UNIVERSIDAD DE BELGRANO

Responsabilidad bancaria por fraudes electrónicos:

La protección del consumidor bancario frente a los riesgos digitales.

Alumna: María Micaela Pardo

Tutora: Dra. Camila Di Marino

Carrera: Abogacía

Matricula: 101-34249

DNI: 38.389.635

Índice

Introducción

En las últimas décadas, el sistema financiero atravesó un proceso de transformación profunda impulsado por el avance de las tecnologías de la información. La incorporación de herramientas digitales a la actividad bancaria modificó de manera estructural la forma en que se prestan los servicios financieros, desplazando progresivamente la operatoria tradicional presencial hacia entornos virtuales. Este proceso de digitalización redefinió los canales de vinculación entre las entidades financieras y sus clientes, así como las condiciones en que se celebran y ejecutan las operaciones bancarias. Impulsada tanto por la innovación tecnológica como por la creciente demanda de inmediatez por parte de los usuarios, esta transformación generó indudables beneficios en términos de accesibilidad e inclusión financiera para los usuarios.

Sin embargo, este nuevo escenario también introdujo riesgos específicos vinculados al uso de los canales electrónicos. La expansión de herramientas como el *homebanking*, las aplicaciones móviles y las billeteras virtuales incrementó la exposición de los usuarios a diversas modalidades de fraude, configurando un escenario en el que la seguridad de las operaciones adquiere una relevancia central. Modalidades como el *phishing*, el *vishing*, la suplantación de identidad, la interceptación de credenciales, entre otras, se presentan con mayor frecuencia y mediante mecanismos cada vez más complejos, afectando a usuarios que operan bajo la confianza depositada en los sistemas provistos por las entidades financieras. Estas maniobras no solo se caracterizan por el uso de herramientas tecnológicas, sino también por las dificultades que presentan para su prevención y detección, lo que plantea desafíos específicos en materia jurídica y, particularmente, en el ámbito de la responsabilidad.

El eje del problema en estos supuestos radica en determinar quién debe soportar las consecuencias del daño derivado del fraude. Frente a una operación bancaria no autorizada, surge el interrogante acerca de si el perjuicio debe ser asumido por el cliente (en razón de su eventual intervención en la maniobra o de su falta de diligencia en el resguardo de sus credenciales) o por la entidad financiera, en su carácter de organizadora y administradora profesional del sistema a través del cual la operación se ejecuta. Este interrogante no puede resolverse únicamente a partir de la conducta individual de las partes, sino que exige analizar la estructura del servicio, el nivel de seguridad del canal y la distribución de riesgos propia de la actividad bancaria digital.

La problemática adquiere una dimensión particular cuando la relación entre las partes se encuadra en el marco de una relación de consumo. En este ámbito, el usuario o consumidor bancario es considerado un sujeto especialmente vulnerable, no solo por la asimetría económica y contractual que caracteriza su vínculo con la entidad bancaria, sino también por la complejidad técnica del servicio que utiliza. Esta vulnerabilidad se intensifica en los entornos digitales, donde el consumidor opera a través de sistemas cuya arquitectura desconoce y cuyos mecanismos de

seguridad no controla, en tanto su gestión depende, en gran medida, del proveedor. A ello se suma que, en la mayoría de los casos, el consumidor resulta cautivo del canal electrónico, dado que numerosas operaciones han dejado de ofrecerse en forma presencial, de manera que la utilización de estos medios no responde a una elección libre sino a una imposición derivada de la propia organización del servicio bancario. En tales condiciones, la confianza que el usuario deposita en la entidad se erige como un elemento estructural de la relación jurídica, lo que justifica la aplicación de un régimen tuitivo orientado a equilibrar las posiciones de las partes. En este marco, el derecho del consumidor introduce criterios específicos que inciden en el análisis de la responsabilidad. Entre ellos, adquiere especial relevancia el deber de seguridad, entendido como la obligación del proveedor de garantizar que los servicios ofrecidos no generen riesgos indebidos para la persona o los bienes del consumidor. En el ámbito de la actividad bancaria, este deber se proyecta sobre la protección del patrimonio del usuario y se vincula con la exigencia de implementar mecanismos adecuados de prevención y detección frente a operaciones fraudulentas. Su alcance y contenido resultan especialmente relevantes para examinar cómo deben distribuirse los riesgos derivados de la operatoria digital y, en consecuencia, para abordar el problema de la responsabilidad frente a los daños producidos por fraudes electrónicos.

A su vez, el análisis de esta problemática no puede prescindir del rol del Banco Central de la República Argentina como autoridad de regulación y supervisión del sistema financiero. A través de un conjunto de normas técnicas y organizativas, el organismo ha establecido estándares mínimos en materia de seguridad de la información, autenticación de usuarios, monitoreo transaccional y prevención del fraude. Estas disposiciones, si bien tienen naturaleza administrativa, adquieren relevancia jurídica como parámetros de conducta profesional, en tanto permiten delimitar el contenido del deber de seguridad exigible a las entidades financieras en el entorno digital.

En virtud de lo expuesto, el presente trabajo se propone analizar el siguiente interrogante: ¿cuál es el alcance de la responsabilidad de las entidades bancarias frente a fraudes electrónicos en el marco de una relación de consumo, y en qué medida puede eximirse de dicha responsabilidad? La respuesta a esta pregunta exige articular distintos subsistemas normativos: el régimen de protección del consumidor previsto en la Ley 24.240 y en el Código Civil y Comercial de la Nación, y las normas reglamentarias del Banco Central de la República Argentina en materia de seguridad de canales electrónicos.

El trabajo se estructura en cinco capítulos. El primero examina el derecho del consumidor y su aplicación al sistema bancario, con especial atención a la figura del consumidor bancario y su vulnerabilidad en entornos digitales. El segundo analiza la transformación digital del sistema financiero y las características de los fraudes electrónicos que emergen en este contexto. El tercero estudia el marco regulatorio del Banco Central en materia de seguridad de canales electrónicos y su relevancia jurídica como parámetro de conducta. El cuarto aborda el régimen

de responsabilidad civil aplicable, con especial énfasis en el factor de atribución, el deber de seguridad y las causales de exoneración. Por último, el quinto capítulo examina el tratamiento jurisprudencial de la cuestión, a fin de identificar las tendencias actuales y los criterios predominantes en la resolución de estos conflictos.

I. Hipótesis

La expansión de los canales digitales en el sistema bancario argentino ha incrementado la exposición de los consumidores a fraudes electrónicos. Frente a ello, las entidades bancarias, en su carácter de organizadoras profesionales del sistema a través del cual se ejecutan dichas operaciones, deben asumir una responsabilidad de naturaleza objetiva, fundada en el deber de seguridad y en el riesgo propio de la actividad bancaria digital. El incumplimiento de estos deberes genera responsabilidad frente al consumidor por los daños derivados de operaciones digitales no consentidas, sin que la entidad pueda eximirse invocando la ausencia de culpa o el cumplimiento formal de la normativa regulatoria, sino únicamente acreditando una causa ajena que reúna los requisitos de imprevisibilidad, inevitabilidad y ajenidad respecto del sistema que organiza y explota.

II. Objetivos

Objetivo general: Analizar el alcance de la responsabilidad de las entidades financieras frente a fraudes electrónicos en el marco de las relaciones de consumo, a fin de determinar el factor de atribución aplicable, el contenido del deber de seguridad y los criterios de imputación desarrollados por la doctrina, la normativa y la jurisprudencia.

Objetivos específicos:

- Examinar la aplicación del régimen de defensa del consumidor a la actividad bancaria, con especial referencia a la figura del consumidor o usuario bancario y su situación de vulnerabilidad, particularmente en entornos digitales.
- Analizar el proceso de digitalización del sistema financiero y su impacto en la configuración de nuevos riesgos, en especial los fraudes electrónicos y sus principales modalidades.
- Estudiar el marco normativo dictado por el Banco Central de la República Argentina en materia de seguridad de los canales electrónicos, identificando los estándares de conducta exigibles a las entidades financieras.
- Determinar el factor de atribución aplicable a la responsabilidad bancaria por fraudes electrónicos, evaluando las limitaciones del modelo subjetivo y los fundamentos del régimen objetivo en este ámbito.

- Analizar el contenido y alcance del deber de seguridad en la actividad bancaria digital, como eje estructural de imputación de responsabilidad.
- Evaluar en qué medida la conducta del usuario o el hecho de terceros pueden interrumpir el nexo causal y operar como eximentes de la responsabilidad bancaria, determinando los supuestos en que dichas causales son admitidas y los criterios restrictivos con que la jurisprudencia las interpreta.
- Analizar el tratamiento jurisprudencial de los fraudes electrónicos bancarios, identificando tendencias en materia de factor de atribución, deber de seguridad y admisión de eximentes.

III. Metodología

El presente trabajo se inscribe en el campo de la investigación jurídica y tiene por objeto analizar el alcance de la responsabilidad de las entidades financieras frente a fraudes electrónicos en el marco de relaciones de consumo. En función de dicho objetivo, la estrategia metodológica adoptada responde a la necesidad de articular el estudio del marco normativo vigente, los desarrollos doctrinarios y la forma en que estos han sido receptados por la jurisprudencia.

Tipo de investigación: la investigación desarrollada es de carácter descriptivo-analítico (dogmático-jurídico), en tanto se orienta al análisis, interpretación y sistematización de normas jurídicas, principios y categorías conceptuales aplicables a la responsabilidad civil en el ámbito de los servicios financieros digitales. Este enfoque permite reconstruir el régimen jurídico vigente, identificar sus fundamentos y evaluar su coherencia interna frente a los supuestos de fraude electrónico. A su vez, el trabajo incorpora un componente empírico de tipo cualitativo, reflejado en el análisis de precedentes jurisprudenciales relevantes. Este componente no tiene por finalidad la medición estadística de resultados, sino la observación e interpretación de los criterios utilizados por los tribunales en la resolución de casos concretos, con el objeto de identificar tendencias y verificar la recepción práctica de los postulados teóricos desarrollados. Este enfoque resulta adecuado en la medida en que el problema de investigación no se agota en la identificación de normas aplicables, sino que requiere analizar cómo estas interactúan entre sí, cómo son interpretadas por la doctrina y cómo son aplicadas por los tribunales frente a situaciones concretas.

Diseño de la investigación: el diseño de la investigación es descriptivo y analítico. Es descriptivo, ya que se orienta a caracterizar el régimen jurídico aplicable a la responsabilidad de las entidades financieras frente a fraudes electrónicos, identificando sus elementos, fundamentos y alcances. Es analítico, en la medida en que se examinan críticamente las distintas fuentes normativas, doctrinarias y jurisprudenciales, estableciendo relaciones entre ellas y evaluando su adecuación para dar respuesta al problema planteado. El desarrollo del trabajo sigue una lógica progresiva: parte del encuadre conceptual del derecho del consumidor y la actividad bancaria,

avanza hacia la comprensión del fenómeno tecnológico y sus riesgos, analiza el marco regulatorio específico y, finalmente, construye el régimen de responsabilidad y lo contrasta con su aplicación jurisprudencial.

Técnicas de recolección de datos: La investigación se sustenta en técnicas propias del análisis jurídico, entre las que se destacan:

- Análisis normativo: se examinan las disposiciones relevantes del ordenamiento jurídico argentino, en particular la Constitución Nacional (art. 42), la Ley 24.240 de Defensa del Consumidor, el Código Civil y Comercial de la Nación y la normativa dictada por el Banco Central de la República Argentina en materia de seguridad de los canales electrónicos y protección de usuarios de servicios financieros.
- Análisis doctrinario: se revisan aportes de la doctrina nacional especializada en derecho del consumidor, responsabilidad civil y derecho bancario, con el objeto de identificar las principales posiciones teóricas en torno al factor de atribución, el deber de seguridad y la distribución de riesgos en la actividad bancaria digital.
- Análisis jurisprudencial: se estudian pronunciamientos judiciales relevantes en materia de fraudes electrónicos bancarios, a fin de observar cómo los tribunales interpretan y aplican las normas y principios analizados en el plano teórico.

En definitiva, la metodología adoptada posibilita examinar de manera integral la responsabilidad de las entidades financieras frente a fraudes electrónicos, considerando no solo el marco normativo aplicable, sino también su interpretación doctrinaria y su concreción en la jurisprudencia, lo que resulta indispensable para formular conclusiones sólidas y jurídicamente fundadas.

IV. Marco Teórico

Capítulo 1. El derecho del consumidor y su aplicación al sistema bancario

1.1. El derecho del consumidor en el ordenamiento legal argentino

El derecho del consumidor es una rama del ordenamiento jurídico orientada a equilibrar las relaciones de poder desigual que se generan entre consumidores y proveedores en el ámbito de la economía de mercado. Su finalidad radica en la necesidad de corregir las desigualdades derivadas de la posición de vulnerabilidad del consumidor final frente al poder económico y técnico de quienes producen y comercializan bienes o servicios. En palabras de Farina, *"el derecho del consumidor es el conjunto orgánico de normas, capaces de constituir una rama del*

derecho, que tiene por objeto la tutela de quienes contratan para la adquisición de bienes y servicios destinados, en principio, a las necesidades personales".[1]

Como sostiene Álvarez Larrondo, el surgimiento de esta disciplina se vincula con los profundos cambios sociales y económicos que acompañaron la transición de la sociedad industrial, basada en la ética del trabajo y la producción, hacia la sociedad de consumo, centrada en el poder adquisitivo y la circulación constante de bienes. La producción en masa, la expansión del crédito, la estandarización contractual y la influencia de la publicidad generaron un nuevo modelo de intercambio económico en el que los consumidores quedaron expuestos a prácticas comerciales cada vez más complejas. En este contexto, comenzó a gestarse un cuerpo normativo destinado a moderar los efectos de esas transformaciones, dando origen al derecho del consumidor como respuesta jurídica frente a las nuevas dinámicas del mercado y la necesidad de garantizar relaciones más equitativas entre sus participantes.[2]

En el ámbito normativo, en Argentina se sancionó en 1993 la ley 24.240, Ley de Defensa del Consumidor (en adelante, la "LDC"). Dicha ley introdujo una regulación específica para las relaciones de consumo y tal como afirman Mosset Iturraspe y Lorenzetti: *"el dictado de la Ley de Defensa del Consumidor es, por una parte, la culminación de una normativa que a través de muchos años se ha ido ocupando de fenómenos de mercado, de cuestiones juzgadas abusivas o inadmisibles para una economía con pretensión de justicia y equidad".*[3] Con esta ley, se consolidó una nueva lógica jurídica basada en el reconocimiento de la vulnerabilidad estructural del consumidor frente al proveedor y en la necesidad de garantizar relaciones contractuales más equilibradas y transparentes.

Luego, la reforma de la Constitución Nacional del año 1994 incorporó el artículo 42 en donde se otorgó jerarquía constitucional a la protección de los derechos de los consumidores y usuarios. Dicho artículo reconoce que *"los consumidores y usuarios de bienes y servicios tienen derecho, en la relación de consumo, a la protección de su salud, seguridad e intereses económicos; a una información adecuada y veraz; a la libertad de elección, y a condiciones de trato equitativo y digno".*[4] Además, impone al Estado el deber de proveer educación para el consumo y garantizar mecanismos eficaces de protección frente a prácticas abusivas. Esta reforma resultó especialmente relevante porque elevó a rango constitucional la tutela del consumidor, consolidando su carácter de derecho fundamental dentro del sistema jurídico argentino.

---

[1] FARINA, Juan M., *Contratos comerciales modernos: Modalidades de contratación empresaria*, 2.ª ed., 1.ª reimp., Buenos Aires: Astrea, 1999, p. 248.
[2] ÁLVAREZ LARRONDO, Fernando M., "La lógica de la sociedad de consumo", en Fernando M. Álvarez Larrondo (ed.), *Manual de derecho del consumo*, Buenos Aires: Erreius, 2017, pp. 3-11.
[3] MOSSET ITURRASPE, Jorge y LORENZETTI, Ricardo L., cit. por CAMPOS, Pablo A., "La ley de defensa del consumidor y sus implicancias actuales", en *Revista Perspectivas de las Ciencias Económicas y Jurídicas*, Vol. 1 N.º 1, 2011, p. 100.
[4] Constitución de la Nación Argentina, art. 42.

Con posterioridad, la LDC fue objeto de sucesivas reformas (entre ellas, la ley 24.568, 24.787 y 24.999) que ampliaron y fortalecieron su alcance. El cambio más significativo se produjo con la sanción de la Ley 26.361 en 2008, la cual reformó de manera profunda numerosos artículos, amplió derechos sustanciales e incorporó figuras innovadoras orientadas a reforzar la tutela del consumidor frente a prácticas abusivas. Entre sus innovaciones más relevantes se destacan la ampliación del concepto de consumidor, equiparando a quienes, sin ser parte directa del contrato, resultan alcanzados por una relación de consumo (art. 1 LDC); la incorporación de mecanismos procesales más eficaces, como las acciones colectivas (art. 52 LDC), el daño punitivo (art. 52 bis LDC); y la reafirmación de principios esenciales como la información veraz que debe ser gratuita (art. 4 LDC) y el trato digno (art. 8 bis LDC).[5]

Finalmente, un nuevo avance se materializó con la promulgación de la Ley 26.994 en 2015, que dio origen al Código Civil y Comercial de la Nación (en adelante, "CCyCN"). Este cuerpo normativo integró al derecho común una regulación específica de los contratos de consumo, sistematizando principios y criterios ya reconocidos por la legislación especial e introduciendo modificaciones complementarias a la propia LDC. El Código no derogó la ley especial, sino que la complementó, estableciendo un piso mínimo de tutela que puede ser ampliado, pero nunca restringido, por las disposiciones de la LDC. De esta forma, el sistema jurídico argentino consolidó un modelo de protección integral, de jerarquía constitucional, que sitúa al consumidor en el centro de las relaciones económicas y promueve un mercado más justo, transparente y equilibrado.

1.1.1 Consumidor, proveedor y relación de consumo

El consumidor o usuario es el objeto de protección de la LDC y se define como aquella persona humana o jurídica que adquiere o utiliza, en forma gratuita u onerosa, bienes o servicios como destinatario final, en beneficio propio o de su grupo familiar o social.[6] Esta definición fue ampliada por la Ley 26.361 y distingue tres categorías de consumidor: el consumidor directo, que es quien adquiere o utiliza el bien o servicio para su propio beneficio o el de su entorno inmediato; el consumidor indirecto, aquel que aunque no contrata de forma directa, utiliza o se beneficia del producto o servicio; y el consumidor expuesto, entendido como toda persona que, sin haber intervenido en la contratación ni en el uso del bien o servicio, se encuentra igualmente alcanzada por las prácticas comerciales o por los daños que éstas puedan ocasionar.[7]

El concepto de proveedor se encuentra definido en el artículo 2 de la LDC, que lo describe como la persona humana o jurídica, de naturaleza pública o privada, que desarrolla de manera

[5] CAMPOS, ob. cit., pp. 102-114

[6] Ley N° 24.240, Ley de Defensa del Consumidor ("LDC"), art. 1; Código Civil y Comercial de la Nación ("CCyCN"), art. 1092

[7] ÁLVAREZ LARRONDO, Fernando M., "Elementos de la relación de consumo. El concepto de consumidor", en Fernando M. Álvarez Larrondo (ed.), *Manual de derecho del consumo*, Buenos Aires: Erreius, 2017, pp. 63-98.

profesional, aún de forma ocasional, actividades de producción, montaje, creación, comercialización, etc. de bienes y servicios destinados a consumidores o usuarios. La enumeración de actividades contenida en la norma es meramente enunciativa, lo que permite comprender dentro de esta categoría a cualquier sujeto que participe profesionalmente en el circuito económico. La ley exceptúa expresamente a quienes prestan servicios profesionales liberales que requieran título universitario y matrícula habilitante, dado que dichos servicios se encuentran regulados por normativas específicas.

Por último, resulta fundamental definir el concepto de relación de consumo, entendido como el *"vínculo jurídico que se establece entre el proveedor y el consumidor o usuario"*.[8] Este vínculo constituye el marco general dentro del cual se desarrollan las interacciones entre ambos sujetos y sirve de base para la aplicación de las normas del derecho del consumidor. Es importante destacar que la naturaleza jurídica de la relación de consumo es de orden público, lo que implica que las normas que la regulan son inderogables y no pueden ser modificadas por acuerdo de las partes en perjuicio del consumidor.[9]

A diferencia del contrato de consumo, la relación de consumo trasciende el marco estrictamente contractual, ya que puede tener su origen en diversas fuentes jurídicas, como hechos lícitos, ilícitos o declaraciones unilaterales de voluntad.[10] Es decir, la protección del derecho del consumidor no se limita al acto de contratar, sino que se extiende a cualquier situación en la que un proveedor ejerza su poder económico o técnico en el mercado frente a un consumidor. El contrato de consumo, en cambio, representa la forma más característica y habitual de este vínculo jurídico. Según el art. 1093 CCyCN, se trata de aquel *"celebrado entre un consumidor o usuario final con una persona humana o jurídica que actúe profesional u ocasionalmente o con una empresa productora de bienes o prestadora de servicios, pública o privada, que tenga por objeto la adquisición, uso o goce de los bienes o servicios por parte de los consumidores o usuarios, para su uso privado, familiar o social".*[11] Su estructura responde al modelo de contrato de adhesión, en el que el proveedor predispone las condiciones generales mientras el consumidor solamente puede aceptarlas o rechazarlas, sin posibilidad real de negociación individual. Este desequilibrio justifica la intervención del Estado mediante normas de orden público que buscan restablecer la equidad contractual y asegurar una tutela efectiva a la parte más débil.

[8] LDC, art. 3; CCyCN, art. 1092

[9] TAMBUSSI, Carlos E. "El principio de orden público y el régimen tuitivo consumidor en el derecho argentino." *Lex-Revista de la Facultad de Derecho y Ciencias Políticas*, 2016, vol. 14, no 18, pp. 65-81

[10] ZENTNER, Diego, "Régimen general del contrato de los contratos y las relaciones de consumo", en Carlos A. Ghersi y Celia Weingarten (dirs.), *Manual de contratos civiles, comerciales y de consumo*, 4.ª ed., Buenos Aires: La Ley, 2017, pp. 547-567.

[11] CCyCN, art. 1093

1.1.2. Principios rectores del derecho del consumidor

El derecho del consumidor se sustenta en un conjunto de principios que orientan la interpretación y aplicación de toda la normativa protectora. Entre ellos se destaca el deber de información, previsto en el art. 4 de la LDC y en el art. 1100 del CCyCN. Este principio indica que el proveedor tiene la obligación de suministrar al consumidor información adecuada, veraz, clara, detallada y gratuita sobre los bienes y servicios que ofrece, abarcando tanto sus características esenciales como las condiciones de su comercialización. Este deber se encuentra constitucionalizado en el art. 42 de la Constitución Nacional y constituye un elemento esencial del consentimiento, ya que solo mediante información completa y comprensible el consumidor puede tomar decisiones libres y conscientes al momento de contratar, evitando así que haya un vicio de voluntad.[12]

Otro principio esencial, cuyo alcance específico en materia de responsabilidad bancaria por fraudes electrónicos será desarrollado en un capítulo posterior, es el deber de seguridad, consagrado en los arts. 5 y 6 de la LDC. Este principio impone al proveedor la obligación de garantizar que los bienes y servicios ofrecidos en el mercado no generen riesgos irrazonables para la persona o los bienes del consumidor cuando sean utilizados en condiciones normales o previsibles de uso.[13] En caso de que el uso del producto o servicio implique algún peligro, el proveedor debe advertirlo de manera adecuada e informar sobre las medidas necesarias para su correcta utilización.

El principio de trato digno, equitativo y no discriminatorio, previsto en el art. 8 bis de la LDC y en los arts. 1097 y 1098 del CCyCN, impone al proveedor el deber de garantizar un trato respetuoso hacia los consumidores y usuarios y el resguardo de su dignidad conforme a los estándares establecidos por los tratados internacionales de derechos humanos. Los proveedores no pueden establecer diferencias basadas en criterios discriminatorios o contrarios a la garantía constitucional de igualdad. En consecuencia, deben abstenerse de realizar prácticas o conductas que generen situaciones degradantes, humillantes, intimidatorias o vejatorias hacia los usuarios o consumidores.[14]

El principio de protección de los intereses económicos del consumidor busca resguardar los derechos patrimoniales y la equidad en las transacciones. El art. 42 de la Constitución Nacional reconoce expresamente que los consumidores y usuarios tienen derecho a la protección de su salud, seguridad e intereses económicos, lo que implica la exigencia de calidad, eficiencia y

[12] LEIVA, Claudio F., et. al, “Responsabilidad de las plataformas electrónicas”, en Javier Yaquemet y Carlos E. Tambussi (coords.), *Derecho de los usuarios y consumidores*, Buenos Aires: Abeledo Perrot, 2025, pp. 5-17.

[13] BAROCELLI, Sergio S. "El concepto de consumidor de servicios financieros y bursátiles y el rol del Estado", ponencia presentada en la Comisión N° 8 "Protección del consumidor de servicios financieros y bursátiles" de las XXV Jornadas Nacionales de Derecho Civil, Bahía Blanca, 2015

[14] STIGLITZ, Rubén S., “Título III. Contratos de consumo”, en M. Herrera, G. Caramelo y S. Picasso (dirs), *Código civil y comercial de la Nación comentado*, Tomo III, 1ra. ed, Buenos Aires: Infojus, 2015, pp. 492-292

transparencia en los productos y servicios, así como el acceso a mecanismos administrativos y judiciales eficaces. Este principio se concreta, entre otros aspectos, en la posibilidad del consumidor de exigir la restitución de las sumas abonadas o el cumplimiento del contrato ante el incumplimiento del proveedor. Para esto, se encuentran herramientas relevantes para la reparación y sanción de los perjuicios económicos sufridos por los consumidores, como el daño directo (art. 40 bis LDC) y el daño punitivo (art. 52 bis LDC), destinadas a garantizar una compensación adecuada y prevenir y disuadir conductas abusivas.

Finalmente, el principio *in dubio pro consumidor*, consagrado en el art. 3 de la LDC y en el art. 1094 del CCyCN, establece que en caso de duda sobre la interpretación de las normas que regulan las relaciones de consumo, debe prevalecer siempre la interpretación más favorable al consumidor. Este principio refuerza el carácter tuitivo del sistema y asegura que toda controversia sea resuelta desde una perspectiva protectora, en coherencia con el mandato constitucional de defensa de los consumidores.[15]

En conjunto, estos principios configuran un régimen jurídico orientado a la efectividad de los derechos del consumidor, que se apoya en la transparencia, la seguridad, la equidad y la reparación integral frente a los abusos del mercado. Constituyen, en definitiva, la base sobre la cual debe analizarse la actividad bancaria cuando esta se desarrolla en el marco de una relación de consumo.

1.2. Aplicación del régimen de consumo a la actividad bancaria

Definido el concepto de consumidor y delimitada la relación de consumo, corresponde precisar, a los efectos de este trabajo, el encuadre jurídico del cliente bancario dentro del sistema de protección al consumidor. En tal sentido, resulta necesario determinar en qué medida las operaciones y servicios financieros ofrecidos por las entidades bancarias pueden quedar comprendidos en una relación de consumo y, en consecuencia, bajo la tutela del régimen previsto por la LDC y leyes complementarias.

La actividad bancaria consiste esencialmente en la intermediación entre la oferta y la demanda de dinero, mediante la captación de depósitos del público y la concesión de créditos. Estas funciones, a su vez, se complementan con otros servicios bancarios, tales como la gestión de medios de pago y la provisión de servicios financieros diversos que posibilitan el funcionamiento del sistema económico. Esta actividad se encuentra regulada por la Ley 21.526 de Entidades Financieras (en adelante, la “LEF”), cuya autoridad de aplicación es el Banco Central de la República Argentina (en adelante, el “BCRA”).

---

[15] BAROCELLI, Sergio S., "Los principios del derecho del consumidor como orientadores de la interpretación y aplicación en el diálogo de fuentes", en S. S. Barocelli (coord.), *Impactos del nuevo Código Civil y Comercial en el Derecho del Consumidor. Diálogos y perspectivas a la luz de sus principios.,* 1ra. Edición, Instituto de Investigaciones Jurídicas y Sociales Ambrosio L. Gioja, Facultad de Derecho, Universidad de Buenos Aires, Buenos Aires, 2016, pp. 8-37

Desde una perspectiva jurídica, la vinculación entre las entidades financieras y sus clientes se materializa a través de los contratos bancarios, definidos como los acuerdos mediante los cuales el banco asume obligaciones vinculadas a su actividad, tales como la recepción, custodia o entrega de fondos, la concesión de créditos o la ejecución de operaciones accesorias.[16] La mayoría de estos contratos responden al modelo de contrato de adhesión, en el que las condiciones generales son predispuestas unilateralmente por la entidad financiera y el cliente se limita a aceptarlas, sin posibilidad real de negociación individual. En este contexto, surge la cuestión de si los contratos bancarios, en tanto instrumentos jurídicos de la actividad financiera, pueden considerarse contratos de consumo y, en consecuencia, quedar sujetos al régimen tuitivo de la LDC.

La respuesta no es uniforme para toda la actividad bancaria, dado que no todos los contratos bancarios se enmarcan dentro de una relación de consumo. Solo quedan comprendidos en el régimen de consumo aquellos contratos bancarios en los que el cliente actúa como destinatario final del servicio, es decir, cuando lo utiliza para satisfacer necesidades personales, familiares o sociales, sin incorporarlo a un proceso productivo o actividad profesional. Por el contrario, cuando el servicio se integra a una actividad comercial o empresarial, el régimen protectorio no resulta aplicable. Los contratos bancarios que no encuadran en una relación de consumo quedan fuera del objeto del presente trabajo, que se circunscribe al análisis de los supuestos en que el cliente reviste la calidad de consumidor.

En este sentido, las normas de la LDC resultan plenamente aplicables a los contratos bancarios cuando se verifica esa condición de destinatario final. Así lo establece el art. 1384 del CCyCN, al disponer que las disposiciones relativas a los contratos de consumidor son aplicables a los contratos bancarios celebrados en los términos del art. 1093 del CCyCN, norma que define el contrato de consumo por el destino privado, familiar o social del bien o servicio adquirido. Así, la nota definitoria del consumo bancario radica en el agotamiento del servicio en la satisfacción de necesidades privadas, de modo que no habrá contrato de consumo cuando la adquisición o el servicio se incorpore a un proceso de producción. Es precisamente en ese universo de relaciones donde se inscribe el análisis que desarrolla este trabajo.

1.3. El usuario bancario y su especial vulnerabilidad

Establecida la aplicabilidad del régimen de consumo a determinadas relaciones bancarias, corresponde precisar quién son los sujetos protegidos en este ámbito particular. A tales fines, suele emplearse la expresión consumidor o usuario de servicios financieros para referirse, en sentido amplio, a las personas que contratan o utilizan los productos y servicios ofrecidos por los distintos actores que integran el sistema financiero. Bajo esta categoría quedan comprendidos

[16] FERRER DE FERNÁNDEZ, Esther H. S., “El consumidor bancario en el Código Civil y Comercial de la Nación. Primera parte”, en *Revista de Derecho Comercial y de las Obligaciones*, Thomson Reuters, Cita Online AP/DOC/77/2015

tanto los usuarios de entidades bancarias como aquellos que mantienen relaciones contractuales con otros proveedores de servicios financieros, entre ellos las entidades no bancarias, los proveedores de servicios de pago y demás sujetos sometidos a la regulación sectorial correspondiente.

En este sentido, el BCRA, a través del Texto Ordenado "Protección de los Usuarios de Servicios Financieros", define al usuario de servicios financieros como *"las personas humanas y jurídicas que, en beneficio propio o de su grupo familiar o social y en carácter de destinatarios finales, hacen uso de los servicios ofrecidos por los sujetos obligados, como a quienes de cualquier otra manera están expuestos a una relación de consumo con tales sujetos".*[17] Asimismo, dispone que *"se considerará que revisten ese carácter las personas humanas y las personas jurídicas que no adquieran o utilicen productos o servicios financieros ofrecidos por los sujetos obligados para ser incorporados a su actividad comercial".*[18] Y en este aspecto, la norma define a los sujetos obligados como a las entidades financieras, operadores de cambio, fiduciarios de fideicomisos acreedores de créditos cedidos por entidades financieras, empresas no financieras emisoras de tarjetas de crédito y/o compra, proveedores no financieros de crédito, proveedores de servicios de pago que ofrecen cuentas de pago (PSPCP) y los proveedores de servicios de pago que cumplen la función de iniciación (PSI) y prestan el servicio de billetera digital.

Sobre esta base, amerita delimitar, dentro de la categoría amplia de usuarios de servicios financieros, la figura del consumidor o usuario bancario, en tanto el presente trabajo no aborda la totalidad de las relaciones comprendidas en aquella noción general, sino exclusivamente aquellas que se desarrollan entre consumidores y entidades bancarias en el marco de la prestación de servicios bancarios digitales y de los fraudes electrónicos que pueden producirse durante su ejecución. En consecuencia, a los fines de esta investigación se utilizará preferentemente la expresión usuario o consumidor bancario para referirse a la persona que, en calidad de destinatario final, contrata o utiliza productos y servicios ofrecidos por una entidad bancaria para satisfacer necesidades propias o de su grupo familiar, sin incorporarlos a una actividad empresarial o profesional. Se trata, en definitiva, de una categoría particular comprendida dentro del concepto más amplio de usuario de servicios financieros empleado por la normativa del BCRA.

Ahora bien, aunque el usuario bancario no constituye una categoría autónoma desde el punto de vista normativo (dado que se encuentra comprendido dentro de la noción general de consumidor prevista por la LDC y el CCyCN), las características propias de la actividad bancaria justifican su análisis diferenciado dentro del sistema de tutela consumeril. A diferencia de otros vínculos de

[17] Banco Central de la República Argentina ("BCRA"), Texto Ordenado sobre "Protección de los Usuarios de Servicios Financieros" (texto ordenado al 06/05/2026, última comunicación incorporada "A" 8433), Sección 2, punto 2.3.2.1.
[18] Ídem.

consumo, en los servicios bancarios el usuario se inserta en una estructura técnica de elevada complejidad, en la que la entidad bancaria actúa con profesionalidad, organización empresarial, conocimientos especializados y acceso privilegiado a la información, mientras que el cliente carece habitualmente de las herramientas necesarias para evaluar con precisión el alcance económico y jurídico de las operaciones que realiza. De esta forma, esta asimetría es consecuencia directa de las particulares técnicas de la operatoria bancaria, lo que explica la necesidad de contar con normas protectoras específicas que contemplen esta situación.[19]

De ello deriva que el consumidor bancario se encuentre estructuralmente expuesto a una vulnerabilidad que se manifiesta en distintos planos: una vulnerabilidad técnica e informativa, derivada de la asimetría de conocimientos; una vulnerabilidad contractual, derivada del uso generalizado de contratos de adhesión y condiciones predispuestas que impiden una negociación individual y real de las cláusulas; y, finalmente, una vulnerabilidad de carácter tecnológica, propia de los entornos digitales en los que se desarrolla crecientemente la operatoria bancaria.[20]

Esta situación de desigualdad estructural ha sido expresamente reconocida por el BCRA, que en las últimas décadas ha incorporado la protección de los usuarios de servicios financieros como un eje central de su función regulatoria. Tradicionalmente enfocado en la regulación del sistema financiero desde una perspectiva institucional, el ente rector ha ido incorporando progresivamente la tutela del usuario como eje central de su actuación, reconociendo que la protección del cliente constituye un elemento esencial para el funcionamiento adecuado del sistema.[21] Este cambio de paradigma se consolidó a partir de la reforma de su Carta Orgánica mediante la Ley 26.739, que incorporó expresamente entre las funciones del organismo la de *"proveer a la protección de los derechos de los usuarios de servicios financieros y a la defensa de la competencia, coordinando su actuación con las autoridades públicas competentes en estas cuestiones"*.[22] En cumplimiento de ello, el Texto Ordenado sobre “Protección de los Usuarios de Servicios Financieros” establece reglas de conducta imperativas para las entidades bancarias y un sistema de supervisión tendiente a garantizar su cumplimiento, en consonancia con lo previsto en el artículo 36 de la LDC, que asigna al BCRA la responsabilidad de adoptar las medidas necesarias para asegurar que las entidades bajo su órbita ajusten su actuación a las exigencias de dicha normativa.

---

[19] TSCHIEDER, Vanina G., ob. cit.

[20] ALBORNOZ, Elenay GUILISASTI, Jorgelina, “Derechos de los grupos vulnerables: los consumidores de servicios financieros”, ponencia presentada en la Comisión N° 8 "Protección del consumidor de servicios financieros y bursátiles" de las XXV Jornadas Nacionales de Derecho Civil, Bahía Blanca, 2015.

[21] ÁLVAREZ LARRONDO, Fernando M. y RODRÍGUEZ, Gonzalo M., “Derechos de los consumidores en las relaciones con las entidades bancarias”, en Carlos Ghersi, Celia Weingarten y Graciela Lovece (dirs.), *Derechos de los Consumidores y Empresas en las Relaciones con las Entidades Bancarias*, Buenos Aires: Erreius, 2020, pp. 3-46.

[22] Ley N.º 24.144, Carta Orgánica del Banco Central de la República Argentina, art. 4, inc. h (texto según Ley N.º 26.739).

En este marco, el BCRA impone a las entidades financieras una serie de obligaciones que se complementan con las previstas en la LDC, entre las que se destacan: el deber de trato digno, la protección de su seguridad e intereses económicos, la obligación de brindar información clara, cierta y suficiente, la implementación de canales de atención accesibles, la resolución eficaz de reclamos y la adopción de medidas que aseguren la protección de los usuarios frente a riesgos tecnológicos.[23] De esta manera, la normativa del BCRA se alinea con el estándar de protección establecido a nivel constitucional y legal, reforzando los derechos del consumidor en el ámbito específico e imponiéndoles deberes a las entidades financieras que buscan equilibrar la relación con los usuarios y reducir las asimetrías estructurales que la caracterizan.

Asimismo, la dimensión tecnológica de la vulnerabilidad merece un desarrollo específico en el marco de este trabajo, dado que constituye el eje central del problema que se analiza. Cuando el consumidor bancario opera en el entorno digital que le provee la entidad financiera, su situación de desigualdad se intensifica, dado que el consumidor se inserta en un medio cuya arquitectura desconoce, cuyos mecanismos de seguridad no controla y cuyo funcionamiento depende exclusivamente de decisiones técnicas adoptadas por el proveedor. Como señalan Arias y Müler, a las asimetrías tradicionales de la relación de consumo se suma una desigualdad tecnológica de carácter absoluto, dado que la tecnología es cada vez más compleja en su diseño, aunque se presente de modo simplificado ante el usuario, ocultando aspectos que permanecen bajo el control exclusivo del proveedor.[24]

En este sentido, Tambussi destaca que *"el sistema de comercio por medios electrónicos, lejos de atenuar la responsabilidad de los proveedores que lo utilizan, agrava sus obligaciones porque presupone el uso de una tecnología que exige un mayor conocimiento de su parte. En estos casos hay empresas que actúan profesionalmente y consumidores que no son expertos, en los que la distancia económica y cognoscitiva que existe en el mundo real se mantiene en el mundo virtual. Podríamos afirmar que no solo se mantiene, sino que se profundiza".*[25] En igual sentido, Beltramo y Faliero advierten que cuando el consumidor se encuentra inmerso en el entorno electrónico del proveedor, su vulnerabilidad se incrementa porque opera en un medio que le es completamente ajeno, con mayores desafíos técnicos y con una potencialidad de daños que en muchos casos puede resultar irreparable.[26]

---

[23] HERRERA, Sabrina, "Información contractual continua. El CCyCN y su articulación con la Ley de Defensa del Consumidor", en Carlos Ghersi, Celia Weingarten y Graciela Lovece (dirs.), *Derechos de los Consumidores y Empresas en las Relaciones con las Entidades Bancarias*, Buenos Aires: Erreius, 2020, pp. 99-118.

[24] ARIAS, María P. y MÜLER, Germán E. "La obligación de seguridad en las operaciones financieras con consumidores en la era digital. Con especial referencia a la problemática del phishing y del vishing", SJA 14/07/2021, Cita: TR LALEY AR/DOC/1657/2021

[25] TAMBUSSI, Carlos E., "Relación de consumo y responsabilidad objetiva entre los usuarios de plataformas de venta y el proveedor del servicio", cit. ARIAS y MÜLER, ob. cit., p. 1

[26] BELTRAMO, Andrés N., y FALIERO, Johanna C., "El consumidor electrónico como consumidor hipervulnerable", En S. S. Barocelli (Dir.), *Consumidores hipervulnerables*, El Derecho, 2018, pp. 346–382.

Esta acumulación de factores (desconocimiento del medio, ausencia de control sobre los mecanismos de seguridad y profundización de la asimetría técnica) lleva a parte de la doctrina a calificar al consumidor que opera en entornos digitales como un consumidor vulnerable, en tanto suma a las vulnerabilidades propias de toda relación de consumo las específicas del medio electrónico.[27] Como concluyen Arias y Müler, existe consenso en que los consumidores requieren en el entorno digital una protección mayor a la que reciben en el mundo físico, lo que refuerza la necesidad de que el principio protectorio del derecho del consumidor se manifieste con toda su intensidad en este ámbito.[28]

En suma, el régimen de protección del consumidor resulta plenamente aplicable a los usuarios de servicios bancarios, tanto por la naturaleza consumeril del vínculo como por la especial vulnerabilidad que los caracteriza frente a las entidades bancarias. Esta tutela adquiere una intensidad aún mayor en el contexto de la digitalización del sistema bancario, proceso que se aceleró durante la pandemia y que, en la actualidad, se ha consolidado como una imposición de las propias entidades, en tanto la prestación del servicio se desplaza hacia entornos tecnológicos que redefinen los riesgos de la operatoria. Sobre esta base conceptual se construirá, en los capítulos siguientes, el estudio de la digitalización del sistema bancario, la regulación del BCRA aplicable a estos casos y el alcance de la responsabilidad bancaria y el deber de seguridad en las operaciones electrónicas.

Capítulo 2. La digitalización del sistema financiero y los fraudes electrónicos

2.1. Transformación digital del sistema financiero

En las últimas décadas, la ola de digitalización ha transformado de manera profunda la estructura y el funcionamiento de múltiples sectores económicos, y el sistema financiero no ha sido la excepción. En un contexto global marcado por la expansión de las tecnologías de la información, los avances en inteligencia artificial, el uso masivo de datos y la conectividad permanente, las instituciones financieras se han visto obligadas a redefinir su modelo operativo para responder a un usuario cada vez más digitalizado. Los consumidores ya no se conforman con operar en horarios limitados ni en espacios físicos, sino que demandan soluciones inmediatas que les permitan gestionar sus finanzas en cualquier momento y desde cualquier lugar. Este cambio de comportamiento ha sido el principal motor que impulsó a las entidades financieras a replantear su estrategia e incorporar la tecnología como elemento central de su estructura institucional.

En este contexto, la digitalización bancaria se configura como una respuesta estratégica frente a los nuevos desafíos del mercado. Los bancos y demás actores del sistema financiero

[27] BELTRAMO y FALIERO, ob. cit., pp. 346–382.
[28] ARIAS y MÜLER, ob. cit.

comprendieron que la modernización tecnológica no solo optimiza procesos internos y reduce costos, sino que también amplía el alcance de los servicios y promueve la inclusión financiera.[29] Estos procesos de digitalización se intensifican año a año y habilitan nuevas formas de administrar el dinero, efectuar pagos, transferencias e inversiones e interactuar en el sistema financiero.

En el caso argentino, este proceso se intensificó especialmente durante la última década, de la mano del crecimiento del acceso a Internet y la masificación de los dispositivos móviles. La utilización de teléfonos inteligentes como herramienta cotidiana para múltiples actividades (fenómeno que se intensificó significativamente durante la pandemia de COVID-19) convirtió a los dispositivos móviles en el principal canal de interacción con los servicios financieros digitales.[30] En este marco, la expansión del *homebanking*, las billeteras virtuales, los pagos con transferencia y el QR interoperable reflejan la adopción de una infraestructura moderna, capaz de responder a la demanda de inmediatez y disponibilidad que caracteriza a la sociedad actual.

A este escenario se sumó la irrupción de las empresas *fintech*[31], que impulsó a los bancos a incorporar tecnología y a redefinir aún más sus estrategias tradicionales. Estas compañías, cuya ventaja comparativa radica en su dominio del entorno digital y de las redes sociales, introdujeron productos más simples, ágiles y centrados en el usuario. A diferencia de los bancos, cuya función esencial radica en la intermediación financiera y el cumplimiento de rigurosas normas prudenciales, las *fintech* operan con estructuras más livianas, orientadas a servicios digitales específicos (como pagos, créditos o inversiones) y sujetas a exigencias regulatorias menos estrictas. Mientras los primeros representan estabilidad y control estatal, las segundas encarnan dinamismo, flexibilidad y disrupción tecnológica.[32]

Frente a esta nueva dinámica, las entidades tradicionales se vieron impulsadas a acelerar sus procesos de modernización, diversificar sus canales de atención y adoptar modelos de gestión más flexibles y orientados a la experiencia del cliente. De este modo, comenzó a configurarse un escenario de convergencia entre la banca clásica y las firmas tecnológicas, en el cual la cooperación, la interoperabilidad y la integración de plataformas digitales se volvieron elementos esenciales para sostener la competitividad.[33]

---

[29] BERNAL-LUNA, Claudia P., et. al., "La tendencia global de la banca digital como agente de ruptura del mundo monetario", en *593 Digital Publisher CEIT*, N.º 7(3), 2022, pp. 212-229.
[30] Ídem.
[31] *Fintech* proviene de la contracción de dos términos anglosajones: *finance* (finanzas) y *technology* (tecnología). Son empresas que se valen de la innovación y del desarrollo tecnológico como elemento central para la prestación de productos y servicios financieros
[32] BERICUA, Marina, PALAZZI, Pablo A. y MORA, Santiago J., "Breve introducción al Derecho Fintech", en S. Mora y P. Palazzi (comps.), *Fintech: Aspectos legales*, Tomo I, 1.ª ed., Buenos Aires, Pablo Andrés Palazzi, 2019, pp. 23-34.
[33] BARRIO ANDRÉS, Moisés, "La revolución FinTech. Definición, factores desencadenantes, oportunidades y riesgos", en Matilde Cuena Casas y Javier Ibáñez Jiménez (dirs), *Perspectiva legal y económica del fenómeno FinTech,* Madrid: La Ley, 2021, pp. 41-71.

Este proceso de innovación tecnológica consolidó un esquema de operatoria bancaria predominantemente digital, en el cual la interacción presencial perdió centralidad y las transacciones comenzaron a ejecutarse, de manera masiva, a través de plataformas electrónicas. La digitalización de la operatoria modificó sustancialmente la forma en que los usuarios acceden y utilizan los servicios financieros, pero también introdujo nuevos riesgos a la actividad bancaria. En este sentido, la digitalización se presenta así como un fenómeno ambivalente: por un lado, amplía el acceso, mejora la eficiencia y favorece la inclusión financiera; por otro, introduce riesgos específicos cuya adecuada gestión resulta determinante para la protección del usuario.

2.2 La estructura de riesgos en la operatoria bancaria digital

La digitalización del sistema financiero ha alterado sustancialmente la forma en que se celebran y ejecutan las operaciones bancarias. La sustitución del canal presencial por medios electrónicos transformó el modo en que los usuarios interactúan con las entidades, dando lugar a una operatoria remota y altamente automatizada. Esta transformación tecnológica no solo modificó la forma en que los usuarios acceden a los servicios bancarios, sino que también reconfiguró de manera sustancial la estructura de riesgos propia de la actividad.

En el modelo tradicional de banca presencial, la interacción directa entre el cliente y el personal de la entidad, la apertura presencial de cuentas, la verificación física de documentación y la intervención humana en las operaciones funcionaban como mecanismos de control que reducían la posibilidad de maniobras fraudulentas. En el entorno digital, estos controles desaparecen y la operatoria pasa a ejecutarse en tiempo real, de forma automatizada y sin intervención humana directa, trasladando el peso de la seguridad hacia la arquitectura tecnológica del sistema.

En el entorno actual, la mayoría de las operaciones financieras se realizan a través de plataformas digitales, como el *homebanking*, las aplicaciones móviles y las billeteras electrónicas. En este esquema, la ejecución de las operaciones bancarias depende casi exclusivamente del correcto funcionamiento de los sistemas informáticos y de los mecanismos de autenticación implementados por las entidades financieras.[34] La apertura de cuentas, la solicitud de tarjetas, la contratación de préstamos y la aceptación de nuevos productos bancarios pueden realizarse íntegramente a distancia, mediante procedimientos automatizados que prescinden del soporte documental físico y en los que el consentimiento se manifiesta a través de medios electrónicos.

Desde esa perspectiva, la ausencia de contacto personal exige la implementación de mecanismos técnicos que permitan asociar cada operación al titular legítimo de la cuenta o producto bancario. La identidad digital se convierte así en un presupuesto estructural de la

[34] MORA, Santiago J., “Documento electrónico y firma digital. Evolución en el Derecho argentino”, en Santiago Mora y Pablo Palazzi (comps.), *Fintech: Aspectos legales*, Tomo I, 1.ª ed., Buenos Aires: Pablo Palazzi, 2019, pp. 121-176.

operatoria bancaria electrónica, en tanto permite generar confianza respecto de la atribución subjetiva de las transacciones realizadas.[35] Para ello se utilizan mecanismos de autenticación como combinaciones de usuario y contraseña, sistemas de doble factor, *tokens* digitales, validaciones por SMS o dispositivos biométricos, cuyo contenido mínimo exigible ha sido reglamentado específicamente por el BCRA.

Este cambio estructural tiene una consecuencia jurídica relevante, en tanto que el riesgo de la operatoria se concentra en la arquitectura tecnológica del sistema, cuyo diseño, implementación y supervisión corresponden exclusivamente a la entidad financiera. El usuario opera a través de plataformas, aplicaciones y mecanismos de autenticación que no diseñó, no controla y cuyo funcionamiento interno desconoce. Su única posibilidad de interacción con el sistema es la que la propia entidad le habilita, al ingresar las credenciales que le fueron asignadas, ejecutar las acciones que la interfaz le permite y confiar en que los controles de seguridad del proveedor funcionan correctamente. Cuando esos controles fallan o son vulnerados, el perjuicio patrimonial recae sobre el usuario, pero la falla se produjo en una esfera que este no administra.

A ello se suma que la automatización y la inmediatez propia de la banca digital eliminan los márgenes de revisión y corrección que existían en la operatoria tradicional. Una transferencia ejecutada mediante *homebanking* o aplicación móvil puede consumarse en segundos y resultar irreversible antes de que el usuario advierta la irregularidad. Esta característica no solo amplifica el daño potencial del fraude, sino que también dificulta su prevención individual, dado que el consumidor no dispone de los medios técnicos para detectar en tiempo real si una operación está siendo interceptada, si sus credenciales han sido comprometidas o si el canal a través del cual opera ha sido manipulado.

La dependencia estructural del usuario respecto de la arquitectura provista por la entidad es, en definitiva, el elemento que define la distribución de riesgos en la operatoria bancaria digital. No se trata de una vulnerabilidad circunstancial ni de un riesgo que el consumidor pueda neutralizar con mayor diligencia individual, sino de una consecuencia inherente al modelo de prestación del servicio, en el que la entidad financiera centraliza la gestión y el control del entorno tecnológico a través del cual se ejecutan las operaciones. Esta concentración del riesgo en quien organiza y administra el sistema constituye, como se desarrollará en los capítulos siguientes, uno de los fundamentos centrales del deber de seguridad exigible a las entidades bancarias y del factor de atribución aplicable frente a los daños derivados de operaciones electrónicas no consentidas.

[35] MORA, Santiago J., “Documento electrónico y firma digital. Evolución en el Derecho argentino”, en Santiago Mora y Pablo Palazzi (comps.), *Fintech: Aspectos legales*, Tomo I, 1.ª ed., Buenos Aires: Pablo Palazzi, 2019, pp. 121-176.

2.3. Concepto y tipología de los fraudes electrónicos

Identificada la estructura de riesgos que caracteriza a la operatoria bancaria digital, corresponde examinar de qué manera esos riesgos pueden materializarse en la práctica. En este contexto, los fraudes electrónicos se configuran como una de las principales manifestaciones de los riesgos inherentes a la operatoria bancaria digital, lo que conlleva un replanteo del alcance de las obligaciones jurídicas de las entidades financieras frente al consumidor, especialmente en materia de seguridad y prevención del daño.

En términos generales, los fraudes electrónicos constituyen maniobras ilícitas que, mediante el uso de tecnologías de la información y la comunicación, producen un perjuicio patrimonial a las víctimas y un beneficio correlativo para el autor o un tercero.[36] El Código Penal de Argentina en su art. 173, inc. 16 lo define en los siguientes términos *"El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos".* [37] Se trata de conductas que se desarrollan en entornos digitales y que se valen del funcionamiento habitual de sistemas informáticos, redes de comunicación y plataformas electrónicas para generar un engaño, obtener información sensible o inducir la realización de actos que permiten la disposición ilegítima de bienes o recursos económicos.[38]

La mayoría de estas conductas fraudulentas se apoyan en la manipulación de la confianza del usuario, en su desconocimiento técnico o en su exposición a entornos digitales en los que los signos de autenticidad pueden ser fácilmente falsificados. En este sentido, el elemento transversal de los fraudes digitales no reside únicamente en la habilidad del autor para ejecutar la maniobra, sino también en la existencia de vulnerabilidades estructurales vinculadas con la seguridad de los canales utilizados y con la protección de las credenciales de acceso, factores que adquieren especial relevancia cuando el usuario interactúa a través de sistemas que no controla ni administra.

Específicamente en el ámbito bancario digital, el fraude electrónico presenta una particularidad relevante, dado que el daño no se produce por fuera del sistema, sino en el interior de la infraestructura tecnológica organizada por la entidad financiera para la prestación del servicio. Las operaciones fraudulentas se ejecutan utilizando los mismos mecanismos técnicos diseñados para las transacciones legítimas, tales como plataformas de *homebanking*, aplicaciones móviles, sistemas de pago inmediato o herramientas de autenticación electrónica. Esta circunstancia

[36] MARTÍNEZ, Matilde S., "Algunas cuestiones sobre delitos informáticos en el ámbito financiero y económico. Implicancias y consecuencias en materia penal y responsabilidad civil", en Ricardo A. Parada y Juan D. Errecaborde (comps.), *Cibercrimen y delitos informáticos: Los nuevos tipos penales en la era de internet*, Ciudad Autónoma de Buenos Aires: Erreius, 2018, pp. 33-48.
[37] Código Penal de la Nación Argentina, art. 173
[38] Ídem. MARTÍNEZ, ob. cit., pp. 33-48

refuerza la necesidad de analizar el fenómeno desde una perspectiva sistémica, vinculada a la organización del servicio bancario digital y al alcance del deber de seguridad exigible a las entidades financieras, aspectos que serán desarrollados en los apartados siguientes.

En cuanto a su tipología, las modalidades más frecuentes que afectan el sistema bancario pueden agruparse del siguiente modo. En primer término, se encuentran las técnicas de ingeniería social, que inducen al usuario a entregar voluntariamente sus datos o a ejecutar acciones que habilitan el acceso del defraudador. Dentro de esta categoría se ubica, principalmente, el *phishing*, que consiste en el envío de correos electrónicos que aparentan provenir de entidades legítimas y que conducen al usuario a ingresar o entregar sus credenciales, permitiendo así a los delincuentes ingresar de manera fraudulenta a las cuentas de las víctimas.[39] Derivadas de esta modalidad se encuentra el *smishing* (reproduce esta lógica mediante mensajes de texto o aplicaciones de mensajería) y el *vishing* (lo hace a través de llamadas telefónicas en las que el estafador se presenta como representante del banco o de un organismo para obtener claves, *tokens* o validaciones).[40] En todas estas variantes, el engaño opera mediante la simulación de legitimidad institucional y el aprovechamiento de la confianza del consumidor en la marca o en el canal de comunicación.

En segundo lugar, se encuentran las técnicas basadas en la alteración del canal o red de acceso, como el *pharming*, que consiste en redirigir al usuario hacia sitios apócrifos sin que éste lo advierta, aun cuando haya ingresado correctamente la dirección de una página. De esta manera, el usuario cree que está accediendo a su banco en Internet, pero en realidad accede a la IP de una página web falsa.[41] Este tipo de fraude desplaza parcialmente el foco desde el error de la víctima hacia la manipulación del entorno tecnológico, lo que refuerza la necesidad de analizar los estándares de seguridad exigibles a quienes administran sistemas de autenticación y transacción.

En tercer lugar, se ubican los fraudes vinculados con el uso ilegítimo de tarjetas y credenciales, entre los cuales se destacan el *skimming* y el *carding*. El *skimming* consiste en la captación de datos de tarjetas mediante dispositivos instalados en cajeros automáticos o terminales de pago, a fin de duplicar tarjetas o utilizar los datos sustraídos.[42] El *carding*, por su parte, refiere al uso fraudulento de datos de tarjetas ajenas obtenidos mediante malware, filtraciones o técnicas de *phishing*, con el fin de concretar consumos o extracciones no autorizadas.[43] Estas maniobras evidencian que, aun cuando el usuario no entregue voluntariamente sus datos, la vulnerabilidad

[39] DAUVERNÉ, Julián S. y LO GIUDICE, Diego A., “La problemática del phishing en contratos de consumo de servicios financieros por plataformas electrónicas”,LA LEY 12/02/2025, Cita Online AR/DOC/239/2025
[40] Ídem.
[41] MARTÍNEZ, ob. cit., pp. 33-48.
[42] Ídem.
[43] Ídem.

puede derivar de fallas en la protección de los dispositivos o en la seguridad integral del sistema de pagos.

Otra modalidad relevante en el entorno financiero es la asociada al robo y suplantación de identidad digital, que puede implicar la creación de perfiles falsos o la apropiación de credenciales con fines delictivos. En muchos casos, el fraude no se agota en el acceso ilegítimo, sino que constituye un paso previo para la ejecución de nuevas maniobras patrimoniales, como transferencias inmediatas, solicitud de créditos o modificación de datos de contacto para impedir alertas.[44] De este modo, la identidad digital se convierte en un activo crítico dentro de la relación bancaria y este tipo de supuestos evidencia que la vulneración puede producirse incluso en la fase inicial de vinculación con el sistema, cuando la apertura de cuentas o la validación de identidad se realiza sobre la base de controles deficientes.

La incidencia práctica de estas modalidades ha sido reconocida por el propio BCRA. Según el Informe sobre Protección a las Personas Usuarias de Servicios Financieros correspondiente al período diciembre de 2024, a comienzos de ese año se conformó un equipo de trabajo dedicado exclusivamente al análisis y tratamiento de casos vinculados con ciberincidentes. Durante el año 2024 ingresaron al BCRA un total de 998 casos por fraude o estafa, cuyo análisis permitió identificar las principales modalidades. Del total, el 27,10% correspondió a *pharming*, el 21,94% a *vishing*, el 7,42% a robo de celular, el 4,84% a *phishing* y el 0,97% a malware; un 34,19% fue clasificado sin determinación específica y el 3,54% restante en otras categorías[45].[46]

Estos datos oficiales confirman que las técnicas de ingeniería social y la manipulación del entorno digital constituyen actualmente las principales vías de materialización del fraude en el sistema bancario argentino. A su vez, evidencian que el fenómeno presenta una elevada complejidad técnica y operativa, lo que refuerza la necesidad de estándares regulatorios dinámicos y de una política preventiva activa por parte de las entidades financieras en su calidad de administradoras profesionales de los canales digitales.

En síntesis, los fraudes electrónicos comprenden un conjunto heterogéneo de maniobras que, aunque varían en su metodología, presentan un rasgo común: la explotación de la confianza del usuario y/o de debilidades en los mecanismos de autenticación, en la gestión de credenciales y en la seguridad del ecosistema digital. En un sistema bancario crecientemente desmaterializado, estas modalidades no solo producen impactos patrimoniales directos, sino que también afectan la confianza en los canales electrónicos como vía principal de vinculación entre usuarios y

[44] MARTÍNEZ, ob. cit., pp. 33-48.
[45] Los datos que se exponen reflejan exclusivamente los casos canalizados a través de los canales de reclamo del propio BCRA y no la totalidad de fraudes reportados por las entidades al sistema, cuya dimensión es significativamente mayor según surge de la información de reclamos ante sujetos obligados que el mismo informe sistematiza.
[46] Banco Central de la República Argentina , *Informe sobre Protección a las Personas Usuarias de Servicios Financieros*, diciembre de 2024.

entidades. Sobre esta base conceptual y empírica, corresponde examinar en el capítulo siguiente el marco regulatorio dictado por el BCRA en materia de seguridad de los canales electrónicos, a fin de delimitar los estándares normativos que inciden en la prevención del fraude y en la protección de las personas usuarias de servicios financieros.

Capítulo 3. La regulación del BCRA en materia de seguridad de los canales electrónicos

3.1. Competencia regulatoria del BCRA en materia financiera y de protección de usuarios

El proceso de digitalización del sistema financiero argentino ha llevado al BCRA a dictar, de manera progresiva y sistemática, un conjunto de normas destinadas a regular los riesgos asociados a la utilización de medios electrónicos para la prestación de servicios financieros. Este desarrollo normativo parte del reconocimiento de que la operatoria electrónica incrementa la exposición de los usuarios a amenazas vinculadas con la seguridad informática, la suplantación de identidad y los fraudes electrónicos, lo que llevó al organismo a imponer a las entidades financieras deberes específicos de prevención, detección y mitigación de conductas fraudulentas en los canales digitales.

La competencia del BCRA para dictar este tipo de regulaciones encuentra su fundamento en dos pilares normativos complementarios. Por un lado, la LEF lo designa como autoridad de aplicación del régimen bancario, confiriéndole amplias facultades para dictar normas reglamentarias, supervisar el cumplimiento de las disposiciones vigentes e imponer sanciones ante su inobservancia. Por otro lado, su Carta Orgánica (Ley 24.144 y modificatorias) define sus objetivos y funciones, entre los que se encuentra *"regular el funcionamiento del sistema financiero y aplicar la Ley de Entidades Financieras y las normas que, en su consecuencia, se dicten"* (art. 4, inc. a), así como *"proveer a la protección de los derechos de los usuarios de servicios financieros"* (art. 4, inc. h, texto según Ley 26.739).

Dentro de la función de regulación y supervisión del sistema financiero, uno de los ejes centrales consiste en la identificación y gestión de los riesgos a los que se encuentran expuestas las entidades financieras. Dentro de dichos riesgos, el BCRA advirtió que la posibilidad de celebrar contrataciones y prestar servicios bancarios a través de medios digitales introduce riesgos específicos propios del entorno tecnológico, lo que motivó la emisión de diversas comunicaciones orientadas a fortalecer la seguridad de la operatoria y resguardar a los usuarios.[47]

Desde esta perspectiva, la regulación reconoce que el consumidor bancario actúa en un entorno tecnológicamente complejo y asimétrico, en el cual deposita su confianza en los sistemas

[47] ARIAS y MÜLER, ob. cit. .

diseñados y administrados por las entidades. Por ello, el BCRA ha optado por un enfoque preventivo, imponiendo a los bancos la obligación de adoptar medidas técnicas y procedimentales adecuadas para resguardar la información de los clientes de manera segura, asegurar la autenticidad de las operaciones, proteger la identidad digital, garantizar la trazabilidad de las transacciones y en definitiva ejecutar políticas de protección de sus canales electrónicos.

Este esquema regulatorio se inscribe dentro del principio de estabilidad y confianza del sistema financiero, en tanto la seguridad de los canales electrónicos constituye un presupuesto indispensable para el funcionamiento de la intermediación financiera en entornos digitales. En este sentido, las normas del BCRA no solo regulan la operatoria, sino que distribuyen deberes de conducta, establecen estándares mínimos de seguridad, definen obligaciones de información y atención al cliente, y asignan consecuencias frente a operaciones no autorizadas o fraudulentas. El eje común de estas disposiciones es claro: el deber de seguridad en los entornos digitales recae principalmente sobre las entidades financieras, quienes deben anticiparse a los riesgos propios de la tecnología que emplean.

A continuación, se analizan las principales normas que integran el ordenamiento del BCRA en materia de seguridad digital y prevención del fraude, con especial atención a su impacto en la protección del consumidor bancario.

3.2 Regulación en materia de gestión de riesgos tecnológicos y seguridad de la información

Conforme lo expuesto en el apartado precedente, ocupan un lugar central las normas contenidas en los Textos Ordenados sobre “Requisitos mínimos para la gestión y control de los riesgos de tecnología y seguridad de la información” y sobre “Requisitos mínimos para la gestión de los riesgos de tecnología y seguridad de la información asociados a los servicios financieros digitales”.

El Texto Ordenado sobre “Requisitos mínimos para la gestión y control de los riesgos de tecnología y seguridad de la información” establece el marco general aplicable a todas las entidades financieras bajo supervisión del BCRA y, a partir de la Comunicación “A” 8398 emitida el 05/02/2026, también a los Proveedores de servicios de pago (PSP) [48]. Este cuerpo normativo adopta un enfoque integral de gestión de riesgos tecnológicos, imponiendo a las entidades la obligación de identificar, evaluar, monitorear y mitigar los riesgos vinculados al entorno operativo de tecnología y seguridad de la información.

Desde una perspectiva jurídica, los aspectos más relevantes de este régimen pueden agruparse en tres dimensiones. La primera es la de gobierno y organización institucional. La norma exige

[48] Esta comunicación es de reciente incorporación y, a la fecha de presentación de este trabajo, se encuentra en período de implementación por parte de los sujetos alcanzados (PSP)

la implementación de un esquema formal de gobierno de tecnología y seguridad de la información, con definición clara de responsabilidades a nivel de alta dirección y directorio. Para esto, exige la constitución de un Comité de Gobierno de Tecnología y Seguridad de la Información, encargado de supervisar el funcionamiento del marco de gestión tecnológica, monitorear los planes estratégicos en la materia y asegurar la implementación de acciones correctivas.[49] Asimismo, impone la creación de un área específica de gestión de riesgos tecnológicos con independencia funcional respecto de las áreas que originan los riesgos y de las líneas de negocios.[50] Estas exigencias revelan que la seguridad informática no es concebida como una cuestión meramente operativa, sino como un componente estratégico del sistema de control interno y de la gestión prudencial.

La segunda dimensión es la de los controles técnicos de seguridad. La norma impone la implementación de controles de seguridad lógica y física, incluyendo protección perimetral, segmentación de redes, protección contra software malicioso y mecanismos de detección temprana de intrusiones. Complementariamente, exige la adopción de políticas de criptografía y resguardo de claves que aseguren la confidencialidad de la información transmitida y almacenada, así como esquemas de autenticación robusta, control de accesos basado en roles y monitoreo continuo de actividades sensibles.

La tercera dimensión es la de gestión de incidentes y continuidad operativa. La norma exige la definición de un proceso estructurado de gestión de incidentes de seguridad que contemple su detección, análisis, contención, erradicación, recuperación y documentación, incluyendo la obligación de registrar y reportar ciberincidentes relevantes. A ello se suma la implementación de un marco de continuidad del negocio y recuperación ante desastres, con identificación de procesos críticos, análisis de impacto y realización periódica de pruebas. Finalmente, la norma extiende estos estándares a los terceros proveedores de servicios tecnológicos, exigiendo mecanismos de supervisión continua y estándares de seguridad equivalentes a los propios de la entidad.

En conjunto, este régimen adquiere especial relevancia en tanto no se limita a exigir una reacción posterior al incidente, sino que impone estructuras organizativas y procedimientos formales orientados a anticipar amenazas, detectar vulnerabilidades y, en definitiva, evitar la materialización del riesgo. La seguridad informática se configura, así, como un deber estructural y permanente, cuya omisión o deficiencia puede traducirse en incumplimiento del estándar de diligencia profesional exigible a las entidades financieras.

[49] Banco Central de la República Argentina, Texto Ordenado sobre "Requisitos Mínimos para la Gestión y Control de los Riesgos de Tecnología y Seguridad de la Información" (texto ordenado al 13/02/2026, última comunicación incorporada "A" 8401), Sección 2, punto 2.2.4
[50] Ibídem, sección 3

De manera complementaria al régimen general, el BCRA dictó el Texto Ordenado "Requisitos mínimos para la gestión de los riesgos de tecnología y seguridad de la información asociados a los servicios financieros digitales", cuyo objeto es establecer estándares específicos aplicables a los servicios financieros prestados por medios digitales, tales como *homebanking*, aplicaciones móviles, billeteras virtuales y otros entornos remotos.

La norma define como "servicio financiero digital" a *"toda aquella prestación de servicios financieros a clientes por medios digitales para efectuar al menos, transferencias, pagos, extracciones, consultas u otras operaciones en línea, permitidas por las regulaciones vigentes".*[51] Asimismo, establece que el Directorio o autoridad equivalente es el responsable primario de definir la estructura organizacional, los modelos de control y la gestión de los riesgos asociados a la provisión de dichos servicios, quedando la Alta Gerencia a cargo de su implementación. Esta asignación de responsabilidades confirma que la seguridad digital no es concebida como una cuestión meramente técnica, sino como un componente estratégico de la gobernanza institucional.

Mientras el régimen general regula la arquitectura tecnológica integral de la entidad, este texto ordenado se focaliza específicamente en los riesgos derivados de la interacción digital con el usuario. En consecuencia, impone a los sujetos obligados el deber de identificar y documentar formalmente los servicios financieros digitales ofrecidos y las funcionalidades asociadas a cada uno de ellos, así como de implementar medidas de protección adecuadas durante todo su ciclo de vida. Los aspectos más relevantes de este régimen específico pueden sintetizarse del siguiente modo.

En materia de autenticación y control transaccional, la norma impone la autenticación obligatoria para toda transacción digital y la aplicación de mecanismos de autenticación multifactor en función del nivel de riesgo, especialmente ante acciones críticas como la suscripción de nuevos productos, la modificación de datos de contacto, la incorporación de cuentas para transferencias o la validación de operaciones que se aparten de patrones habituales.[52] En materia de seguridad de dispositivos y aplicaciones, exige medidas de protección para garantizar la confidencialidad e integridad de la información procesada en plataformas de banca móvil, *homebanking* y billeteras digitales, así como resistencia frente a accesos indebidos, *malware* y vulnerabilidades del entorno tecnológico. [53] En cuanto a la identificación digital en altas no presenciales, la norma

[51] Banco Central de la República Argentina, Texto Ordenado sobre "Requisitos Mínimos para la Gestión de los Riesgos de Tecnología y Seguridad de la Información Asociados a los Servicios Financieros Digitales" (texto ordenado al 02/06/2023, última comunicación incorporada "A" 7783), Sección 1, punto 1.2
[52] Ibídem, sección 3, punto 3.1
[53] Ibídem, sección 3, punto 3.2

exige mecanismos que permitan verificar que la persona es real mediante prueba de vida, validar elementos biométricos y comprobar la autenticidad de la documentación presentada.[54]

Asimismo, la norma impone la protección de los factores de autenticación durante todo su ciclo de vida, desde su generación hasta su revocación[55]; obliga a implementar programas de capacitación y concientización en materia de servicios financieros digitales, orientados tanto al personal como a los usuarios frente a técnicas de ingeniería social [56]; y exige la disponibilidad de canales de comunicación permanentes que permitan a los clientes denunciar ciberincidentes u operaciones sospechosas con atención continua[57].

De especial relevancia resulta la Sección 4, que impone la obligación de definir e implementar una estrategia de monitoreo transaccional capaz de detectar actividades inusuales o sospechosas en tiempo real. La norma exige que, en función de las alertas generadas, las entidades definan modelos de acción adecuados al nivel de riesgo del servicio ofrecido. Ello implica integrar herramientas de análisis de comportamiento, monitoreo dinámico y respuesta inmediata ante incidentes, ajustando los controles conforme evolucionan las amenazas digitales.[58]

Otro aspecto central del régimen es la regulación de la conservación e integridad de la información, plasmada en el Texto Ordenado “Instrumentación, conservación y reproducción de documentos”. El BCRA admite la utilización de soportes electrónicos en la instrumentación y archivo de documentación financiera, siempre que los registros sean inalterables y susceptibles de verificación pericial que permita acreditar su autenticidad y autoría. En este sentido, la desmaterialización del soporte documental no implica la flexibilización de las exigencias probatorias, sino su adaptación al entorno tecnológico, imponiendo requisitos de trazabilidad y auditabilidad de las operaciones realizadas por medios digitales. [59]

En definitiva, este conjunto de normas parte del reconocimiento de que el entorno digital incrementa la exposición a ataques de ingeniería social, suplantación de identidad, accesos indebidos y manipulación de credenciales. Por tal motivo, desplaza el eje de la protección hacia la entidad financiera como administrador del canal tecnológico, en donde la seguridad de los canales electrónicos deja de depender exclusivamente de la conducta individual del usuario y

[54] BCRA, Texto Ordenado sobre "Requisitos Mínimos para la Gestión de los Riesgos de Tecnología y Seguridad de la Información Asociados a los Servicios Financieros Digitales", sección 3, punto 3.3
[55] Ibídem, sección 3, punto 3.4
[56] BCRA, Texto Ordenado “Requisitos Mínimos para la Gestión de los Riesgos de Tecnología y Seguridad de la Información…” sección 3, punto 3.5
[57] Ibídem, sección 3, punto 3.6
[58] Ibídem, sección 4
[59] Banco Central de la República Argentina, Texto Ordenado sobre "Instrumentación, Conservación y Reproducción de Documentos" (texto ordenado al 06/12/2016, última comunicación incorporada "A" 6112).

pasa a sustentarse en un entramado de controles internos, monitoreo permanente y gestión estructurada del riesgo tecnológico.

3.3 Otras disposiciones sobre prevención del fraude en los servicios financieros digitales

Además del régimen estructural en materia de gestión de riesgos tecnológicos y seguridad de la información, el BCRA ha incorporado previsiones específicas en distintos cuerpos normativos que inciden directamente en la operatoria digital. Estas disposiciones desarrollan y concretan el deber de seguridad en ámbitos particulares del sistema financiero, trasladando los principios generales de prevención, control y monitoreo al funcionamiento operativo de los instrumentos y canales de pago electrónicos.

Específicamente, en el marco del Sistema Nacional de Pagos, la regulación operativiza el deber de seguridad en los distintos esquemas de pago, en especial en las transferencias inmediatas y en las billeteras digitales, que constituyen hoy el núcleo de la operatoria transaccional electrónica. En primer lugar, el Texto Ordenado **"**Sistema Nacional de Pagos – Transferencias" establece en su punto 2.3.1 que las entidades financieras y los proveedores de servicios de pago participantes deben *"arbitrar los mecanismos de seguridad apropiados dentro de su competencia para asegurar la transmisión y recepción de las transacciones".*[60] Esta previsión consagra un deber activo de protección que trasciende la mera infraestructura interna y se proyecta sobre todo el proceso de cursado de transferencias. A su vez, el punto 2.3.3.5 impone la obligación de *"utilizar herramientas de mitigación de fraude que permitan identificar patrones sospechosos y alertar a los usuarios"*[61]*,* incorporando expresamente el monitoreo transaccional y la detección temprana de operaciones inusuales como estándares regulatorios obligatorios.

Por su parte, el Texto Ordenado "Sistema Nacional de Pagos – Transferencias – Normas Complementarias" profundiza este enfoque en su punto 2.6 ("Prevención y gestión de fraude"). Allí se establece que cada esquema de transferencias inmediatas debe, entre otras cosas: definir claramente las responsabilidades de sus participantes en la gestión del fraude; respaldar el análisis con herramientas que permitan identificar patrones sospechosos y coordinar acciones preventivas; establecer procedimientos formales para la resolución de reclamos con plazos máximos de respuesta; garantizar la trazabilidad de extremo a extremo de las operaciones; y documentar los circuitos y procesos vinculados a la prevención y gestión del fraude, los cuales deben estar disponibles para la SEFyC cuando así lo requiera.[62]

---

[60] Banco Central de la República Argentina, Texto Ordenado sobre "Sistema Nacional de Pagos – Transferencias" (texto ordenado al 07/08/2025, última comunicación incorporada "A" 8295), Sección 2, punto 2.3.1

[61] Ibídem, sección 2, punto 2.3.3.5

[62] Banco Central de la República Argentina, Texto Ordenado sobre "Sistema Nacional de Pagos – Transferencias – Normas Complementarias" (texto ordenado al 14/05/2026, última comunicación incorporada "A" 8436), Sección 2, punto 2.6

Asimismo, el punto 3.4.3.2 regula expresamente la responsabilidad frente al fraude en las transferencias inmediatas tipo “pull”. Allí se dispone que el proveedor de la cuenta en la que se acrediten fondos obtenidos por medios fraudulentos deberá responder por su devolución. El cliente cuenta con un plazo de 60 días para desconocer el débito, y la entidad debitada debe reintegrar el importe dentro de los tres días hábiles, efectuando luego un contracargo automático contra la entidad originante. Además, los administradores de los esquemas deben exigir garantías específicas a las entidades ordenantes para afrontar estos contracargos, calibradas conforme a su perfil de riesgo. Este régimen evidencia la importancia sistémica que las transferencias inmediatas han adquirido en el ecosistema digital.[63]

En este contexto, resulta particularmente relevante la creación por parte del BCRA de la Central de Prevención del Fraude (CPF), concebida como una herramienta sistémica de coordinación e intercambio de información dentro del ecosistema de pagos. La CPF tiene por objeto centralizar y consolidar la información provista por entidades financieras y proveedores de servicios de pago respecto de casos, cuentas y titulares vinculados con sospechas o denuncias de fraude, con el fin de prevenir su consumación y generalización, generar trazabilidad, detectar nuevas modalidades y anticipar medidas de mitigación. El funcionamiento del sistema impone a las entidades y a las PSP que ofrecen cuentas de pago (“PSPCP”) la obligación de reportar a la CPF las transferencias inmediatas denunciadas como desconocidas por su originante o sospechosas de fraude. Ante la notificación, la entidad receptora debe analizar la cuenta destinataria, verificar la licitud de la operación, contactar al cliente involucrado y actualizar el estado del caso dentro de los plazos previstos. La información centralizada debe ser consultada por los distintos participantes del sistema a los fines de reforzar el monitoreo transaccional.

A partir de esta implementación, la prevención del fraude deja de ser una obligación aislada de cada entidad para configurarse como un mecanismo de cooperación regulada, estructurado y con trazabilidad formal. La relevancia que el BCRA asigna a este instrumento quedó evidenciada en la Comunicación “B” 13117 del 10/02/2026, mediante la cual el organismo recordó expresamente el carácter obligatorio de la CPF para todas las entidades financieras y PSPCP, enfatizando la necesidad de reportar la totalidad de los eventos de fraude y de consultar activamente la información disponible. Este recordatorio pone de manifiesto que la cooperación informativa no constituye una facultad opcional, sino un deber regulatorio esencial dentro de la estrategia sistémica de prevención del fraude.

Por otra parte, en el ámbito del Texto Ordenado “Sistema Nacional de Pagos – Servicios de Pago”, se establecen exigencias específicas para las billeteras digitales. El punto 5.5 (“Medidas para mitigar el fraude”) impone, entre otras obligaciones: la implementación de mecanismos de

[63] BCRA, Texto Ordenado sobre "Sistema Nacional de Pagos – Transferencias – Normas Complementarias", Sección 3, punto 3.4.3.2

detección de actividades sospechosas o inusuales; la vinculación de la billetera únicamente a cuentas o instrumentos cuyo titular coincida con el titular del servicio; la aplicación de mecanismos robustos de identificación y autenticación; la verificación de identidad en la apertura de cuentas; la exigencia de consentimiento expreso y verificable en el enrolamiento y autorización de pagos; la posibilidad de que el cliente establezca límites operativos, modifique parámetros o desvincule su cuenta de manera inmediata ante sospecha de fraude; y la trazabilidad y auditabilidad de los procesos vinculados a enrolamiento, autenticación y vinculación de instrumentos. Resulta particularmente relevante que, en pagos con tarjeta iniciados desde billeteras digitales interoperables mediante QR, la responsabilidad por fraude será asumida por la billetera, salvo supuestos específicos vinculados a estándares técnicos de tokenización o acuerdos entre participantes. Con ello, la regulación identifica al administrador del canal como sujeto primario de imputación del riesgo fraudulento. [64]

También se encuentran regulados los procesos de apertura no presencial de cuentas, respecto de los cuales la normativa impone exigencias específicas orientadas a resguardar la seguridad del sistema desde la etapa inicial del vínculo contractual. En particular, en las normas sobre Depósitos de Ahorro, Cuenta Sueldo y Especiales (punto 4.16) y sobre Reglamentación de la cuenta corriente bancaria (punto 12.10) establecen que, cuando las entidades financieras admiten la apertura de cuentas a través de medios electrónicos y/o de comunicación, deberán implementar mecanismos de identificación remota que permitan verificar de manera adecuada la identidad del cliente y dar cumplimiento a las exigencias regulatorias vigentes. Asimismo, disponen que los procedimientos, tecnologías y controles empleados en la apertura remota deben asegurar el cumplimiento de las disposiciones aplicables en materia de canales electrónicos, así como aquellas relativas a la conservación, integridad, autenticidad y confidencialidad de la información y documentación utilizada en el proceso, a fin de protegerla contra su alteración, destrucción, acceso o uso indebidos. De este modo, la normativa integra la prevención del fraude y la protección de la identidad digital al momento mismo de incorporación del usuario al sistema financiero.

Finalmente, la regulación del BCRA extiende el deber de seguridad digital también a instrumentos tradicionales que han sido adaptados al entorno electrónico, reforzando la coherencia sistémica del modelo regulatorio. En este sentido, el Texto Ordenado sobre Reglamentación de la Cuenta Corriente Bancaria impone obligaciones vinculadas al correcto funcionamiento de los mecanismos de seguridad del ECHEQ y a la prevención de su uso no autorizado, así como al resguardo de la genuinidad de las operaciones de crédito y débito. De manera concordante, el Texto Ordenado sobre Depósitos de Ahorro, Cuenta Sueldo y Especiales exige la

[64] Banco Central de la República Argentina, Texto Ordenado sobre "Sistema Nacional de Pagos – Servicios de Pago" (texto ordenado al 18/08/2025, última comunicación incorporada "A" 8303), Sección 5, punto 5.2

implementación de mecanismos de seguridad informática para transferencias electrónicas, extracciones y demás operaciones.

En conjunto, el marco normativo del BCRA en materia de seguridad digital configura un sistema coherente y preventivo, que reconoce los riesgos propios de la digitalización y asigna a las entidades financieras la carga principal de anticiparlos, gestionarlos y neutralizarlos. Estas normas no solo organizan técnicamente la operatoria bancaria digital, sino que fijan estándares jurídicos de diligencia profesional cuyo incumplimiento resulta determinante para el análisis de la responsabilidad bancaria frente a fraudes electrónicos. Sobre esta base normativa se apoyará el examen que se desarrollará en el capítulo siguiente, orientado a determinar el alcance de la responsabilidad de las entidades financieras ante operaciones digitales no consentidas.

Capítulo 4. La responsabilidad de las entidades financieras frente a fraudes electrónicos

4.1. Fundamentos normativos de la responsabilidad civil

La responsabilidad civil constituye una de las fuentes de las obligaciones, y surge cuando una persona lesiona el deber general de no causar daños a otros o incumple una obligación existente, naciendo a su cargo el deber jurídico de reparar económicamente el perjuicio ocasionado.[65] De este modo, el sistema de responsabilidad civil se estructura como un mecanismo de tutela frente al daño injustamente causado, articulando tanto la prevención como la reparación de los perjuicios.

4.1.1. Funciones de la responsabilidad civil

La responsabilidad civil cumple diversas funciones dentro del ordenamiento jurídico. Tradicionalmente se le han reconocido tres: la función preventiva, la función resarcitoria y, en ciertos supuestos específicos, una función punitiva. El sistema del CCyCN estructura la responsabilidad como un régimen orientado tanto a la prevención como a la reparación del daño injustamente causado, superando una visión exclusivamente resarcitoria y otorgando centralidad a la función preventiva.

La función preventiva tiene por objeto actuar antes de que el daño ocurra o, si ya se produjo, evitar su agravamiento. De esta forma, el derecho de daños centra su propósito principal en la prevención, desplazando el enfoque tradicionalmente resarcitorio para priorizar la intervención

[65] CALVO COSTA, Carlos A., *Derecho de las obligaciones. Tomo 2: Derecho de daños*, 2.ª ed., Buenos Aires: Hammurabi, 2016.

temprana que impida la producción del perjuicio.[66] De acuerdo con el art 1710 CCyCN, el deber de prevenir el daño comprende tres aspectos: abstenerse de causar un perjuicio injustificado, realizar acciones tendientes a evitar o a reducir su alcance, y no empeorar las consecuencias cuando el daño ya se ha verificado.

La función resarcitoria tiene por objetivo reparar el perjuicio ocasionado sea cual fuera la fuente de la responsabilidad. Una vez producido el daño y verificados los presupuestos de la responsabilidad, surge a favor del damnificado un derecho de crédito que consiste en obtener su reparación, cuyo objetivo es lograr una *"reparación plena"* de los perjuicios sufridos por el damnificado.[67] En este sentido, el art. 1716 CCyCN dispone: *"La violación del deber de no dañar a otro, o el incumplimiento de una obligación, da lugar a la reparación del daño causado, conforme con las disposiciones de este Código."*[68]

Por último, existe la llamada función punitiva, aunque su reconocimiento dentro del derecho de daños continúa siendo un punto altamente debatido. Esta tercera finalidad ya no estaría orientada a prevenir o reparar el daño, sino a sancionar a quien lo ocasiona de manera deliberada o con la intención de obtener un beneficio. Una parte de la doctrina sostiene que al derecho civil no le corresponde *"castigar",* sino únicamente resarcir el perjuicio sufrido por la víctima dentro del límite del daño efectivamente causado; mientras que otra, en cambio, admite la conveniencia de una finalidad sancionatoria o disuasiva en supuestos de dolo o culpa grave, cuando la mera reparación resulta insuficiente para restablecer la legalidad o eliminar el beneficio obtenido mediante el ilícito. Nuestro CCyCN no incorporó esta función como principio general: el Anteproyecto contemplaba la *"sanción pecuniaria disuasiva",* pero el texto finalmente aprobado la eliminó, manteniendo al sistema de responsabilidad centrado en las funciones preventiva y resarcitoria. No obstante, la LDC (art. 52 bis) sí recepta expresamente los daños punitivos, con el propósito de sancionar y desalentar conductas graves de los proveedores frente a los consumidores.

4.1.2. Presupuestos de la responsabilidad civil

Para que se configure la responsabilidad civil, es necesario que concurran ciertos presupuestos cuya acreditación resulta indispensable para que nazca el deber de responder. Estos son la antijuridicidad, el factor de atribución, la relación de causalidad y el daño.

La antijuridicidad, conforme al art. 1717 CCyCN, se define como toda acción u omisión que causa un daño a otro de manera no justificada. En otras palabras, se configura cuando una conducta

[66] PICASSO, Sebastián y SÁENZ, Luis R., "Título V. Otras fuentes de las obligaciones. Capítulo I. Responsabilidad Civil", en Marisa Herrera, Gustavo Caramelo y Sebastián Picasso (dirs.), *Código Civil y Comercial de la Nación comentado*, Tomo IV, Buenos Aires: Infojus, 2015, pp. 414-523.
[67] UBIRÍA, Fernando A. *Derecho de daños en el Código Civil y Comercial*, Buenos Aires: Abeledo Perrot, 2015.
[68] CCyCN, art. 1716

vulnera las reglas de comportamiento establecidas por el ordenamiento jurídico, las cuales reflejan el deber general de no dañar a otro.[69]

El factor de atribución representa el fundamento jurídico que permite imputar a una persona la obligación de reparar un daño. A través de él se determinan los criterios mediante los cuales se imputa el daño a uno o más responsables, estableciendo el nexo entre la conducta (acción u omisión) y el resultado dañoso. Según el art. 1721 del CCyCN, la atribución puede basarse en factores subjetivos u objetivos.

La relación de causalidad permite vincular jurídicamente la conducta del autor con el daño producido. Es el vínculo material que une una acción u omisión (hecho antecedente) con el resultado dañoso (hecho consecuente) y supone la existencia de una relación de causalidad adecuada entre el hecho que genera el daño y quien lo realiza.[70] De acuerdo con el art. 1726 del CCyCN, son reparables únicamente las consecuencias que tengan un nexo adecuado de causalidad con el hecho que produjo el daño. La carga de probar ese nexo recae en quien la invoca, mientras que la demostración de una causa ajena corresponde a quien pretende eximirse de responsabilidad (art. 1734 CCyCN).

El daño resarcible constituye otro de los presupuestos indispensables de la responsabilidad civil, ya que sin daño no hay deber de reparar. Conforme al art. 1737 del CCyCN, existe daño cuando se lesiona un derecho o interés jurídicamente protegido, referido a la persona, al patrimonio o a un derecho de incidencia colectiva. El perjuicio debe ser cierto, actual o futuro pero previsible, y susceptible de apreciación económica. En todos los casos, el daño debe ser resarcible y debe guardar una relación adecuada con el hecho antijurídico que lo generó.

4.2. El factor de atribución en la responsabilidad de las entidades financieras frente a fraudes electrónicos

4.2.1. Factor de atribución: objetivo o subjetivo

Como se mencionó, el factor de atribución constituye uno de los presupuestos de la responsabilidad civil, en tanto determina bajo qué criterios se imputa el daño a una persona. Su determinación en el ámbito de la responsabilidad de las entidades financieras reviste particular relevancia, ya que de ello dependerá si corresponde exigir al consumidor la prueba de culpa del banco o si, por el contrario, la responsabilidad se configura con prescindencia de dicho reproche subjetivo.

El CCyCN distingue entre factores de atribución subjetivos y objetivos (art. 1724 CCyCN). Los primeros se basan en el reproche de la conducta del autor y comprenden la culpa (entendida

[69] CALVO COSTA, ob. cit.
[70] UBIRÍA, ob. cit.

como la omisión de la diligencia debida según la naturaleza de la obligación y las circunstancias de las personas, el tiempo y el lugar) y el dolo (la producción intencional del daño o con manifiesta indiferencia por los intereses ajenos). Bajo este esquema, el autor solo responde si se acredita que actuó negligentemente, y podría eximirse demostrando que obró con la diligencia adecuada y probando su falta de culpa. Cuando el factor de atribución es objetivo, en cambio, la culpa resulta irrelevante a los fines de la imputación (art. 1722 CCyCN) y el deber de responder se configura por la sola producción del daño dentro del ámbito de organización y riesgo del responsable, quien únicamente puede liberarse mediante la acreditación de una causa ajena que reúna los requisitos del caso fortuito (imprevisibilidad, inevitabilidad y exterioridad).

La determinación acerca de si la responsabilidad de las entidades financieras por operaciones electrónicas no consentidas debe encuadrarse dentro de un régimen subjetivo u objetivo constituye uno de los ejes centrales del presente trabajo. En consecuencia, corresponde examinar en primer lugar el alcance del modelo subjetivo en este ámbito y sus limitaciones, para luego determinar si resulta procedente la aplicación de un criterio de atribución objetivo en materia de fraudes electrónicos bancarios.

4.2.2. La responsabilidad subjetiva y sus limitaciones en la banca digital

Bajo un esquema subjetivo, el deber de responder se encontraría condicionado a la verificación de culpa en la conducta del banco, que solo respondería en la medida en que se acredite que actuó de manera negligente, imprudente o con impericia en la prestación del servicio (art. 1724 CCyCN).

Cabe señalar que, incluso dentro de este modelo, el estándar de diligencia exigible a una entidad financiera se encuentra agravado. El art. 1725 CCyCN dispone que cuanto mayor sea el deber de obrar con prudencia y pleno conocimiento de las cosas, mayor será la diligencia exigible al agente y la previsibilidad de las consecuencias de sus actos. Esta previsión adquiere especial relevancia en el ámbito bancario, dado que las entidades financieras actúan profesionalmente, cuentan con una organización técnica compleja y operan en un sector fuertemente regulado. En consecuencia, su conducta debe valorarse conforme a un estándar calificado, superior al del común de los sujetos, que impone un elevado grado de previsión, control y profesionalismo en la prestación del servicio.[71]

Sin perjuicio de ello, en el presente trabajo se sostiene que el modelo subjetivo presenta limitaciones estructurales cuando se proyecta sobre la prestación de servicios bancarios a

[71] RUIZ DÍAZ, Estefanía L., “Publicidad bancaria. Normativas específicas. BCRA y CCyCN”, en Carlos Ghersi, Celia Weingarten y Graciela Lovece (dirs.), *Derechos de los Consumidores y Empresas en las Relaciones con las Entidades Bancarias*, Buenos Aires: Erreius, 2020, pp. 3-46.

consumidores en entornos digitales, que lo tornan insuficiente para dar respuesta adecuada al fenómeno del fraude electrónico.

En primer lugar, el modelo subjetivo resulta difícilmente compatible con el régimen de protección del consumidor. Cuando la relación entre banco y usuario se encuadra dentro de una relación de consumo, el factor de atribución aplicable no es la culpa. La LDC establece un sistema de imputación propio, de naturaleza objetiva, fundado en lo dispuesto por los artículos 5, 6, 10 bis y 40. Bajo este esquema, la responsabilidad del proveedor se configura con prescindencia de su diligencia o intención, de modo que no puede eximirse acreditando la ausencia de culpa, sino únicamente demostrando la existencia de una causa ajena que reúna los requisitos legales para interrumpir el nexo causal.[72]

En segundo lugar, un esquema subjetivo le exige al perjudicado probar la negligencia del autor del daño, lo que resulta especialmente problemático en el entorno digital. En un contexto caracterizado por una fuerte asimetría informativa y técnica, el consumidor se encuentra en una situación de evidente desventaja para acreditar cómo, en qué etapa y por qué motivo falló un sistema que no controla. Exigirle al usuario la prueba de la culpa del banco traslada sobre la parte más débil un riesgo que se origina en la propia organización del servicio por parte del proveedor, resultado que resulta incompatible con los principios que estructuran el derecho del consumidor.

En tercer lugar, el modelo subjetivo desplaza el análisis hacia la conducta culposa del agente, dejando en un segundo plano el funcionamiento del sistema en el que el daño se produce. Sin embargo, en los fraudes electrónicos, el daño ocurre dentro de una infraestructura tecnológica con plataformas, aplicaciones, mecanismos de autenticación y sistemas de validación que son diseñados y controlados por el banco. En este contexto, centrar la responsabilidad exclusivamente en la existencia o no de culpa individual resulta insuficiente para dar respuesta a un fenómeno que se vincula directamente con el riesgo inherente al sistema organizado por la propia entidad.

En definitiva, la responsabilidad subjetiva, aún agravada por el estándar profesional, es insuficiente para analizar la responsabilidad bancaria en el caso de los fraudes electrónicos dentro de una relación de consumo. La combinación de digitalización del sistema, asimetría técnica, dificultad probatoria y régimen protectorio de consumo exige desplazar el análisis hacia un modelo de atribución que no dependa exclusivamente de la acreditación de la culpa, sino que permita imputar el daño en función del riesgo de la actividad y de la naturaleza de las obligaciones asumidas por la entidad financiera.

[72] RODRÍGUEZ, Gonzalo M., “Responsabilidad por daños en el ámbito del consumo”, en Fernando M. Álvarez Larrondo (ed.), *Manual de derecho del consumo*, Buenos Aires: Erreius, 2017, pp. 661-724.

4.2.3 La responsabilidad objetiva en la actividad bancaria

A diferencia del modelo subjetivo, la responsabilidad objetiva prescinde del análisis de la conducta del agente, de modo que la culpa resulta irrelevante a los fines de la imputación. En estos supuestos, el deber de responder se configura por la sola producción del daño, con independencia de que el sujeto haya obrado diligentemente. En el ámbito de la actividad bancaria digital, la aplicación de un factor de atribución objetivo encuentra fundamento en múltiples vías normativas que, lejos de excluirse, se refuerzan mutuamente y convergen en una misma conclusión.

El primer fundamento proviene del régimen de protección del consumidor. La LDC estructura un sistema de responsabilidad de naturaleza objetiva que impregna toda relación de consumo. Los arts. 5 y 6 consagran el deber de seguridad del proveedor, imponiéndole la obligación de garantizar que los bienes y servicios ofrecidos no generen riesgos para la persona o los bienes del consumidor. Este deber, de raigambre constitucional en virtud del art. 42 de la Constitución Nacional, no admite exoneración por ausencia de culpa y el proveedor solo puede liberarse acreditando una causa ajena.[73] En igual sentido, el art. 40 LDC establece la responsabilidad objetiva de todos los integrantes de la cadena de producción y comercialización del bien o servicio dañoso. La consecuencia práctica de este esquema es que, verificado el daño sufrido por el consumidor en el marco de la relación bancaria, la entidad financiera no puede eximirse demostrando que actuó con diligencia, sino únicamente acreditando que el daño fue causado por un hecho ajeno a su organización.[74] Así lo confirma el art. 10 bis LDC, que regula las consecuencias del incumplimiento del proveedor y admite como única eximente el caso fortuito o la fuerza mayor, reforzando el carácter objetivo del régimen consumeril.

El segundo fundamento se asienta en la naturaleza de la obligación asumida por la entidad financiera. Conforme al art. 1723 CCyCN, cuando de las circunstancias de la obligación surge que el deudor debe obtener un resultado determinado, su responsabilidad es objetiva. En materia bancaria, y principalmente en aquellos contratos celebrados con consumidores o usuarios, no es frecuente encontrar obligaciones de resultado expresamente pactadas, dado que los contratos son predispuestos por las entidades financieras y estructurados de modo tal que evitan asumir este tipo de compromisos de manera explícita. Sin embargo, ello no impide que la obligación de resultado surja de las circunstancias de la prestación. En materia de operaciones bancarias, la entidad no se limita a desplegar una conducta diligente, sino que se obliga a proveer un canal seguro para proteger los fondos del usuario. Ello se traduce en el deber de garantizar que las operaciones ejecutadas a través de sus plataformas respondan a instrucciones genuinas del titular y en el de resguardar la integridad del sistema que ella misma diseña, administra y controla.

[73] RODRÍGUEZ, ob. cit., pp. 661-724.
[74] Ídem.

Esa obligación, cuyo contenido mínimo ha sido fijado con precisión por la normativa del BCRA analizada en el capítulo anterior, tiene las características propias de una obligación de resultado: no basta con intentar proveer seguridad, sino que la seguridad debe efectivamente garantizarse. Cuando ese resultado no se alcanza y el usuario sufre un perjuicio patrimonial por una operación no consentida, la responsabilidad se configura con independencia de la diligencia desplegada por la entidad.[75]

El tercer fundamento emerge de la calificación de la actividad bancaria digital como actividad riesgosa en los términos del art. 1757 CCyCN. Dicho artículo establece que toda persona responde objetivamente por el daño causado por las cosas y actividades que resulten riesgosas o peligrosas, ya sea por su propia naturaleza, por los medios empleados o por las circunstancias en que se desarrollan. Asimismo, la norma dispone expresamente que ni la autorización administrativa para realizar la actividad ni el cumplimiento de las técnicas de prevención constituyen causas de exoneración. En lo que respecta a la actividad bancaria, si bien no todas sus operaciones pueden ser calificadas como intrínsecamente peligrosas, el carácter riesgoso se ve especialmente acentuado por los medios empleados. Tal como se analizó en el Capítulo 2, la creciente informatización de los servicios financieros ha incrementado significativamente la exposición a accesos indebidos, fallas operativas y maniobras fraudulentas. En este sentido, la actividad bancaria puede ser considerada riesgosa en razón de los medios tecnológicos utilizados, en tanto estos introducen nuevas fuentes de daño cuya prevención depende fundamentalmente de la entidad financiera.[76] Esta solución encuentra además sustento en la denominada teoría del riesgo-provecho, elaborada por la doctrina y la jurisprudencia e incorporada expresamente al CCyCN a través del artículo 1758. A diferencia de la teoría del riesgo creado, que justifica la responsabilidad por la sola introducción de una cosa o actividad riesgosa en la sociedad, el riesgo-provecho agrega un fundamento adicional: debe soportar las consecuencias dañosas quien organiza una actividad riesgosa y obtiene un beneficio de ella. El provecho no se limita a una utilidad estrictamente económica, sino que comprende cualquier ventaja derivada del desarrollo de la actividad. En este sentido, el artículo 1758 considera responsable no solo a quien realiza la actividad riesgosa, sino también a quien se sirve u obtiene provecho de ella. [77]

Este criterio adquiere especial relevancia en la actividad bancaria digital. Las entidades financieras diseñan, administran y explotan profesionalmente los canales electrónicos mediante los cuales prestan sus servicios, obteniendo un beneficio económico derivado de esa operatoria, ya sea mediante la reducción de costos operativos o la ampliación de su actividad comercial, por

[75] DE NÚÑEZ, Rodrigo, “La responsabilidad objetiva en la actividad bancaria”, SJA, 27/06/2018, Thomson Reuters, cita online: AR/DOC/3012/2018.
[76] ARIAS y MÜLER, ob. cit.
[77] RUIZ DÍAZ, Estefanía L., Capítulo II, en Derechos de los Consumidores y Empresas en las Relaciones con las Entidades Bancarias, Erreius, Buenos Aires, 2020, pp. 34-35.

ejemplo. Paralelamente, dichos canales introducen riesgos tecnológicos propios, vinculados con accesos indebidos, suplantación de identidad y fraudes electrónicos. En consecuencia, resulta razonable que sea la entidad financiera quien soporte las consecuencias derivadas de la materialización de esos riesgos, dado que es quien organiza el sistema, controla su funcionamiento y, al mismo tiempo, obtiene el provecho de ello.En este marco, en los supuestos de fraude electrónico, el daño no se presenta como un evento externo y ajeno al servicio, sino como la materialización de un riesgo inherente al funcionamiento del sistema que la propia entidad organiza, administra y explota económicamente. La utilización indebida de credenciales, la manipulación de los canales de acceso y la ejecución de operaciones no consentidas son contingencias del entorno digital en el que la actividad bancaria se desarrolla, y no hechos que escapen a la lógica del servicio prestado. A ello se suma que esos riesgos son introducidos unilateralmente por el proveedor para su beneficio y se imponen al consumidor, quien no participa en su configuración ni dispone de los medios para neutralizarlos. Por ello, deben ser soportados por quien los genera, los controla y obtiene provecho de ellos. Como señala Mendieta, la entidad financiera debe garantizar un nivel de seguridad equivalente al que cabría razonablemente esperar en las operaciones realizadas de manera presencial, trasladando al usuario únicamente los riesgos que este pueda efectivamente controlar.[78]

En definitiva, los tres fundamentos descritos convergen en una misma conclusión, y es que en los supuestos de fraude electrónico bancario, la responsabilidad de las entidades financieras se configura bajo un factor de atribución objetivo. El elemento común que los articula radica en que el daño se produce dentro de un ámbito de organización, controlado por el propio del banco, lo que torna irrelevante el análisis de su conducta diligente y desplaza el eje de imputación hacia el riesgo creado por la propia actividad y hacia el incumplimiento de las obligaciones de resultado asumidas frente al usuario. Esta lógica se ve reforzada en el marco de las relaciones de consumo, donde la tutela del usuario impone privilegiar criterios de responsabilidad que aseguren una reparación efectiva frente a daños derivados del funcionamiento del sistema. Desde esta perspectiva, el deber de responder no se agota en la mera reacción frente al daño, sino que encuentra su fundamento en la obligación previa de prevenirlo, lo que conduce necesariamente al análisis del deber de seguridad como eje estructural de la responsabilidad bancaria en el entorno digital, cuestión que será abordada en el siguiente apartado.

[78] MENDIETA, Ezequiel N., “La obligación de seguridad y el trato digno en el marco de las relaciones de consumo bancarias en el entorno digital. A propósito de la emergencia sanitaria, las sanciones dictadas por la Dirección Nacional de Defensa del Consumidor y la protección de los consumidores hipervulnerables”, RCCyC 2021 (septiembre), 13/09/2021, 10, cita online: TR LALEY AR/DOC/2292/2021.

4.3. El deber de seguridad en la actividad bancaria y su proyección en entornos digitales

4.3.1. Concepto y fundamento normativo del deber de seguridad

El deber u obligación de seguridad constituye uno de los pilares fundamentales del derecho del consumidor en el ordenamiento jurídico argentino. En términos generales, la doctrina lo conceptualiza como un deber jurídico que pesa sobre quien provee bienes o servicios, orientado a preservar la integridad de las personas y la indemnidad de sus bienes frente a los riesgos derivados de la actividad desarrollada. Es un derivado del principio de buena fe (art. 9 CCyCN), que implica la obligación de evitar la generación de daños y perjuicios en las personas y bienes que adquieren o utilizan los productos y servicios que ofrecen los proveedores.[79]

Desde esta perspectiva, el deber de seguridad no se limita al cumplimiento estricto de la prestación principal asumida por el proveedor, sino que constituye un deber complementario destinado a evitar que el consumidor sufra daños derivados del producto o servicio ofrecido.[80] En consecuencia, quien introduce bienes o servicios en el mercado debe adoptar las medidas necesarias para prevenir perjuicios previsibles vinculados con su utilización, incluso cuando tales medidas no hayan sido específicamente pactadas entre las partes. Como ha sostenido Pizarro, *"pesa sobre el proveedor profesional una obligación de seguridad y garantía respecto del adquirente o del consumidor con el que ha contratado, que le impone suministrar productos que no causen daños a este último en su persona o en sus bienes".*[81]

El fundamento constitucional del deber de seguridad se encuentra en el artículo 42 de la Constitución Nacional, en donde se establece que *"los consumidores y usuarios de bienes y servicios tienen derecho, en la relación de consumo, a la protección de su salud, seguridad e intereses económicos; a una información adecuada y veraz; a la libertad de elección, y a condiciones de trato equitativo y digno".* [82] La jerarquización constitucional de la seguridad como derecho implica que esta deja de ser una cuestión estrictamente contractual para convertirse en un mandato constitucional que exige que la actividad económica se desarrolle en condiciones que no generen riesgos indebidos para quienes participan en el mercado como consumidores o usuarios.

En concordancia con ello, este principio protectorio se proyecta de manera directa en la LDC. El art. 5 establece que *"las cosas y servicios deben ser suministrados o prestados en forma tal que,*

[79] STIGLITZ, Gabriel A., "El deber de seguridad en el derecho del consumidor", en Gabriel A. Stiglitz y Carlos A. Hernández (dirs.), *Tratado de derecho del consumidor*, Tomo III, Buenos Aires: La Ley, 2015, pp. 39-44.
[80] Ídem.
[81] PIZARRO, Ramón D., "Responsabilidad por productos y por servicios en la Ley de Defensa del Consumidor", en Gabriel A. Stiglitz y Carlos A. Hernández (dirs.), *Tratado de derecho del consumidor*, Tomo III, Buenos Aires: La Ley, 2015, p. 204.
[82] Constitución Nacional, art. 42

utilizados en condiciones previsibles o normales de uso, no presenten peligro alguno para la salud o integridad física de los consumidores o usuarios."[83] Si bien la norma alude expresamente a la integridad física, su lógica protectora resulta extensible a la integridad patrimonial cuando se trata de servicios bancarios, en los que el principal interés comprometido es precisamente el patrimonio del usuario.[84] Por su parte, el artículo 6 impone el deber de advertir adecuadamente sobre los riesgos que puedan derivarse del uso del bien o servicio, reforzando la dimensión preventiva del régimen.

En cuanto a su naturaleza jurídica, la posición doctrinaria y jurisprudencial predominante caracteriza al deber de seguridad como una obligación de resultado. En esta línea, las Sextas Jornadas Bonaerenses de Derecho Civil, la Comisión N.º 2 presidida por el doctor Alberto Bueres concluyó que la obligación de seguridad se funda en el principio de buena fe, posee autonomía funcional respecto de la obligación principal del contrato y, por regla general, implica una obligación de resultado, adquiriendo jerarquía constitucional en el ámbito de las relaciones de consumo a partir de su reconocimiento en el art. 42 de la Constitución Nacional.[85] En igual sentido se ha pronunciado Garrido Cordobera, destacando que la relevancia de los bienes jurídicos involucrados y la finalidad protectora que inspira el derecho del consumidor imponen caracterizar esta obligación como de resultado.[86] En el marco de este trabajo se adopta esta posición, en tanto resulta coherente con el régimen de atribución objetiva sostenido en el apartado anterior y con la exigencia de garantizar la indemnidad del consumidor frente a los riesgos propios de la actividad desarrollada por el proveedor.

A partir de lo expuesto, puede sostenerse que el deber de seguridad constituye una obligación jurídica compleja que encuentra fundamento tanto en el principio de buena fe como en el sistema constitucional y legal de protección del consumidor. Su finalidad consiste en garantizar que la actividad económica se desarrolle sin generar daños a quienes participan en el mercado como consumidores o usuarios.

4.3.2. Alcance del deber de seguridad en los servicios bancarios digitales

En el ámbito de la contratación bancaria con consumidores, el deber de seguridad constituye una obligación que pesa de manera permanente sobre las entidades financieras. El sistema bancario se estructura sobre la confianza que los usuarios depositan en las instituciones encargadas de custodiar y administrar su patrimonio. Cuando una persona decide operar con una entidad bancaria lo hace bajo la expectativa de que su dinero será resguardado adecuadamente y que

[83] LDC, art. 5
[84] STIGLITZ, "El deber de seguridad en el derecho del consumidor", ob. cit.,, pp. 39-44.
[85] ARIAS y MÜLER, ob. cit.
[86] GARRIDO CORDOBERA, María R., "La obligación de seguridad y el derecho del consumidor", en Fernando M. Álvarez Larrondo (ed.), *Manual de derecho del consumo*, Buenos Aires: Erreius, 2017, pp. 265-284.

podrá disponer de él en condiciones de seguridad. Dado que estas operaciones inciden directamente sobre el patrimonio de los usuarios, el banco debe garantizar que los servicios ofrecidos se presten en condiciones que aseguren la integridad y protección de los fondos involucrados.[87] Por este motivo, el deber de seguridad se encuentra presente en toda la contratación bancaria celebrada con consumidores, con independencia del canal a través del cual se ejecute la operación.

Bajo esta perspectiva, la obligación de seguridad impone a las entidades financieras el deber de brindar a sus clientes un marco adecuado de protección en todas las operaciones que se realizan dentro del sistema bancario, ya sea por canales presenciales o por medios electrónicos. El banco debe adoptar todas las medidas necesarias para evitar que los riesgos inherentes a su actividad se traduzcan en daños para sus clientes, y solo podrá liberarse de responsabilidad acreditando la existencia de una causa ajena que reúna los requisitos de imprevisibilidad, inevitabilidad y exterioridad con aptitud suficiente para romper el nexo causal.[88]

En el entorno digital, este deber adquiere una intensidad mayor. Como se analizó en los capítulos precedentes, la digitalización del sistema financiero ha desplazado la operatoria hacia plataformas y aplicaciones digitales cuyo diseño y control permanecen en la esfera del proveedor. El usuario interactúa con interfaces simplificadas, pero no controla la arquitectura técnica del sistema ni está en condiciones de auditar su seguridad. Esta asimetría técnica profundiza la vulnerabilidad del consumidor y refuerza la exigencia de protección.[89]

En este contexto, la introducción de canales digitales no puede traducirse en una disminución del nivel de seguridad ofrecido. Por el contrario, cuando la entidad sustituye la operatoria presencial por mecanismos automatizados, asume la obligación de que esos mecanismos ofrezcan un nivel de seguridad por lo menos equivalente al que el consumidor razonablemente esperaría en un entorno tradicional. Como señala Chamatropulos, cuando el proveedor reemplaza la intervención humana por tecnología, debe soportar las consecuencias dañosas derivadas de la insuficiencia del sistema implementado debiendo garantizar que ese canal opere en condiciones adecuadas de seguridad.[90]

De esta manera, el deber de seguridad en los servicios bancarios digitales exige a las entidades financieras garantizar un entorno operativo que minimice razonablemente los riesgos inherentes al uso de tecnologías electrónicas. Su contenido concreto se determina en función de las

[87] RUIZ DÍAZ, ob. cit.
[88] ARIAS y MÜLER, ob. cit.
[89] ABAD, Gabriela A., "Análisis de la responsabilidad bancaria en casos de estafas electrónicas mediante redes sociales desde la óptica del derecho de consumo", elDial.com, 07/05/2021, cita online: elDial.com - DC2DE4.
[90] CHAMATROPULOS, Demetrio A., "El deber de seguridad de los bancos y los daños derivados de la utilización de cajeros automáticos", en *Revista de Responsabilidad Civil y Seguros*, N.º 12 Vol., 2010, pp. 95-103.

características del servicio prestado y de los estándares técnicos y organizativos exigibles a quien opera profesionalmente en el sector bancario digital, abarcando medidas de autenticación, monitoreo, prevención, trazabilidad y respuesta inmediata frente a incidentes. En todo caso, este deber no puede considerarse satisfecho por la mera existencia formal de protocolos o herramientas, ni por el simple cumplimiento de las exigencias regulatorias, sino por la aptitud efectiva del sistema implementado para impedir que los riesgos previsibles se traduzcan en daños concretos para el consumidor.

4.4. Causales de exoneración y ruptura del nexo causal en los fraudes electrónicos

La determinación del alcance de las eximentes resulta decisiva para definir la efectiva operatividad del régimen de responsabilidad objetiva en materia de fraudes electrónicos. En el marco de un régimen de responsabilidad objetiva, como se analizó en el apartado 4.3 y en el que concluimos que resulta aplicable en la actividad bancaria digital con consumidores, la entidad financiera sólo puede eximirse de responsabilidad mediante la acreditación de una causa ajena. Esta se caracteriza por consistir en un hecho externo al sujeto a quien se pretende imputar el daño, con aptitud suficiente para interrumpir el nexo causal. Estas causales comprenden el hecho de la víctima, el hecho de un tercero por quien no se debe responder y el caso fortuito o fuerza mayor (arts. 1729, 1730 y 1731 CCyCN).

La delimitación de estas causales eximentes adquiere particular relevancia en el ámbito de las relaciones de consumo, donde su admisión no puede efectuarse de manera amplia o automática. Por el contrario, su valoración debe realizarse con criterio restrictivo, en atención a la situación de vulnerabilidad estructural del consumidor y al carácter tuitivo del régimen aplicable.[91] En la práctica, las entidades financieras frente a una situación de fraude digital, suelen invocar principalmente dos defensas. Por un lado, le atribuyen el daño a la conducta del propio usuario, alegando que éste facilitó sus credenciales, incumplió las pautas de seguridad o actuó con negligencia en el resguardo de sus datos. Por otro lado, remiten al accionar de terceros por los cuales no debe responder (los autores del fraude) como hechos ajenos a su esfera de control.[92]

La admisibilidad de estas eximentes debe evaluarse con especial rigor, en tanto su aplicación no puede desvirtuar el deber de seguridad que pesa sobre el proveedor ni trasladar al usuario los riesgos propios del sistema que la entidad organiza y explota. Para ello, no basta con su mera invocación, sino que debe reunir los requisitos necesarios para producir la ruptura del nexo causal. En este sentido, la carga de la prueba recae sobre la entidad financiera (art. 1734), que

[91] STIGLITZ, Gabriel A., “Restricciones a la exoneración por causa ajena. Culpa del consumidor. Hiposuficientes. Autorización administrativa”, en Gabriel A. Stiglitz y Carlos A. Hernández (dirs.), *Tratado de derecho del consumidor*, Tomo III, Buenos Aires: La Ley, 2015, pp. 39-44.
[92] MENDIETA, ob. cit.

deberá acreditar que el daño no guarda relación con su actividad ni con el funcionamiento del sistema que organiza.

En este sentido, la distribución de la carga probatoria se explica a partir de dos reglas que operan de manera complementaria. La primera deriva del propio régimen de responsabilidad objetiva. Una vez acreditados por el consumidor el daño y su vinculación con el servicio bancario, corresponde a la entidad financiera demostrar la existencia de una causa ajena con aptitud suficiente para interrumpir el nexo causal, quedando el usuario relevado de probar la culpa del proveedor (arts. 1734 CCyCN y 40 LDC). La segunda responde al principio de las cargas probatorias dinámicas, receptado por el art. 1735 CCyCN, que faculta al juez a distribuir la carga de la prueba según cuál de las partes se encuentre en mejores condiciones de acreditar los hechos controvertidos. Este criterio encuentra una manifestación específica en el art. 53, tercer párrafo, de la LDC, que impone al proveedor el deber de aportar al proceso todos los elementos de prueba que obren en su poder y de prestar la colaboración necesaria para el esclarecimiento de la controversia.

Estas reglas adquieren especial relevancia en los supuestos de fraude electrónico. La información técnica necesaria para reconstruir la operatoria cuestionada (como los registros de acceso, los mecanismos de autenticación utilizados, la trazabilidad de las transacciones, los sistemas de monitoreo, las alertas de seguridad generadas, etc.) se encuentra bajo el control exclusivo de la entidad financiera. Por el contrario, el consumidor carece de acceso a esos elementos y no se encuentra en condiciones de demostrar en qué etapa o por qué motivo el sistema permitió la ejecución de una operación no consentida. Exigirle esa prueba implicaría imponerle la acreditación de hechos que se desarrollan íntegramente dentro de una infraestructura tecnológica diseñada, administrada y controlada por el banco. [93] En consecuencia, corresponde a la entidad financiera demostrar tanto el correcto funcionamiento de sus sistemas de seguridad como la configuración de una causa ajena capaz de excluir su responsabilidad. La ausencia de una actividad probatoria suficiente en ese sentido debe ser valorada en su contra, pues es quien dispone de los medios técnicos e informativos necesarios para acreditar el cumplimiento del deber de seguridad y la efectiva ruptura del nexo causal. [94]

4.4.1 El hecho de la víctima como eximente y su interpretación restrictiva

Como se mencionó precedentemente, la principal defensa invocada por las entidades financieras frente a supuestos de fraude electrónico consiste en atribuir el daño a la conducta del propio consumidor, alegando que éste proporcionó sus credenciales, incumplió las pautas de seguridad o facilitó de algún modo el acceso al sistema. En términos generales, la defensa se estructura

[93] PÉREZ, Lucía C., “El deber de seguridad de los bancos frente al consumidor financiro”, Abogados.com.ar, 2024
[94] Ídem

sobre la base de que el propio usuario habría facilitado sus credenciales (usuario, clave, *token* u otros datos confidenciales), posibilitando la concreción de la maniobra fraudulenta y, en consecuencia, interrumpiendo el nexo causal en los términos del art. 1729 del CCyCN. Si bien dicho artículo reconoce esta eximente, en el ámbito del derecho del consumidor, el hecho de la víctima no opera de manera automática como causal de exoneración de la responsabilidad del proveedor frente a los daños sufridos por el consumidor. Específicamente en supuestos vinculados con el incumplimiento del deber de seguridad, la mera intervención del consumidor no resulta suficiente para interrumpir el nexo causal.[95]

En esta línea, la Corte Suprema de Justicia de la Nación (en adelante, la "CSJN") ha tenido oportunidad de pronunciarse sobre el alcance de esta eximente en los casos de la responsabilidad por incumplimiento de la obligación de seguridad. En el precedente "Ledesma" el Tribunal sostuvo que, tratándose de una obligación de seguridad de carácter objetivo, las causales de exoneración deben analizarse exclusivamente desde la perspectiva de la ruptura del nexo causal, descartando que la conducta de la víctima tuviera entidad suficiente para configurar una causa interruptiva, especialmente cuando el daño se encontraba vinculado con una omisión previa del prestador.[96] Este criterio fue reafirmado posteriormente en el caso "Uriarte", en el cual la Corte consideró que, aun cuando la víctima se hubiera colocado en una situación potencialmente riesgosa, dicha circunstancia no resultaba idónea para interrumpir el nexo causal cuando el daño se explicaba, en definitiva, por el incumplimiento previo de las obligaciones de seguridad a cargo del proveedor[97]. [98]

A partir de estos precedentes se ha consolidado un estándar según el cual la conducta del consumidor debe ser la causa adecuada y exclusiva del daño para tener virtualidad exoneratoria. Cuando se presenta como una mera circunstancia concurrente o como un efecto del propio funcionamiento del sistema diseñado por el proveedor, carece de relevancia a estos fines.[99] Esta tendencia restrictiva en la valoración de la conducta de la víctima se justifica en la situación de vulnerabilidad estructural que caracteriza al consumidor, quien se encuentra sometido a riesgos crecientes, condicionado por la asimetría informativa y técnica, y privado de los instrumentos necesarios para controlar el entorno en el que opera. Esa posición de inferioridad constituye una razón suficiente para apreciar con criterio restrictivo la eventual culpa del damnificado y para exigir, a fin de que el hecho de la víctima tenga aptitud exoneratoria, una culpa calificada que

[95] MENDIETA, ob. cit.
[96] Corte Suprema de Justicia de la Nación, *""Ledesma, María Leonor c/ Metrovías SA"*, 22/04/2008
[97] CSJN, *"Uriarte Martínez, Héctor Víctor y otro c/ Transportes Metropolitanos General Roca S.A. y otros"*, 09/03/2010, Fallos 333:203
[98] Cabe señalar que ambos precedentes "Ledesma" y "Uriarte" se refieren al ámbito del transporte público. Sin embargo, la doctrina allí sentada sobre el alcance del hecho de la víctima como eximente en obligaciones de seguridad ha sido extendida por la jurisprudencia y la doctrina a otros supuestos de consumo, en tanto establece criterios de alcance general aplicables a toda relación en la que el proveedor asume un deber de seguridad frente al usuario.
[99] MENDIETA, ob. cit.

equivalga a culpa grave, en tanto solo ese nivel de reproche podría tener relevancia causal en el marco de una relación de consumo.[100]

Este criterio adquiere especial relevancia en el ámbito de los fraudes electrónicos. La conducta del usuario (por ejemplo, al interactuar con un sitio falso o responder a una comunicación engañosa), no constituye por sí sola un hecho suficiente para romper el nexo causal, en tanto el daño se vincula con la posibilidad misma de que el sistema permita la ejecución de operaciones fraudulentas con esos datos. La conducta del consumidor debe analizarse teniendo en cuenta la confianza que el propio sistema genera y la imposibilidad práctica de distinguir entre comunicaciones legítimas y fraudulentas, circunstancia que no puede ser imputada al usuario como negligencia cuando resulta de las propias características del entorno digital organizado por la entidad.[101] En consecuencia, no basta con acreditar una conducta imprudente del consumidor para tener por configurada la eximente y debe demostrarse que esa conducta constituye la causa exclusiva y determinante del daño, extremo que rara vez se verifica en los fraudes digitales, donde la materialización del perjuicio depende siempre, en alguna medida, de las deficiencias o limitaciones del sistema de seguridad administrado por la entidad financiera.

4.4.2 El hecho de terceros frente al riesgo propio de la actividad bancaria digital

Otra de las defensas habituales invocadas por las entidades financieras consiste en atribuir el daño al accionar de un tercero por quien no se debe responder, esto es, el accionar del autor del fraude. Sin embargo, para que esta causal tenga aptitud liberatoria, debe reunir los requisitos del caso fortuito conforme lo dispuesto en los art. 1730 y 1731 CCyCN. Es decir, no basta con la mera intervención de un tercero para eximir de responsabilidad al proveedor, sino que es necesario que dicho hecho sea imprevisible, inevitable y ajeno al ámbito de organización y control del deudor.

Bajo este enfoque, corresponde analizar si el accionar delictivo de un tercero en el entorno digital puede ser calificado como imprevisible e inevitable. A tal efecto, la imprevisibilidad no debe evaluarse desde la percepción del consumidor ni desde el carácter sorpresivo del caso concreto, sino desde la posición del proveedor que organiza profesionalmente el servicio y conoce los riesgos propios del sistema.[102] Teniendo en cuenta que los fraudes electrónicos constituyen un fenómeno extendido y recurrente dentro del funcionamiento del sistema bancario digital, su ocurrencia difícilmente puede ser considerada imprevisible o ajena a la actividad.

Asimismo, la exigencia de inevitabilidad tampoco se verifica en estos supuestos. La evitabilidad del daño se vincula directamente con la organización del servicio y con las decisiones

[100] STIGLITZ., “Restricciones a la exoneración por causa ajena…”, ob. cit., pp. 39-44.
[101] MENDIETA, ob. cit.
[102] Ídem.

empresariales adoptadas por la entidad. En el ámbito de la banca digital, la implementación de mecanismos de autenticación robustos, monitoreo transaccional, detección de patrones inusuales y respuesta inmediata frente a incidentes constituye una obligación propia del proveedor. Si tales medidas resultan insuficientes, el daño no puede considerarse inevitable, sino una consecuencia de las deficiencias del sistema implementado.[103]

Por lo tanto, la intervención del tercero no puede ser considerada una causa ajena con aptitud liberatoria, dado que no constituyen hechos extraordinarios o ajenos al sistema. La reiteración de estas conductas, su previsibilidad y su regulación específica evidencian que no se trata de contingencias extremas, sino de fenómenos propios del entorno tecnológico en el que se desarrolla la actividad. Esta conclusión se ve reforzada por lo dispuesto en el artículo 1733 del CCyCN que establece que el caso fortuito no libera de responsabilidad cuando constituye una contingencia propia del riesgo de la cosa o de la actividad. Aplicado al ámbito bancario, ello implica que los fraudes electrónicos no pueden ser considerados hechos ajenos con aptitud liberatoria, sino riesgos propios del sistema que la entidad organiza y explota.

Es por esto que la intervención de un tercero en los fraudes electrónicos no reúne, en la mayoría de los casos, los requisitos necesarios para configurar una causa ajena que interrumpa el nexo causal. Por el contrario, se trata de hechos previsibles, evitables y vinculados al riesgo propio de la actividad bancaria digital, lo que impide que sean utilizados como eximentes de responsabilidad por parte de las entidades financieras. Admitir lo contrario implicaría desnaturalizar el régimen de responsabilidad objetiva, permitiendo al proveedor liberarse por la sola intervención de un tercero, aun cuando el daño se haya producido en el ámbito de un sistema cuya organización y control le pertenecen.

4.4.3. La normativa del BCRA como parámetro de conducta y sus límites como eximente

Una tercera defensa que las entidades financieras suelen invocar consiste en acreditar el cumplimiento de la normativa dictada por el BCRA como fundamento de su exoneración. Sin embargo, esa invocación no resulta suficiente para excluir la responsabilidad cuando el sistema implementado se revela ineficaz para prevenir daños previsibles.

Para comprender por qué, es necesario distinguir entre el plano regulatorio y el plano de la responsabilidad civil. Las normas del BCRA tienen naturaleza administrativa y cumplen una función de organización y supervisión del sistema financiero. Por el contrario, el deber de seguridad que deriva del art. 42 de la Constitución Nacional, de los arts. 5 y 6 de la LDC y del art. 1710 del CCyCN opera en un plano más amplio y se proyecta sobre la tutela efectiva del

[103] GHERSI, Carlos, “Obligación de seguridad. Alcance temporal y espacial de la responsabilidad”, en Carlos Ghersi, Celia Weingarten y Graciela Lovece (dirs.), *Derechos de los Consumidores y Empresas en las Relaciones con las Entidades Bancarias*, Buenos Aires: Erreius, 2020, pp. 3-46.

consumidor frente al daño concreto sufrido.[104] En este sentido, el art. 1757 CCyCN establece expresamente que el cumplimiento de normas técnicas o regulatorias no constituye por sí solo una causa de exoneración de responsabilidad, principio que adquiere especial relevancia en el ámbito de la banca digital, donde la rápida evolución de las modalidades de fraude exige una respuesta dinámica y adaptativa que no siempre puede anticiparse en una norma administrativa.

En este sentido, la normativa del BCRA debe ser entendida como un piso mínimo de diligencia técnica exigible a las entidades financieras, mientras que el techo lo fijan el principio de prevención del daño, el deber de seguridad y la especial tutela de los intereses económicos del consumidor financiero. El incumplimiento de dichas normas constituye un indicio especialmente relevante de insuficiencia del sistema de seguridad. Pero el cumplimiento formal de estas disposiciones no agota el contenido del deber de seguridad ni libera automáticamente al banco de responsabilidad. Una entidad puede acreditar que observó las exigencias reglamentarias del BCRA y, aun así, resultar responsable si en el caso concreto las medidas implementadas se revelaron insuficientes para prevenir el fraude. El deber de seguridad exige no solo adecuarse a la regulación vigente, sino garantizar efectivamente la indemnidad del consumidor frente a los riesgos propios del sistema que la entidad organiza y explota.

En definitiva, el análisis de las causales de exoneración en los fraudes electrónicos permite advertir que su admisión en el ámbito de la banca digital debe ser de interpretación estricta. Ello se explica no solo por el carácter objetivo del régimen de responsabilidad aplicable, sino también por el rol central que cumple el deber de seguridad como parámetro de imputación. En este contexto, ni la conducta del consumidor, ni la intervención de terceros, ni el cumplimiento formal de la normativa regulatoria pueden ser invocados de manera automática como eximentes, sino que deben ser evaluados a la luz del funcionamiento del sistema organizado por la entidad financiera y de su capacidad para prevenir los riesgos propios de la actividad.

De este modo, la responsabilidad del banco en los fraudes electrónicos no se ve desplazada por la mera concurrencia de factores externos, sino únicamente en aquellos supuestos en los que se acredite una verdadera ruptura del nexo causal, caracterizada por la imprevisibilidad, inevitabilidad y ajenidad del hecho. Fuera de estos casos excepcionales, el daño debe ser imputado al proveedor en tanto consecuencia del riesgo creado por el sistema que diseña, controla y explota, en coherencia con los principios del derecho del consumidor y la responsabilidad civil.

Capítulo 5. El tratamiento jurisprudencial de los fraudes electrónicos bancarios

[104] PÉREZ, ob. cit.

El análisis del tratamiento jurisprudencial de los fraudes electrónicos en el marco de las relaciones de consumo bancarias permite observar, en términos concretos, el modo en que los principios desarrollados en los capítulos precedentes se proyectan en la resolución de conflictos reales. El objetivo del presente capítulo es comprobar en qué medida los fundamentos desarrollados a lo largo de este trabajo han sido efectivamente receptados por los órganos de decisión.

Los fallos jurisprudenciales analizados comprenden a pronunciamientos dictados entre 2021 y 2026, emanados de tribunales de distintas jurisdicciones del país, incluyendo cámaras nacionales y provinciales, juzgados de primera instancia y un tribunal superior provincial. La selección incorpora tanto pronunciamientos favorables al consumidor como decisiones que rechazan la responsabilidad bancaria, con el objeto de reconstruir un panorama representativo del estado actual de la cuestión, identificando no sólo las soluciones dominantes, sino también sus matices y límites.

Del análisis conjunto de estos precedentes no surge una dispersión desordenada de criterios contrapuestos, sino más bien una paulatina consolidación de una línea jurisprudencial que coloca al deber de seguridad y al riesgo inherente a la actividad bancaria digital como ejes centrales de imputación. En ese marco, el foco del análisis judicial se desplaza desde la conducta individual del usuario hacia la evaluación del sistema bancario digital en su conjunto, atendiendo a su carácter profesional, tecnológicamente complejo y estructuralmente riesgoso. Los tribunales tienden a reconstruir los fraudes electrónicos no como hechos aislados o excepcionales, sino como manifestaciones de riesgos propios del sistema de banca digital. Este enfoque resulta determinante para la atribución de responsabilidad, en tanto permite comprender que la intervención de terceros o la eventual conducta del consumidor no operan, por regla, como factores autónomos de ruptura del nexo causal.

Sobre esta base, el presente capítulo se propone identificar las principales tendencias jurisprudenciales en materia de fraudes electrónicos, analizando: el factor de atribución aplicado por los tribunales, el alcance del deber de seguridad como criterio central de imputación y el tratamiento restrictivo de las eximentes, en particular el hecho de la víctima y el hecho de terceros.

5.1. La configuración de un régimen de responsabilidad objetiva

Uno de los rasgos más consistentes que emerge del análisis de los fallos relevados es la consolidación de un modelo de responsabilidad objetiva en materia de fraudes electrónicos bancarios en el marco de relaciones de consumo. Determinar si la responsabilidad bancaria es subjetiva u objetiva no es una cuestión meramente técnica, sino que define el eje del litigio, distribuye las cargas probatorias y condiciona decisivamente el resultado del caso. En este

sentido, los tribunales muestran una tendencia clara y sostenida a aplicar un factor de atribución objetivo para estos casos.

En primer lugar, y para justificar dicha solución, los tribunales encuadran de manera uniforme estos conflictos dentro de una relación de consumo, aplicando el artículo 40 de la LDC y, en forma complementaria, las disposiciones del CCyCN. En este marco, el análisis se desplaza desde la valoración de la conducta subjetiva del banco hacia la verificación del daño y su vinculación con el servicio prestado, trasladando a la entidad la carga de acreditar la ruptura del nexo causal.

En el precedente *“Fernández Quintana c/ Banco Patagonia S.A*.” el tribunal afirmó que la *"responsabilidad civil del banco deviene objetiva y para liberarse debió demostrar que la causa le fuera ajena (art. 40 de la ley 24.240), circunstancia esta última que no se presenta"*.[105] La remisión al artículo 40 de la LDC ubica a la entidad en su carácter de proveedora y le impone la carga de demostrar la ruptura del nexo causal como condición de su exoneración. En igual sentido, en "*C.S. c/ Banco Itaú Argentina S.A.",* el Juzgado de Primera Instancia en lo Contencioso Administrativo, Tributario y de Relaciones de Consumo N.º 27 de C.A.B.A. resolvió que *"resulta atribuible el daño a la entidad bancaria demandada, conforme la responsabilidad objetiva y solidaria de la cadena de comercialización y producción de bienes y servicios, dispuesta en el art. 40 de la LDC”*.[106]

Por su parte, en *"González c/ Banco de la Provincia de Buenos Aires”* la Jueza formuló con especial precisión que *"corresponde analizar la responsabilidad de la entidad bancaria en cumplimiento de la obligación de seguridad cuyo factor de atribución es objetivo y de la que sólo puede liberarse probando la causa ajena, que en el caso debe reunir los caracteres de imprevisibilidad e inevitabilidad del caso fortuito"*[107], lo que evidencia que la discusión no se centra en la culpa del banco, sino en la existencia de una causa externa con entidad suficiente para interrumpir el nexo causal.

Este esquema se ve reforzado por una segunda línea argumental, que califica a la actividad bancaria digital como una actividad riesgosa, por lo que el riesgo que genera su utilización debe ser asumido por quien lo organiza. En el caso *"Fernández c/ Banco de la Provincia de Buenos Aires"* el tribunal encuadra la prestación del servicio dentro del artículo 1757 del CCyCN, señalando que la banca digital *"resulta ser riesgosa”* en tanto incorpora *"el riesgo empresario que*

[105] Unidad Jurisdiccional Civil N.º 5, San Carlos de Bariloche*, "Fernández Quintana, Patricia del V. c/ Banco Patagonia S.A. s/ Ordinario - Daños y Perjuicios"*, 21/11/2024, pp. 10-11
[106] Juzgado de Primera Instancia en lo Contencioso Administrativo, Tributario y de Relaciones de Consumo N.º 27, Secretaría Única, Ciudad Autónoma de Buenos Aires, *"C.S., J.V. c/ Banco Itaú Argentina S.A. s/ Contratos y Daños - RC - Bancos, Productos y Servicios Financieros",* 2024, p. 18
[107] Cámara de Apelación en lo Civil y Comercial de Necochea, *"González, Verónica Graciela c/ Banco de la Provincia de Buenos Aires y Otro/a s/ Nulidad de Contrato",* 09/08/2022, p. 17

resulta de una actividad económica" desarrollada mediante *"tareas, servicios, productos o prestaciones" que generan para sus beneficiarios un provecho económico"*.[108]

Es relevante destacar que incluso en aquellos fallos en los que la responsabilidad bancaria es descartada, la jurisprudencia no abandona el esquema objetivo de imputación. Los precedentes analizados que rechazan la pretensión del consumidor no lo hacen sobre la base de un retorno a criterios subjetivos, sino a partir de la verificación de una causa ajena con aptitud suficiente para interrumpir el nexo causal. En *"Pesce c/ Banco Patagonia S.A."* el tribunal reconoció expresamente que "*la responsabilidad objetiva encuentra fundamento en el art. 40"* y que *"la demandada sólo podría eximirse acreditando... culpa de la víctima"*.[109]

En consecuencia, puede afirmarse que la jurisprudencia reciente consolida un modelo uniforme en el cual la responsabilidad bancaria frente a fraudes electrónicos en el marco de una relación de consumo se estructura sobre un factor objetivo, sustentado en el régimen de consumo y en el riesgo propio de la actividad, desplazando definitivamente los esquemas basados en la culpa.

5.2. El deber de seguridad como criterio de imputación

Si el factor de atribución define el marco de responsabilidad, el deber de seguridad constituye el eje a partir del cual los tribunales construyen la imputación concreta del daño. Es el parámetro a partir del cual los tribunales evalúan el cumplimiento de las obligaciones del banco, la idoneidad del sistema que éste puso a disposición del consumidor y, en definitiva, la existencia de un incumplimiento jurídicamente relevante que habilite la atribución de responsabilidad.

La jurisprudencia reciente no se limita a reconocer este deber en términos abstractos, sino que le asigna un contenido sustantivo y dinámico, que excede ampliamente el mero cumplimiento formal de las normas regulatorias y desplaza el análisis desde la búsqueda del autor material del fraude hacia la evaluación del sistema organizado por el proveedor. En este sentido, el deber de seguridad se configura como una verdadera obligación de resultado en el marco de la relación de consumo, en tanto impone a la entidad financiera garantizar un funcionamiento del sistema que no genere daños al usuario dentro de los riesgos previsibles de la operatoria digital.

5.2.1 La relación de consumo como fundamento del deber de seguridad

El principal fundamento que los tribunales le atribuyen al deber de seguridad se encuentra en la relación de consumo que vincula a las partes, en tanto es esta la que determina la aplicación de

[108] Juzgado Civil y Comercial N.º 23, Departamento Judicial La Plata, Provincia de Buenos Aires, *"Fernández, Liliana Ester c/ Banco de la Provincia de Buenos Aires s/ Daños y Perjuicios. Incumplimiento Contractual (Exc. Estado)",* 13/10/2025, p. 9

[109] Cámara Nacional de Apelaciones en lo Comercial, Sala D, "Pesce, Julián c/ Banco Patagonia S.A. s/ Ordinario", 18/02/2025. Publicado en: La Ley Online, Cita: TR LALEY AR/JUR/8777/2025, p. 6

un régimen de protección reforzada del usuario bancario y redefine los parámetros tradicionales de imputación de responsabilidad.

En *"González c/ Banco de la Provincia de Buenos Aires"*, se afirma que *"siendo indiscutible la relación de consumo que une a las partes, debe analizarse la cuestión por incumplimiento del deber de seguridad inherente a las entidades bancarias (arts. 1384, 1093, 1094 y cc del CCC) con sustento en los derechos del consumidor de fuente constitucional (art. 42 de la CN) receptado, entre otras normas, en los artículos 5, 6, 40 y ss. de la ley 24.240; y que se integra además con las reglamentaciones que ha dictado la autoridad de aplicación -BCRA- por tratarse de un usuario de servicios financieros. Esta obligación de seguridad es expresa e importa una obligación de resultado en mérito a la naturaleza de la actividad y de la metodología empleada por la entidad y puesta a disposición del usuario para realizar sus operaciones"*.[110]

A partir de esta formulación, el deber de seguridad no aparece como una obligación meramente contractual, sino como el resultado de un entramado normativo que articula normas constitucionales, legislación consumeril y regulación administrativa. Dos aspectos resultan particularmente relevantes: en primer lugar, su carácter expreso, lo que impide reducirlo a una derivación implícita del contrato; en segundo lugar, su naturaleza de obligación de resultado, que desplaza el análisis desde la razonabilidad de las medidas adoptadas hacia la eficacia concreta del sistema.

En esa línea, el Superior Tribunal de Justicia de Río Negro en "Bartorelli c/ Banco Patagonia S.A." reafirma que la responsabilidad debe analizarse *"en base al reprochado incumplimiento del deber de seguridad inherente a las entidades bancarias, de conformidad a lo establecido en los arts. 1384, 1092, 1093, 1094, 1097 y concordantes del CCyC, que se complementa con las reglamentaciones dictadas por el Banco Central de la República Argentina en su condición de autoridad de aplicación. Ello, en el marco de una relación de consumo, que impone el resguardo de un amplio catálogo de derechos y garantías (art. 42 CN; arts. 5, 6, 40 y cc LDC)"*[111]. La relevancia de esta formulación radica en que el deber de seguridad no se deduce de una única norma, sino de la convergencia de múltiples fuentes que, en conjunto, configuran el estándar exigible a la entidad financiera.

El fuero local de la C.A.B.A. recepta esta misma construcción y, además, refuerza los estándares de tutela consumeril con reglas procesales propias del fuero especializado. En *"C.S. c/ Banco Itaú Argentina S.A."*, el tribunal encuadró la obligación de seguridad en los artículos 5 y 6 de la LDC, junto con los artículos 271, 386, 390, 391 y 1384 del CCyCN y la normativa del BCRA, concluyendo que *"se encuentra configurado un incumplimiento al deber de seguridad en los términos de lo normado por los artículos 5 y 6 de la ley 24.240, como así también el deber de*

[110] Cám. Apel. Civ. y Com. Necochea, "González", cit. nota 108, p. 17
[111] STJ Río Negro, Sec. Civil N.º 1, "Bartorelli", cit. Nota 106, p. 4

brindar información clara y precisa al cliente"[112]. El pronunciamiento incorpora además la dimensión del consumidor hipervulnerable en razón de la edad del actor, de 66 años al momento de los hechos, destacando que esa condición *"habilita la aplicación de mecanismos de tutela judicial efectiva con mayor rigurosidad"* y trae aparejado *"un deber reforzado de colaboración por parte del proveedor"* en la resolución del reclamo.[113] Este enfoque añade una capa adicional al análisis del deber de seguridad, dado que no se trata únicamente de garantizar la seguridad técnica del sistema, sino también de adoptar medidas diferenciadas cuando el usuario integra un grupo especialmente expuesto a las maniobras de fraude digital, como lo son las personas mayores.

En definitiva, el deber de seguridad no constituye un deber accesorio del contrato bancario, sino una exigencia estructural del régimen de consumo que redefine el modo en que se atribuye responsabilidad, no se trata de analizar la conducta individual del usuario, sino de exigir al proveedor la garantía efectiva de un sistema que, por su propia configuración y riesgos, le resulta enteramente imputable.

5.2.2 El sistema bancario y sus riesgos como eje del análisis

Una de las características más relevantes de la jurisprudencia reciente en materia de fraude electrónico bancario es que el análisis de responsabilidad no se estructura a partir de la identificación del autor material del ilícito, sino desde la evaluación del sistema de prestación del servicio y de los riesgos que éste genera.

En este enfoque, la cuestión deja de centrarse en quién ejecutó la maniobra fraudulenta para enfocarse en si el sistema tecnológico, en tanto estructura organizada por la entidad financiera, se encontraba en condiciones de prevenir el daño. En consecuencia, la responsabilidad no se construye a partir de la conducta aislada de terceros o del propio usuario, sino sobre la base de la idoneidad, seguridad y confiabilidad del sistema implementado por el proveedor.

En esta línea, en *"Herrera, Marta Florencia y Otros c/ Banco Patagonia S.A."* la Cámara de Cipolletti lo expresó con particular claridad: *"en el marco de una relación de consumo el análisis de responsabilidad no se agota en determinar quién fue el autor material de la maniobra fraudulenta, sino verificar si el servicio brindado por el proveedor resultó defectuoso desde el punto de vista del deber de seguridad que pesa sobre quien organiza profesionalmente la actividad"*.[114] El análisis no se encuadra en quién cometió el fraude, sino si el sistema bancario estaba en condiciones de prevenirlo.

---

[112] Juzg. 1ª Inst. Cont. Adm., Trib. y Rel. Consumo N.º 27, CABA, "C.S., J.V.", cit. nota 107, p. 18

[113] Íbidem, p. 12

[114] Cámara Civil, Comercial, de Familia y Minería de la IV Circunscripción Judicial, Cipolletti, Provincia de Río Negro, *"Herrera, Marta Florencia y Otros c/ Banco Patagonia S.A. s/ Daños y Perjuicios"*, 30/03/2026, p. 2

El mismo fallo agregó que *"el servicio de banca electrónica constituye una actividad organizada profesionalmente por la entidad demandada, que introduce en el mercado un sistema de contratación y operatoria digital cuyos riesgos propios deben ser evaluados a la luz del deber de seguridad que pesa sobre ella en calidad de proveedor del servicio frente a los usuarios consumidores"*, lo que implica que el fraude no puede ser tratado como un hecho externo, sino como una manifestación de los riesgos inherentes al sistema.

Sobre esta base, la imputación de responsabilidad se estructura en torno al incumplimiento de una obligación específica, que es la de garantizar la seguridad del sistema que el propio banco introduce en el mercado. La cuestión no radica en si la entidad participó o no en la maniobra fraudulenta, sino en si adoptó las medidas necesarias para evitar que un riesgo propio de su actividad se concretara en un daño al consumidor. Como señaló la misma Cámara *"el sistema de banca electrónica constituye una herramienta tecnológica cuya implementación ha sido decidida e introducida por las propias entidades financieras como parte de su actividad empresarial, siendo ellas quienes deben velar por la seguridad del sistema, y la protección de sus clientes y de los fondos depositados por éstos, más aún cuando las modalidades de fraude virtual mediante ingeniería social constituyen un fenómeno ampliamente conocido dentro del ámbito de la actividad bancaria"*[115].

Precisamente porque esas modalidades son conocidas y recurrentes, los tribunales han exigido que el sistema bancario esté en condiciones de detectarlas y responder ante ellas. En *"Martínez c/ Banco BBVA Argentina S.A."*, la Cámara señaló que la peligrosidad de las operaciones con canales electrónicos exigía *"mayores precauciones de las entidades especialmente si se detectaban actividades sospechosas como movimientos nocturnos, fuera de lo habitual, por altos montos o desde ubicaciones desconocidas"*.[116] En igual sentido, en *"Fernández Quintana c/ Banco Patagonia S.A."*, el tribunal destacó que *"es el banco demandado quien tiene la obligación de extremar las medidas de seguridad para evitar los previsibles y reiterados ataques informáticos que son de público conocimiento"*, y que la ausencia de un sistema de protección ante operaciones sospechosas constituye en sí misma un incumplimiento del deber de seguridad, dado que *"no resulta seguro para cualquier cliente, que ante tales operatorias referidas [otorgamiento de crédito instantáneo y transferencia de esas sumas de dinero a cuentas bancarias de terceros], que aparecen como sospechosas, no exista un sistema de protección al momento de efectivizarse"*.[117]

[115]Cámara Civil, Comercial, de Familia y Minería de la IV Circunscripción Judicial, Cipolletti, Provincia de Río Negro, "Herrera, Marta Florencia y Otros c/ Banco Patagonia S.A. s/ Daños y Perjuicios", 30/03/2026, p. 17

[116] Cámara Nacional de Apelaciones en lo Comercial, Sala F, "Martínez, César Roberto y Otro c/ Banco BBVA Argentina S.A. s/ Sumarísimo", 28/03/2025, p. 9

[117] Unidad Jurisdiccional Civil N.º 5, San Carlos de Bariloche*, "Fernández Quintana, Patricia del V. c/ Banco Patagonia S.A. s/ Ordinario - Daños y Perjuicios"*, 21/11/2024, p. 6

En idéntica dirección, el fallo porteño *"C.S. c/ Banco Itaú Argentina S.A."* puso el acento en la dinámica concreta de las operaciones cuestionadas como indicador del incumplimiento sistémico. El tribunal señaló que en cuestión de horas y en horario inhábil se extrajeron $228.751 de la cuenta del actor, dejándola con un saldo de $0,82, y que *"frente a esta situación, no se contempló que dichas operaciones podrían resultar extrañas, teniendo en cuenta el perfil de actividad del cliente, por lo que, en los términos de lo normado por las comunicaciones del BCRA mencionadas, debió disparar las alertas, tendientes a cotejar la veracidad de las mismas. Máxime cuando las operaciones reseñadas, no eran realizadas desde los canales utilizados habitualmente por el cliente"*.[118] A ello sumó que el carácter sistemático del problema quedó acreditado por la prueba informativa producida en autos: entre 2020 y 2023, el Banco Itaú acumuló 1.699 denuncias ante la Dirección de Conciliación Previa en las Relaciones de Consumo de la Ciudad de Buenos Aires, siendo el fraude y la estafa una de las temáticas recurrentes. Este dato refuerza la premisa de que el banco no podía desconocer el fenómeno ni alegar imprevisibilidad ante maniobras de ese tipo.

Esta lógica es coherente con el principio de asignación de riesgos desarrollado en el capítulo anterior, según el cual quien introduce una actividad que genera riesgos en el mercado y obtiene beneficios de ella debe asumir las consecuencias de su concreción. En el ámbito de la banca digital, ello se traduce en la exigencia de que la entidad financiera gestione activamente los riesgos propios del sistema que organiza, con independencia de que el daño haya sido ejecutado materialmente por un tercero. La responsabilidad no surge del fraude en sí, sino de la omisión en la adopción de medidas adecuadas para prevenirlo, de modo que el banco responde por no haber evitado la concreción de un riesgo que le es propio, dentro de un sistema cuya seguridad le corresponde garantizar.

5.2.3. La normativa del BCRA como piso mínimo del deber de seguridad

Un aspecto particularmente relevante en la jurisprudencia es la interpretación del alcance de la normativa del BCRA en materia de seguridad. Lejos de considerar que su cumplimiento agota el deber de seguridad, los tribunales coinciden en que dichas disposiciones constituyen un piso mínimo regulatorio.

Las entidades financieras suelen invocar el cumplimiento de las normas del BCRA como demostración de que han observado sus obligaciones de seguridad. Sin embargo, la jurisprudencia rechaza consistentemente este argumento, afirmando que la obligación de seguridad *"no resulta abastecida por el solo cumplimiento de los recaudos previstos por la normativa del BCRA en materia de seguridad, en tanto ello es un piso mínimo regulatorio"*.[119] En consecuencia, no basta con acreditar la observancia formal de dichas disposiciones, sino que

[118] Juzg. 1ª Inst. Cont. Adm., Trib. y Rel. Consumo N.º 27, CABA, "C.S., J.V.", cit. nota 107, p. 17
[119] STJ Río Negro, Sec. Civil N.º 1, "Bartorelli", cit. Nota 106, p. 3

resulta exigible la adopción de todas aquellas medidas adecuadas y necesarias según el estado de la técnica y la previsibilidad del riesgo.

Esta construcción permite distinguir con claridad dos planos normativos. Por un lado, el plano regulatorio-administrativo, en el que el BCRA fija estándares mínimos de cumplimiento obligatorio para las entidades financieras. Por otro lado, el plano de la responsabilidad civil, en el que se evalúa si el sistema implementado resultó efectivamente suficiente para prevenir el daño sufrido por el consumidor. Esta distinción resulta coherente con lo desarrollado en los capítulos precedentes respecto del valor jurídico de la normativa del BCRA, dado que tiene naturaleza administrativa y cumplen una función de organización y supervisión del sistema financiero, pero no definen por sí solas el estándar de diligencia exigible en materia de responsabilidad civil frente al consumidor.

La jurisprudencia construye a partir de allí un criterio dual. Por un lado, el incumplimiento de la normativa del BCRA constituye un indicio claro de incumplimiento del deber de seguridad. En "Bartorelli c/ Banco Patagonia S.A.", el STJ observó que la entidad *"nada expuso ni intentó probar respecto de las medidas complementarias de seguridad que hubiese adoptado en atención a lo establecido en la Comunicación BCRA A Nº 6017"*.[120] En igual sentido, en "Fernández c/ Banco Provincia de Buenos Aires", la pericia informática acreditó que el banco no cumplía con los requisitos de monitoreo y control de acceso establecidos en la normativa, circunstancia que el tribunal consideró directamente vinculada con la concreción del fraude. Del mismo modo, en "Martínez c/ Banco BBVA Argentina S.A.", se sostuvo que *"el BBVA no cumplió acabadamente con la normativa a la que se hallaba obligado y que, de haberla cumplido, las transferencias cuestionadas en estos actuados no habrían tenido lugar."*[121] En estos supuestos, el incumplimiento de la normativa prudencial no sólo configura una infracción administrativa, sino que opera como un elemento central para acreditar la insuficiencia del sistema de seguridad y, en consecuencia, la responsabilidad de la entidad.

Por otro lado, el cumplimiento formal de estas disposiciones no resulta suficiente para tener por satisfecho el deber de seguridad. Una entidad que acredita haber observado las normas del BCRA no queda por ello automáticamente exonerada si el sistema implementado se revela ineficaz para prevenir el daño concreto sufrido por el consumidor. Esta posición ha sido sostenida de manera reiterada por distintos tribunales al afirmar que *"el deber de cuidado exigible a las instituciones bancarias es sensiblemente mayor al cumplimiento de las medidas de la autoridad de aplicación, debiendo adoptar no sólo las medidas de seguridad mínimas obligatorias sino las adecuadas y necesarias"*.[122] De este modo, aun cuando la entidad acredite haber observado

[120] STJ Río Negro, Sec. Civil N.º 1, "Bartorelli", cit. Nota 106, p. 4
[121] CNCom., Sala F, "Martínez", cit. nota 117, p. 19
[122] Cám. Apel. Civ. y Com. Necochea, "González", cit. nota 108; Cám. Civ., Com., Fam. y Min. Cipolletti, "Herrera", cit. nota 115; STJ Río Negro, Sec. Civil N.º 1, "Bartorelli", cit. Nota 106, p. 6

formalmente la normativa aplicable, ello no resulta suficiente si el sistema implementado se revela, en los hechos, ineficaz para prevenir el daño.

La regla que emerge de este conjunto de pronunciamientos puede formularse del siguiente modo: el cumplimiento de la normativa del BCRA es condición necesaria pero no suficiente para tener por satisfecho el deber de seguridad. Una entidad que incumple las normas del BCRA incumple también su obligación de seguridad. Pero una entidad que las cumple formalmente no queda por eso exonerada si el sistema implementado se revela ineficaz para prevenir el daño concreto sufrido por el consumidor. En definitiva, la normativa del BCRA delimita el umbral mínimo de actuación exigible, mientras que el régimen de responsabilidad orientado por el deber de seguridad define el estándar definitivo. La entidad financiera debe garantizar no sólo el cumplimiento formal de la regulación, sino la efectiva seguridad del sistema que introduce en el mercado, asumiendo las consecuencias cuando ese sistema falla frente a riesgos que le son propios.

5.3. Tratamiento jurisprudencial de las eximentes

5.3.1. La invocación del hecho de la víctima

La invocación del hecho o culpa de la víctima aparece reiteradamente como defensa por parte de las entidades bancarias en los casos analizados. En “Fernández Quintana c/ Banco Patagonia S.A.”, la entidad demandada sostuvo que *“cuando un cliente proporciona datos de índole absolutamente secreta y privada asume las consecuencias que se derivan de dicho acto, anulando absolutamente el accionar del banco para impedir operaciones que solo pueden efectuarse con claves que deben ser personales y secretas”*, concluyendo que *“el banco no puede tener responsabilidad alguna sobre la propia negligencia de los clientes”*.[123] En términos similares, en “González c/ Banco de la Provincia de Buenos Aires”, se argumentó que *“la clienta/cliente al brindar voluntariamente acceso a su cuenta a terceras personas, arbitró los medios para que se efectuaran las transacciones que reclama”* por lo que su comportamiento implicó *“un rechazo a las precauciones más elementales que estaban a su alcance”*, calificando su accionar como una *“temeridad activa”* con aptitud para interrumpir el nexo causal.[124]

En la misma línea, en “Fernández c/ Banco de la Provincia de Buenos Aires”, la demandada alegó que la actora *“reconoció haber suministrado sus credenciales a terceros desconocidos”* y que *“no existió falla ni negligencia en su accionar, toda vez que las operaciones fueron generadas desde el usuario habilitado de la actora, con sus claves correctas y token válido, enfatizando que el comportamiento negligente de la propia usuaria interrumpió el nexo causal que podría haber atribuido responsabilidad a la entidad financiera”*.[125] Asimismo, en “Herrera c/ Banco Patagonia

[123] Unidad Jurisd. Civil N.º 5, Bariloche, "Fernández Quintana", cit. nota 118, p. 4
[124] Cám. Apel. Civ. y Com. Necochea, "González", cit. nota 108, p. 9
[125] Juzg. Civ. y Com. N.º 23, La Plata, "Fernández", cit. nota 109, p. 3-4

S.A.", la entidad sostuvo que *"la maniobra fraudulenta solo pudo concretarse porque la coactora (…) proporcionó a terceros datos personales y confidenciales (…) lo que configuraría una ruptura total del nexo causal"*, invocando expresamente el art. 1729 del CCyCN.[126]

La invocación por parte de las entidades financieras del hecho de la víctima como eximente revela una estrategia procesal consistente en los casos analizados. A través de ella, las entidades financieras procuran desplazar el eje del análisis desde el sistema de seguridad que organizan hacia la conducta individual del usuario, presentando el daño como consecuencia de una decisión personal del consumidor y no como la materialización de un riesgo propio del servicio. Sin embargo, como se desarrolla en los apartados siguientes, la jurisprudencia ha respondido a esta estrategia con un criterio marcadamente restrictivo, que exige condiciones excepcionales para que la conducta del consumidor tenga aptitud suficiente para interrumpir el nexo causal.

5.3.2. La interpretación restrictiva de las eximentes

Frente a la reiterada invocación del hecho de la víctima como causal de exoneración, la jurisprudencia ha construido un criterio marcadamente restrictivo en su admisión, en línea con el régimen de responsabilidad objetiva y el deber de seguridad.

El punto de partida de este criterio es que la conducta del consumidor solo puede operar como eximente cuando configure una causa exclusiva del daño, circunstancia cuya acreditación pesa sobre la entidad financiera. En *"Herrera c/ Banco Patagonia S.A."*, la Cámara de Apelaciones de Cipolletti afirmó que *"la eventual conducta descuidada del usuario solo podría operar como eximente o atenuante cuando configure una causa exclusiva del daño, circunstancia cuya acreditación pesa sobre el proveedor del servicio conforme al régimen de responsabilidad establecido por el art. 40 de la Ley de Defensa del Consumidor"*.[127]

Para alcanzar ese umbral, la conducta del usuario debe reunir los caracteres propios de la causa ajena (exterioridad, imprevisibilidad e inevitabilidad). Sin embargo, la jurisprudencia es categórica en señalar que esos requisitos no se verifican en los supuestos típicos de fraude mediante ingeniería social. En el mismo fallo se señaló que, aun cuando el usuario haya sido inducido a revelar sus credenciales, dicha circunstancia *"no configura una causa exclusiva del daño (…) ni constituye un hecho extraño, imprevisible e inevitable capaz de eximir de responsabilidad a la entidad bancaria, en tanto este tipo de maniobras integra los riesgos propios del sistema de banca electrónica que las entidades financieras introducen y explotan profesionalmente en el mercado"*.[128]

[126] Cám. Civ., Com., Fam. y Min. Cipolletti, "Herrera", cit. nota 115, p. 4
[127] Ibídem, p. 9
[128] Ibídem, p. 16

La importancia de este razonamiento radica en que redefine el análisis causal. La entrega de credenciales por parte del usuario no es considerada la causa del daño, sino una condición dentro de una secuencia más amplia dominada por la insuficiencia del sistema de seguridad. En esta línea, en *"Fernández c/ Banco de la Provincia de Buenos Aires"* se afirmó que *"la facilitación de los datos fue condición del hecho dañoso, pero no la causa"* precisando que la causa radica en *"la falta de seguridad en el sistema informático que el Banco de la Provincia de Buenos Aires puso a disposición de la actora"* y por lo tanto, la eximente invocada *"no reúne los requisitos para eximirlo de responsabilidad en cuanto no se trata de un hecho exterior ajeno a la actividad, a sus riesgos intrínsecos y especialmente a la obligación de seguridad en cabeza del demandado"*.[129]

En igual sentido, en *"González c/ Banco de la Provincia de Buenos Aires",* se sostuvo que la conducta atribuida a la actora *"no reúne los requisitos para eximir de responsabilidad, en tanto no se trata de un hecho exterior ajeno a los riesgos intrínsecos de la actividad; tampoco imprevisible (…) ni inevitable"*, destacándose además que las maniobras de ingeniería social *"forman parte de los riesgos asegurables"* del sistema.[130]

Este criterio también se refleja en *"Martínez c/ Banco BBVA Argentina S.A.",* donde se afirmó que *"aún cuando, por vía de hipótesis, se considere que un tercero haya podido obtener los datos de acceso a la cuenta por alguna acción atribuible a la negligencia de la parte actora, las defensas del Banco no resultan suficientes para eximirla de responsabilidad"*, agregando que *"aún en caso de un obrar negligente del consumidor no había ruptura del nexo causal si hubo un incumplimiento previo del proveedor"*.[131]

En el mismo sentido, el fallo del fuero local de la CABA en *"C.S. c/ Banco Itaú Argentina S.A."* señaló con claridad que *"el acceso a los datos de la cuenta bancaria por parte de terceros no rompe el nexo causal, en virtud de que el banco tiene en su cabeza un deber de seguridad que opera como una obligación de resultado, debiendo diseñar sistemas operativos aptos para detectar movimientos extraños, que no se condigan con el perfil transaccional del cliente"*.[132] El pronunciamiento agrega una consideración que potencia la restricción de la eximente: el banco conocía, o debía conocer, que su cliente era una persona mayor con escasos conocimientos digitales, lo que intensificaba su deber de detectar operaciones sospechosas. Esa circunstancia no solo refuerza la responsabilidad del banco desde el punto de vista del deber de seguridad, sino que también incide en el juicio sobre la conducta del usuario, dado que no puede exigirse a un adulto mayor sin habilidades digitales el mismo nivel de precaución que a un usuario con pleno dominio de las herramientas tecnológicas. La hipervulnerabilidad del consumidor, en este

[129] Juzg. Civ. y Com. N.º 23, La Plata, "Fernández", cit. nota 109, p. 10
[130] Cám. Apel. Civ. y Com. Necochea, "González", cit. nota 108, p. 25
[131] CNCom., Sala F, "Martínez", cit. nota 117, p. 18
[132] Juzg. 1ª Inst. Cont. Adm., Trib. y Rel. Consumo N.º 27, CABA, "C.S., J.V.", cit. nota 107, p. 17

marco, opera como un factor que torna aún menos admisible la invocación del hecho de la víctima como eximente.

5.3.3. El fallo Herrera: de la concausalidad a la responsabilidad íntegra del banco

El análisis del caso *"Herrera c/ Banco Patagonia S.A."* merece un tratamiento especial, en tanto constituye un ejemplo paradigmático de la tensión que puede darse en la resolución judicial de estos conflictos entre dos formas de abordar la atribución de responsabilidad en los fraudes electrónicos, una centrada en la conducta del usuario y otra enfocada en el sistema y el deber de seguridad. Su valor no reside únicamente en el resultado alcanzado, sino también en el modo en que permite observar, a través de dos instancias con criterios opuestos, el desplazamiento desde un modelo de concausalidad hacia otro centrado en la organización del servicio y en los riesgos que le son propios.

En primera instancia, el juez de grado adoptó un modelo de concausalidad, en donde le atribuyó responsabilidad en un cincuenta por ciento (50%) a la conducta de la usuaria que había proporcionado sus credenciales, y el restante cincuenta por ciento (50%) al banco, por no haber activado mecanismos de control frente a una operatoria inusual. El razonamiento del magistrado partía de que las operaciones habían sido realizadas mediante el uso correcto de usuario, clave y *token*, sin registrarse fallas técnicas en el sistema, lo que evidenciaba la intervención de la actora en la producción del daño.

En ese marco, el juez concluyó que existió una conducta de la actora *"con entidad suficiente para constituir una ruptura del nexo causal en los términos del art. 1729 del CCC"*, destacando que el acceso de terceros *"no hubiera sido posible sin la proporción de los datos efectuados a terceros por la Sra. Quintana, quien no obró con un mínimo de cuidado y previsión"*.[133] Sin embargo, simultáneamente reconoció que la entidad bancaria no había desplegado mecanismos adecuados de control, señalando que, frente a una secuencia de operaciones atípicas (modificación de datos, activación de *token* y transferencias de magnitud en pocos minutos), ello *"no implicó señal de alarma alguna en los sistemas del Banco"*. Sobre esa base, entendió configurada una concausalidad, afirmando que *"se configura entonces en el caso de autos una concausalidad en la que la conducta del banco demandado por una parte y la de la actora (víctima) por la otra, confluyen en la producción del daño sufrido por las accionantes"*, lo que lo llevó a distribuir la responsabilidad en partes iguales.

Sin embargo, la Cámara revocó este criterio y, aplicando la doctrina del Superior Tribunal de Justicia de Rio Negro en *"Bartorelli c/ Banco Patagonia S.A."*, estableció la responsabilidad íntegra a la entidad financiera. El fundamento central de la decisión radica en que el uso de credenciales válidas no excluye responsabilidad cuando el sistema no cuenta con mecanismos

[133] Cám. Civ., Com., Fam. y Min. Cipolletti, "Herrera", cit. nota 115, p. 3

adecuados de prevención. El tribunal destacó que *"el análisis de responsabilidad no puede limitarse a constatar que las operaciones fueron realizadas mediante credenciales válidas ni que el sistema no haya sido vulnerado en sentido técnico"*, sino que debe verificarse si el banco contaba con mecanismos razonables de detección y reacción frente a una secuencia de operaciones atípicas.[134]

Asimismo, el tribunal enfatizó que la conducta de la usuaria al revelar sus credenciales bajo engaño no configuraba una causa exclusiva del daño en los términos del artículo 40 de la LDC, y que *"no puede trasladarse al consumidor el riesgo propio del sistema que el propio proveedor ha puesto en funcionamiento, ni imputarse al usuario la responsabilidad por maniobras delictivas que resultan previsibles dentro del entorno digital en el que se desarrollan las operaciones bancarias actuales*"[135], ya que corresponde evaluar si el sistema contaba con mecanismos para advertir o neutralizar la operatoria irregular. En consecuencia, concluye que *"la responsabilidad por los daños derivados de la operatoria fraudulenta analizada debe ser atribuida íntegramente a la entidad bancaria demandada, en tanto no acreditó haber cumplido adecuadamente con las obligaciones de seguridad que le impone la normativa aplicable"*.[136]

La relevancia de este caso radica en que permite observar con claridad el cambio de enfoque entre ambas instancias. La sentencia de primera instancia no desconoce el deber de seguridad bancario, pero lo pondera junto con la conducta del usuario mediante la concausalidad. La Cámara, en cambio, rechaza ese encuadre porque considera que, en el marco del art. 40 de la LDC, la concausalidad no constituye la respuesta adecuada, dado que la conducta del usuario solo puede operar como eximente cuando configura la causa exclusiva del daño, no cuando concurre con una omisión del proveedor. De este modo, el fallo de la Cámara consolidó un criterio claro: la intervención del consumidor, aun cuando implique la entrega de credenciales, no tiene aptitud suficiente para interrumpir el nexo causal si el sistema de seguridad resulta deficiente. Solo en supuestos excepcionales, en los que la conducta del usuario pueda calificarse como causa exclusiva del daño, la eximente puede prosperar.

En definitiva, la jurisprudencia dominante restringe el alcance del hecho de la víctima y reafirma que, en el ámbito de la banca digital, la imputación de responsabilidad se estructura prioritariamente en torno al deber de seguridad y a los riesgos propios del sistema, desplazando la relevancia de la conducta del consumidor a un plano estrictamente excepcional.

5.3.4. Supuestos excepcionales de admisión de la eximente

Si bien el criterio dominante en la jurisprudencia es claramente restrictivo respecto de la admisión del hecho de la víctima como causal de exoneración, existen precedentes en los que dicha

[134] Cám. Civ., Com., Fam. y Min. Cipolletti, "Herrera", cit. nota 115, p. 8
[135] Ibídem, p. 17
[136] Ídem.

eximente ha sido admitida. Estos casos no contradicen la regla general, sino que permiten delimitar con mayor precisión su alcance y los requisitos exigidos para su procedencia. En estos supuestos, la responsabilidad bancaria es descartada cuando la conducta del usuario reviste un grado de gravedad tal que permite considerarla como causa exclusiva del daño, desplazando completamente la incidencia del sistema y del deber de seguridad.

En *"Pesce c/ Banco Patagonia S.A.",* la Cámara rechazó íntegramente la demanda. El tribunal reconoció la aplicabilidad del factor objetivo y que la entidad solo podría eximirse acreditando el hecho de la víctima como causa ajena, pero consideró ese estándar cumplido en este caso. El actor había concurrido personalmente al cajero, blanqueado sus claves y entregado el *token*, lo que llevó al tribunal a concluir que *"nada pudo haber hecho el Banco"* para evitar el daño. Lo que diferencia a este caso del supuesto general no es la mera entrega de credenciales, sino la configuración de una conducta del consumidor calificada como *"gravemente negligente"* que constituyó, en el contexto específico, la causa exclusiva y eficiente del daño sin que existiera falla concurrente del sistema bancario. En palabras del magistrado: *"el propio relato de los hechos efectuado por el actor, denota un actuar gravemente negligente por parte de este último que, a mi entender, exime al Banco de responsabilidad"*.[137] En este precedente, la admisión de la eximente se apoya en una caracterización particularmente intensa de la conducta del usuario, que excede la mera imprudencia y es calificada como una negligencia grave o temeraria, con aptitud suficiente para interrumpir el nexo causal incluso dentro de un régimen de responsabilidad objetiva.

De manera similar, en *"Yacuzzi c/ Banco de la Nación Argentina",* se descartó la responsabilidad de la entidad financiera al verificarse que las operaciones cuestionadas fueron realizadas por el propio usuario mediante el uso de su tarjeta de débito y clave personal, es decir, a través de los mecanismos habituales de autenticación del sistema, sin que se registraran irregularidades o anomalías que permitieran al banco advertir la existencia de una operatoria fraudulenta . El tribunal destacó que *"el modo en que se efectuaron las operatorias cuestionadas no exigió de parte del Banco un accionar diferente, por haberse efectuado dentro de la normal operatoria que puede desplegar cualquier cliente o usuario del servicio"*.[138] La diferencia con los casos de phishing es que no se trata de una maniobra de ingeniería social que aprovecha una brecha del sistema, sino de operaciones ejecutadas directamente por el titular mediante los factores de autenticación personalísimos dentro de la operatoria normal del servicio. En ese escenario, el sistema bancario funcionó exactamente como estaba diseñado para funcionar, y no es posible identificar omisión alguna del banco que hubiera podido prevenir el daño.

[137] CNCom., Sala D, "Pesce", cit. nota 110, p. 6
[138] Cámara Federal de Apelaciones de Corrientes, "Yacuzzi, José Luis c/ Banco de la Nación Argentina s/ Ley de Defensa del Consumidor", 15/11/2024, p. 4

En estos supuestos, a diferencia de lo que ocurre en la línea jurisprudencial dominante, el análisis no pone el acento en la insuficiencia del sistema, sino en la conducta del usuario como factor determinante y excluyente del daño. La eximente se admite cuando el comportamiento del consumidor rompe completamente el nexo causal, ya sea por su carácter groseramente negligente o por desarrollarse en un contexto en el que el sistema no presentaba fallas ni generaba señales de alerta que exigieran la intervención del banco.

En esta línea, resulta ilustrativo el antecedente *"Juárez c/ Banco de la Provincia de Buenos Aires"* en el cual en el marco de un proceso cautelar, se revocó una medida favorable a la actora, poniendo énfasis en que *"la propia accionante ha reconocido de modo expreso haber suministrado su nombre de usuario y clave de token a los presuntos autores de la estafa electrónica"*[139], lo que debilitaba la verosimilitud del derecho invocado. Sin embargo, este precedente presenta una particularidad relevante desde el punto de vista evolutivo. En su voto en disidencia, la Dra. Scaraffía sostuvo que, aun frente a una conducta reprochable del usuario, *"resultaría a priori esperable la adopción de un estándar más elevado de seguridad por parte del Banco demandado para este tipo de transacciones en consonancia con la responsabilidad por riesgo"*, destacando además que no se encontraba acreditado que la entidad hubiese *"adoptado en el caso concreto acciones o medidas adicionales tendientes a neutralizar este tipo de maniobra delictiva"*[140]. El valor de este voto disidente radica en que anticipa el criterio que la jurisprudencia posterior consolidaría como dominante: la centralidad del deber de seguridad y la insuficiencia de la conducta del consumidor como factor exoneratorio cuando el sistema no resulta adecuado para prevenir riesgos previsibles. En este sentido, *"Juárez c/ Banco de la Provincia de Buenos Aires"* permite observar, en un mismo pronunciamiento, la coexistencia de ambos enfoques y el desplazamiento progresivo hacia un modelo centrado en el sistema y en la asignación de riesgos al proveedor.

En definitiva, del análisis conjunto de estos precedentes se desprende que la admisión del hecho de la víctima como eximente requiere la concurrencia de condiciones particularmente estrictas. Por un lado, una conducta del usuario que exceda la mera imprudencia y alcance niveles de negligencia grave o temeraria, revelando un apartamiento de las precauciones más elementales. Por otro, la inexistencia de deficiencias en el sistema de seguridad que hubieran permitido prevenir o al menos detectar la operatoria fraudulenta. En ausencia de alguno de estos elementos, la jurisprudencia tiende a rechazar la eximente, en tanto considera que la conducta del usuario se inserta dentro de los riesgos propios del sistema de banca digital y no constituye una causa ajena en sentido técnico.

[139] Cámara de Apelaciones en lo Civil y Comercial de Pergamino, "Juárez, Andrea Natalia c/ Banco de la Provincia de Buenos Aires s/ Medidas Cautelares (Traba/Levantamiento)", 06/04/2021, p. 3
[140] Ibídem, p. 5

V. Conclusión

El presente trabajo se propuso analizar el alcance de la responsabilidad de las entidades financieras frente a fraudes electrónicos en el marco de las relaciones de consumo, interrogándose específicamente acerca de si corresponde atribuirles responsabilidad por los daños derivados de operaciones no consentidas y en qué medida pueden eximirse de ella. La hipótesis planteada sostuvo que, en el contexto de la banca digital, las entidades financieras deben responder en forma objetiva por tales daños, en virtud del deber de seguridad y del riesgo propio de la actividad, pudiendo liberarse únicamente mediante la acreditación de una causa ajena con los caracteres de imprevisibilidad, inevitabilidad y exterioridad.

A partir del desarrollo de los distintos capítulos, puede afirmarse que dicha hipótesis ha sido confirmada. En primer lugar, el análisis del derecho del consumidor permitió establecer que la relación entre el banco y el usuario de servicios financieros se inscribe dentro de una relación de consumo. Esta calificación no resulta meramente formal, sino que implica la aplicación de un régimen jurídico de carácter tuitivo, que reconoce la vulnerabilidad estructural del consumidor bancario, especialmente intensificada en entornos digitales. La asimetría técnica, informativa y organizacional que caracteriza a esta relación constituye el punto de partida para la asignación de responsabilidades en caso de daño.

En segundo término, el examen del proceso de digitalización del sistema financiero evidenció que la operatoria bancaria actual se desarrolla en un entorno tecnológicamente complejo y altamente automatizado, en el cual los riesgos de fraude electrónico no solo se incrementan, sino que adquieren características propias. Las maniobras de ingeniería social, la suplantación de identidad y el uso indebido de credenciales no pueden ser consideradas hechos excepcionales, sino contingencias previsibles dentro del funcionamiento del sistema. Esta constatación resulta central, en tanto desplaza el análisis desde la conducta individual del usuario hacia la estructura del servicio y los riesgos que ésta genera.

Sobre esta base, el estudio del marco regulatorio del BCRA permitió identificar la existencia de un conjunto de estándares técnicos y organizativos orientados a la prevención del fraude y a la protección de los usuarios. Estas normas configuran un sistema preventivo que impone a las entidades financieras la obligación de gestionar activamente los riesgos tecnológicos. Sin embargo, también se demostró que tales disposiciones operan como un piso mínimo de conducta, cuyo cumplimiento no agota el contenido del deber de seguridad ni resulta suficiente, por sí solo, para excluir la responsabilidad en caso de daño.

El núcleo del trabajo se desarrolló en torno al régimen de responsabilidad civil aplicable. En este punto, el análisis doctrinario y normativo permitió concluir que la responsabilidad de las entidades financieras frente a fraudes electrónicos en relaciones de consumo se estructura sobre un factor

de atribución objetivo, sustentado en una doble base: por un lado, la lógica del régimen consumeril que desplaza la exigencia de culpa y centra el análisis en el incumplimiento del deber de seguridad y, por otro, la configuración de la actividad bancaria digital como una actividad riesgosa en los términos del CCyCN. En este contexto, la responsabilidad no depende de la acreditación de una conducta negligente del banco, sino de la verificación del daño y su vinculación con el sistema organizado por la entidad.

En este esquema, el deber de seguridad emerge como el eje estructural de la imputación. Su fundamento constitucional, legal y doctrinario, así como su proyección en el ámbito de la actividad bancaria, permiten afirmar que las entidades financieras no solo deben abstenerse de causar daño, sino que están obligadas a garantizar que los servicios que prestan no generen riesgos indebidos para los usuarios. En entornos digitales, este deber adquiere una intensidad reforzada, en tanto la seguridad del sistema depende casi exclusivamente del proveedor. En consecuencia, la producción de un fraude electrónico se presenta como la manifestación de un incumplimiento del deber de seguridad cuando el sistema resulta insuficiente para prevenirlo.

Por su parte, el análisis de las causales de exoneración permitió advertir que, en el marco de un régimen objetivo, su admisión debe ser de carácter excepcional. Ni la conducta del consumidor ni la intervención de terceros poseen, en principio, aptitud suficiente para interrumpir el nexo causal, salvo que configuren una causa exclusiva del daño con los caracteres propios de la causa ajena. Esta interpretación restrictiva se justifica en la necesidad de no trasladar al usuario los riesgos propios del sistema que el proveedor organiza y controla.

Asimismo, el estudio jurisprudencial corroboró empíricamente estas conclusiones. Los tribunales han consolidado una línea interpretativa que adopta el factor de atribución objetivo, reconoce al deber de seguridad como criterio central de imputación y analiza los fraudes electrónicos como manifestaciones de riesgos inherentes al sistema de banca digital. En este marco, el foco del razonamiento judicial se desplaza desde la conducta del usuario hacia la evaluación de la idoneidad del sistema implementado por la entidad financiera. Asimismo, la jurisprudencia ha delimitado con claridad el carácter de piso mínimo de la normativa del BCRA y ha restringido la admisión de las eximentes a supuestos verdaderamente excepcionales.

En definitiva, la responsabilidad de las entidades financieras frente a fraudes electrónicos no puede ser comprendida desde esquemas tradicionales centrados en la culpa individual, sino que debe ser abordada desde una lógica sistémica, que atienda a la organización del servicio, a los riesgos que éste genera y a la posición del consumidor dentro de esa estructura. La consolidación de un modelo de responsabilidad objetiva, articulado en torno al deber de seguridad, constituye una respuesta jurídicamente adecuada a los desafíos planteados por la digitalización del sistema financiero y una condición necesaria para garantizar una tutela efectiva del consumidor en el entorno digital.

VI. Bibliografía

A. Doctrina

ABAD, Gabriela A., “Análisis de la responsabilidad bancaria en casos de estafas electrónicas mediante redes sociales desde la óptica del derecho de consumo”, elDial.com, 07/05/2021, cita online: elDial.com - DC2DE4. Disponible en: https://www.abogadovergara.com.ar/2021/05/analisis-de-la-responsabilidad-bancaria.html [consulta: 12/10/2025].

ALBORNOZ, Elena y GUILISASTI, Jorgelina; "Derechos de los grupos vulnerables: los consumidores de servicios financieros", ponencia presentada en la Comisión N° 8 "Protección del consumidor de servicios financieros y bursátiles" de las XXV Jornadas Nacionales de Derecho Civil, Bahía Blanca, 2015, Recuperado el 15-10-2025 de https://jndcbahiablanca2015.com/wp-content/uploads/2015/09/ALBORNOZ-y-otro_DERECHOS.pdf [consulta: 15/10/2025].

ÁLVAREZ LARRONDO, Fernando M., “La lógica de la sociedad de consumo”, en Fernando M. Álvarez Larrondo (ed.), *Manual de derecho del consumo,* Buenos Aires: Erreius, 2017, pp. 3-11

ÁLVAREZ LARRONDO, Fernando M., “Elementos de la relación de consumo. El concepto de consumidor”, en Fernando M. Álvarez Larrondo (ed.), *Manual de derecho del consumo,* Buenos Aires: Erreius, 2017, pp. 63-98

ÁLVAREZ LARRONDO, Fernando M. y RODRÍGUEZ, Gonzalo M., “Derechos de los consumidores en las relaciones con las entidades bancarias”, en Carlos Ghersi, Celia Weingarten y Graciela Lovece (dirs.), *Derechos de los Consumidores y Empresas en las Relaciones con las Entidades Bancarias*, Buenos Aires: Erreius, 2020, pp. 3-46.

ARIAS, María P. y MÜLER, Germán E. "La obligación de seguridad en las operaciones financieras con consumidores en la era digital. Con especial referencia a la problemática del phishing y del vishing", SJA 14/07/2021, Cita: TR LALEY AR/DOC/1657/2021. Disponible en: https://www.colabro.org.ar/resources/original/biblioteca%20virtual//LA%20OBLIGACION%20DE%20SEGURIDAD%20EN%20LAS%20OPERACIONES%20FINANCIERAS%20EN%20EL%20ENTORNO%20DIGITAL.pdf [consulta: 11/10/2025].

BAROCELLI, Sergio S.; "El concepto de consumidor de servicios financieros y bursátiles y el rol del Estado", ponencia presentada en la Comisión N° 8 "Protección del consumidor de servicios financieros y bursátiles" de las XXV Jornadas Nacionales de Derecho Civil,

Bahía Blanca, 2015. Disponible en: https://jndcbahiablanca2015.com/wp-content/uploads/2015/09/Barocelli_EL-CONCEPTO.pdf [consulta: 11/10/2025].

BAROCELLI, Sergio S., "Los principios del derecho del consumidor como orientadores de la interpretación y aplicación en el diálogo de fuentes", en S. S. Barocelli (coord.), *Impactos del nuevo Código Civil y Comercial en el Derecho del Consumidor. Diálogos y perspectivas a la luz de sus principios*., 1ra. Edición, Instituto de Investigaciones Jurídicas y Sociales Ambrosio L. Gioja, Facultad de Derecho, Universidad de Buenos Aires, Buenos Aires, 2016, pp. 8-37

BARRIO ANDRÉS, Moisés, "La revolución FinTech. Definición, factores desencadenantes, oportunidades y riesgos", en Matilde Cuena Casas y Javier Ibáñez Jiménez (dirs), *Perspectiva legal y económica del fenómeno FinTech*, Madrid: La Ley, 2021, pp. 41-71.

BELTRAMO, Andrés N. y FALIERO, Johanna C., "El consumidor electrónico como consumidor hipervulnerable", en Sergio S. Barocelli (dir.), *Consumidores hipervulnerables*, El Derecho, 2018, pp. 346-382.

BERICUA, Marina, PALAZZI, Pablo A. y MORA, Santiago J., "Breve introducción al Derecho Fintech", en S. Mora y P. Palazzi (comps.), *Fintech: Aspectos legales*, Tomo I, 1.ª ed., Buenos Aires: Pablo Andrés Palazzi, 2019, pp. 23-34.

BERNAL-LUNA, Claudia P., VITERI-RADE, Layla Y. y MALDONADO-DE LA CRUZ, Walter J., "La tendencia global de la banca digital como agente de ruptura del mundo monetario", en 593 Digital Publisher CEIT, N.º 7(3), 2022, pp. 212-229.

CALVO COSTA, Carlos A., *Derecho de las obligaciones. Tomo 2: Derecho de daños*, 2.ª ed., Buenos Aires: Hammurabi, 2016.

CAMPOS, Pablo A., "La ley de defensa del consumidor y sus implicancias actuales", en *Revista Perspectivas de las Ciencias Económicas y Jurídicas*, Vol. 1 N.º 1, Santa Rosa: EdUNLPam, 2011, pp. 99-116. Disponible en: https://doi.org/10.19137/perspectivas-2011-v1n1a04 [consulta: 20/10/2025].

CHAMATROPULOS, Demetrio A., "El deber de seguridad de los bancos y los daños derivados de la utilización de cajeros automáticos", en *Revista de Responsabilidad Civil y Seguros*, N.º 12 Vol., 2010, pp. 95-103.

DAUVERNÉ, Julián S. y LO GIUDICE, Diego A., "La problemática del phishing en contratos de consumo de servicios financieros por plataformas electrónicas",LA LEY 12/02/2025, Cita Online AR/DOC/239/2025.

DE NÚÑEZ, Rodrigo, “La responsabilidad objetiva en la actividad bancaria”, SJA, 27/06/2018, Thomson Reuters, cita online: AR/DOC/3012/2018.

FARINA, Juan M., *Contratos comerciales modernos: Modalidades de contratación empresaria*, 2.ª ed., 1.ª reimp., Buenos Aires: Astrea, 1999, p. 248.

FERRER DE FERNÁNDEZ, Esther H. S., “El consumidor bancario en el Código Civil y Comercial de la Nación. Primera parte”, en *Revista de Derecho Comercial y de las Obligaciones*, Thomson Reuters, Cita Online AP/DOC/77/2015. Disponible en: https://www.derecho.uba.ar/institucional/pacem/pdf/ferrer-de-fernandez-el-consumidor-bancario-parte-1.pdf [consulta: 20/10/2025]

GARRIDO CORDOBERA, María R., “La obligación de seguridad y el derecho del consumidor”, en Fernando M. Álvarez Larrondo (ed.), *Manual de derecho del consumo*, Buenos Aires: Erreius, 2017, pp. 265-284.

GHERSI, Carlos, “Obligación de seguridad. Alcance temporal y espacial de la responsabilidad”, en Carlos Ghersi, Celia Weingarten y Graciela Lovece (dirs.), *Derechos de los Consumidores y Empresas en las Relaciones con las Entidades Bancarias*, Buenos Aires: Erreius, 2020, pp. 3-46.

HERRERA, Sabrina, “Información contractual continua. El CCyCN y su articulación con la Ley de Defensa del Consumidor”, en Carlos Ghersi, Celia Weingarten y Graciela Lovece (dirs.), *Derechos de los Consumidores y Empresas en las Relaciones con las Entidades Bancarias*, Buenos Aires: Erreius, 2020, pp. 99-118.

LEIVA, Claudio F., VALDEZ LÓPEZ, Claudio y FURLOTTI, Silvina, “Responsabilidad de las plataformas electrónicas”, en Javier Yaquemet y Carlos E. Tambussi (coords.), *Derecho de los usuarios y consumidores*, Buenos Aires: Abeledo Perrot, 2025, pp. 5-17.

MARTÍNEZ, Matilde S., “Algunas cuestiones sobre delitos informáticos en el ámbito financiero y económico. Implicancias y consecuencias en materia penal y responsabilidad civil”, en Ricardo A. Parada y Juan D. Errecaborde (comps.), *Cibercrimen y delitos informáticos: Los nuevos tipos penales en la era de internet*, Ciudad Autónoma de Buenos Aires: Erreius, 2018, pp. 33-48.

MENDIETA, Ezequiel N., “La obligación de seguridad y el trato digno en el marco de las relaciones de consumo bancarias en el entorno digital. A propósito de la emergencia sanitaria, las sanciones dictadas por la Dirección Nacional de Defensa del Consumidor y la protección de los consumidores hipervulnerables”, RCCyC 2021 (septiembre), 13/09/2021, 10, cita online: TR LALEY AR/DOC/2292/2021.

MORA, Santiago J., “Documento electrónico y firma digital. Evolución en el Derecho argentino”, en Santiago Mora y Pablo Palazzi (comps.), *Fintech: Aspectos legales*, Tomo I, 1.ª ed., Buenos Aires: Pablo Andrés Palazzi, 2019, pp. 121-176.

PÉREZ, Lucía Camila, "El deber de seguridad de los bancos frente al consumidor financiero", Abogados.com.ar, 22/02/2024, disponible en https://abogados.com.ar/el-deber-de-seguridad-de-los-bancos-frente-al-consumidor-financiero/34305 (fecha de consulta: 17/07/2026).

PICASSO, Sebastián y SÁENZ, Luis R., “Título V. Otras fuentes de las obligaciones. Capítulo I. Responsabilidad Civil”, en Marisa Herrera, Gustavo Caramelo y Sebastián Picasso (dirs.), *Código Civil y Comercial de la Nación comentado*, Tomo IV, Buenos Aires: Infojus, 2015, pp. 414-523.

PIZARRO, Ramón D., “Responsabilidad por productos y por servicios en la Ley de Defensa del Consumidor”, en Gabriel A. Stiglitz y Carlos A. Hernández (dirs.), T*ratado de derecho del consumidor,* Tomo III, Buenos Aires: La Ley, 2015, pp. 195-219

RODRÍGUEZ, Gonzalo M., “Responsabilidad por daños en el ámbito del consumo”, en Fernando M. Álvarez Larrondo (ed.), *Manual de derecho del consumo*, Buenos Aires: Erreius, 2017, pp. 661-724.

RUIZ DÍAZ, Estefanía L., “Publicidad bancaria. Normativas específicas. BCRA y CCyCN”, en Carlos Ghersi, Celia Weingarten y Graciela Lovece (dirs.), *Derechos de los Consumidores y Empresas en las Relaciones con las Entidades Bancarias*, Buenos Aires: Erreius, 2020, pp. 3-46.

STIGLITZ, Gabriel A., “El deber de seguridad en el derecho del consumidor”, en Gabriel A. Stiglitz y Carlos A. Hernández (dirs.), *Tratado de derecho del consumidor*, Tomo III, Buenos Aires: La Ley, 2015, pp. 39-44.

STIGLITZ, Gabriel A., “Restricciones a la exoneración por causa ajena. Culpa del consumidor. Hiposuficientes. Autorización administrativa”, en Gabriel A. Stiglitz y Carlos A. Hernández (dirs.), *Tratado de derecho del consumidor*, Tomo III, Buenos Aires: La Ley, 2015, pp. 39-44.

STIGLITZ, Rubén S., “Título III. Contratos de consumo”, en M. Herrera, G. Carmelo y S. Picasso (dirs), *Código civil y comercial de la Nación comentado*, Tomo III, 1ra. ed, Buenos Aires: Infojus, 2015, pp. 492-292

TSCHIEDER, Vanina G., “*La contratación bancaria en el nuevo Código Civil y Comercial de la Nación*”, en *Revista de la Facultad de Ciencias Jurídicas y Sociales. Nueva Época,* N.º

10, 2017, pp. 148-161.Disponible en: https://doi.org/10.14409/ne.v0i10.6239 [consulta 15/11/2025]

UBIRÍA, Fernando A. *Derecho de daños en el Código Civil y Comercial*, Buenos Aires: Abeledo Perrot, 2015.

ZENTNER, Diego, "Régimen general del contrato de los contratos y las relaciones de consumo", en Carlos A. Ghersi y Celia Weingarten (dirs.), *Manual de contratos civiles, comerciales y de consumo,* 4.ª ed., Buenos Aires: La Ley, 2017, pp. 547-567.

TAMBUSSI, Carlos E. "El principio de orden público y el régimen tuitivo consumidor en el derecho argentino." *Lex-Revista de la Facultad de Derecho y Ciencias Políticas*, 2016, vol. 14, no 18., pp. 65-81. Disponible en: http://dx.doi.org/10.21503/lex.v14i18.1236 [consulta: 25/10/2025].

B. Jurisprudencia

Cámara Civil, Comercial, de Familia y Minería de la IV Circunscripción Judicial, Cipolletti, Provincia de Río Negro, *"Herrera, Marta Florencia y Otros c/ Banco Patagonia S.A. s/ Daños y Perjuicios"*, 30/03/2026. Disponible en: https://documento.errepar.com/jurisprudencia/20260410094130126 [consulta: 10/04/2026].

Cámara de Apelación en lo Civil y Comercial de Necochea, *"González, Verónica Graciela c/ Banco de la Provincia de Buenos Aires y Otro/a s/ Nulidad de Contrato",* 09/08/2022. Disponible en: https://aldiaargentina.microjuris.com/2023/01/30/fallos-phishing-se-condena-a-una-entidad-bancaria-a-indemnizar-a-su-cliente-por-el-deficiente-cumplimiento-de-su-obligacion-de-seguridad-a-fin-de-impedir-la-estafa-del-que-fue-victima/ [consulta: 13/01/2026]

Cámara de Apelaciones en lo Civil y Comercial de Pergamino, *"Juárez, Andrea Natalia c/ Banco de la Provincia de Buenos Aires s/ Medidas Cautelares (Traba/Levantamiento)",* 06/04/2021. Publicado en: La Ley Online, Cita: TR LALEY AR/JUR/8242/2021.

Cámara Federal de Apelaciones de Corrientes*, "Yacuzzi, José Luis c/ Banco de la Nación Argentina s/ Ley de Defensa del Consumidor"*, 15/11/2024. Disponible en: https://aldiaargentina.microjuris.com [consulta: 09/03/2026]

Cámara Nacional de Apelaciones en lo Comercial, Sala D, *"Pesce, Julián c/ Banco Patagonia S.A. s/ Ordinario"*, 18/02/2025. Publicado en: La Ley Online, Cita: TR LALEY AR/JUR/8777/2025. Disponible también en: https://www.eldial.com/nuevo/nuevo_diseno/v2/fallo4.asp?id=63133&base=14&h=u [consulta: 10/03/2026].

Cámara Nacional de Apelaciones en lo Comercial, Sala F, *"Martínez, César Roberto y Otro c/ Banco BBVA Argentina S.A. s/ Sumarísimo"*, 28/03/2025. Disponible en: https://www.saij.gob.ar/FA25130015 [consulta: 13/03/2026].

Juzgado Civil y Comercial N.º 23, Departamento Judicial La Plata, Provincia de Buenos Aires, *"Fernández, Liliana Ester c/ Banco de la Provincia de Buenos Aires s/ Daños y Perjuicios. Incumplimiento Contractual (Exc. Estado)"*, 13/10/2025. Disponible en: https://observatorioucu.com.ar/buscador/detalle/2558 [consulta: 20/01/2026].

Juzgado de Primera Instancia en lo Contencioso Administrativo, Tributario y de Relaciones de Consumo N.º 27, Secretaría Única, Ciudad Autónoma de Buenos Aires, *"C.S., J.V. c/ Banco Itaú Argentina S.A. s/ Contratos y Daños - RC - Bancos, Productos y Servicios Financieros"*, 2024. Disponible en: https://aldiaargentina.microjuris.com/wp-content/uploads/2024/11/C.-S.-J.pdf [consulta: 13/02/2026].

Superior Tribunal de Justicia de la Provincia de Río Negro, Secretaría Civil N.º 1, *"Bartorelli, Emma Graciela c/ Banco Patagonia S.A. s/ Daños y Perjuicios (Sumarísimo) - Casación",* 17/10/2023. Disponible en: https://fallos.jusrionegro.gov.ar/protocoloweb/protocolo/protocolo?id_protocolo=2e99f808-1ace-4b59-a868-4c06954681ec&stj=1 [consulta: 11/02/2026].

Unidad Jurisdiccional Civil N.º 5, San Carlos de Bariloche, *"Fernández Quintana, Patricia del V. c/ Banco Patagonia S.A. s/ Ordinario - Daños y Perjuicios",* 21/11/2024. Disponible en: https://fallos.jusrionegro.gov.ar/protocoloweb/protocolo/protocolo?id_protocolo=539a59c0-c965-48b7-b948-832e65d08369&usarSearch=1&option_text=0 [consulta: 21/01/2026].

Legislación

Constitución de la Nación Argentina, sancionada en 1853, con las reformas de 1860, 1866, 1898, 1957 y 1994.

Código Civil y Comercial de la Nación, Ley 26.994, sancionada el 1 de octubre de 2014, promulgada el 7 de octubre de 2014. B.O. 08/10/2014.

Ley de Defensa del Consumidor, Ley 24.240, sancionada el 22 de septiembre de 1993, promulgada parcialmente el 13 de octubre de 1993. B.O. 15/10/1993, con sus modificatorias (Leyes 24.568, 24.787, 24.999, 26.361 y 27.701).

Ley de Entidades Financieras, Ley 21.526, sancionada el 14 de febrero de 1977, promulgada el 14 de febrero de 1977. B.O. 21/02/1977, y sus modificatorias.

Carta Orgánica del Banco Central de la República Argentina, Ley 24.144, sancionada el 22 de septiembre de 1992, con las modificaciones introducidas por la Ley 26.739 (B.O. 28/03/2012).

C. Normativa administrativa

Banco Central de la República Argentina. Texto Ordenado sobre Protección de los Usuarios de Servicios Financieros. Texto ordenado al 06/05/2026.

Banco Central de la República Argentina. Texto Ordenado sobre Requisitos Mínimos para la Gestión y Control de los Riesgos de Tecnología y Seguridad de la Información. Texto ordenado al 13/02/2026.

Banco Central de la República Argentina. Texto Ordenado sobre Requisitos Mínimos para la Gestión de los Riesgos de Tecnología y Seguridad de la Información Asociados a los Servicios Financieros Digitales. Texto ordenado al 02/06/2023.

Banco Central de la República Argentina. Texto Ordenado sobre Depósitos de Ahorro, Cuenta Sueldo y Especiales. Texto ordenado al 05/06/2026.

Banco Central de la República Argentina. Texto Ordenado sobre Reglamentación de la Cuenta Corriente Bancaria. Texto ordenado al 04/06/2026.

Banco Central de la República Argentina. Texto Ordenado sobre Instrumentación, Conservación y Reproducción de Documentos. Texto ordenado al 06/12/2016.

Banco Central de la República Argentina. Texto Ordenado sobre Sistema Nacional de Pagos – Transferencias. Texto ordenado al 07/08/2025.

Banco Central de la República Argentina. Texto Ordenado sobre Sistema Nacional de Pagos – Transferencias – Normas Complementarias. Texto ordenado al 14/05/2026.

Banco Central de la República Argentina. Texto Ordenado sobre Sistema Nacional de Pagos – Servicios de Pago. Texto ordenado al 18/08/2025BCRA.

Informe sobre Protección a las Personas Usuarias de Servicios Financieros, diciembre de 2024. Disponible en: https://www.bcra.gob.ar/archivos/Pdfs/PublicacionesEstadisticas/PUSF-Informe-2024.pdf [consulta: 10/01/2026].