usuario
6	00970-2014	CI: acceso internet → AS → ET (sin OD probado)	Niega entrega datos	Posible ataque externo	Banco no controla canal	—	No se rompe nexo
7	01307-2023	CI desconocido → AS → ET inusual	Conducta diligente	Terceros intervienen	Posible falla control	—	Se mantiene nexo
8	01456-2025	CI: correos falsos → EM → OD → AS → ET	Inducido al error	Suplantación digital	Duda en seguridad	—	Se analiza responsabilidad
9	01477-2011	AS directo → ET (sin intervención usuario)	Correcta	No clara	Falla en protocolos	—	Banco responsable
10	01493-2025	CI: contacto → EM → OD → AS remoto (AnyDesk) → ET	Manipulado	Control remoto por terceros	Falta de prevención	—	Nuevas formas de fraude
11	01701-2025	AS desde IP extranjera → ET	No interviene	Acceso externo	No detecta anomalía	—	Falta de monitoreo
12	01892-2023	AS → ET múltiples transacciones	No habitual	Terceros ejecutan	No bloquea	—	Deber de seguridad reforzado
13	02056-2022	AS con credenciales válidas → ET	Indeterminado	Terceros con datos	Sistema correcto	AJ	Ajenidad rompe nexo
14	02190-2020	CI: llamada → EM → OD → AS → ET	Entrega clave	Terceros ejecutan	Sistema correcto	CV	Culpa de la víctima

Apéndice C. Matriz de análisis jurisprudencial (daño)

Nº	Resolución	¿Existe daño patrimonial?	¿Se otorga?	Tipo de reparación	Criterio sobre daño patrimonial	Daño moral
1	00040-2025	Sí	No	—	Ruptura del nexo causal por culpa de la víctima (ingeniería social)	No
2	00460-2017	Sí	No	—	Custodia deficiente de credenciales (culpa del usuario)	No
3	00686-2014	Sí	No	—	Phishing imputable al usuario (eximente de responsabilidad)	No
4	00778-2012	Sí	Sí	Restitución + intereses + costas	Banco no probó eximentes (se mantiene nexo causal)	No
5	00926-2024	Sí	No	—	Entrega de datos por engaño (hecho de tercero rompe nexo)	No
6	00970-2014	Sí	No	—	No se acredita falla del sistema bancario	No
7	01307-2023	Sí	No	—	No se demuestra vulnerabilidad imputable al banco	No
8	01456-2025	Sí	No	—	Ingeniería social (ajenidad del daño)	No
9	01477-2011	Sí	Sí	Restitución + intereses + costas	Falla en protocolos de seguridad del banco	No
10	01493-2025	Sí	No	—	Fraude por terceros sin imputación al banco	No
11	01701-2025	Sí	Sí	Restitución + intereses + daño moral + costas	No se probó ajenidad del daño (riesgo creado)	Sí, se logra acreditar la afectación emocional directa.
12	01892-2023	Sí	No	—	Patrón anómalo insuficiente para imputar responsabilidad	No
13	02056-2022	Sí	No	—	Acceso con credenciales válidas (ajenidad del daño)	No
14	02190-2020	Sí	No	—	Entrega de claves (culpa de la víctima)	No

Apéndice D. Matriz de análisis normativo con interpretación jurídica de normas civiles y de consumo aplicables a la imputación de responsabilidad bancaria

Norma	Artículo	Contenido normativo relevante	Naturaleza	Interpretación jurídica	Relación con la responsabilidad bancaria	Elemento que incide	Observaciones
Constitución Política de Costa Rica	Art. 46	Reconoce el derecho de los consumidores a la protección de sus intereses económicos y a recibir información veraz y adecuada.	Base constitucional (incide en ambas)	Establece un mandato de protección reforzada al consumidor, imponiendo equilibrio en la relación proveedor–usuario.	Fundamenta la exigencia de servicios bancarios seguros, transparentes y con adecuada información sobre riesgos digitales.	Culpa / Riesgo y daño	Sirve como criterio interpretativo superior en materia de consumo financiero.
Código Civil de Costa Rica	Art. 702	El deudor que incumple su obligación responde por los daños y perjuicios, salvo que la falta provenga del acreedor, fuerza mayor o caso fortuito.	**Contractual**	Consagra la responsabilidad por incumplimiento obligacional, incluyendo incumplimiento defectuoso del servicio.	Permite imputar responsabilidad al banco cuando no cumple adecuadamente el servicio de custodia, seguridad y funcionamiento de plataformas digitales.	Culpa y nexo causal	Norma central para analizar incumplimiento del contrato bancario y sus eximentes.
Código Civil de Costa Rica	Art. 1045	Toda persona que cause daño por dolo, culpa o negligencia está obligada a repararlo.	Extracontractual	Establece el principio general de responsabilidad civil basado en la culpa.	Permite evaluar negligencia del banco en la gestión de sistemas tecnológicos o en la prevención del fraude.	Culpa y daño	Base del régimen clásico de responsabilidad civil.
Código Civil de Costa Rica	Art. 1046 y ss.	Regulan la obligación de reparar el daño y sus alcances.	Extracontractual	Desarrollan el principio de reparación integral del daño.	Aplicables en la determinación del daño indemnizable (patrimonial y moral) en	Daño	Complementan la cuantificación del perjuicio.

Norma	Artículo	Contenido normativo relevante	Naturaleza	Interpretación jurídica	Relación con la responsabilidad bancaria	Elemento que incide	Observaciones
					fraudes bancarios.		
Ley No. 7472 (Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor)	Art. 32	Reconoce derechos fundamentales del consumidor.	Ambas (con énfasis en consumo)	Define al usuario bancario como consumidor protegido.	Permite aplicar el régimen de consumo a los servicios financieros digitales.	Daño y riesgo	Refuerza la posición jurídica del cliente bancario.
Ley No.7472	Art. 34	Establece deberes del proveedor: información, seguridad y calidad del servicio.	Contractual (con efectos objetivos)	Impone deberes de seguridad y prevención de riesgos previsibles.	Obliga a los bancos a advertir riesgos de fraude y adoptar medidas de seguridad en plataformas digitales.	Culpa / Riesgo	Vincula el deber de información con el deber de seguridad.
Ley No. 7472	Art. 35	Responsabilidad por daños derivados del servicio; solo se libera quien demuestre ajenidad.	Objetiva / riesgo creado	Introduce un régimen de responsabilidad objetiva o por riesgo.	Es la norma central para imputar responsabilidad a bancos por fraudes electrónicos.	Riesgo y nexo causal	Permite inversión o redistribución de la carga de la prueba.
Ley No. 7472	Art. 72	Normas de orden público que prevalecen sobre cláusulas contractuales.	Ambas	Impide limitar derechos del consumidor mediante contratos de adhesión.	Evita que bancos excluyan su responsabilidad mediante términos y condiciones.	Culpa / Riesgo	Refuerza carácter imperativo de la protección al consumidor.
Ley No. 8968 (Protección de Datos Personales)	Art. 4	Establece el deber de seguridad en el tratamiento de datos personales.	Extracontractual (con impacto contractual)	Obliga a implementar medidas técnicas y organizativas para proteger la información.	Relaciona la responsabilidad bancaria con la protección de datos financieros y personales del usuario.	Culpa / Riesgo	Refuerza el deber de seguridad tecnológica.

Apéndice E. Matriz de análisis normativo sobre estándares de seguridad tecnológica, deberes regulatorios y caracterización del riesgo tecnológico en la banca digital

Norma	Disposición	Contenido relevante	Tipo de deber	Estándar tecnológico exigido	Riesgo tecnológico asociado	Interpretación jurídica	Relación con responsabilidad bancaria	Observaciones
Acuerdo SUGEF 10-07: Reglamento sobre la Transparencia ante el Usuario Financiero	Capítulo III	Establece controles para prevenir y mitigar estafas informáticas, incluyendo información al usuario, prevención y atención de reclamos.	Seguridad + supervisión	Sistemas de prevención de fraude, monitoreo de operaciones, canales de atención de incidentes	Uso de plataformas digitales y exposición a fraude electrónico	Impone un deber activo de prevención y gestión de incidentes, no solo reactivo.	Permite evaluar si el banco incumplió su deber de seguridad al no prevenir o detectar operaciones fraudulentas.	Norma clave en protección del usuario financiero.
Acuerdo CONASSIF 5-24: Reglamento General de Gobierno y Gestión de TI	Reglamento general	Establece lineamientos sobre gobierno de TI, gestión de riesgos tecnológicos y seguridad informática.	Custodia tecnológica + gestión de riesgos	Implementación de controles de seguridad, gestión de riesgos, auditorías y continuidad del negocio	Riesgos derivados de sistemas informáticos, accesos no autorizados y fallas tecnológicas	Define el estándar técnico mínimo exigible a las entidades financieras.	Permite determinar negligencia técnica del banco en caso de fraude o vulneración del sistema.	Norma central para caracterizar riesgo tecnológico.
Ley Reguladora del Mercado de Valores No. 7732	Art. 171 inc. b	Faculta al CONASSIF a dictar normativa para supervisión del sistema financiero.	Supervisión financiera	Regulación prudencial y técnica del sistema financiero	Riesgo sistémico y tecnológico en operaciones financieras	Reconoce la obligatoriedad de las normas técnicas en materia de seguridad.	Vincula el incumplimiento normativo con la responsabilidad del banco.	Base jurídica de la regulación financiera.
Ley Orgánica	Art. 131 inc. c	Establece facultades	Supervisión	Desarrollo de	Riesgos derivados	Refuerza el marco	Permite exigir	Complementa el

Norma	Disposición	Contenido relevante	Tipo de deber	Estándar tecnológico exigido	Riesgo tecnológico asociado	Interpretación jurídica	Relación con responsabilidad bancaria	Observaciones
del Banco Central No. 7558		de la SUGEF para proponer normativa de supervisión financiera.	financiera	normativa técnica para control del sistema financiero	de innovación tecnológica en servicios financieros	institucional de control y vigilancia del riesgo tecnológico.	cumplimiento de estándares técnicos emitidos por la SUGEF.	sistema de supervisión.
Ley No. 8968 (Protección de Datos Personales)	Art. 4	Establece el deber de adoptar medidas de seguridad para proteger datos personales.	Custodia tecnológica	Medidas técnicas y organizativas para evitar accesos no autorizados	Riesgo de acceso indebido a datos financieros y personales	Impone un deber de seguridad sobre la información gestionada por el banco.	Relaciona la filtración o vulneración de datos con responsabilidad civil bancaria.	Conecta seguridad informática con protección de datos.
Acuerdo SUGEF 10-07 (interpretación sistemática)	Disposiciones sobre información al usuario	Obliga a advertir sobre riesgos del servicio financiero digital.	Seguridad + información	Protocolos de educación al usuario y advertencias de riesgo	Riesgo derivado del uso inadecuado de plataformas digitales	El deber de seguridad incluye el deber de informar riesgos previsibles.	La falta de información puede incidir en la imputación de responsabilidad.	Vincula seguridad con deber de información.
CONASSIF 5-24 (gestión de accesos)	Controles de acceso y autenticación	Exige mecanismos de control de acceso a sistemas y autenticación segura.	Seguridad tecnológica	Autenticación multifactor, control de accesos, gestión de identidades	Riesgo de suplantación de identidad y accesos indebidos	Establece estándares mínimos para evitar intrusiones en sistemas bancarios.	Permite evaluar fallas en autenticación en casos de fraude.	Clave para casos de phishing.
CONASSIF 5-24 (monitoreo y detección)	Gestión de incidentes	Establece mecanismos de monitoreo continuo y	Seguridad + custodia	Sistemas de detección de operaciones inusuales y	Riesgo de transacciones atípicas	El banco debe identificar patrones sospechosos y actuar	Su incumplimiento puede configurar negligencia	Importante para análisis de operaciones atípicas.

Norma	Disposición	Contenido relevante	Tipo de deber	Estándar tecnológico exigido	Riesgo tecnológico asociado	Interpretación jurídica	Relación con responsabilidad bancaria	Observaciones
		respuesta a incidentes.		alertas tempranas	no detectadas	oportunamente.	en el control del sistema.	

Apéndice F. Matriz de análisis probatorio basada en jurisprudencia

Codificación

REG	registros del sistema (logs, accesos)
IP	dirección IP / geolocalización
TRX	transacciones bancarias
TOK	tokens / claves dinámicas
COR	correos electrónicos
PER	peritaje técnico
U	usuario (actor)
B	banco (demandado)
D	dinámica / compartida
EXB	exonera banco
RB	responsabilidad bancaria
NCA	no queda completamente acreditado

Nº	Sentencia	Prueba tecnológica relevante	Tipo de prueba	Valoración de la Sala	Carga de la prueba	Resultado probatorio	Criterio aplicado
1	00040-2025	Acceso a correo + cambio de credenciales	REG / COR	Se acredita acceso mediante datos entregados por la usuaria	B (cumple)	EXB	Ajenidad del daño
2	00460-2017	Informes bancarios + accesos múltiples	REG / TRX	Existencia de terceros con acceso autorizado	U (no prueba)	EXB	Culpa del usuario
3	00686-2014	Acceso a página falsa	REG	Usuario ingresa voluntariamente datos	B (cumple)	EXB	Culpa del usuario
4	00778-2012	Falta de prueba directa	—	Dificultad probatoria del usuario	D	RB	Carga dinámica
5	00926-2024	Tokens y claves entregadas	TOK / TRX	Acceso autorizado por engaño	B (cumple)	EXB	Culpa del usuario
6	00970-2014	Peritaje sobre vulnerabilidad	PER	Banco no controla canal de acceso	B (no cumple)	RB	Riesgo tecnológico
7	01307-2023	Patrón de uso del cliente	TRX	Operaciones inusuales no detectadas	B (no cumple)	RB	Deber de monitoreo
8	01456-2025	Correos y acceso digital	COR / REG	Duda sobre suficiencia de seguridad	B	NCA	Estándar de seguridad
9	01477-2011	Fallas en protocolos	REG	Incumplimiento del sistema	B (no cumple)	RB	Riesgo creado
10	01493-2025	Acceso remoto (AnyDesk)	REG	Nueva modalidad de fraude	B	NCA	Riesgo tecnológico
11	01701-2025	IP extranjera	IP / TRX	Transacciones desde ubicación anómala	B (no cumple)	RB	Falta de monitoreo

Nº	Sentencia	Prueba tecnológica relevante	Tipo de prueba	Valoración de la Sala	Carga de la prueba	Resultado probatorio	Criterio aplicado
12	01892-2023	Múltiples transacciones atípicas	TRX	No se bloquean operaciones irregulares	B (no cumple)	RB	Deber reforzado
13	02056-2022	Uso correcto de credenciales	REG	No hay fallas del sistema	B (cumple)	EXB	Ajenidad del daño
14	02190-2020	Entrega de clave telefónica	REG	Usuario entrega información	B (cumple)	EXB	Culpa del usuario