Servicio Nacional
del Consumidor

Informe Técnico
Fraude en Medios de Pago en Chile.

Tipologías del Fraude

Subdirección de Consumo Financiero
Coordinación de Economía del Comportamiento
Departamento de Investigaciones Colectivas Financieras
Departamento Protección al Consumidor Financiero y Supervisión de Mercado

Santiago, julio de 2025

Servicio Nacional
del Consumidor

Equipo SERNAC responsable de la publicación:
Miguel Pavez Hernández, Subdirector de Consumo Financiero (S)
Marcela Palominos Prado, Coordinadora Economía del Comportamiento
Guillermo Acuña Sanhueza, Analista Senior de la Coordinación de Economía del Comportamiento

Colaboradores de la Subdirección de Consumo Financiero:
Este estudio contó con la valiosa contribución de:
Andrés Pavón, ex Subdirector de Consumo Financiero,
Paulina Urzúa, Jefa del Departamento de Investigaciones Colectivas Financieras
María Catalina Giraudo, Abogada, Departamento de Investigaciones Colectivas Financieras
Felipe Herrera, Abogado, Departamento de Investigaciones Colectivas Financieras
Claudia Navarro, Abogada, Departamento de Investigaciones Colectivas Financieras
María Paz Derpich, Abogada, Departamento de Investigaciones Colectivas Financieras
Yuri Ghisellini, Profesional Analista Financiero, Departamento protección al consumidor financiero y supervisión de mercado
Rosa Flor Sáez, Profesional Analista Financiero, Departamento protección al consumidor financiero y supervisión de mercado
Juan Andrés Muñoz, Profesional, Departamento protección al consumidor financiero y supervisión de mercado

Se agradece la asistencia de los siguientes estudiantes de la Facultad de Economía y Negocios de la Universidad de Chile, en calidad de pasantes: Dominga Atal, Olivia Camus, Ignacia Correa, Agustín Delgado, Natalia Gallo, Carlos García, Francisco Morales, Luis Ojeda, Pedro Olivares, Antonia Paris, Juan Parra, Vicente Perales, Diana Portugal, Ayelen Sandoval, Juan Pablo Sierralta y Gustavo Valladares.

Además, se agradece la valiosa colaboración de Emperatriz Campos, Raimundo Figueroa, Rodolfo Martínez, Karla Rojas, Felipe Urrutia, en su calidad de postulantes de la Corporación de Asistencia Judicial, en la Subdirección de Consumo Financiero.

Índice

I. Introducción

En el entorno digital contemporáneo, el fraude financiero online ha emergido como una amenaza significativa que afecta tanto a individuos como a corporaciones y gobiernos a nivel global. Según el Informe Global de Riesgos del *World Economic Forum* del año 2024, la inseguridad cibernética ocupa el cuarto lugar en el listado de los riesgos globales de mayor gravedad en el corto plazo. En este contexto, Chile no ha sido la excepción. De acuerdo con estadísticas sobre las reclamaciones por fraudes financieros presentados por los consumidores a las entidades bancarias, se ha observado un incremento significativo en los últimos años, tanto en la cantidad de reclamaciones por fraude como en los montos involucrados, alcanzando su mayor nivel durante el segundo semestre de 2023. Los montos reclamados en 2023 en las instituciones bancarias más que se duplicaron respecto del año anterior, alcanzando aproximadamente $243 mil millones. En tanto, en el 2024 alcanzaron $275 mil millones.

A medida que la digitalización de los servicios financieros avanza, también lo hacen las técnicas de los delincuentes para explotar las vulnerabilidades de los sistemas y de los usuarios. Este escenario plantea la necesidad evaluar cuáles son los tipos de fraude de medios de pago online más prevalentes en Chile conforme a los datos disponibles y si existen vulnerabilidades de seguridad particularmente explotadas.

Para ello, el presente informe analiza cuantitativa y cualitativamente 9.899 reclamos en materia de fraude ingresados por los consumidores al SERNAC durante el año 2023, con la finalidad de identificar tipologías o *modus operandi* del fraude en medios de pagos, conforme a la descripción provista por los consumidores, y explorar las eventuales vulnerabilidades de seguridad que facilitan la ocurrencia de estos fraudes. Comprender la experiencia de fraude del consumidor, en base a sus propios relatos, resulta relevante por dos razones principales. En primer lugar, si bien existe abundante literatura comparada sobre el fraude financiero, las formas en que opera el fraude varían conforme a las vulnerabilidades de cada país. En consecuencia, sistematizar la experiencia de fraude que expone el propio consumidor, resulta esencial para detectar riesgos de vulnerabilidad en Chile. En segundo lugar, la literatura académica destaca que los fraudes en medios de pago, particularmente el *phishing* o engaño a través de técnicas de ingeniería social altamente sofisticadas, explotan el comportamiento de los consumidores. Por lo tanto, la propia experiencia del consumidor, contada mediante sus reclamos, es la fuente primaria para comprender cómo opera el fraude en medios de pago en Chile.

El análisis de texto permitió identificar 3 patrones comunes en la descripción del consumidor, a saber: *phishing* (9,1%), suplantación de identidad (24,2%) y desconocimiento general de movimientos y/o cobros (66,7%). Mientras la última categoría corresponde a reclamos cuyo texto no entrega información suficiente para identificar un *modus operandi* específico de fraude, las dos primeras nos entregan información valiosa sobre cómo opera el *phishing* y la suplantación de identidad. Para cada uno de estos casos, el informe presenta cómo opera el fraude descrito por el consumidor y, en base a dicha información, destaca eventuales vulnerabilidades.

El ***phishing*** es un tipo de fraude que se origina a través de correos electrónicos, mensajes de texto, llamadas telefónicas u otras formas de comunicación, con el objetivo de engañar al destinatario, a través de técnicas sofisticadas de ingeniería social, para que el consumidor realice la acción deseada por el atacante, particularmente, revelar información financiera, credenciales de acceso al sistema u otra información sensible. La

ingeniería social es el conjunto de técnicas empleadas para manipular a las personas para que realicen acciones o divulguen información confidencial. Los reclamos revisados permitieron caracterizar tres patrones específicos de phishing y su forma de operar: (i) las llamadas fraudulentas –también denominadas "*vishing";* (ii) el fraude a través de correos electrónicos (*phishing*), mensajes de textos *(smishing)* y el uso de *malware; y* (iii) fraudes mediante el registro de compras o ventas fraudulentas, por ejemplo, mediante réplicas de sitios web reales.

De los 638 reclamos relacionados con llamadas fraudulentas, en el 68% de los casos el estafador se hizo pasar por un ejecutivo bancario, mientras que solo en un 5% se hizo pasar por un funcionario público**.** Además, en el 37% de las ocasiones, el motivo de la llamada fue invocar una supuesta vulneración de la seguridad de la cuenta bancaria, mientras que en el 18% fue la comunicación de un supuesto beneficio o devolución de dinero.

Por su parte, los reclamos sobre suplantación de identidad (N=2.396) demuestran cinco *modus operandi* comunes: (i) fraudes originados por el robo o la pérdida de celular y/o documentos personales y bancarios; (ii) aquellos asociados al uso fraudulento de billeteras digitales; (iii) fraudes que se originan a través de portabilidades numérica fraudulenta (*SIM swapping*); (iv) fraudes a partir de la apertura de productos financieros sin la autorización del titular (*new account fraud*); y (v) fraudes relacionados a la clonación de tarjetas u otros productos.

En cuanto al tipo de respuestas entregadas por los proveedores financieros al reclamo, se observó que las modalidades con mayor porcentaje de cierres favorables, es decir, reclamos aceptados total o parcialmente por el emisor, son los fraudes asociados a la "portabilidad numérica fraudulenta" (74% del total) y la "suplantación de identidad con apertura de productos" (63% total). En tanto, dentro de las modalidades con menor porcentaje de cierres favorables se encuentra el *phishing*, en particular, los casos de llamadas fraudulentas o *vishing*, con un porcentaje favorable de solo el 36%.

En los reclamos estudiados, el *phishing* se encuentra presente más frecuentemente en productos bancarios, mientras que reclamos por suplantación de identidad a través de la "portabilidad numérica fraudulenta" y la "apertura de productos a través de la usurpación de identidad", presentan mayor frecuencia en productos asociados a proveedores del retail financiero. El análisis identifica riesgos asociados a los medios de verificación de identidad utilizados, por ejemplo, en el uso de billeteras digitales, así como la explotación del procedimiento de portabilidad numérica de teléfonos móviles en forma fraudulenta.

Ante la proliferación de brechas de seguridad, las autoridades reguladoras han implementado una serie de medidas destinadas a fortalecer el marco normativo. Por un lado, la Comisión para el Mercado Financiero (CMF) y la Subsecretaría de Telecomunicaciones (Subtel) se encuentran en proceso de normar la implementación de métodos de autenticación reforzada de la identidad. Paralelamente, la protección de datos personales se ha visto robustecida con la promulgación de la Ley N° 21.719. Esta legislación no solo refuerza la normativa existente, sino que también establece la creación de la Agencia de Protección de Datos Personales, un organismo cuya plena operatividad se proyecta para finales de 2026. Adicionalmente, la Ley de Ciberseguridad (Ley N° 21.663) ha sentado las bases institucionales, principios y la normativa general para la ciberseguridad a nivel nacional, con el objetivo primordial de resguardar la

infraestructura crítica y los sistemas de información, tanto públicos como privados, frente a las crecientes ciberamenazas.

En lo que respecta a la autenticación reforzada de la identidad, se busca masificar el empleo de factores de inherencia, tales como el reconocimiento facial y el escaneo de huellas dactilares, que verifican "lo que el usuario es". Sin embargo, resulta crucial reconocer que, si bien la identificación biométrica ofrece un nivel de seguridad superior a los sistemas tradicionales (contraseñas, tokens), también conlleva riesgos significativos. Estos riesgos derivan tanto de los avances en inteligencia artificial —ejemplificados por los *deepfakes*— como por la posibilidad de filtraciones de datos. La protección de los datos biométricos es de vital importancia, dado que, a diferencia de una contraseña que puede ser modificada, una característica biométrica como el rostro es inmutable. Si estos datos son comprometidos o sus bases de almacenamiento vulneradas, el riesgo de suplantación de identidad y otros usos ilícitos es permanente e irreparable (FATF, 2020; CPMI & WBG, 2020; Jans, 2024; Nicoletti, 2021; Politou, et al., 2022).

En este contexto, el Servicio Nacional del Consumidor (SERNAC), en su rol de velar por los derechos de los consumidores, ha manifestado una particular preocupación por este tema. Mediante distintas acciones, el SERNAC ha buscado resguardar y obtener compensaciones o restituciones directas para los grupos de consumidores afectados, especialmente en aquellos casos que involucren perjuicios económicos. Precisamente, en el marco de su facultad para interponer demandas colectivas, en febrero de 2023 el SERNAC demandó a un actor importante del mercado. El objetivo de esta acción fue que se cancelaran los cargos mal cobrados o se restituyera el dinero reclamado a todos los consumidores afectados por operaciones no reconocidas en sus medios de pago, tras haber dado aviso de extravío, hurto, robo o fraude. Así mismo, desde la entrada en vigencia de la Ley N° 21.234, que modificó la Ley N° 20.009 en mayo de 2020, el SERNAC ha requerido periódicamente a todos los proveedores financieros información sobre la cancelación o restitución de fondos correspondientes a operaciones que son desconocidas por los consumidores, así como la judicialización de solicitudes. Esta información permite la identificación de brechas de conducta y el monitoreo de la evolución que ha tenido la implementación de la norma.

El diagnóstico presentado en este informe busca contribuir a que los distintos componentes del ecosistema financiero –i.e. emisores, usuarios y supervisores- mitiguen el riesgo de fraude al consumidor.

Este estudio se organiza en varias secciones clave para abordar el fenómeno del fraude. En primer lugar, se examina la evolución de las reclamaciones por fraude en Chile, contrastándolas con la situación a nivel internacional. Posteriormente, se realiza un análisis cuantitativo y cualitativo de cerca de 10.000 reclamos de fraude en medios de pago, ingresados al SERNAC durante 2023. El objetivo es identificar las tipologías y modus operandi del fraude, así como explorar las vulnerabilidades de seguridad que facilitan su ocurrencia. Luego, se profundiza en los avances normativos más recientes en Chile, que buscan promover la autenticación reforzada de identidad y la protección de datos personales. Se pone un énfasis especial en las ventajas y riesgos de la biometría facial en este contexto. A continuación, se revisa el alcance y debilidades de diversas campañas de ciberseguridad impulsadas por las instituciones financieras mencionadas en los reclamos. Es importante señalar que los análisis de vulnerabilidad y de las campañas de ciberseguridad se basaron en información disponible hasta mayo de 2024, permitiendo identificar las brechas de seguridad existentes al momento que se

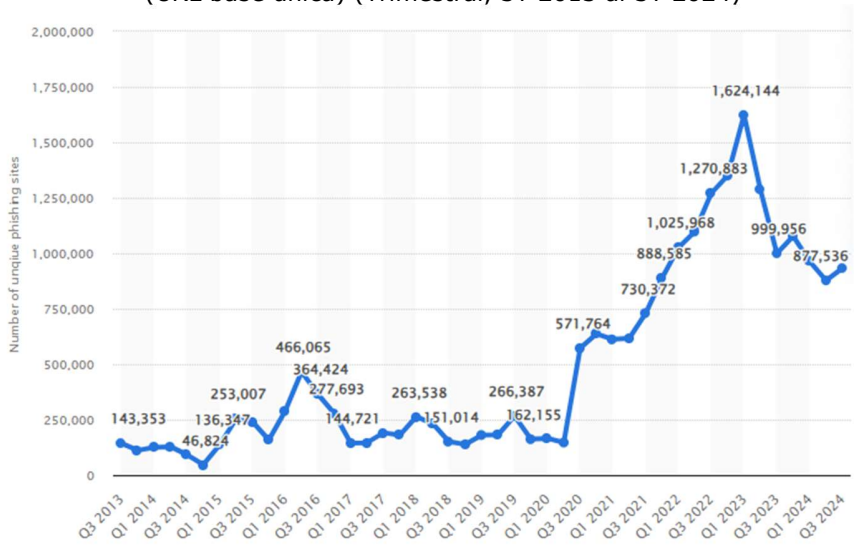
materializaron los episodios de fraudes reclamados por los consumidores. Finalmente, se presentan conclusiones y recomendaciones orientadas a ayudar al ecosistema financiero a mitigar los riesgos de fraude para los consumidores.

II. Evolución de los Fraudes en Chile y el mundo

De acuerdo con el informe Global de Riesgos del *World Economic Forum* del año 2024, la inseguridad cibernética se encuentra en el cuarto lugar del ranking de Riesgos Globales de corto plazo más graves (WEF, 2024). A la vez, las cifras internacionales de cibercrimen dan cuenta de un crecimiento exponencial de las denuncias por fraude cibernético a nivel mundial en los últimos años, destacando especialmente el periodo posterior al brote de la pandemia del Coronavirus. Este episodio impulsó de manera significativa la adopción de medios de pago digitales a nivel internacional, lo que ha contribuido a un aumento en este tipo de delitos (Jung & Katz, 2022). Se observa que esta tendencia está presente en la mayoría de los países, con la excepción de la Unión Europea, donde mejoras regulatorias han contribuido a mitigar el impacto de los fraudes, especialmente aquellos vinculados con tarjetas de crédito y débito (Banco Central Europeo, 2023).

Según el Grupo de Trabajo Anti-Phishing (APWG), coalición internacional comprometida con la lucha contra el cibercrimen a nivel global, durante el 2023 se registraron cerca de 5 millones de ataques de *phishing*, marcando así el año más crítico registrado en cuanto a esta amenaza (en comparación con los 4,7 millones reportados en 2022) **(Gráfico 1).** El *phishing* es un tipo de estafa en línea que utiliza técnicas de manipulación o ingeniería social y subterfugios técnicos, con el propósito de engañar al destinatario para que revele información personal y financiera confidencial. Se dirige a las personas a través del correo electrónico, mensajes de texto, llamadas telefónicas y otras formas de comunicación (APWG, 2024).

Gráfico 1: Número de sitios de phishing detectados en todo el mun
(URL base única) (Trimestral, 3T 2013 al 3T 2024)

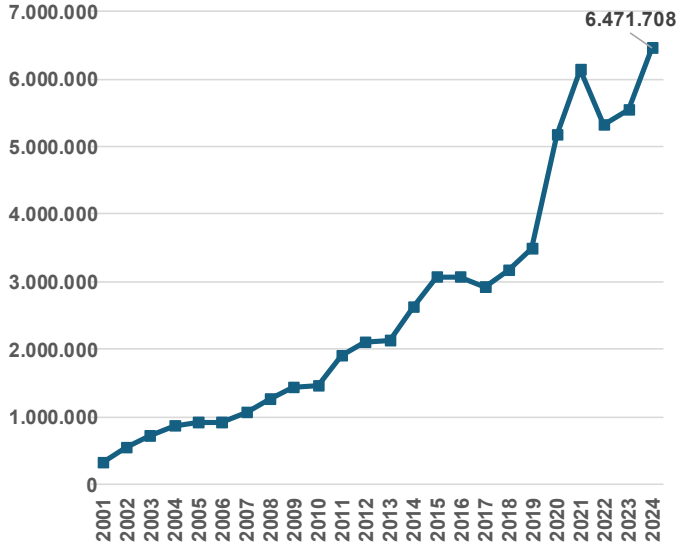


Fuente: https://www.statista.com sobre la base de observaciones de APWG.

El alza en el número de reclamaciones por fraude financiero también ha estado presente en EE.UU. Según el último informe sobre fraude de la Federal Trade Commission (FTC),

en 2023 recibió más de 5,5 millones de denuncias por fraude financiero, lo que representó un aumento del 4% en comparación con 2022. Esta tendencia ascendente continuó en 2024, con cerca de 6,5 millones de denuncias, un aumento del 17% en comparación con 2023 **(Gráfico 2).** En cuanto a los métodos de contacto utilizados para llevar a cabo el fraude denunciado el último año, la FTC indicó que el correo electrónico representó el método más utilizado, presente en el 25% de las denuncias de fraude cuando se identificó un medio de contacto. Le siguen las llamadas telefónicas, con un 19%, y los mensajes de texto, con un 16% (FTC, 2024).

Gráfico 2: Número de reclamos por fraudes, suplantación de identidad y otros tópicos por año



Fuente: FTC (2024).

Por su parte, de acuerdo con el último Informe sobre Delitos Cibernéticos del FBI correspondiente al cierre del año 2023, este recibió un total de 880.418 denuncias por *phishing* en 2023, con pérdidas superiores a los 12.500 millones de dólares. Los esquemas de *phishing* fueron el principal tipo de delito, con 298.878 denuncias (34%). El grupo más vulnerable fueron personas mayores a los 60 años, de quienes recibió 101.068 quejas con pérdidas superiores a los 3.400 millones de dólares (FBI, 2023).

En el caso de Europa, reportes recientes indican que, tras la implementación de medidas regulatorias que exigieron nuevos estándares de seguridad a la industria, se redujo considerablemente las denuncias o reclamaciones por fraude en medios de pago en la región (BCE, 2023). En 2021, el fraude con tarjetas como porcentaje del valor total de los pagos con tarjetas emitidas alcanzó su nivel más bajo (0,028%) desde que el Eurosistema comenzó a recopilar dicha información de los sistemas de pago con tarjetas en 2008 (Idem) **(Gráfico 3 y 4).** En particular, en 2020 y 2021, el fraude de forma remota (*card-not-present fraud*) representó aproximadamente el 84% del valor total del fraude con tarjetas. Esta proporción había ido creciendo de manera constante hasta 2020, en consonancia con la importancia cada vez mayor del comercio electrónico y el uso de pagos con tarjeta a través de Internet. Sin embargo, dicha tendencia se revirtió en 2021, disminuyendo un 12%, lo que ha sido atribuido al impacto beneficioso de la regulación sobre normas técnicas para la autenticación reforzada de los clientes (*strong customer authentication*) y estándares de comunicación abiertos, comunes y seguros

(*common and secure open standards of communication*), en el marco de la Directiva 2015/2366, conocida como la Directiva sobre Servicios de Pago (PSD2) -*EU Payment Services Directive*- y su regulación delegada[1]. Por otra parte, el denominado fraude con tarjeta presente, esto es, aquél mediante el uso de tarjetas falsificadas en tiendas y cajeros automáticos, disminuyó un 37 % en 2020 y un 42% en 2021 (BCE, 2023).

Recientemente, la experiencia europea ha demostrado que la adopción de regulaciones para la autenticación reforzada y protocolos de comunicación seguros ha reducido considerablemente el fraude con tarjetas. Específicamente, se observan tasas de fraude más bajas en los pagos con tarjeta en comparación con las transacciones sin SCA (EBA, 2024). Además, según la Autoridad Bancaria Europea, las tasas de fraude en los pagos con tarjeta fueron aproximadamente diez veces mayores cuando la contraparte se encuentra fuera del espacio económico europeo, donde la autenticación reforzada (SCA) no siempre se puede aplicar (EBA, 2024).

Gráfico 3: Valor total del Fraude con Tarjetas (millones de euros, valor del fraude como porcentaje del valor de las transacciones)

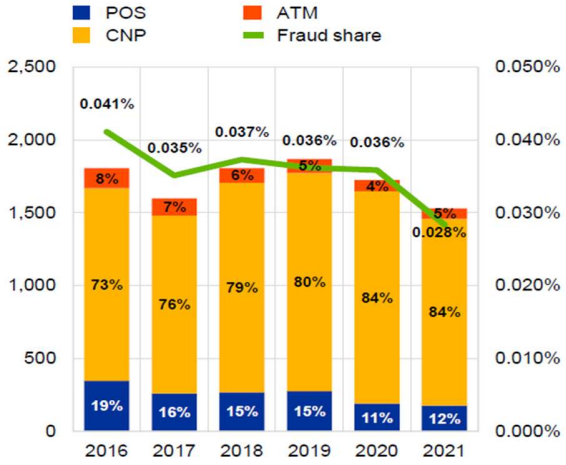
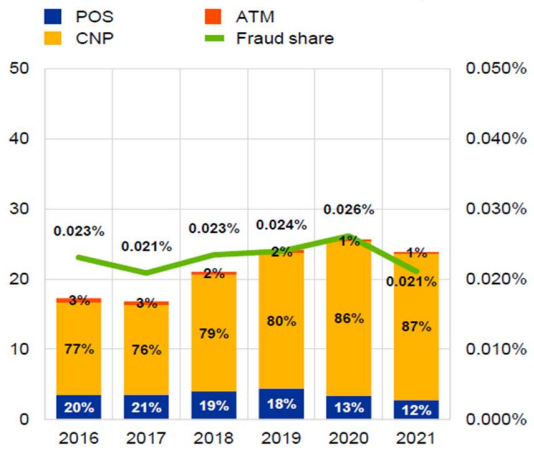


Gráfico 4: Volumen total del Fraude con tarjetas (millones de transacciones, volumen del fraude como porcentaje del volumen de transacciones)



Fuente: BCE, 2023.

Reclamaciones por fraude en Chile (2do sem 2020 a 2do sem. 2024).

En el caso chileno, las cifras de reclamaciones presentaron una trayectoria ascendente comparable a la observada en el contexto internacional. No obstante, esta tendencia fue revertida recientemente con la entrada en vigencia, el 30 de mayo de 2024, de la Ley N.º 21.673, que modificó la Ley N.º 20.009 sobre la limitación de la responsabilidad de los usuarios de tarjetas de pago y transacciones electrónicas en casos de extravío, hurto, robo o fraude. El incremento sostenido en las reclamaciones durante el año 2023, generó una creciente preocupación, tanto por su impacto económico en las instituciones financieras como por el volumen de recursos potencialmente vinculados a actividades ilícitas. Este contexto fue uno de los principales impulsores de la reciente reforma normativa, la cual se materializó en la promulgación de la Ley N.º 21.673.

[1] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication

Particularmente en el sector bancario —el cual concentra aproximadamente el 93 % del monto total reclamado—, y conforme a los antecedentes proporcionados por doce instituciones financieras, se evidenció un incremento sostenido en las reclamaciones por cargos desconocidos efectuados por los consumidores. Esta dinámica se intensificó a partir del segundo semestre de 2022, alcanzando su punto culminante durante el segundo semestre de 2023, con un total de 433 mil reclamaciones, que dieron lugar a restituciones o cancelaciones de cargos por un monto estimado en $169 mil millones **(Gráficos 5 y 6).** Sin embargo, a partir de la entrada en vigor de la Ley N.º 21.673, se observa una corrección significativa en dicha tendencia. Durante el segundo semestre de 2024, los niveles de reclamaciones retornaron a valores similares a los registrados en 2021-22, lo que sugiere un efecto regulatorio relevante en la contención del problema.

Gráfico 5: Número de reclamaciones semestrales (número)

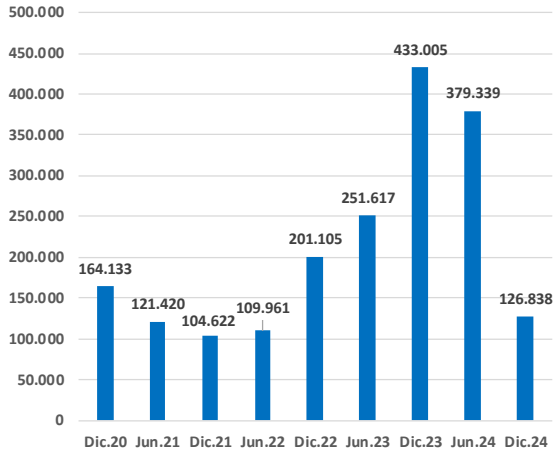
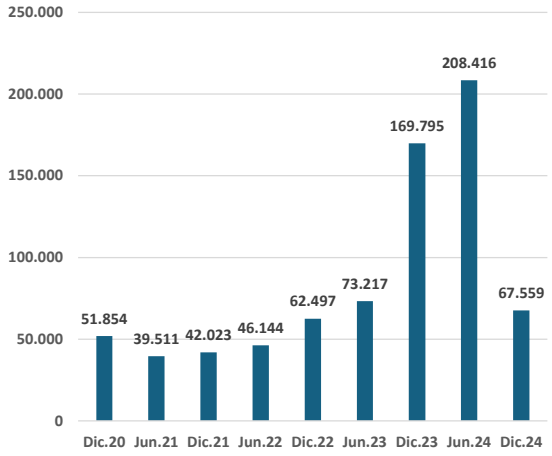


Gráfico 6: Monto total reclamado por semestre (millones de pesos)



Fuente: SERNAC, en base a datos auto reportados por las instituciones.

A nivel general, durante todo el periodo reportado (2° Semestre 2020 al 2° semestre 2024), las reclamaciones de restitución o cancelación de fondos por fraude se concentraron principalmente en la Banca (93%), seguido por el Retail Financiero (7%). La institución bancaria con mayor número de reclamaciones acumuladas en el período fue Banco Estado, con el 48% del total. Le siguen Banco de Chile, Banco Falabella y Banco Santander, con un 13%, 13% y 12%, respectivamente **(Gráfico 7).** Al diferenciar según el tipo de producto y/o servicio en que se materializó el fraude, a nivel general en la banca, las reclamaciones por fraude en Tarjetas de Débito representaron el 35% del total, seguido por los reclamos asociadas a Tarjetas de Crédito (32%), a Cajeros (20%) y Transferencias (12%). Sin embargo, en el caso de Banco Estado, las reclamaciones se concentraron en el producto tarjeta de débito y el servicio de giro en cajeros automáticos **(Gráfico 8).**

Gráfico 7: Número de reclamaciones acumuladas por Proveedores (número, porcentaje, periodo 2S.20-2S.24)

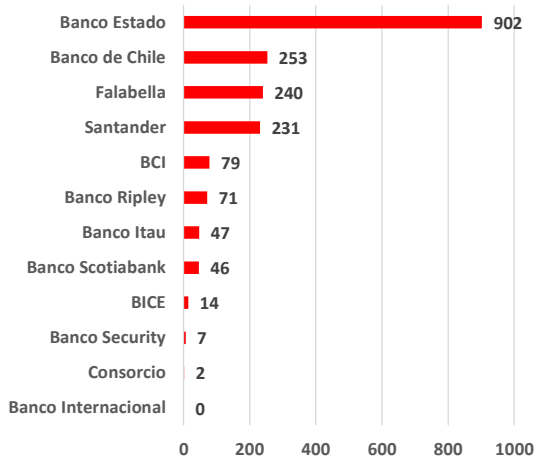
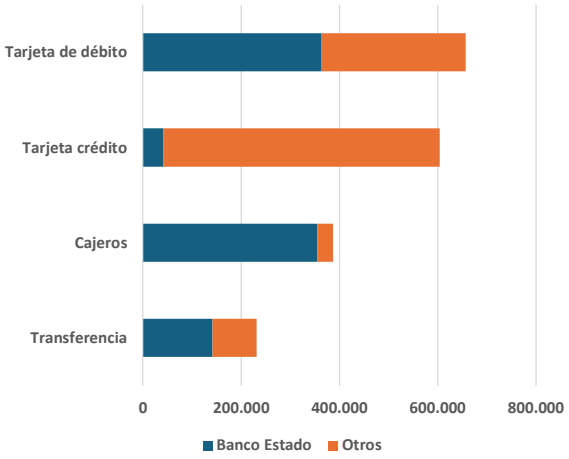


Gráfico 8: Número de reclamaciones acumuladas por tipo de producto: Banco Estado vs Otros (periodo 2S.20-2S.24)



Fuente: SERNAC, en base a datos auto reportados por las instituciones.

El monto restituido por la banca, acumulado en el periodo reportado (2do sem. 2020 a 2do. Sem. 2024) ascendió a $761 mil millones, donde Banco Estado representó el 45% de dicho monto, seguido de Banco Santander (18%) y Banco de Chile (11%) **(Gráfico 9).** El monto promedio restituido durante el periodo, por reclamación, fue de $402.219. Sin embargo, entre proveedores existe heterogeneidad respecto del monto promedio restituido por reclamación **(Gráfico 10)**.

Gráfico 9: Montos acumulados reclamados a proveedores ($ millones, porcentaje)

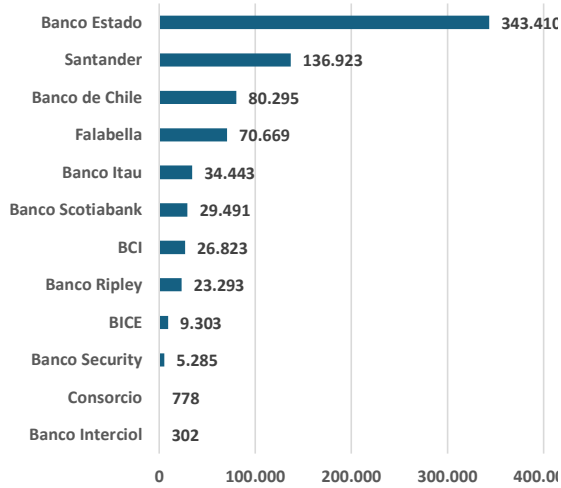
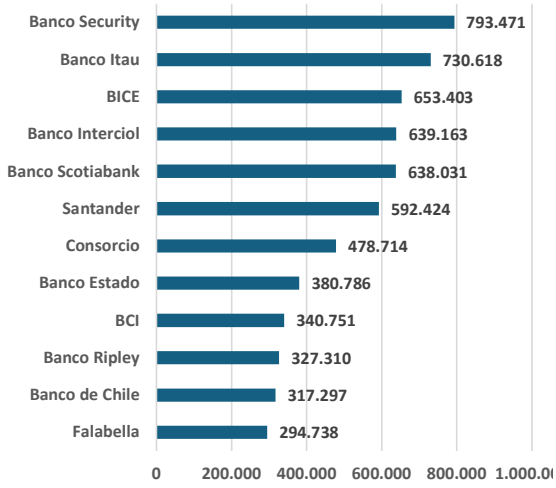


Gráfico 10: Montos promedio reclamados en el periodo 2S.20- 2S.24 ($)



Fuente: Datos auto reportados por las instituciones en cumplimiento al art.11 de la Ley N°21.234.

Resulta relevante destacar el comportamiento atípico de las reclamaciones asociadas a Banco Estado, el cual se desalineó significativamente de la tendencia general observada en el resto de la industria financiera. En primer lugar, esta institución registró un incremento sin precedentes en el número de reclamaciones durante el año 2023. En efecto, el volumen de reclamaciones aumentó en un 323 %, pasando de 95.035 casos en 2022 a 401.588 en 2023. A su vez, los montos involucrados se incrementaron en un 749 %, desde $15.612 millones en 2022 a $132.547 millones en 2023. Además, a diferencia de los patrones predominantes en otras entidades financieras, las reclamaciones dirigidas a Banco Estado se concentraron principalmente en fraudes vinculados a operaciones con cajeros automáticos y tarjetas de débito, lo que configura un perfil de riesgo distinto al observado en instituciones donde las reclamaciones se relacionan mayoritariamente con tarjetas de crédito **(Gráfico 8).**

La información disponible evidencia un incremento significativo en el monto promedio reclamado en Banco Estado durante el segundo semestre de 2023 y el primer semestre de 2024, alcanzando los $655 mil en ese último semestre **(Gráfico 11).** Este aumento se explica tanto por el mayor número de reclamaciones registradas durante dicho lapso, como por el incremento en los montos reclamados. Posteriormente, tras la entrada en vigencia de la Ley N.º 21.673 el 30 de mayo del 2024, Banco Estado experimentó una corrección significativa en sus niveles de reclamación, los que volvieron a cifras cercanas a las registradas en 2022 **(Gráficos 12 y 13).** En términos generales, durante el 2024, el número de reclamaciones cayó un 40% situándose en cifras cercanas a 241 mil, mientras que los montos totales de año aumentaron un 15%, alcanzando los $153 mil millones.

Gráfico 11: Monto promedio reclamado por semestre: Banco Estado vs Otros ($)

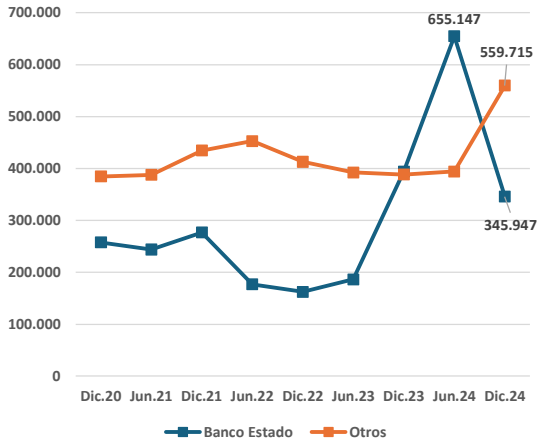
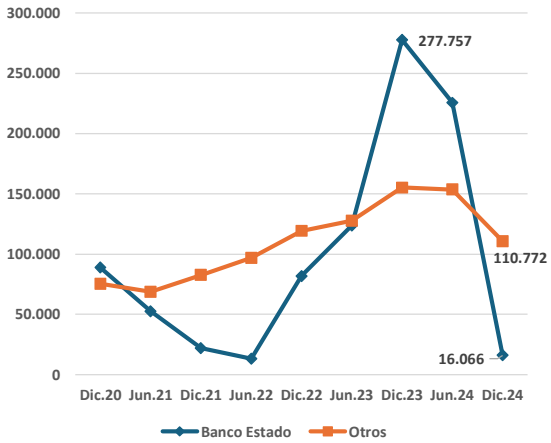


Gráfico 12: Número de reclamaciones semestrales: Banco Estado vs Otros (número)



Fuente: Datos auto reportados por las instituciones en cumplimiento al art.11 de la Ley N°21.234, y en respuesta al oficio Ord. N° 1114 (enero 2025), SERNAC.

Gráfico 13: Monto reclamado por semestre: Banco Estado vs Otros (millones de pesos)

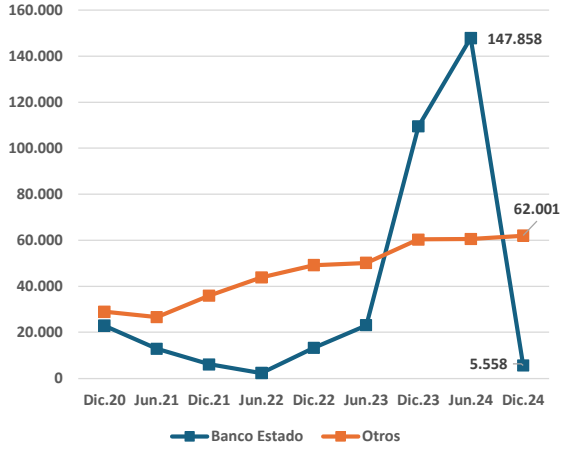
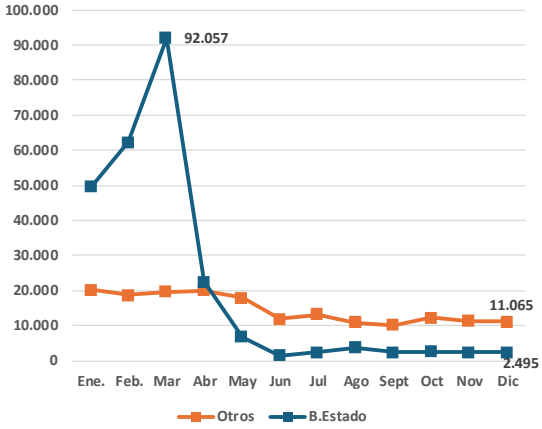


Gráfico 14: Número de reclamaciones por mes durante el año 2024: Banco Estado vs Otros (número)



Fuente: Datos auto reportados por las instituciones en cumplimiento al art.11 de la Ley N°21.234, y en respuesta al oficio Ord. N° 1114 (enero 2025), SERNAC.

En relación con la judicialización de las reclamaciones formuladas por los consumidores, los datos reportados por los proveedores financieros al SERNAC indican que, durante el período 2022-2023, el 1,2 % del total de reclamaciones recibidas fue objeto de acciones judiciales, mientras que los montos judicializados representaron el 10,3 % del total reclamado. En tanto, para el año 2024, el porcentaje de judicialización aumentó al 1,6% de las reclamaciones ingresadas, con montos judicializados equivalentes al 10,3 % del total reclamado. A la vez, mientras que el monto promedio de las reclamaciones con restitución fue de aproximadamente $340 mil en 2023 y $510 mil en 2024, los montos involucrados en reclamaciones judicializadas fueron sustancialmente mayores: en torno a $3,9 millones en 2022, $2,73 millones en 2023 y $3,33 millones en 2024.

En términos absolutos, los datos indican que en 2022 se judicializaron 4.549 reclamaciones, por un monto total de $17.935 millones; en 2023, la cifra aumentó a 8.059 casos judicializados, por un total de $22.000 millones; y en 2024, se registraron 8.862 reclamaciones con acciones judiciales, por un monto equivalente a $29.497 millones. Estos antecedentes evidencian un aumento tanto en el número de casos como en los montos promedio judicializados en 2024, lo que podría estar relacionado a los cambios regulatorios recientes.

Cabe señalar que, durante la tramitación legislativa del proyecto que dio origen a la Ley N.º 21.673 en 2024, diversos actores de la industria financiera plantearon que el crecimiento sustantivo en los patrones de reclamación por fraude podría estar asociado a fenómenos de riesgo moral o incluso a conductas de auto-fraude, lo que dio lugar a un debate relevante en torno a la adecuación de los incentivos reguladores y la efectividad de los mecanismos de control.

Entre las principales modificaciones introducidas por la Ley N.º 21.673 —que podrían contribuir a explicar la reciente disminución en las cifras de reclamaciones—, se destacan los siguientes cambios normativos:

- **Reducción de plazos para desconocer transacciones:** Se acorta el plazo que tienen los usuarios para desconocer operaciones no reconocidas, disminuyéndolo de 120 a 60 días corridos desde la fecha de la transacción.

- **Nuevos requisitos para solicitar reembolsos**: El emisor podrá exigir al usuario, al momento de presentar un reclamo por fraude, la entrega de: i) Una declaración jurada simple, en la que se indique el monto reclamado y el medio utilizado en la transacción fraudulenta; ii) Una denuncia presentada ante uno de los siguientes organismos: el Ministerio Público, Carabineros de Chile, la Policía de Investigaciones (PDI), o ante un tribunal con competencia penal (Juzgado de Garantía o Tribunal Oral en lo Penal). En caso de que el usuario no presente este respaldo dentro de los 30 días corridos siguientes al reclamo, se entenderá que se ha desistido del mismo, y no procederá la cancelación de los cargos ni la restitución de los fondos.

- **Modificación de los plazos de reembolso:** Se establece un plazo general de 10 días hábiles para la restitución de fondos o cancelación de cargos una vez presentada la denuncia. En el caso de transacciones relacionadas con giros en efectivo o en cajeros automáticos, el plazo se amplía a 15 días hábiles. Esta medida busca facilitar una revisión más eficiente de los antecedentes y, eventualmente, la preparación de acciones judiciales en casos de fraude doloso.

- **Creación de un procedimiento de suspensión en casos de dolo o culpa grave:** Se faculta al emisor a suspender el reembolso, cualquiera sea el monto reclamado, cuando existan indicios suficientes de dolo o culpa grave por parte del usuario. En tales casos, deberá remitir los antecedentes al Juzgado de Policía Local correspondiente, solicitando autorización para mantener la suspensión mientras se resuelve el fondo del caso.

- **Catálogo de presunciones de dolo o culpa grave**: Se presumirá el dolo o la culpa grave del usuario cuando ocurra alguna de las siguientes hipótesis, para efectos de los procedimientos ante el juez de policía local:

a) Que la operación desconocida haya sido realizada exclusivamente entre cuentas que sean de su titularidad, contratadas con anterioridad.
b) Que la operación desconocida haya sido realizada exclusivamente entre cuentas de su titularidad y de su cónyuge o conviviente civil, o de parientes por consanguinidad en toda la línea recta y la colateral hasta el cuarto grado inclusive, o bien por afinidad en toda la línea recta y la colateral hasta el segundo grado inclusive.
c) Que los fondos transferidos hayan sido enviados a una o más cuentas registradas con al menos cuarenta y ocho horas de anticipación al desconocimiento de la operación por el usuario, o se hubiere realizado transferencias a la o las cuentas de destino dos o más veces antes de las cuarenta y ocho horas previas al desconocimiento de la operación.
d) Que el usuario haya reconocido expresamente haber entregado sus claves voluntariamente a terceros, a sabiendas de que podrán ser usadas para giros o transacciones.
e) Que el usuario tenga una o más sentencias firmes en el período de cinco años, en que se reconozca la existencia de dolo o culpa grave.
f) Si el emisor tuviere indicios suficientes de coordinación maliciosa entre los usuarios para reclamar una o más operaciones en una misma oportunidad.

g) Si el emisor tuviere indicios suficientes de que fue el mismo usuario quien realizó la operación reclamada en canales físicos previo a la solicitud de restitución y/o cancelación de cargos.
h) Si la operación desconocida hubiere sido realizada con autenticación reforzada, siendo al menos uno de los factores de autenticación de inherencia. Sin perjuicio de lo anterior, si la operación desconocida hubiere sido realizada con autenticación reforzada, en los términos del referido artículo, considerando sólo factores de posesión o conocimiento, podrá servir como base de presunción judicial."

- **Deber del usuario y de las entidades reguladas:** Los usuarios deberán informarse y adoptar todas las medidas necesarias para prevenir el uso indebido, el fraude u otros riesgos afines a la utilización de los medios de pago a que se refiere esta ley y los mecanismos de autenticación asociados. Para estos efectos, las entidades reguladas por esta ley deberán proporcionar, de manera periódica, clara, accesible y actualizada, toda la información necesaria sobre las medidas de seguridad y las instrucciones de uso seguro a sus usuarios, promoviendo las prácticas responsables en el manejo de los medios de pago.

III. Tipologías de Fraude en Medios de Pago

La presente sección analiza cuantitativa y cualitativamente 9.899 reclamos en materia de fraude ingresados por los consumidores al SERNAC durante el año 2023, con la finalidad de identificar tipologías o *modus operandi* del fraude en medios de pago, conforme a la descripción provista por los consumidores.

Cabe destacar que, dado que el análisis tiene por objeto de estudio los reclamos formulados por los consumidores y su propia descripción del problema de consumo, se trata de información auto reportada, que no corresponde a observaciones periciales, sino a la experiencia de fraude del consumidor. Comprender la experiencia de fraude del consumidor, en base a sus propios relatos, resulta relevante por dos razones principales. En primer lugar, si bien existe abundante literatura comparada sobre el fraude financiero, las formas en que opera el fraude varían conforme a las vulnerabilidades de cada país. En consecuencia, sistematizar la experiencia de fraude que expone el propio consumidor, resulta esencial para detectar riesgos de vulnerabilidad en Chile. En segundo lugar, la literatura académica destaca que los fraudes en medios de pago, particularmente el *phishing* o engaño a través de técnicas de ingeniería social altamente sofisticadas, explotan el comportamiento de los consumidores. Por lo tanto, la propia experiencia del consumidor, contada mediante sus reclamos, es la fuente primaria para comprender cómo opera el fraude en medios de pago en Chile.

La base de datos utilizada corresponde a reclamos del 2023 que fueron originalmente categorizados por funcionarios del Departamento de Atención a Usuarios del SERNAC, en el Modelo de Atención al Consumidor (MAC) del SERNAC, como: (i) "Cobros después de dar aviso de tarjeta perdida robada"; (ii) "Consumidor no reconoce transacción, clonación"; (iii) "Consumidor no reconoce transacción, suplantación". Adicionalmente, se agregaron 400 reclamos correspondientes a las subcategorías (iv) "Cobros por productos o servicios no contratados" y (v) "No reversa cargos mal efectuados", cuyo texto de la descripción del reclamo contiene palabras y expresiones comunes a prácticas de fraude financiero.

El análisis de texto de cada reclamo por parte del equipo de la Subdirección de Consumo Financiero, permitió identificar los siguientes 3 patrones comunes en la descripción del consumidor: i) Casos de *Phishing* (9,1%); ii) Casos de Suplantación de Identidad (24,2%); y (iii) Desconocimiento general de movimientos y/o cobros (66,7%) **(Gráfico 15).** A continuación, se presenta la estadística descriptiva general de esta clasificación, a fin de categorizar los problemas de consumo reclamados. La sección siguiente profundiza en los *modus operandi* descritos por los consumidores en el caso de *phishing* y la suplantación de identidad.

El desconocimiento de movimientos y/o cobros considera todos aquellos reclamos en los cuales se enuncian cobros y/o transferencias bancarias no reconocidos por el titular, pero cuyo texto, debido a su variabilidad y/o falta de información detallada, por sí mismo, no entrega información suficiente para identificar un *modus operandi* específico de fraude. Esto representa el 67% de los reclamos analizados.

Los ***casos de phishing* corresponden al 9% del total de los reclamos analizados (N=900).** La principal característica del *phishing* es el uso de técnicas de manipulación denominadas "ingeniería social", que son utilizadas para lograr el acceso a información del consumidor y su medio de pago. Dentro de los reclamos revisados, se pueden identificar los siguientes tres patrones específicos expuestos por los consumidores: (1)

Fraudes a través de llamadas fraudulentas –también denominado "*vishing";* (2) Fraudes a través de mensajes de textos o correos electrónicos –comúnmente denominado *Phishing/Malware; y* (3) Fraudes a través del registro de compras o ventas fraudulentas **(Gráfico 16).**

La **Suplantación de Identidad representan el 24% de los reclamos analizados** (N=2.396). La descripción formulada por los reclamantes ante SERNAC permite identificar los siguientes mecanismos en los cuales se origina el fraude: (1) Fraudes originados a partir del robo o la pérdida de celular y/o documentos personales y bancarios; (2) Fraudes asociados al uso indebido de las billeteras digitales; (3) Fraudes que se originan a través de portabilidad numérica fraudulenta (*SIM swapping*); (4) Fraudes que involucran la apertura de productos financieros sin la autorización del titular (*New Account Fraud*); y (5) Fraudes relacionados a la clonación de tarjetas u otros productos **(Gráfico 17).**

Gráfico 15: Categorías de Fraudes (%)

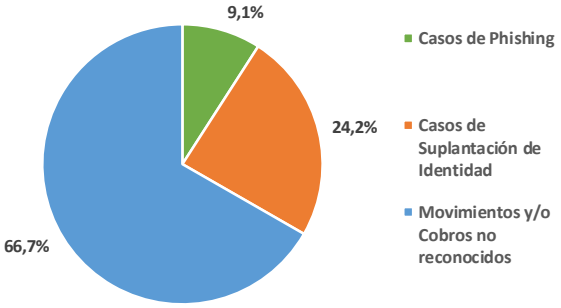


Gráfico 16: Tipos de Fraudes según la Categoría "Phishing" (%)

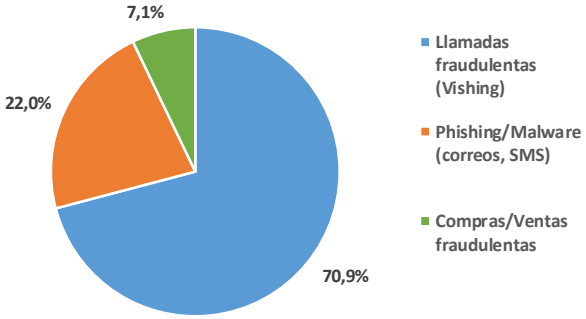
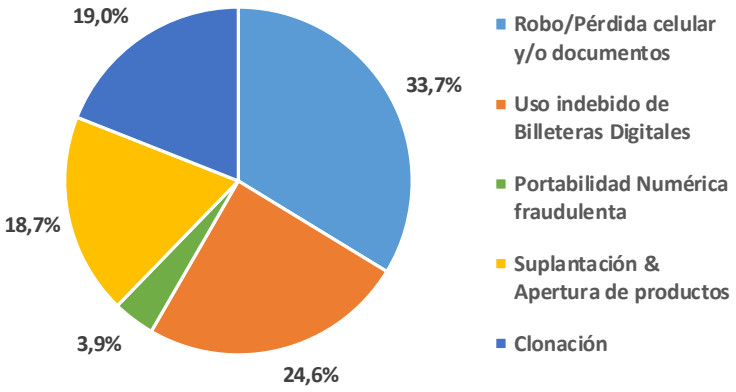


Gráfico 17: Tipos de Fraude según la Categoría "Suplantación de Identidad" (%)



Fuente: Elaboración propia en base a datos Sernac

La **Tabla 1** describe someramente cada una de estas subcategorías de modalidades de fraude.

Tabla 1: Tipología de Fraudes analizados a partir de los Reclamos 2023, Sernac

Cat.	Subcategoría	Descripción	% del Total	% de la Subc.
Casos de Phishing	**Llamadas Fraudulentas (Vishing)**	El vishing es una forma de estafa que implica la manipulación de las personas a través de llamadas telefónicas para obtener datos confidenciales, como números de tarjetas de crédito, contraseñas u otros datos personales sensibles.	6,4% (n=638)	71%
	Compras/Ventas Fraudulentas	En estos casos, mientras la víctima compra o vende un producto, el estafador utiliza técnicas de ingeniería social para engañarla y lograr que realice transacciones financieras bajo falsos pretextos, como la compra de productos inexistentes o la revelación de datos confidenciales. Esto se logra mediante la manipulación y falsificación de información, a menudo a través del phishing.	0,6% (n=64)	7%
	Phishing / Malware / smishing (Correos, SMS)	Son episodios que pueden combinar las técnicas del *phishing* con el ataque de *malware*. Es una técnica de ciberdelincuencia que consiste en enviar correos electrónicos fraudulentos con archivos infectados o enlaces a páginas web maliciosas. El objetivo es robar información personal o infectar el dispositivo de la víctima	2% (n=198)	22%
Casos de Suplantación de Identidad	**Robo/Pérdida celular y/o documentos**	Son episodios de fraudes que suceden luego de que la víctima haya sufrido el robo o pérdida del celular o documentos personales (carnet de identidad, documentos bancarios, etc). Incluye, por ejemplo, la utilización fraudulenta de las aplicaciones bancarias instaladas en los dispositivos móviles.	8,2% (n=807)	34%
	Uso indebido de Billeteras Digitales	Son episodios en los cuales el estafador accede y hace mal uso de la billetera digital de la víctima, ya sea a través del robo del dispositivo o a través de la falsificación de identidad haciendo, por ejemplo, solicitudes de restablecimiento de contraseña o cambios en la información de la cuenta, para posteriormente, retirar dinero de las cuentas de las víctimas.	6% (n=590)	25%
	Portabilidad Numérica fraudulenta	Es un tipo de fraude en el que se intenta portar ilegalmente el número de teléfono móvil de una persona a otro proveedor de Telefonía sin el consentimiento de la víctima. En el caso de la estafa denominada "*SIM Swapping*" el defraudador solicita duplicado de la tarjeta SIM tras reportar extravío o daño del celular, suplantando la identidad del titular.	0,9% (n=94)	4%
	Suplantación & Apertura de productos financieros	Estafadores utilizan la información personal de una persona, sin su consentimiento, para abrir cuentas bancarias, tarjetas de crédito, préstamos u otros productos financieros.	4,5% (n=449)	19%
	Clonación de productos financieros	Son episodios en que la persona declara haber sido víctima de una clonación de sus productos financieros o de otros medios que permitieron el fraude.	4,6% (n=456)	19%
TNR	**Movimientos y/o Cobros no reconocidos**	La categoría de 'Movimientos y/o Cobros no reconocidos' abarca reclamos en los cuales, debido a su variabilidad y/o falta de información detallada, no se han identificado patrones comunes de fraude durante el análisis preliminar.	66,7% (n=6.603)	100%

El análisis de los datos por género revela una mayor incidencia de fraude en mujeres en todas las subcategorías. Sin embargo, destaca su alta prevalencia en el *phishing*, donde aproximadamente dos tercios de las víctimas son mujeres **(Gráfico 18).**

En cuanto al rango etario, los fraudes de portabilidad numérica afectan principalmente a personas mayores, mientras que los jóvenes son más afectados por el mal uso de billeteras digitales y las compras o ventas fraudulentas **(Gráfico 19).**

Gráfico 18: Modalidad de Fraude por género de la víctima (%)

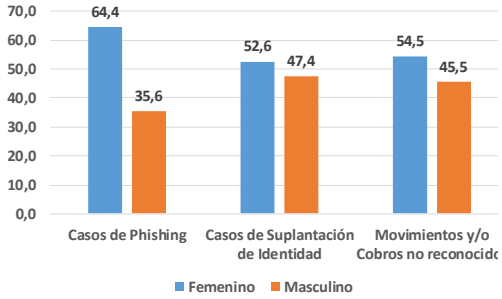
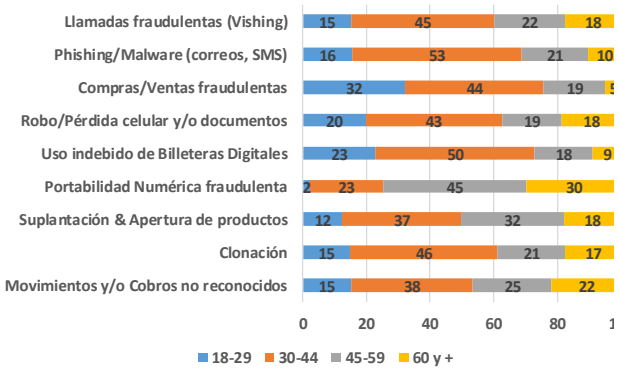


Gráfico 19: Modalidad de Fraude por Rango Etario (%)



Fuente: Elaboración propia en base a datos Sernac

Respecto a las respuestas de los proveedores financieros a los reclamos, las modalidades con mayor porcentaje de cierres favorables (reclamos aceptados total o parcialmente) son los fraudes asociados a la "portabilidad numérica fraudulenta" (74%) y la "suplantación de identidad con apertura de productos" (63%). En contraste, los casos reclamos asociados al *phishing* presenta un menor porcentaje de cierres favorables, especialmente en los casos de "compra o ventas fraudulentas" (31%) y "llamadas fraudulentas" (36%) **(Gráfico 20).**

En los reclamos analizados, el phishing es más frecuente en productos bancarios, mientras que la suplantación de identidad (a través de la "portabilidad numérica fraudulenta" y la "apertura de productos a través de la usurpación de identidad") predomina en productos de proveedores del retail financiero **(Gráfico 21).**

Gráfico 20: Modalidad de Fraude por Tipo de Cierre del Reclamo (%)

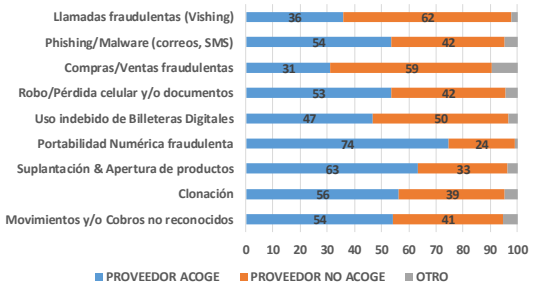
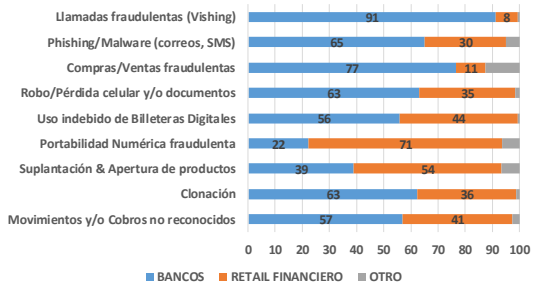


Gráfico 21: Modalidad de Fraude por Mercado del Proveedor del producto afectado por el fraude (%)



Fuente: Elaboración propia en base a datos Sernac

III.1. Phishing

El phishing es un tipo de fraude que se origina a través de correos electrónicos, mensajes de texto, llamadas telefónicas u otros medios de comunicación. Su objetivo es engañar al destinatario, mediante sofisticadas técnicas de ingeniería social, para que realice la acción deseada por el atacante, como revelar información financiera, credenciales de acceso u otros datos sensibles. La ingeniería social es el conjunto de técnicas empleadas para manipular a las personas con el fin de que realicen acciones o divulguen información confidencial. El phishing se basa en la psicología del engaño y la manipulación, explotando las vulnerabilidades humanas en lugar de las técnicas (Ferreira, Coventry & Lenzini, 2015).

En los casos de phishing, el estafador busca inicialmente ganarse la confianza de la víctima para obtener más fácilmente información confidencial. Una técnica común es la ingeniería social inversa. A diferencia de la ingeniería social tradicional, donde el atacante se presenta directamente ante la víctima para engañarla, en la ingeniería social inversa, el atacante crea una situación en la que la víctima se siente obligada a buscarlo y proporcionar la información deseada. Esto genera un alto grado de confianza entre la víctima y el atacante, ya que la víctima cree ser quien inicia el contacto (Irani, et al., 2011).

Las acciones de phishing pueden resultar especialmente convincentes cuando estas incluyen datos personales y datos financieros del consumidor que sólo debiesen ser de conocimiento del emisor del medio de pago, tales como el nombre de su ejecutivo de cuentas o detalles de transacciones pasadas, entre otros. Los accesos no autorizados a bases de datos personales de los consumidores financieros en poder de sus instituciones financieras representan un alto riesgo de ser fuente de información para futuras acciones de phishing. De hecho, aunque estas filtraciones de datos no impliquen el acceso a las claves de seguridad de los consumidores, el conocimiento que proporcionan sobre el consumidor aumenta la efectividad de las técnicas de engaño o ingeniería social.

En el ámbito del phishing, la literatura académica ha identificado varias técnicas de ingeniería social y persuasión que son cruciales para entender cómo los estafadores manipulan a sus víctimas. Cialdini (2007) describe seis principios de influencia que los estafadores suelen explotar:

1. **Autoridad**: Los individuos tienden a no cuestionar a figuras de autoridad. En el *phishing*, los estafadores pueden suplantar la identidad de representantes de instituciones legítimas para ganarse la confianza de sus víctimas.
2. **Prueba Social**: Las personas buscan conformarse con el comportamiento de los demás, especialmente cuando perciben un riesgo compartido. Los ataques de phishing a menudo emplean falsas evidencias de conformidad social para persuadir a las víctimas de que la acción solicitada es segura.
3. **Agrado/Similitud**: La confianza y la persuasión aumentan cuando existe agrado o similitud. Los estafadores pueden crear perfiles falsos que reflejen los intereses y valores de sus objetivos para establecer confianza.
4. **Compromiso/Consistencia**: La tendencia a mantener la coherencia con compromisos previos influye en el comportamiento. En el phishing, esto puede manifestarse en una serie de pequeñas solicitudes que llevan a la víctima a comprometerse con una acción más significativa.

5. **Escasez**: La percepción de disponibilidad limitada genera una fuerte respuesta emocional. Los estafadores utilizan amenazas de pérdida de acceso o plazos limitados para inducir a las víctimas a actuar precipitadamente.
6. **Reciprocidad**: Las personas se sienten obligadas a devolver favores. Los estafadores pueden ofrecer ayuda o pequeños regalos para crear una sensación de deuda en la víctima.

Por su parte, Gragg (2003) identifica siete desencadenantes psicológicos que pueden ser utilizados en fraudes para influir en las decisiones de las víctimas:

1. **Emoción Fuerte**: Emociones intensas, como el miedo o la excitación, pueden reducir la capacidad de pensar críticamente. Los ataques de phishing a menudo inducen pánico o urgencia para que las víctimas actúen sin pensar.
2. **Sobrecarga**: La presentación excesiva de información o demandas inesperadas puede abrumar a las víctimas, llevándolas a aceptar información sin una evaluación crítica.
3. **Reciprocidad**: Similar al principio de Cialdini, se basa en la tendencia a devolver favores, facilitando que las víctimas se sientan en deuda con el estafador.
4. **Relaciones Engañosas**: Los estafadores construyen relaciones falsas para generar confianza, compartiendo información o intereses comunes para manipular emocionalmente a sus víctimas.
5. **Difusión de Responsabilidad y Deber Moral**: Hacer que las víctimas sientan que no son las únicas responsables de sus acciones o que están cumpliendo un deber moral puede ser una táctica efectiva para reducir la resistencia a participar en actividades fraudulentas.
6. **Autoridad**: La deferencia a la autoridad es explotada por los estafadores que se presentan como figuras autoritarias para minimizar las dudas de las víctimas.
7. **Integridad y Coherencia**: Las personas tienden a actuar de manera coherente con sus compromisos previos y creen en la honestidad de los demás, lo que los estafadores pueden explotar al solicitar acciones aparentemente inofensivas inicialmente.

Finalmente, Stajano y Wilson (2011) proponen una serie de principios que explican cómo los estafadores explotan las vulnerabilidades humanas, entre aquellos adicionales a los ya señalados, se encuentran:

1. **Distracción**: Los estafadores aprovechan la distracción de las víctimas para actuar sin ser detectados.
2. **Cumplimiento social (Autoridad)**: La tendencia social a respetar la autoridad reduce la sospecha hacia quienes la aparentan, facilitando el engaño.
3. **Rebaño (Prueba Social)**: La creencia de que es seguro seguir a la multitud disminuye la vigilancia de las víctimas al ver a otros involucrados en la misma actividad.
4. **Deshonestidad**: El involucramiento en acciones ilegales durante una estafa aumenta la vulnerabilidad de la víctima y dificulta la denuncia.
5. **Amabilidad**: La disposición natural a ayudar a los demás, incluso de forma voluntaria, es explotada por los estafadores, quienes se aprovechan de la buena fe de las personas.
6. **Necesidad y codicia**: Las necesidades y deseos pueden nublar el juicio, haciendo que las personas sean menos críticas ante ofertas que los satisfacen. La vulnerabilidad aumenta cuando los estafadores identifican estas necesidades

y deseos, permitiéndoles manipular a sus víctimas. En la estafa, la situación personal de la víctima es tan relevante como su posible codicia.

7. **Tiempo**: La presión del tiempo reduce la capacidad de las víctimas para evaluar racionalmente la situación, lo que los estafadores explotan para inducir decisiones rápidas.

Estas taxonomías proporcionan un marco comprensivo para entender cómo los estafadores emplean técnicas de ingeniería social y persuasión en el phishing y otros fraudes financieros.

La sección siguiente analiza las tres categorías de *Phishing* identificadas como *modus operandi* del fraude en los reclamos ingresados al Sernac: (i) llamadas fraudulentas o v*ishing;* (ii) correos o SMS fraudulentos -*phishing*/malware/*smishing*; y (iii) compras o ventas fraudulentas. A fin de identificar las técnicas empleadas por los defraudadores, para cada una de las modalidades se generó un caso representativo de *phishing* según la descripción contenida en los reclamos.

A. Llamadas fraudulentas o *Vishing*

El vishing es un tipo de fraude telefónico que, mediante técnicas de ingeniería social, busca obtener datos personales o financieros de los usuarios. Generalmente, el estafador suplanta la identidad de un tercero de confianza, como un ejecutivo bancario, el cual utiliza información personal y financiera de la víctima para ganarse su confianza. A través de mensajes alarmantes o promesas de beneficios atractivos, el estafador obtiene acceso a información que facilita fraudes posteriores.

A continuación, a modo de ejemplo, se recrea el contenido de elementos comunes de reclamos en que se describe el modus operandi en comento.

> *El reclamante declara haber recibido una llamada de una persona que se hizo pasar por un ejecutivo bancario, quien mencionó sus datos personales y bancarios, incluida información detallada sobre las transacciones realizadas, las tarjetas que poseía y los montos asociados a éstas. Esta situación hizo creíble el discurso del estafador, según declara el reclamante.*
>
> *El supuesto ejecutivo le informó que había sido víctima de un intento de fraude a través de la banca por internet ese mismo día. El reclamante declara que esto le generó ansiedad.*
>
> *El supuesto ejecutivo le indica que necesita su autorización para bloquear las transacciones fraudulentas que se han realizado desde su cuenta, de lo contrario, estos cobros se cargarían a su cuenta corriente.*
>
> *Siguiendo las indicaciones del supuesto ejecutivo, la víctima realizó un cambio de clave, para lo cual recibió un correo con la nueva clave. Según declara el reclamante, los mensajes enviados parecían haber sido enviados desde el banco y el contenido parecía confiable (el logotipo del banco era visible y se utilizaban fuentes y colores similares).*
>
> *Posteriormente, el supuesto ejecutivo le solicitó la tarjeta de coordenadas y la tercera clave para bloquear el movimiento, asegurando que, por razones de seguridad, no debía entregar en ningún momento sus claves, sino que solo debía*

digitar en el teclado del teléfono dichas claves. Dado que no se le solicitó dictar su clave, la víctima indica que confió en la confidencialidad de la operación.

Tras ello, el estafador habría logrado cambiar la clave de la banca en línea, asociar la cuenta a una billetera digital y realizar compras a través de ella.

Los reclamos por vishing revelan variaciones en esta tipología de fraude, como la identidad suplantada por el estafador (por ejemplo, funcionario público, amigo o familiar) o el motivo de la llamada (beneficios, devolución de dinero, actualización de datos, etc.). De los 638 reclamos relacionados con llamadas fraudulentas, el 68% involucró la suplantación de un ejecutivo bancario, mientras que solo el 5% la de un funcionario público **(Gráfico 22).** Además, el 37% de las llamadas se originaron por una supuesta vulneración de la seguridad de la cuenta bancaria, y el 18% por la comunicación de un supuesto beneficio o devolución de dinero **(Gráfico 23).**

En cuanto a las características de los reclamantes, aproximadamente dos tercios son mujeres **(Gráfico 24),** y el 50% se encuentra en el rango de edad de 30 a 49 años.

Gráfico 22: Tipos de suplantación en las llamadas fraudulentas (%)

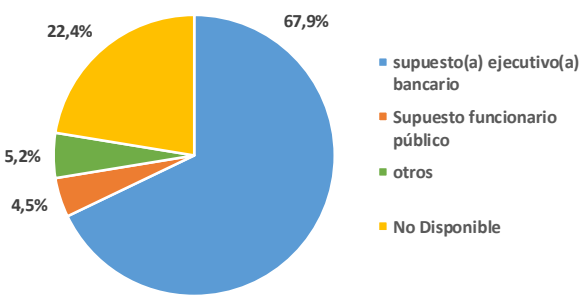


Gráfico 23: Tipos de Motivos en las llamadas fraudulentas (%)

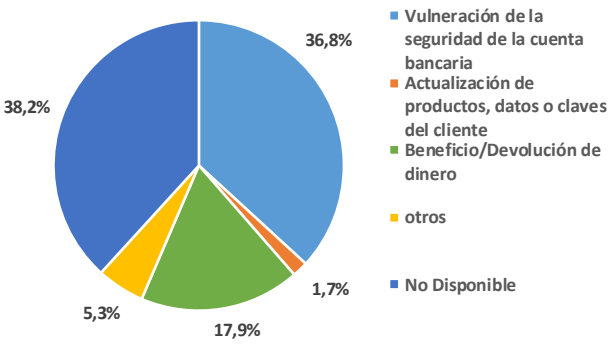


Gráfico 24: Llamadas Fraudulentas (Vishing) de acuerdo con el género de las víctimas (%)

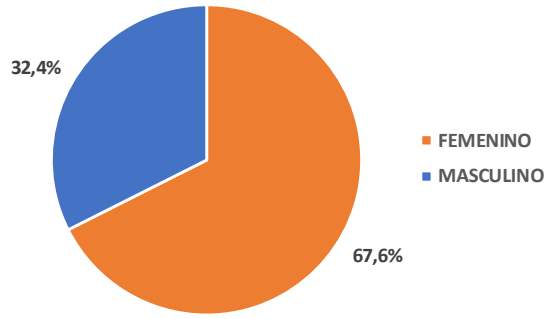
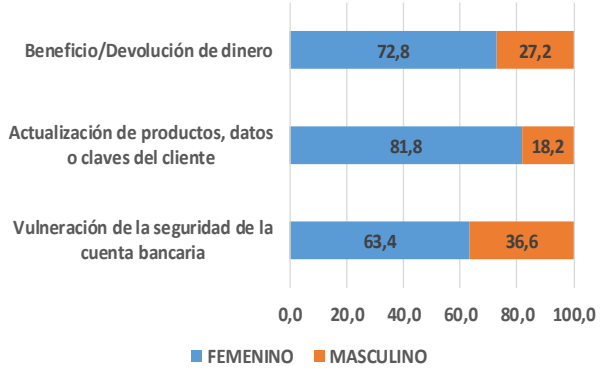


Gráfico 25: Género de la víctima de acuerdo al motivo de la llamada fraudulenta (%)



Fuente: Elaboración propia en base a datos Sernac

Acceso a claves vía Dual-Tone Multi-Frequency (DTMF)

Según los reclamos analizados, una técnica común en los ataques de vishing es que el estafador solicita a la víctima ingresar sus claves a través del teclado del teléfono, en lugar de dictarlas oralmente. Esto puede generar en la víctima la falsa sensación de seguridad y aumentar su confianza en el supuesto ejecutivo bancario.

Sin embargo, la tecnología Dual-Tone Multi-Frequency (DTMF) permite identificar los números digitados por los tonos específicos que genera cada uno. Al ingresar la clave, el estafador puede obtener los números a través de estos tonos, ya que cada número se asocia a un sonido distinto. Cada botón genera dos tonos (de alta y baja frecuencia), y estos sonidos permiten al estafador descifrar la contraseña numérica de la víctima[2].

B. Correos o SMS (Phishing/ Smishing / Malware)

Los correos electrónicos de *Phishing* y los SMS fraudulentos (*Smishing*) están diseñados para engañar al destinatario, a través de técnicas de ingeniería social, para que realice la acción deseada por el atacante. Los correos electrónicos o SMS llevan al destinatario a sitios web falsificados que engañan a los destinatarios para que divulguen datos financieros como nombres de usuarios y contraseñas (APWG, 2024).

A continuación, a modo de ejemplo, se recrea el contenido de elementos comunes de reclamos en que se describe el modus operandi de este tipo de fraude.

Correo Phishing
El reclamante declara haber recibido un correo del Banco, señalando que era beneficiaria del Bono Marzo. Ingresó al link del mensaje, tras lo cual se abrió una nueva ventana del navegador con la página de inicio del Banco. Ingreso su Rut y su contraseña de la banca en línea, pero terminado ese proceso se cerró instantáneamente la pestaña del navegador. Ingreso a la aplicación del banco, pero esta se había reiniciado y tras volver a entrar se percata que habían sustraído dinero de su cuenta a través de una transferencia hacia una persona que no conocía.

SMS Smishing
La persona declara que recibió un mensaje SMS del Banco, consultando si había intentado hacer un giro por $800.000, ante lo cual debía responder "R" si rechazaba el giro. La persona responde inmediatamente, siguiendo las instrucciones señaladas. Cómo respuesta, el supuesto Banco le envía otro SMS señalando que procederá a bloquear su tarjeta. Al día siguiente se da cuenta de un cargo desconocido por el monto señalado.

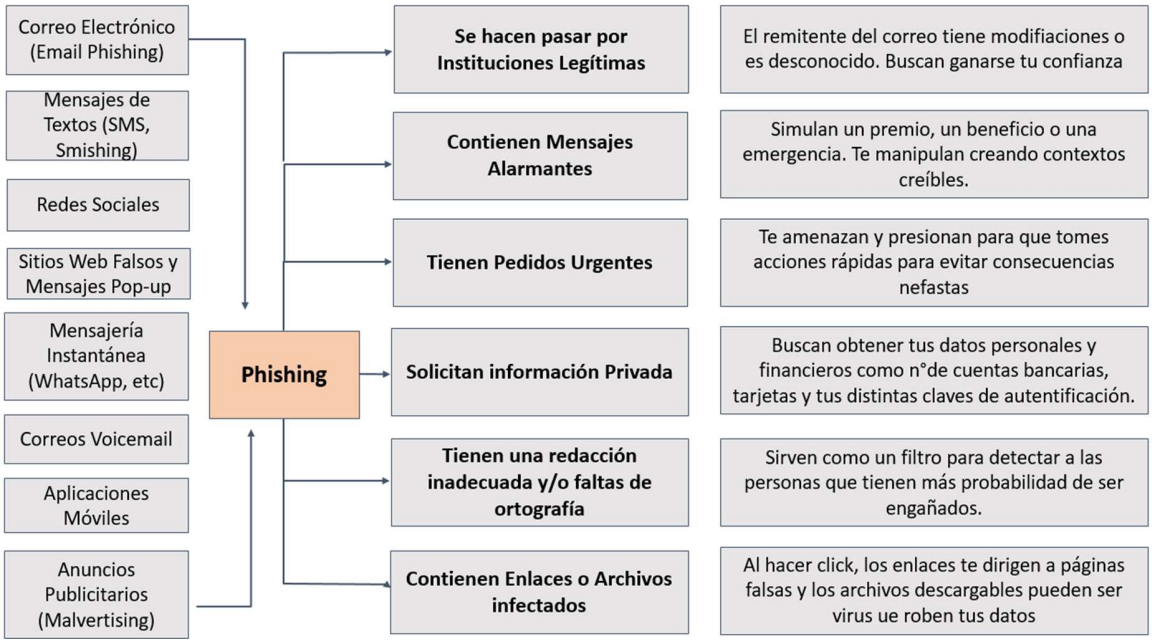
La persona declara haber recibido un mensaje de texto que indicaba que su compra no podía ser entregada por falta de información. Recientemente había realizado una compra por internet, por lo cual pensó que se trataba de ella. Ingresó al link que la derivó a una página que le indicaba que su paquete estaba en Aduanas y que, para liberarlo, debía pagar un impuesto de $2.900. Hizo el pago con su Tarjeta de Crédito en la plataforma de pagos señalada en el mensaje y, posteriormente, recibió un correo del supuesto banco, indicando que su tarjeta había sido enrolada exitosamente para

[2] Gesprodat. (2023). Cómo evitar el robo de claves mediante lectura de tonos. Recuperado de https://gesprodat.com/2023/11/02/como-evitar-el-robo-de-claves-mediante-lectura-de-tonos/

pagos a través de Código QR. No se dio cuenta del fraude, hasta que días después comenzó a recibir notificaciones por compras internacionales a través de su Tarjeta de Crédito.

Adicionalmente, resulta común que estos esquemas de subterfugios coloquen Malware en las computadoras para robar credenciales directamente, a menudo utilizando sistemas que interceptan los nombres de usuario y contraseñas de las cuentas de los consumidores o los desvían hacia sitios web falsificados (APWG, 2024) **(véase Diagrama 1).**

Diagrama 1: Canales de exposición y señales habituales del Phishing



Fuente: Elaboración propia.

Por otra parte, una variante cada vez más frecuente del *phishing* es el QRshing, que utiliza códigos QR (*Quick Response Code*) para dirigir al usuario, mediante el escaneo del código, a un sitio web fraudulento que solicita información confidencial o lo induce a descargar malware. Estos códigos QR fraudulentos pueden encontrarse en correos electrónicos o superpuestos a códigos QR legítimos en menús de restaurantes, publicidad exterior, estacionamientos, etc. También existe el "código QR inverso", donde el estafador crea un código malicioso que, bajo la apariencia de un método de pago, sustrae dinero del establecimiento o persona afectada, y puede robar datos personales y bancarios[3].

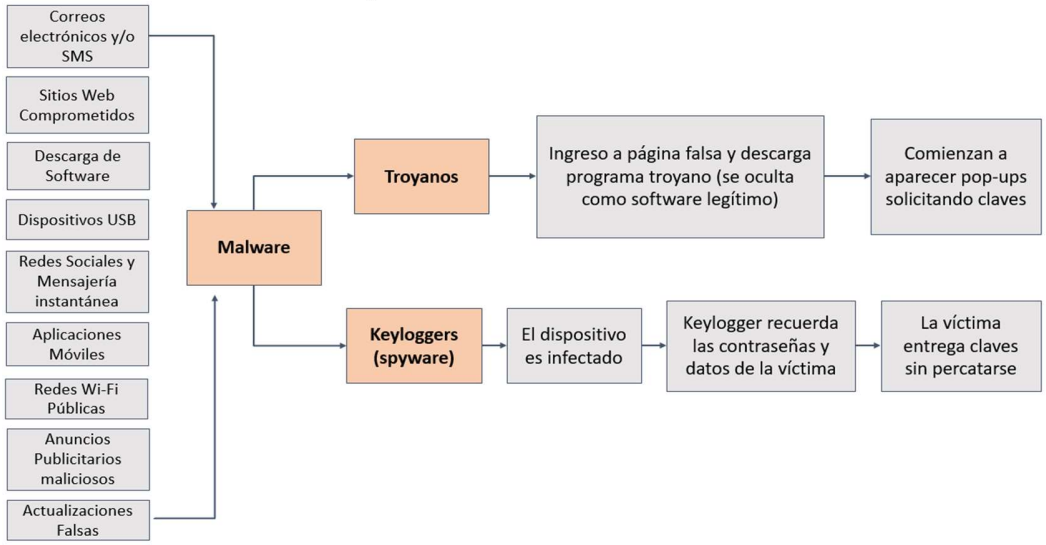
Por su parte, el malware, o software malicioso, abarca un amplio espectro de programas intrusivos diseñados para dañar sistemas informáticos. Este término general engloba diversas amenazas en línea, como virus, spyware, adware, ransomware y otros tipos de software perjudicial. El **Diagrama 2** ilustra sus principales modos de operación. En esencia, el malware puede comprometer la confidencialidad de la información, robando

[3] Véase Santander. Estafa código QR. Recuperado de https://www.santander.com/es/stories/estafa-codigo-qr

datos financieros, credenciales de cuentas y contraseñas (como lo hacen el spyware, los troyanos, los gusanos y los keyloggers). Además, puede manifestarse a través de anuncios no deseados, barras de herramientas y ventanas emergentes engañosas (programas potencialmente no deseados o PUPs, por sus siglas en inglés). Otra forma de ataque común es la ejecución de campañas masivas de phishing o spam, orquestadas por bots y botnets[4].

El malware se propaga a través de diversos métodos, entre los que destacan: i) Correos electrónicos: Mediante archivos adjuntos infectados o enlaces a sitios web maliciosos; ii) Ingeniería social: A través de alertas de seguridad falsas que inducen al usuario a descargar software de seguridad fraudulento; iii) Descargas no deseadas: Ya sea de forma accidental o inadvertida, al instalar software contaminado. Además de estos, existen otros medios de propagación, lo que subraya la importancia de la precaución y la seguridad informática.

Diagrama 2: Canales de Exposición y Procesos a través de los cuales el estafador roba datos personales mediante Malware



Fuente: Elaboración propia.

C. Transacciones en sitios web fraudulentos

La categoría denominada transacciones en sitios web fraudulentos corresponde a casos en los cuales la víctima se encuentra contratando, comprando o vendiendo un producto, y el estafador utiliza técnicas de ingeniería social y subterfugios técnicos para engañar a las personas para que realicen transacciones financieras bajo pretensiones falsas, ya sea comprando productos inexistentes o entregando información confidencial, aprovechando la manipulación y la falsificación de información a través del *phishing*. En estos casos se suelen hacer réplicas de sitios web reales y ofrecer grandes descuentos por tiempo limitado para inducir a los consumidores a hacer una compra.

Los fraudes digitales más comunes en el comercio electrónico se basan, en gran medida, en ingeniería social y en la suplantación de identidades electrónicas[5]:

[4] Kaspersky. (n.d.). Types of malware. Recuperado de https://www.kaspersky.es/resource-center/threats/types-of-malware

[5] Véase https://www.t13.cl/noticia/tendencias/recomendaciones-pdi-para-evitar-estafas-cyberday-31-5-2024; https://www.cnnchile.com/pais/protegerte-estafas-cyberday-pdi-recomendaciones-compra-online_20240603/; https://portalinnova.cl/las-principales-estafas-a-las-que-estar-atentos-en-el-cyber-

El **phishing y el smishing** consisten en correos electrónicos o mensajes de texto que aparentan provenir de comercios, apelan a la urgencia u ofrecen promociones atractivas e incluyen enlaces que conducen a páginas que se presentan como legítimas pero en realidad son falsas, donde se capturan contraseñas, datos de tarjetas o números de identificación personal; la víctima puede terminar expuesta a robo de fondos y a la suplantación de su identidad, con escasas posibilidades de recuperar el dinero transferido directamente.

Una evolución de esta técnica son los sitios **web clonados**: páginas espejo que imitan con gran fidelidad la apariencia de comercios legítimos y utilizan dominios casi idénticos. Al ingresar datos o efectuar un pago, la información va directamente a manos de los delincuentes, quienes no solo se apropian de fondos y credenciales, sino que también pueden instalar malware en los dispositivos del usuario, dificultando la detección y el reclamo posterior.

En redes sociales y marketplaces poco regulados proliferan las llamadas **"ofertas fantasmas":** anuncios patrocinados o publicaciones de productos inexistentes a precios demasiado bajos. Una vez captado el interés, el estafador deriva la conversación a canales privados y exige transferencias persona-a-persona sin protección. El resultado habitual es la pérdida total del dinero y la exposición de datos personales, pues no existe una plataforma formal que respalde la transacción ni un mecanismo efectivo de restitución.

El **fraude "card-not-present"** —y su variante conocida como carding— explota la falta de verificación física de la tarjeta al realizar pagos en línea o por teléfono. Con datos robados, los delincuentes ejecutan pequeños cargos de prueba para confirmar que la tarjeta está activa y luego realizan compras mayores o revenden la información en mercados ilegales, generando cargos que pueden pasar desapercibidos entre las transacciones legítimas del titular.

Otra modalidad frecuente son los **enlaces de seguimiento o de "delivery" falsos**: mensajes que pretenden informar sobre el estado de un envío e incluyen un enlace a un supuesto sistema de rastreo. Al hacer clic, el usuario es conducido a una página que solicita datos bancarios o descarga software malicioso, con el propósito de robar credenciales —incluidos códigos de autenticación de dos factores— o instalar spyware que permita interceptar comunicaciones y acceder a cuentas financieras.

La **publicidad engañosa** también afecta a los consumidores cuando se anuncian descuentos inexistentes, se aceptan pagos y luego se cancela la venta o se entrega un producto distinto o de calidad inferior. Estas prácticas vulneran el derecho a recibir información veraz y a que se respete el precio y las condiciones ofrecidas, generando sobrepagos y frustración.

El **quishing** traslada el engaño al uso masivo de códigos QR. Los atacantes difunden códigos en afiches, volantes, correos o redes sociales que redirigen a sitios fraudulentos para sustraer credenciales o instalar malware. Dado que la URL permanece oculta hasta después de escanear, el usuario no puede verificar la legitimidad del destino y, además,

monday-2024/; https://portalinnova.cl/cyber-day-2025-las-recomendaciones-de-los-expertos-para-no-caer-en-estafas/.

suele utilizar su teléfono —dispositivo vinculado a aplicaciones bancarias y redes sociales—, lo que agrava el riesgo.

Finalmente, las **aplicaciones falsas** imitan el nombre y el ícono de apps legítimas de bancos, comercios o servicios de mensajería. Se distribuyen mediante enlaces en mensajes o incluso logran infiltrarse en tiendas oficiales si no son detectadas a tiempo. Una vez instaladas, solicitan permisos excesivos, presentan formularios de inicio de sesión ficticios y capturan toda clase de datos sensibles; en los casos más graves, instalan troyanos que otorgan control total sobre el dispositivo, posibilitando transferencias no autorizadas y el acceso a otras cuentas del usuario.

En conjunto, estas modalidades evidencian la importancia de la verificación cuidadosa de enlaces, dominios y aplicaciones, el uso de métodos de pago protegidos y la vigilancia continua de los movimientos bancarios para detectar cargos anómalos a tiempo.

A la vez, durante eventos de alto consumo digital como el CyberDay, los consumidores se enfrentan a un entorno especialmente propicio para el fraude. ¿Qué hace que estas estafas sean tan efectivas, incluso ante usuarios informados? La respuesta no solo radica en las tácticas técnicas de los estafadores, sino también en cómo estas explotan atajos mentales y sesgos cognitivos comunes en situaciones de presión. A continuación, se detallan las estrategias más utilizadas y los mecanismos psicológicos que las hacen prosperar:

- Urgencia y escasez simuladas: Los ciberdelincuentes denuncian "últimas unidades" o "promoción flash" para que el comprador actúe sin verificar detalles.
- Confianza en grandes marcas: Réplicas casi idénticas de sitios conocidos –a veces impulsadas por IA– inducen a introducir datos sensibles; en móviles la URL incompleta facilita el engaño.
- Dificultad para detectar falsificaciones: Páginas clonadas exhiben diseño pulido y hasta un candado HTTPS falso. Solo acceder vía cyber.cl o teclear la web oficial evita este riesgo.
- Publicidad pagada maliciosa: Anuncios patrocinados colocan sitios fraudulentos por encima de los legítimos en buscadores y redes, dirigiendo tráfico ansioso al fraude.

Sesgos cognitivos explotados

Sesgo	Cómo lo aprovecha el estafador	Efecto en el consumidor
Heurística de urgencia/escasez	Límite de tiempo/unidades	Compra impulsiva, poca revisión
Aversión a la pérdida	"No te pierdas el descuento"	Miedo a quedar fuera → acción apresurada
Sesgo de optimismo	"A mí no me pasará"	Subestima la probabilidad de fraude
Prueba social	Testimonios falsos, "miles ya lo compraron"	Confianza por imitación
Autoridad	Logos oficiales o de bancos falsificados	Credibilidad automática
Anclaje de precios	Precio "antes" inflado + falso descuento	Ilusión de ahorro extraordinario

Campañas de prevención que contrarresten estos sesgos –con mensajes que destaquen las pérdidas reales, muestren que la mayoría compra de forma segura y alertas just-in-time antes de pagar– elevan la tasa de recordación y reducen los clics inseguros.

A continuación, a modo de ejemplo, se recrea el contenido de elementos comunes de reclamos en que se describe el modus operandi de este tipo de fraude.

Caso 1: El reclamante declara que estaba vendiendo un artículo por Facebook, cuando un supuesto interesado le indica que realizaría el pago a través de un código QR, para lo cual le pidió sus datos de coordenadas. El reclamante, dado que no conocía esa nueva modalidad de pago, entregó los datos. Con esa información, el defraudador cambió las claves de la aplicación, y posteriormente, realizó un retiro de fondos.

Caso 2: El reclamante declara que estaba vendiendo un artículo por Facebook, cuando un supuesto comprador lo contacta para efectuar la compra. Le menciona que, para transferir el dinero, debe el vendedor autorizar, con la clave de su aplicación bancaria, la vinculación de la cuenta del supuesto comprador, cuando lleguen las notificaciones a la app del banco. El reclamante indica que pasó un tiempo en que se diera cuenta que no había recibido dinero a su cuenta sino, por el contrario, habían hecho transferencias desde su cuenta a terceros.

Caso 3: El reclamante menciona que intentó realizar una compra de un artefacto a través de la página Web de una famosa Multitienda, utilizando la Tarjeta de Crédito de la misma Multitienda. Sin embargo, pese a que el cargo fue realizado, desde la Multitienda le indican que la compra no se había efectuado, debido a que la había realizado en una página fraudulenta.

Caso 4: El reclamante declara que se encontraba realizando una venta de un producto por internet, cuando lo contacta un supuesto comprador, que lo engaña aludiendo ser un funcionario público y que por error había transferido a su cuenta un monto mayor al pactado. Para materializar la venta, le había mandado sus datos de transferencia (entre los cuales estaba su correo electrónico, Rut y número de cuenta). Tras enviarle el comprobante de la supuesta transferencia, le solicita devolver el dinero. En el momento en que estaba realizando la transferencia, accedieron a su cuenta y solicitaron una serie de créditos y avances, para posteriormente retirar el dinero. Los movimientos fueron aprobados por el banco sin que la persona fuera notificada de ninguna de esas operaciones. El reclamante estima que fue víctima de un virus que permitió al delincuente acceder a sus datos bancarios.

Vulnerabilidades asociadas a páginas web fraudulentas.

Datos reportados por el CSIRT (*Computer Security Incident Response Team)* y la Comisión para el Mercado Financiero (CMF) dan cuenta de la creciente presencia del phishing en el mercado nacional. El CSIRT, equipo de respuesta ante incidentes de Seguridad Informática, dependiente del Ministerio del Interior y Seguridad Pública, publica periódicamente alertas de phishing en el país y campañas de difusión de malware a través de email (*malspam*) (https://csirt.gob.cl/). Durante el 2023, el CSIRT publicó aprox. 700 alertas de phishing materializados vía sitios web fraudulentos, correos electrónicos y SMS fraudulentos. Del total, el 40% correspondió a suplantación de bancos, el 34% a Retail y el 15% a instituciones de gobierno. A la vez, cerca del 47% de los casos bancarios, correspondían a falsificaciones de Banco Estado.

Por su parte, el sitio web de alertas ciudadanas de la Comisión para el Mercado Financiero publica una lista de entidades que se presume pueden estar cometiendo delitos de estafa, usura e invasión del giro bancario. Estas entidades ofrecen créditos fraudulentos o representan plataformas de inversión fraudulentas. Durante el 2023, se alertaron de

16 sitios que ofrecían aplicaciones, algunas de ellas con páginas web que, al tiempo de este informe, seguían activas. A la vez, la CMF publicó 56 entidades que ofrecieron créditos fraudulentos, las cuales operaban a través de páginas web, WhatsApp y/o redes sociales (principalmente Facebook) y se identificaron 13 entidades que ofrecieron inversiones online a través de páginas web y redes sociales.

Sin embargo, las plataformas online y los motores de búsqueda, como Google, suelen permitir reportar sitios web fraudulentos, pero no cerrarlos directamente, ya que la clausura de una web implica un proceso legal y de jurisdicción que no siempre corresponde a esas plataformas. La denuncia puede ayudar a que la página sea retirada de los resultados de búsqueda y a que las autoridades puedan investigar el caso[6].

III.2. Casos de Suplantación de Identidad

En relación a los casos de suplantación de identidad, el estudio de más de 2.000 reclamos en la materia ha permitido identificar 5 tipos de fraude: (i) aquellos que se origina a partir del robo o pérdida del celular y/o documentos personales y bancarios; (ii) aquellos que tienen por base el uso fraudulento de billeteras digitales; (iii) aquellos que realizan la portabilidad numérica de forma fraudulenta; (iv) la apertura de productos financieros sin la autorización del titular; y, finalmente, (v) los que se originan en la clonación de tarjetas u otros productos financieros.

A diferencia de los casos de *phishing* previamente analizados, en estos casos no se registra interacción entre el defraudador y la víctima mediante técnicas de manipulación o ingeniería social.

En términos generales, independiente del mecanismo que de origen al fraude, las consecuencias suelen ser similares: acceso y uso indebido de las cuentas financieras de la víctima (a través de aplicaciones bancarias y/o billeteras digitales, principalmente), apertura de productos financieros (cómo tarjetas de multitiendas), así como solicitudes de créditos y avances de dinero.

Otro punto en común que tienen ciertas tipologías de fraudes, es que las víctimas suelen desconocer el fraude, hasta que son contactadas por una deuda impaga o las mismas personas revisan su situación financiera para postular a algún crédito.

A. Fraudes originados a partir del robo o pérdida del celular y/o documentos personales y bancarios

El celular se ha convertido en un medio clave para la verificación de identidad en trámites digitales. El uso de códigos enviados por SMS para la autenticación de dos factores (2FA) o verificación de identidad es una práctica muy común y extendida en la mayoría de los servicios en línea. Asimismo, es frecuente que se pueda acceder al correo electrónico del titular desde el celular, ya que muchas aplicaciones de correo se sincronizan automáticamente. El correo electrónico también constituye un medio de verificación de identidad (por ejemplo, para recuperación de contraseñas o 2FA). Si alguien obtiene acceso al celular de una persona, podría acceder a su correo electrónico si la sesión está

6 Véase https://developers.google.com/search/help/report-quality-issues?hl=es
Y https://protecciondatos-lopd.com/empresas/como-denunciar-una-pagina-web

abierta, no hay bloqueo de pantalla o si la autenticación de dos factores (2FA) del correo está configurada para usar el mismo dispositivo de forma vulnerable.

Junto con lo anterior, las numerosas funcionalidades de los teléfonos celulares brindan enormes ventajas a los consumidores, pero también implican riesgos significativos, ya que "tu smartphone es la entrada a tus datos personales". Entre los riesgos identificados están[7]:

a) Hacer compras no autorizadas utilizando tus tarjetas de crédito.
b) Clonación de su número IMEI o *International Mobile System Equipment Identity* para que sea comercializado en el mercado negro. Este es un código de 15 dígitos único pregrabado en el teléfono que identifica el equipo telefónico a nivel mundial.
c) Acceso a sus contraseñas e información de inicio de sesión de tus cuentas.
d) Hackeo de cuentas de correo electrónico y bloqueo de acceso.
e) Violación de cuentas bancarias o aplicaciones de inversión.
f) Hackeo de ID de Google o Apple y eliminación de la autenticación de dos factores (2FA) en otras aplicaciones.
g) Ejecución de estafas de *phishing* dirigidas a amigos y familiares.
h) Uso de fotos confidenciales para realizar chantajes o extorsión.

A continuación, se presentan recreaciones de reclamos ingresados a SERNAC, donde los episodios de fraude se originan a partir del robo o pérdida del celular u otros documentos personales de las víctimas:

Tras la pérdida del celular del reclamante, menciona que externos tomaron control de su dispositivo y de su aplicación bancaria instalada en este. A través de la aplicación se realizaron pagos y giros a través de Códigos QR. A través de este medio efectuaron un giro por $100.000.

La persona reclama que, tras el robo de su carnet de identidad, el delincuente abrió una Tarjeta de Crédito de forma presencial, firmando digitalmente con su huella, pero utilizando la foto de su carnet. Con la Tarjeta hicieron un avance en efectivo y compras en el comercio.

B. Fraudes que se originan a través de la portabilidad numérica fraudulenta

En el año 2010, la Ley N°20.471 estableció las bases para instaurar la portabilidad numérica y permitió a usuarios de telefonía, especialmente celular, cambiar de compañía sin tener que cambiar su número telefónico[8][9]. Actualmente, la portabilidad numérica puede solicitarse de manera presencial o a través del sitio web de la empresa de telecomunicaciones. También se puede realizar de manera telefónica. En este contexto, la portabilidad numérica fraudulenta, conocida también como "*port-out fraud*", es un tipo de fraude en el que los delincuentes transfieren el número de teléfono de una víctima a una nueva cuenta o proveedor de servicios sin el consentimiento del titular. Esto generalmente se logra obteniendo previamente la información personal de la víctima. Con esta información, el delincuente se comunica con el nuevo proveedor de servicios y

[7] Véase https://es.linkedin.com/pulse/gu%C3%ADa-de-supervivencia-ante-robo-o-p%C3%A9rdida-tel%C3%A9fono-consorcio
[8] Biblioteca del Congreso Nacional de Chile. (2010.). Ley N°20.471. Crea Organismo implementador para la Portabilidad Numérica. Recuperado de https://www.bcn.cl/leychile/navegar?idNorma=1020620
[9] Portabilidad Numérica. (n.d.). ¿Qué es la portabilidad numérica? Recuperado de https://www.portabilidadnumerica.cl/que-es-la-portabilidad-numerica/

solicita la portabilidad del número a una nueva tarjeta SIM que controla. Una vez que la transferencia se completa, al igual que en el caso de robo o pérdida del celular, el estafador puede usar el número de teléfono para recibir mensajes de texto de verificación y llamadas, accediendo así a cuentas bancarias, correos electrónicos y otros servicios en línea de la víctima. Al lograr vulnerar las cuentas, se utiliza el dinero del afectado para comprar, transferir y hasta pagar cuentas personales[10].

La información personal de la víctima, necesaria para la portabilidad, puede ser obtenida a partir de ataques previos de *phishing* o recolección de datos, para acceder a datos personales de cada usuario, tales como su nombre, RUT, número de serie del documento de identidad, cuentas de Retail o de instituciones bancarias a las que está adscrito, redes sociales, entre otros[11].

Por otro lado, existe otro tipo de fraude con consecuencias similares, conocido como intercambio de SIM o secuestro de SIM (*SIM Swapping*). Este fraude ocurre cuando los atacantes toman el control de su número de teléfono móvil, no mediante el proceso de portabilidad, sino a través de engaños dirigidos al proveedor de telefonía celular, suplantando la identidad del titular de la línea telefónica. De este modo, logran que se genere un duplicado de la tarjeta SIM al reportar un extravío o daño del celular. Este método también permite la compra fraudulenta de teléfonos móviles, cargando la deuda a la cuenta del titular[12].

A continuación, se presentan elementos del modus operandi del fraude, recreadas a partir de los reclamos ingresados a SERNAC:

Caso 1. El reclamante indica que se percató que su teléfono celular se encontraba sin señal y se comunicó con su compañía de teléfonos. Allí le informan que se había realizado la portabilidad de su número a otra compañía. Ante ello, realiza los trámites para anular la portabilidad y hace la denuncia ante la PDI. Tiempo después, recibe el llamado de una empresa de cobranza por una deuda que mantiene por el uso de una Tarjeta de Multitienda, que ella jamás habilitó.

Caso 2. El reclamante señala que, tras sufrir una portabilidad numérica fraudulenta, robaron su documentación y con ésta lograron abrir una Tarjeta de Crédito a través de la autorización vía WhatsApp por parte de la empresa. Con la Tarjeta activada realizaron varias compras a su nombre. Al percatarse de lo sucedido, asiste a la empresa donde constata que los datos asociados a la cuenta no corresponden a los suyos.

Vulnerabilidades de las medidas de verificación de identidad en el caso de la portabilidad numérica

Desde el año 2020, diversas autoridades han alertado respecto de la proliferación de este tipo de fraudes, entre ellas la Subsecretaría de Telecomunicaciones, Subsecretaria de Prevención del Delito y PDI[13]. Actualmente, el Decreto N° 379/2010, del Ministerio

[10] Rogers (n.d.). Fraud and SIM Swaps. Recuperado de: https://about.rogers.com/stories/port-fraud-and-sim-swaps/
[11] Macquarie Bank (n.d.). How to protect yourself from a phone porting fraud. Recuperado de: https://www.macquarie.com.au/security-and-fraud/fraud/phone-porting.html
[12] Diario El Día. (2023). Nuevo caso de estafa: Denuncian suplantación de identidad para compra de teléfonos de última generación. Recuperado de https://www.diarioeldia.cl/noticias/2023/03/11/107159-nuevo-caso-de-estafa-denuncian-suplantacion-de-identidad-para-compra-de-telefonos-de-ultima-generacion.
[13] Policía de Investigaciones de Chile. (2022). Presentan plan de acción contra estafas telefónicas. Recuperado de https://www.pdichile.cl/centro-de-prensa/detalle-prensa/2022/07/26/presentan-plan-de-acci%C3%B3n-contra-estafas-

de Transporte y Telecomunicaciones, establece el reglamento que fija las obligaciones para el adecuado funcionamiento del sistema de portabilidad de números telefónicos. En este se establece que "Todo suscriptor o usuario que desee portar su número deberá requerir dicha facilidad a la Proveedora Receptora. Para este efecto, el Requirente deberá presentar su Cédula de Identidad e indicar a la Proveedora Receptora cuál es el o los números que requiere portar." "La Proveedora Receptora, antes de la activación de una solicitud de portabilidad a través del Sistema de Gestión de la Portabilidad (SGP), deberá constatar la titularidad del Suscriptor, respecto del o los números que se requiera portar. Dicha constatación deberá efectuarse solicitando al Requirente que exhiba el documento de cobro relativo a él o los números a portar que lo identifique y el RUT al cual aquél o aquéllos se encuentren asociados, o en su defecto verificando a través del SGP que el RUT tiene asociados el o los números respecto de los cuales el Requirente solicita la portabilidad. Esta verificación se hará con la Proveedora Donante a través de los mecanismos informáticos disponibles del SGP".

Sin embargo, denunciantes de este tipo de estafas sostienen que existen escasas medidas de seguridad implementadas por las empresas de telecomunicaciones. Por ejemplo, porque la portabilidad se realizó vía telefónica, donde no se comprobó la identidad del solicitante o porque no hubo una verificación de los datos personales aportados por el defraudador[14].

De acuerdo con la información web de empresa de telecomunicaciones a mayo 2024, el proceso para materializar la Portabilidad del número se explica en el **Diagrama 3**, mientras que el procedimiento para realizar el *SIM swapping* se explica en el **Diagrama 4**.

Diagrama 3: Procedimiento a través del cual se realizaría la Portabilidad Numérica Fraudulenta

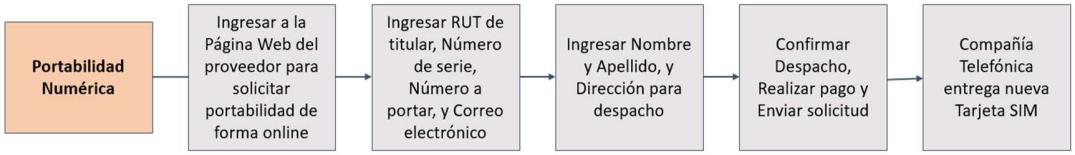
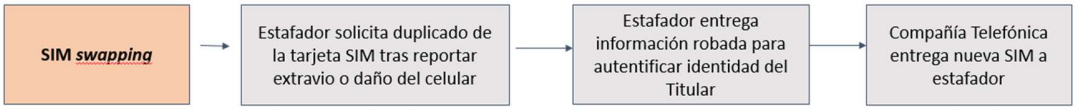


Diagrama 4: Procedimiento a través del cual se realiza la Clonación telefónica (*SIM swapping*)



Fuente: Página Web de Empresa de Telecomunicaciones.

telef%C3%B3nicas Subsecretaría de Telecomunicaciones de Chile. (n.d.). Subtel en alerta por aumento de estafas de suplantación de tarjeta SIM. Recuperado de https://www.subtel.gob.cl/subtel-en-alerta-por-aumento-de-estafas-de-suplantacion-de-tarjeta-sim/

[14] BioBioChile. (2022). Estafa en portabilidad numérica: Hombre acusa que lo cambiaron de compañía sin su autorización. Recuperado de https://www.biobiochile.cl/noticias/nacional/chile/2022/03/25/estafa-en-portabilidad-numerica-hombre-acusa-que-lo-cambiaron-de-compania-sin-su-autorizacion.shtml
Chilevisión. (n.d.). Compras millonarias y apertura de cuentas bancarias: denuncian engaños. Recuperado de https://www.chilevision.cl/noticias/nacional/compras-millonarias-y-apertura-de-cuentas-bancarias-denuncian-enganos

El Ministerio de Transportes y Telecomunicaciones, mediante la Resolución N.º 566/2024 y su modificación en la Resolución Exenta N.º 1470, fijó exigencias mínimas de verificación de identidad y estándares de seguridad que regirán desde el 4 de febrero de 2025 para todos los proveedores de telecomunicaciones en Chile.

A partir de esa fecha, para celebrar, modificar o terminar un contrato, activar tarjetas SIM o vender equipos cuyo pago se incluya en la boleta del proveedor, las empresas deberán —en cualquier canal de atención, ya sea presencial, telefónico o virtual— implementar al menos uno de los siguientes mecanismos de autenticación:

a) Solicitar la cédula de identidad del solicitante y confirmar su identidad mediante biometría de huella dactilar viva, capturando la huella y cotejándola con la registrada en el Servicio de Registro Civil e Identificación.

b) Verificar la identidad mediante biometría facial, comprobando la coincidencia entre la fotografía de la cédula y el rostro escaneado, aplicando pruebas de detección de vida y descartando intentos de suplantación con, al menos, fotos, videos, sustitución de imágenes, proyecciones de video o máscaras.

C. Fraudes asociados al uso indebido de billeteras digitales

Las billeteras digitales (también conocidas como *e-wallets*, billeteras electrónicas o monedero digital) son aplicaciones móviles que se utilizan para realizar operaciones financieras sin necesariamente tener que contar con una cuenta en un banco tradicional. Algunas billeteras permiten registrar tarjetas de crédito, debido o prepago de diferentes emisores desde una sola aplicación móvil, para ser utilizadas principalmente en compras en el comercio. En Chile, cerca del 20% de los pagos en el e-Commerce se realizan con estos dispositivos, de acuerdo a datos difundidos por Transbank[15].

Entre las billeteras digitales, existen aquellas que utilizan el proceso de 'tokenización' de tarjetas y permite que los bancos "digitalicen" una tarjeta de crédito. Esto permite pagos sin contacto en una máquina POS en un local comercial. También existen billeteras asociadas a su propio medio de pago que posibilitan comprar en comercios, recargar el celular y pagar servicios básicos, pudiendo agregar otras tarjetas de crédito o débito. Adicionalmente, se encuentra billeteras virtuales cerradas, que son únicamente de prepago, y funcionan a través de la recarga de una tarjeta de prepago, generalmente también virtual[16].

Dentro de las ventajas de las billeteras digitales se encuentra el hecho de que permite que personas no bancarizadas las usen. Además, a través de las billeteras se puede pagar de manera sencilla y rápida, por ejemplo, por medio de un código QR o vía *contactless* acercando el dispositivo a un dispositivo de pagos (POS). En concreto, los usuarios no requieren portar una tarjeta de crédito o débito física para pagar y pueden hacer transacciones en línea de forma más rápida que a través de otros medios de pagos tradicionales.

[15] Universidad de Chile. (2023). Expertos analizan los beneficios de las billeteras digitales. Recuperado de https://uchile.cl/noticias/214313/expertos-analizan-los-beneficios-de-las-billeteras-digitales-
[16] El Mercurio. (2020). Billeteras virtuales y tarjetas de prepago se multiplican en Chile con el nuevo reto digital. Recuperado de https://www.dii.uchile.cl/wp-content/uploads/2020/06/13-EL-MERCURIO-Billeteras-virtuales-y-tarjetas-de-prepago-se-multiplican-en-Chile-con-el-nuevo-reto-digital.pdf

Sin embargo, como otros medios de pago, las billeteras digitales no están exentas de vulnerabilidades, particularmente en caso de robo o pérdida del dispositivo en el cual están instaladas y técnicas de suplantación de identidad si se cuenta con información personal de la víctima. A continuación, se recrean las distintas modalidades de fraude asociados a billeteras digitales, a partir de los reclamos ingresados a SERNAC.

Caso 1. Acceso y uso indebido a partir del robo del celular.
El reclamante declara que, tras el robo del celular, el delincuente accedió a la billetera digital instalada en el dispositivo, cambiando los datos personales (correo electrónico y número de celular) y tomando el control de las cuentas bancarias asociadas a la billetera. El defraudador logró transferir dinero desde las cuentas bancarias a la billetera digital, para luego retirar los fondos a diferentes cuentas, ya que la aplicación permite realizar transferencias bancarias utilizando el número de celular.

Caso 2. Apertura Fraudulenta. *La víctima señala haber sufrido una posible filtración de datos personales, con los cuales se abrió una billetera digital a su nombre, y a través de la cual sustrajeron su dinero e hicieron compras y transferencias.*

Caso 3. Cobros no reconocidos. *La persona señala que se vulneraron los sistemas de seguridad de su billetera digital y se hicieron compras y transferencias que no reconoce haber realizado*

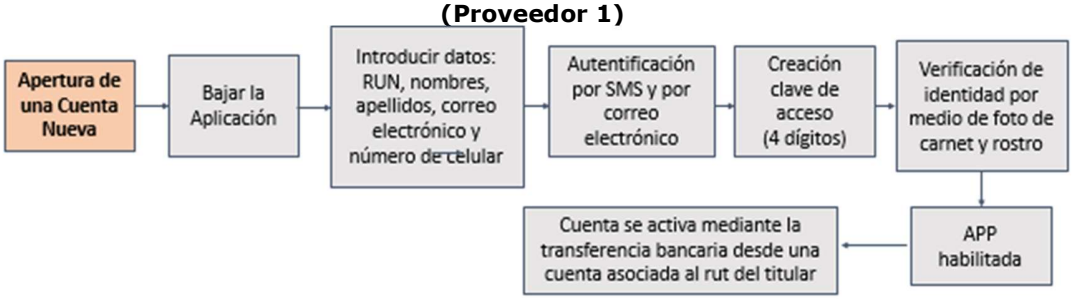
Es importante destacar que, dada la funcionalidad de las billeteras digitales, en caso de ser intervenidas de manera fraudulenta, podrían facilitar el movimiento de dinero entre las cuentas de la víctima durante el episodio de fraude y la posterior sustracción del dinero por parte del defraudador.

Proceso y vulnerabilidades en la apertura de billeteras digitales.

Considerando que el 6% (n=590) del total de reclamos analizados en la sección previa eran posibles fraudes asociados al mal uso de las billeteras digitales de la víctima, a continuación, se describen los procedimientos básicos que utilizan las billeteras digitales para poder inferir si existen posibles puntos ciegos de seguridad que faciliten este tipo de fraudes. Para este fin, se utilizó la información publicada en las páginas Web de dos proveedores, así como información recogida de la experiencia usuario como cliente oculto en las aplicaciones. Los datos proporcionados reflejan la información disponible en mayo de 2024.

En primer lugar, respecto del procedimiento de instalación y habilitación de la billetera digital, en el caso de Proveedor 1, requiere entregar información personal (como nombre, Rut, número de serie del Carnet de Identidad, correo electrónico y número celular, éstos últimos tienen un proceso de validación a través de códigos de verificación). Posteriormente se pide crear una clave de acceso de 4 dígitos y, finalmente, verificar la identidad a través de adjuntar una foto del carnet (por los dos lados) y una foto del rostro **(Diagrama 5).**

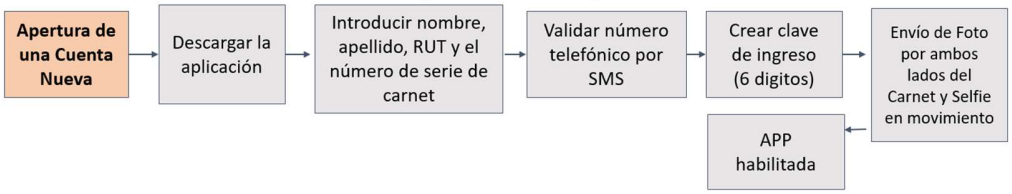
Diagrama 5. Procedimiento para instalar una cuenta nueva en una billetera digital (Proveedor 1)



Fuente: Pagina Web y aplicación de la Billetera Digital del Proveedor 1.

En tanto, en el caso del proveedor 2, el procedimiento es similar, salvo que se realiza la comprobación de identidad a través de un paso adicional que es el envío de un video de la cara en movimiento del titular y comprobación de voz. **(Diagrama 6).**

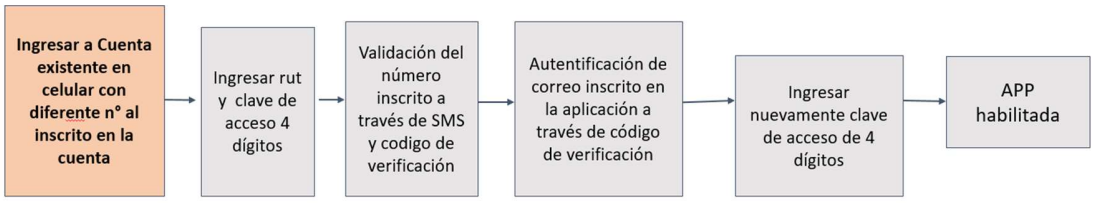
Diagrama 6. Procedimiento para instalar una cuenta nueva en una billetera digital (Proveedor 2)



Fuente: Pagina Web y aplicación de la Billetera Digital del Proveedor 2.

Por otra parte, en el caso que un estafador quisiera apropiarse de una cuenta ya existente, las cuentas asociadas a billeteras digitales tanto del proveedor 1 como del 2 pueden ser instaladas y utilizadas en celulares que tienen un número distinto al que está inscrito en la cuenta. En este caso, para acceder a la cuenta de la billetera del proveedor 1, se deben realizar validaciones con Rut, claves de acceso, verificación con el celular inscrito, a través de código de verificación enviado por SMS a ese número, validación de correo y volver a colocar la clave de acceso **(Diagrama 7).**

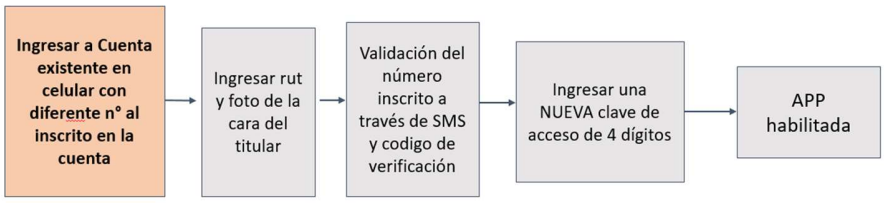
Diagrama 7: Apertura de la cuenta de Billetera Proveedor 1 en celular con diferente número al inscrito en la cuenta



Fuente: Pagina Web y aplicación de la Billetera Digital del Proveedor 1.

En el caso de billetera del proveedor 2, se ingresa el Rut, una foto de la cara del titular, validación del celular inscrito originalmente a través de código de verificación enviado por SMS a ese número y solicita crear una nueva clave (en ningún momento pide clave de acceso vigente de la cuenta) **(Diagrama 8).**

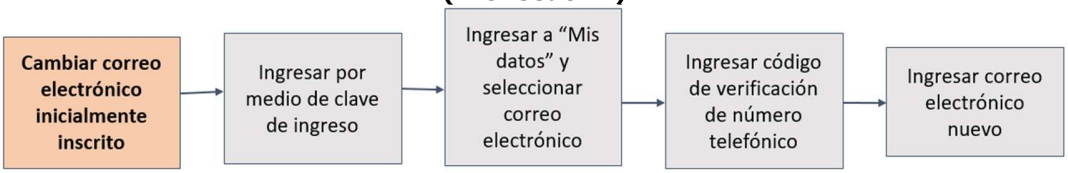
Diagrama 8: Apertura de la cuenta de Billetera Proveedor 2 en celular con diferente número al inscrito en la cuenta



Fuente: Pagina Web y aplicación de la Billetera Digital del Proveedor 2.

Adicionalmente a lo anterior, se verificaron los procedimientos para el cambio del número celular y correo inscritos al momento de inscribir la cuenta. Para aquello, el proveedor 1 requiere ingresar la clave de acceso, a través del medio de verificación alterno (ya sea mail o número de teléfono) y hacer el proceso de identificación por medio de un código de verificación **(Diagrama 9 y 10).** En el caso del proveedor 2, no es posible cambiar el número de celular inscrito en el registro inicial.

Diagrama 9: Procedimiento para cambiar correo electrónico inicialmente inscrito (Proveedor 1)



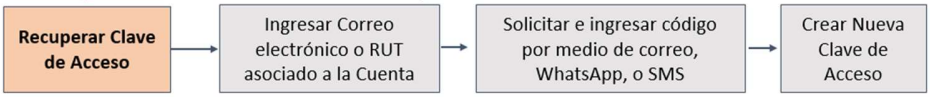
Fuente: Pagina Web y aplicación de la Billetera Digital del Proveedor 1.

Diagrama 10: Procedimiento para cambiar número telefónico inicialmente inscrito (Proveedor 1)

Fuente: Pagina Web y aplicación de la Billetera Digital del Proveedor 1.

Para cambiar la clave de acceso a la billetera, en el caso del Proveedor 1, se puede recuperar la clave a través del código de verificación que llega como SMS, al WhatsApp o al correo. Sin embargo, tanto el número como el correo son aquellos registrados en la aplicación por el titular **(Diagrama 11).**

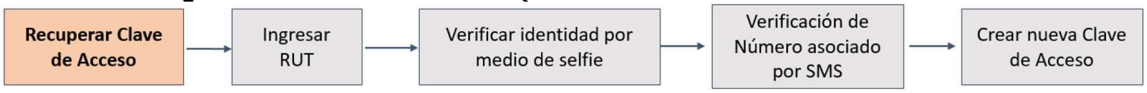
Diagrama 11: Procedimiento para cambiar la clave en Proveedor 1



Fuente: Pagina Web y aplicación de la Billetera Digital del Proveedor 1.

En el caso del proveedor 2, para recuperar clave de acceso a la billetera se puede introducir un número de teléfono distinto al registrado por el titular al inscribir la cuenta (sólo requiere que el nuevo número no esté previamente vinculado con otra cuenta del proveedor). Previo a este paso, debe haber pasado el control de seguridad con el envío de una Selfie **(Diagrama 12).**

Diagrama 12: Procedimiento para cambiar la clave en Proveedor 2



Fuente: Pagina Web y aplicación de la Billetera Digital del Proveedor 2.

En suma, las diferencias de diagramas de flujo anteriores entre proveedor 1 y 2 muestran que, en el caso que el defraudador tenga control del celular de la víctima, ya sea tras robar su celular, realizar una portación numérica fraudulenta o clonado su tarjeta SIM *(SIM Swapping*), podría acceder a estos medios de verificación para realizar estos cambios. Lo anterior, pues el correo electrónico suele estar indexado en las aplicaciones del celular y de fácil acceso para quien tiene control de éste, por lo que se contaría con estos dos medios de verificación. En efecto, se evidencia que Proveedor 1 utiliza como principal medio de verificación el número de teléfono o correos registrados por el titular, ya que, a través de estos, se podrían recuperar distintas claves utilizadas en las billeteras. Estos protocolos de seguridad podrían ser vulnerados a través del robo del celular o la portabilidad numérica fraudulenta.

D. Fraudes que involucran la apertura de productos financieros sin la autorización del titular

La suplantación de identidad y apertura de productos, conocida en la literatura de habla inglesa como "*New Account Fraud*", es un tipo de robo de identidad donde el estafador usa identidades robadas o fabricadas para abrir cuentas en nombre de otra persona. Esto puede incluir cuentas bancarias, tarjetas de crédito, préstamos, u otros productos financieros. La meta de este fraude es usualmente obtener un crédito o hacer compras bajo una identidad robada, dejando a la víctima con facturas y daño financiero potencialmente de largo plazo.

A continuación, se presentan elementos de la operatividad del fraude, recreadas a partir de los reclamos ingresados a SERNAC:

***Caso 1**. El reclamante declara haber ingresado al sitio de la CMF, donde constató que mantenía una deuda con una casa comercial, pese a que nunca había solicitado una tarjeta de crédito en esa multitienda, ni era cliente habitual. Al acercarse a la tienda a realizar el reclamo formal, pudo comprobar que los datos que fueron utilizados para abrir la Tarjeta no correspondían a los suyos (como dirección, correo y número de teléfono). Hizo la denuncia ante Carabineros, pues estima que sería un evidente caso de usurpación de identidad, que perjudicó directamente sus antecedentes financieros.*

***Caso 2**. La persona señala que suplantaron su identidad con un carnet falso y burlaron las medidas de seguridad del banco, con lo cual pudieron abrir una cuenta corriente y tarjetas a su nombre.*

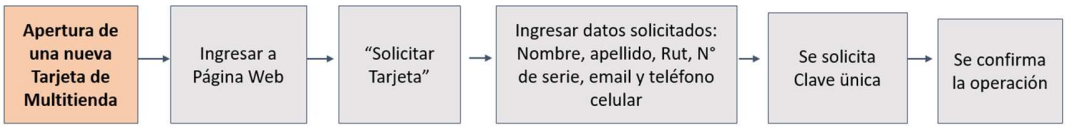
***Caso 3**. La reclamante señala que fue víctima de suplantación de identidad, estando afectado respecto de dos entidades financieras. En primer lugar, desconocidos solicitaron un avance al banco donde ella mantiene una cuenta y, posteriormente, abrieron una cuenta vista en otro banco con sus datos, donde hicieron el traspaso de dinero y lograron vaciar la cuenta. Sostiene que la primera institución dio lugar a la devolución parcial del monto defraudado, mientras que la segundo institución habría reconocido que se abrió una cuenta con una copia falsa de su carnet de identidad.*

Vulnerabilidades en la apertura de productos financieros

Considerando que el 4,5% (n=449) del total de reclamos analizados correspondían a fraudes asociados a la apertura de nuevos productos financieros sin el consentimiento del titular, y considerando que más del 50% de estos reclamos estaban asociados a productos del retail financiero, a continuación, se analiza el flujo para abrir una tarjeta de crédito en dos de estas entidades. La información se obtuvo de los sitios webs de las y de la experiencia de cliente oculto realizando la gestión de apertura.

En el caso de la Multitienda 1, el **Diagrama 13** recrea el procedimiento para la apertura de la Tarjeta a través de la página Web de la empresa. Una vez seleccionado el producto que se desea obtener, el proceso presenta 3 pasos: En la primera se solicita el nombre, apellido, Rut, número de serie, email y celular. En la segunda sección, se pide la **clave única para confirmar la identidad de la persona** y, finalmente, en la tercera etapa, se confirma la operación y se solicita la tarjeta. Es importante destacar que, en el caso que la víctima haya inscrito previamente su clave única en las oficinas del Registro Civil, tendrá una dirección de correo electrónica asociada, con la cual podrá restaurar la clave en caso de olvido. El proceso de recuperación se realiza en la página de Clave Única del Registro civil.

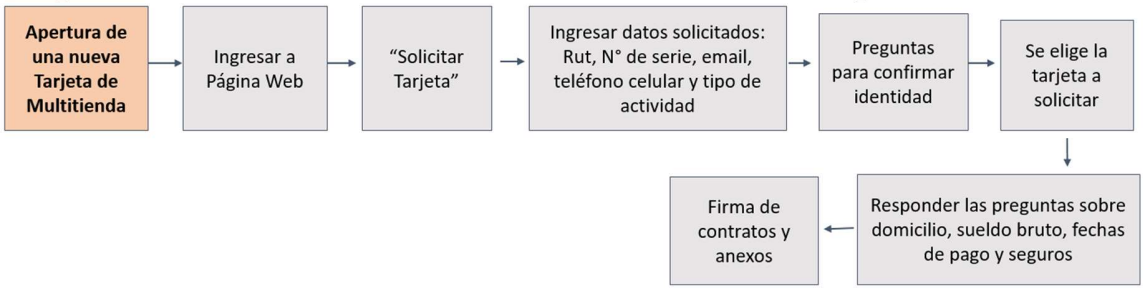
Diagrama 13: Procedimiento a través del cual se solicita una Tarjeta de Multitienda 1



Fuente: Pagina Web MultiTienda 1.

En el caso de la Multitienda 2, el **Diagrama 14** muestra el procedimiento utilizado por la compañía para la apertura de una nueva Tarjeta a través de su página Web. Al igual que en el caso anterior, una vez seleccionado el producto que se desea obtener, el proceso tiene 3 etapas: "Autenticación", "Confirmación de identidad" y "Confirmación". En la primera se solicitan RUT, N° de Serie de Carnet, número telefónico, email y tipo de actividad. En la segunda se hacen preguntas personales donde la información preguntada tiene como base Equifax y Registro Civil. Estas preguntas requieren contar con un conocimiento específico del titular y de sus familiares cercanos. Luego, se pregunta qué tarjeta se quiere solicitar, datos acerca del domicilio del solicitante, sueldo bruto, la fecha de pago de la tarjeta, si se quiere o no contratar un seguro. Finalmente, en la tercera parte se confirma la solicitud para dar lugar a la firma de los contratos y anexos.

Diagrama 14: Procedimiento a través del cual se solicita una Tarjeta de Multitienda 2



Fuente: Pagina Web MultiTienda 2.

E. Fraudes relacionados a la clonación de tarjetas u otros productos

La clonación de tarjetas utiliza técnicas como el *skimming*, que consiste en el robo de la información de las tarjetas de crédito o débito, utilizando dispositivos capaces de extraer la información de la banda magnética de la tarjeta. Cuando el usuario introduce su tarjeta en este lector, los estafadores logran extraer la información de la misma sin que el afectado sea consciente de lo que ha ocurrido. Los estafadores suelen instalar estos lectores en cajeros automáticos. En muchos casos, los estafadores también logran conocer el PIN de la tarjeta, haciendo uso de una cámara escondida en el cajero. Además, ha habido casos en los que se ha empleado un POS modificado para capturar la información de la tarjeta cuando el cliente va a pagar[17].

A la vez, existen una modalidad online de este tipo de fraude (*e-skimming* o web *skimming*), que consiste en que los estafadores, aprovechando vulnerabilidades en pequeños comercios online legítimos, acceden a la tienda y logran modificar el código de la misma. De esta forma, cuando un cliente introduce los datos de su tarjeta para realizar una compra, estará facilitando su información bancaria a los estafadores sin saberlo. El skimming representa un riesgo significativo, ya que a menudo las víctimas no detectan el fraude hasta días o incluso semanas después. Esto depende de cómo los estafadores utilicen la información robada de las tarjetas y de la frecuencia con la que la persona revise su cuenta bancaria.

Relacionado con esto, existe el fraude por prueba de tarjetas (Card Testing Fraud). En esta modalidad, los estafadores validan la operatividad de números de tarjetas de crédito robadas. Generalmente, realizan múltiples transacciones de bajo valor en diferentes sitios web. Estas pequeñas compras suelen pasar desapercibidas tanto para el titular de la tarjeta como para los sistemas de detección de fraude, que suelen enfocarse en patrones de gasto más elevados e irregulares. El objetivo de estas transacciones de prueba es determinar si la tarjeta sigue activa y si no ha sido reportada como robada, bloqueada o cancelada[18].

[17] Xataka Móvil. (n.d.). ¿Qué es el skimming y cómo puedes evitar que dupliquen tu tarjeta con este método? Recuperado de https://www.xatakamovil.com/seguridad/que-skimming-como-puedes-evitar-que-dupliquen-tu-tarjeta-este-metodo
[18] Stripe. (n.d.). ¿Qué es el fraude de pruebas de tarjetas? Aquí te mostramos cómo puedes proteger tu negocio. Recuperado de https://stripe.com/es-us/resources/more/what-is-card-testing-fraud-heres-how-you-can-protect-your-business

IV. Autentificación Reforzada de Identidad y Protección de datos personales

Como se mencionó previamente, algunos fraudes ocurren por la debilidad en los controles de autentificación de la identidad de los consumidores por parte de los proveedores financieros. Ante esto, la regulación ha avanzado en dos frentes clave: promover una autentificación de identidad más robusta y, a la vez, regular la protección y el tratamiento de los datos personales.

El 14 de abril de 2025, la Comisión para el Mercado Financiero (CMF) sometió a consulta pública un proyecto de Norma de Carácter General que impone estándares mínimos de seguridad, registro y autenticación a emisores de medios de pago y prestadores de servicios financieros (CMF, 2025).

En esta norma se establecerían directrices respecto a la autenticación reforzada del cliente (conocida en inglés como *Strong Customer Authentication* o SCA), que es un procedimiento basado en la utilización de al menos dos factores de autenticación independientes y diferentes entre sí (de dos categorías diferentes), lo que significa que la vulneración de uno no compromete la fiabilidad de los demás. Además, debe estar diseñada de tal manera que proteja la confidencialidad de los datos de autentificación (Gurrea et al., 2020).

Los factores de autenticación pertenecen a las siguientes categorías:

- Conocimiento: Algo que solo el usuario conoce (por ejemplo, contraseñas o números de identificación personal o PIN).
- Posesión: Algo que solo el usuario posee (por ejemplo, un dispositivo token o un mensaje enviado a un dispositivo confiable previamente registrado).
- Inherencia: Algo que el usuario es (por ejemplo, biometría facial, huella dactilar, o datos biométricos conductuales, tales como ritmo de tecleo o dinámica de uso del dispositivo).

De igual modo, la Ley 21.521 ("Ley Fintech") y sus normas técnicas de 2024 —la NCG 502 y la regulación del Sistema de Finanzas Abiertas— refuerzan los requisitos de KYC[19] y autenticación multifactor para los prestadores de servicios Fintech, incluidos los iniciadores de pago y custodios de fondos (Carey, 2024). Aunque la normativa no impone un método biométrico concreto, muchos actores del mercado —por ejemplo, Mercado Pago y MACH— han actualizado entre 2024 y 2025 sus flujos de *onboarding*[20] incorporando verificación de documento y selfie con detección de vida. Apple Pay, por su parte, utiliza Face ID o Touch ID como factor biométrico en el dispositivo, mientras el KYC inicial recae en el banco emisor de la tarjeta (Apple, 2025; Mercado Libre, s.f.; Martel, 2024).

Adicional a estas normativas, la Resolución Exenta Nº 566/2024 de Subtel —vigente desde el 4 de febrero de 2025— obliga a las empresas de telecomunicaciones a verificar la identidad de los usuarios en cualquier trámite que cree o modifique un servicio (portabilidad, contratación, cambios de plan, activación de SIM, etc.) mediante al menos

[19] KYC, o "Know Your Customer" (Conoce a Tu Cliente), es un proceso esencial que las instituciones financieras y otras entidades reguladas emplean para verificar la identidad de sus clientes. Su propósito principal es combatir actividades ilícitas y el fraude. El proceso de KYC generalmente implica: Verificación de identidad, Comprender la naturaleza de la relación, Monitoreo continuo.

[20] "Onboarding" se refiere al proceso de incorporación de un nuevo cliente a un servicio o plataforma. Es el conjunto de pasos que una persona debe seguir para registrarse y empezar a usar algo.

uno de estos métodos: (i) huella dactilar viva contrastada con información del Registro Civil; (ii) biometría facial con prueba de vida cotejada con la fotografía del documento; o (iii) firma electrónica avanzada (SUBTEL, 2025).

Por otra parte, la Ley N° 21.719, promulgada el 25 de noviembre de 2024 y publicada el 13 de diciembre de 2024, regula la protección y el tratamiento de los datos personales en Chile, y crea la Agencia de Protección de Datos Personales. Sus modificaciones entrarán en vigencia el 1 de diciembre de 2026. Esta ley tiene como objetivo principal regular las condiciones para el tratamiento y la protección de los datos personales de personas naturales. Su aplicación abarca todo tratamiento de datos personales, ya sea realizado por una persona natural, jurídica o un organismo público. A la vez, la ley crea la Agencia de Protección de Datos Personales como una corporación autónoma de derecho público, técnica y descentralizada. Su misión es velar por la efectiva protección de los derechos relacionados con los datos personales y fiscalizar el cumplimiento de la ley.

Finalmente, en abril de 2024, Chile promulgó la Ley Marco de Ciberseguridad (Ley 21.663), un avance legislativo fundamental para salvaguardar la infraestructura digital del país ante el creciente panorama de amenazas cibernéticas. Esta normativa establece un marco integral de protección frente a ataques cada vez más frecuentes y sofisticados. La Ley impacta directamente a organismos públicos, empresas privadas consideradas operadores de servicios esenciales y operadores de importancia vital, así como a toda organización que gestione infraestructura crítica. Adicionalmente, la ley formaliza la creación de la Agencia Nacional de Ciberseguridad (ANCI), que asumirá el rol de entidad fiscalizadora en esta materia.

En este contexto, es importante destacar que, ante estos nuevos estándares de autentificación, la protección de los datos biométricos de las personas adquiere una importancia crítica. A diferencia de una contraseña que puede modificarse tras una filtración, el rostro u otros elementos biométricos no se pueden "cambiar". Si estos datos son capturados o la base que los almacena es vulnerada, el riesgo es permanente. Una vez expuestos, estos registros pueden habilitar suplantaciones de identidad y otros usos ilícitos que **comprometen de forma irreparable la identidad y seguridad de los clientes** (Jans, 2024; Nicoletti, 2021; Politou, et al., 2022).

A continuación, se detallan los principales riesgos asociados a la identificación biométrica, seguidos de una serie de recomendaciones y estrategias propuestas por especialistas y organismos internacionales para mitigar dichos riesgos:

i. <u>Ataques Potenciados por IA</u>

- <u>Vulnerando la biometría</u>: La IA es capaz de engañar los sistemas biométricos estándar utilizando huellas dactilares sintéticas, imágenes faciales manipuladas en 3D o máscaras sofisticadas (Xu, 2022).
- <u>*Deepfakes*</u>[21] <u>y suplantación de identidad</u>: Los *deepfakes son una amenaza creciente. Hacen que la identidad de un atacante sea indisti*nguible de la de una persona real, aumentando significativamente la probabilidad de que alguien responda erróneamente a una amenaza (Engemann & Witty, 2024).

[21] Los deepfakes son creaciones de medios sintéticos (videos, audios o imágenes) que han sido manipuladas digitalmente utilizando inteligencia artificial (IA). El objetivo principal de un deepfake es hacer que una persona parezca decir o hacer algo que en realidad nunca dijo o hizo. La clave de los deepfakes es su realismo convincente, que puede hacer que sea extremadamente difícil distinguir entre el contenido real y el falso, incluso para el ojo humano entrenado.

- Bots con comportamiento humano: Los bots, software automatizado que realiza tareas repetitivas, están siendo diseñados con una sofisticación creciente para imitar el comportamiento humano. Esto incluye replicar características como la vacilación y respuestas más lentas. Como resultado, los intentos de apropiación de cuentas online (ATO) se vuelven mucho más sutiles y difíciles de detectar al analizar patrones de comportamiento amplios (Saporta & Maraney, 2022).
- Manipulación emocional: Los algoritmos de IA son cada vez más convincentes al replicar las peculiaridades de las emociones humanas en la escritura. Esta capacidad podría usarse para manipular a las personas de formas muy efectivas (Gurrea & Remolina, 2020).

ii. Desafíos en la Precisión de los Sistemas Biométricos

La precisión de los sistemas biométricos puede variar significativamente debido a diversos factores. Condiciones como la iluminación deficiente, ángulos extremos, la edad del usuario, el vello facial o el uso de accesorios pueden incrementar tanto los falsos positivos (permitiendo el acceso a impostores) como los falsos negativos (bloqueando a usuarios legítimos) (Xu, 2022; Sherif, 2016; Allums, 2014; Vacca, 2007).
La fiabilidad de estos sistemas depende en gran medida de la calidad de la cámara. Mientras que las aplicaciones comunes pueden funcionar con el sensor RGB estándar de un teléfono, los entornos de alto riesgo exigen sensores infrarrojos o de profundidad. Estos últimos, aunque considerablemente más costosos, son esenciales para reforzar la detección de vida y la resistencia a la suplantación (Brooks, 2018; Jans, 2024).

iii. Riesgos de Compromiso y Robo de Datos Biométricos

El uso creciente de la biometría conlleva riesgos significativos, principalmente el robo masivo de características biométricas desde bases de datos centrales. A diferencia de las contraseñas o tokens, los autenticadores biométricos robados son extremadamente difíciles de revocar o reemplazar (FATF, 2020). Si estas bases de datos son comprometidas, las identidades de los clientes podrían ser usadas con fines maliciosos, y dado que una persona "solo tiene una huella dactilar o una cara", el daño potencial es casi irreparable (CPMI & World Bank Group, 2020; Wirtz & Lovelock, 2016).

Para robustecer la seguridad biométrica, se promueven las siguientes recomendaciones y estrategias:

a. Detección de vida (*liveness detection*)

Es la primera y más crucial barrera en la seguridad biométrica. Esta técnica integra el análisis de video en tiempo real, iluminación multiespectral y la lectura de microseñales fisiológicas (pulso, flujo sanguíneo y temperatura). Además, incorpora desafíos activos como parpadeos, sonrisas o movimientos de cabeza. A esto se suma la detección de vida pasiva, basada en *deep learning*. Esta tecnología puede identificar patrones imperceptibles para el ojo humano y ya está integrada en SDKs comerciales (Fang, 2025; Kimery, 2024; Burt, 2025; Jadhav, 2024; Crouse, 2024; FATF, 2020; Rathgeb & Busch, 2017; Drahansky, 2018; Jain, 2011; Scharcanski, 2014).

b. La Necesidad de Enfoques Robustos y Combinados:

Los sistemas biométricos multimodales también ofrecen una capa adicional de seguridad. Estos utilizan múltiples características biométricas —como huella dactilar, voz o patrón de movimiento— o combinan sus resultados, aumentando significativamente la precisión general del sistema y dificultando la falsificación de una identidad (Vacca, 2007).

Para una seguridad aún mayor, se recomienda un enfoque de "autenticación trifactorial". Esta combina "algo que tienes" (como un token), "algo que sabes" (una contraseña) y "algo que eres" (biometría), creando una barrera mucho más difícil de superar (Vacca, 2007).

c. Cifrado y Aislamiento de Plantillas en Hardware Seguro

Proteger las plantillas biométricas o de autenticación mediante cifrado y aislamiento en hardware seguro es una estrategia fundamental para mitigar una amplia gama de ataques. El objetivo principal es salvaguardar la confidencialidad e integridad de estos datos críticos frente a la interceptación, manipulación o acceso no autorizado (Sherif, 2016).

- Cifrado de Plantillas: El cifrado es el proceso de codificar datos, transformándolos para su seguridad y protegiéndolos de accesos no autorizados. La criptografía de clave pública juega un papel esencial aquí: una clave privada cifra el mensaje, y solo su clave pública correspondiente puede descifrarlo. (Gurrea & Remolina, 2020).
- Aislamiento en Hardware Seguro: El aislamiento implica proteger las plantillas y las operaciones criptográficas dentro de componentes de hardware diseñados específicamente para ser resistentes a la manipulación y el acceso no autorizado. Esta capa de seguridad es importante para salvaguardar los activos de hardware y los dispositivos contra el robo, el daño o el acceso no autorizado (Kosseff, 2020).

d. Defensa en Profundidad con IA, Inteligencia de Amenazas y Respuesta Orquestada

Para una seguridad robusta, es esencial una defensa en profundidad que integre analítica de Inteligencia Artificial (IA), inteligencia de amenazas y una respuesta orquestada. Este enfoque multicapa asume que ninguna defensa es infalible por sí sola, buscando diversificar los métodos de protección para reducir el riesgo de manera integral. Consiste en una serie de controles de seguridad superpuestos y complementarios que cubren sistemas, datos y comunicaciones, e incluyen mecanismos de detección y prevención de ataques. Los sistemas de control internos son fundamentales, estableciendo reglas y procesos para la gestión de riesgos y la salvaguarda de activos (Zhao & Zhang, 2021; Nadotti et al., 2022).

Integración de la Analítica de IA

La IA y el aprendizaje automático (ML) son herramientas transformadoras en la gestión de riesgos y seguridad (Gurrea & Remolina, 2020; Nadotti et al., 2022). Su integración en una defensa en profundidad permite integridad:

- Evaluación y Protección**:** Identifican las mejores formas de proteger sistemas, datos y clientes, valorando el patrimonio informativo como ventaja competitiva.
- Análisis y Detección de Patrones: Analizan el comportamiento de empleados y clientes, sus redes de relaciones y comunicaciones para identificar patrones sospechosos, transacciones fraudulentas o mala conducta.
- Identificación de Anomalías y Predicción: Descubren patrones ocultos y correlaciones, calculan resultados probables y evalúan riesgos, incluso prediciendo delitos o resultados judiciales.
- Mejora de la Eficiencia Operativa: Examinan volúmenes de documentos más rápido que los humanos, detectan tendencias y optimizan procesos como la *due diligence*.

Sin embargo, es crucial abordar la "caja negra" de los algoritmos de IA, reforzando la prevención de riesgos operativos y de seguridad mediante la interpretabilidad de sus decisiones para evitar problemas de cumplimiento.

Inteligencia de Amenazas
La inteligencia de amenazas, nutrida por la analítica de IA, permite un proceso dinámico y continuo de identificación y mitigación de riesgos (Gurrea & Remolina, 2020; Nadotti et al., 2022). Esto implica:

- Monitoreo Continuo y Verificación Estricta: Un monitoreo constante y una verificación rigurosa para mejorar la robustez y seguridad de la IA, priorizando controles organizativos y sistemas de gobierno fiables.
- Prevención y Adaptación: Planificación de un "modo de confrontación" para el mantenimiento, verificación y prevención de ataques, con algoritmos capaces de adaptarse a las "peculiaridades" del mercado.
- Identificación Proactiva de Riesgos: Anticipación a situaciones de crisis mediante una identificación cuidadosa de los riesgos operativos y de mercado, detectando tempranamente señales de anomalía potencial.

Respuesta Orquestada
Una vez detectada una amenaza, una respuesta orquestada implica la coordinación y ejecución de acciones predefinidas o adaptativas para mitigar el riesgo (Gurrea & Remolina, 2020; Nadotti et al., 2022). Esto se logra mediante:

- Gestión y Mitigación de Riesgos: Definición de estrategias operativas para mantener el riesgo dentro de los límites de la "propensión al riesgo" (Risk Appetite Framework - RAF), salvaguardando activos y asegurando la eficacia de los procesos.
- Automatización y Asistencia en Decisiones: La IA amplía la capacidad de trabajo, automatizando tareas rutinarias y liberando a los profesionales para actividades de alto valor añadido, como clasificar documentos o recomendar argumentos clave en el ámbito legal, apoyando la toma de decisiones estratégicas.
- Coordinación y Robustez del Sistema: La necesidad de una coordinación eficaz entre equipos de seguridad y la implementación de una autenticación multifactorial (como la biometría respaldada por factores independientes) aseguran que múltiples factores de seguridad trabajen de forma sinérgica para proteger la información y reducir la vulnerabilidad general del sistema.

e. Marcos Regulatorios y Éticos para la Biometría y la IA

La implementación de la autenticación multifactor (MFA) con biometría se debería desarrollar en un entorno regulatorio dinámico. Esto exigiría una estrecha coordinación entre las autoridades financieras, de protección de datos, privacidad, fiscalización y prevención del blanqueo de capitales. Por lo mismo, se recomienda adoptar un enfoque regulatorio basado en riesgos, principios y actividades, en lugar de uno centrado únicamente en licencias por tipo de entidad. Esta flexibilidad permite una mayor adaptabilidad ante las tecnologías emergentes (Gurrea & Remolina, 2020).
La regulación de los robo-advisors —sistemas que también procesan grandes volúmenes de datos de clientes— resalta la necesidad de mayor control, supervisión y auditorías periódicas para fortalecer la resiliencia del mercado. Finalmente, se sugiere la capacitación continua a usuarios y equipos antifraude y la creación de comités de ética dentro de las organizaciones que integren IA, reconociendo que estos sistemas, aunque emulan funciones humanas, carecen de voluntad, intuición, acervo cultural o moral (Gurrea & Remolina, 2020).

En resumen, de acuerdo a la literatura consultada, para enfrentar los riesgos emergentes de la biometría, es fundamental fortalecer estos cinco pilares mencionados. Solo la convergencia de tecnología avanzada, procesos maduros y una regulación exigente permitiría que la autenticación facial se consolide como una defensa robusta contra el fraude, sin sacrificar la confianza del usuario ni su derecho a la privacidad (Gurrea & Remolina, 2020; Cendrowski et al., 2007; Vacca, 2007).

Lo anterior cobra aún más urgencia, dado los datos más recientes de ataques de ciberseguridad:

Según la encuesta *Deepfake Trends 2024* de Regula[22], en 2024, una de cada dos empresas a nivel mundial reportó incidentes de fraude *deepfake*, lo que revela una tendencia creciente en los delitos relacionados con IA en los últimos dos años. Específicamente, el 49 % de las empresas ya ha sufrido ataques de audio o vídeo falsificados (Regula, 2024).

En el sector financiero, el informe *Battle Against AI-Driven Identity Fraud* de Signicat[23] calcula que 42,5% de los intentos de fraude utilizan IA generativa y 29% resultan exitosos. El documento examina la evolución reciente del fraude de identidad alimentado por inteligencia artificial (IA) y concluye que, pese a la creciente conciencia del problema, las organizaciones siguen mostrando confusión y una respuesta insuficiente. El estudio advierte que nos encontramos ante un punto de inflexión: la amenaza se intensifica más rápido de lo que las defensas se adaptan. (Signicat, 2024).

Sumsub[24] publicó su informe *State of the Crypto Industry* 2025, cuyos datos revelan que el fraude en el sector de las criptomonedas ha aumentado un 48%, lo que representa ahora el 2.2% de todas las verificaciones en las plataformas de criptomonedas a escala mundial. Este aumento pone de relieve la necesidad de que las empresas adopten la detección basada en IA, la biometría y la supervisión continua para mejorar la seguridad. A la vez, el análisis interno de Sumsub —a partir de millones de verificaciones entre el 1T-2023 y el 1T-2024— confirma que los *deepfakes* ya son una de las técnicas de suplantación con mayor crecimiento a escala mundial, motivo por el cual la empresa los trata como un vector de fraude de identidad prioritario. Los deepfakes representan hoy el 7 % de todos los intentos de fraude y su volumen se multiplicó por cuatro entre 2023 y 2024 (Kimery, 2025; Revista Más Seguridad, 2024).

[22] Regula es un desarrollador global de dispositivos forenses y soluciones de verificación de identidad. Su encuesta "Deepfake Trends 2024" recopila datos de empresas de diversas industrias para entender el impacto y la prevalencia del fraude con deepfakes.
[23] Signicat es un proveedor líder de soluciones de identidad digital, que atiende principalmente a la industria de servicios financieros regulados en toda Europa y con alcance global. El informe "Battle Against AI-Driven Identity Fraud" aborda amenazas emergentes en el espacio de la identidad digital.
[24] Sumsub es una plataforma global de verificación de ciclo completo. El informe "State of the Crypto Industry 2025", proporciona un análisis y datos sobre las tendencias del fraude.

V. Campañas de Prevención del Fraude.

Con las recientes modificaciones a la Ley N°20.009 se estableció que los usuarios deberán informarse y adoptar todas las medidas necesarias para prevenir el uso indebido, el fraude u otros riesgos afines a la utilización de los medios de pago a que se refiere esta ley y los mecanismos de autenticación asociados. Para estos efectos, las entidades reguladas por esta ley deberán proporcionar, de manera periódica, clara, accesible y actualizada, toda la información necesaria sobre las medidas de seguridad y las instrucciones de uso seguro a sus usuarios, promoviendo las prácticas responsables en el manejo de los medios de pago.

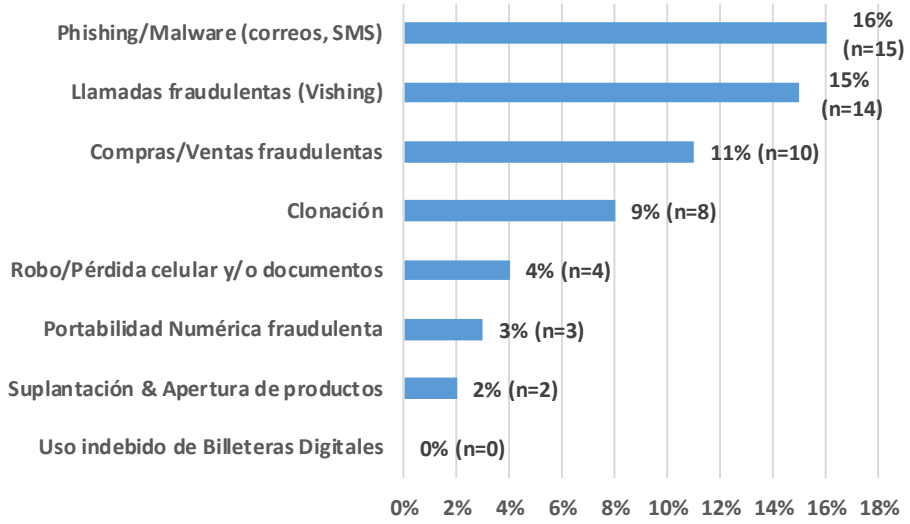
En la actualidad, el medio que tienen las personas para informarse es a través de las campañas de seguridad promovidas por instituciones financieras y reguladores. En este contexto se analizaron las campañas de prevención del fraude que publicaron las instituciones financieras en sus sitios web, durante los meses de abril y mayo del 2024. En particular, se analizaron los sitios web de 91 proveedores financieros. A la vez, se evaluó si hacían referencia de manera explícita a las distintas modalidades de fraudes analizadas en la sección anterior.

Se constató que sólo el 18% de las instituciones (n=16), mantenía alguna campaña disponible en su página web (no se consideraron otros medios como envío de infografías a través de correos electrónicos ni en redes sociales, ni se consideraron las campañas en formato video, sólo se consideraron textos). A la vez, se constata que las campañas más frecuentes son aquellas asociadas a episodios de *phishing*, mientras que otros tipos de fraude está ausente en las campañas de ciberseguridad de las instituciones analizadas **(Gráfico 26).**

Adicionalmente, respecto al contenido de las campañas sobre *Phishing*, se sistematizó el tipo de información entregado, distinguiendo si éste contenía una conceptualización del tipo de fraude, su modus operandi, potenciales consecuencias, consejos sobre cómo reconocerlo, pasos a seguir en caso de exposición al fraude, técnicas preventivas y ejemplos concretos de cómo opera el fraude. Se detectó que, en cuanto a *Phishing* perpetuado a través de correos y SMS, más del 80% de las campañas presentaba, de manera completa o parcial, información relativa al tipo de fraude, cómo reconocerlo y qué hacer de manera preventiva. El 25% explicaba el modus operandi en detalle, pero muy pocas mencionan las consecuencias que podrían tener las personas en caso de caer en el fraude, qué tenían que hacer en caso de caer en este tipo de estafas y la gran mayoría no entregaba ejemplos concretos de correos o SMS fraudulentos (**Gráfico 27**).

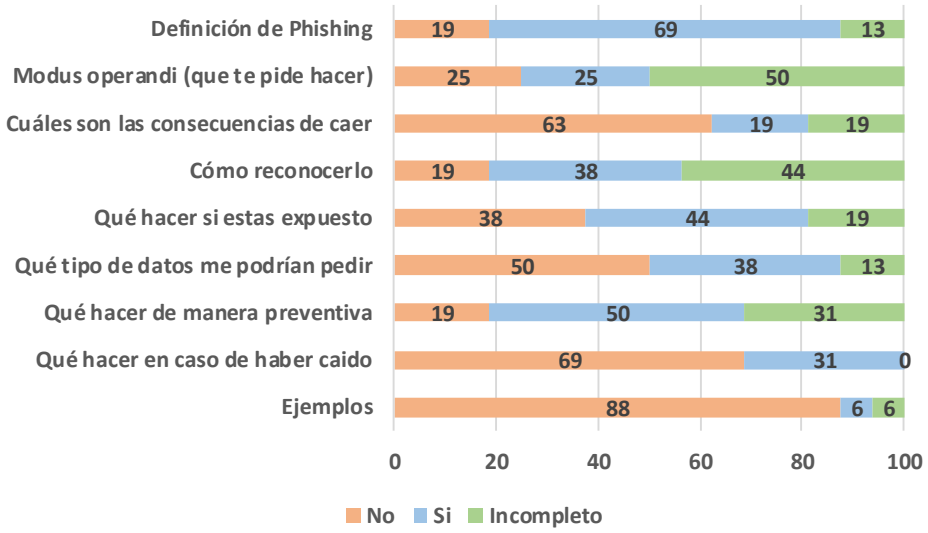
Por otra parte, se evidenció que las campañas de concientización no suelen transparentar que los estafadores pueden manejar información personal detallada de la víctima (nombre, RUT, número de cuenta, saldos, movimientos, productos bancarios, nombre de ejecutivos). Esta situación facilita el engaño y genera en la víctima una falsa sensación de estar interactuando con su banco, lo que sugiere una brecha entre la percepción de seguridad y una posible vulneración de datos bancarios.

Gráfico 26: Número de Campañas por Tipologías de Fraude



Fuente: Elaboración propia en base a campañas de ciberseguridad analizadas en páginas Web de proveedores mencionados en reclamos relacionados a Fraudes de medios de pagos.

Gráfico 27: Contenido de las Campañas de Phishing (%)



Fuente: Elaboración propia en base a campañas de ciberseguridad analizadas

Lo anterior es particularmente importante, debido a que los consumidores pueden no entender los alcances o instrucciones que imparten las campañas. Por ejemplo, se ha enfatizado la importancia de transmitir a los consumidores el mensaje "nunca des tus claves ni contraseñas". Aunque este es un mensaje relevante, extractos de los reclamos ingresados al SERNAC durante el 2023 dan cuenta de que existe el riesgo de que se interprete restrictivamente y las personas terminen revelando datos sensibles (ej., códigos de verificación, datos de tarjeta) ya sea porque no los perciben como una "clave personal" o porque creen estar seguros al digitar la clave en el teclado del teléfono:

Respecto al mensaje de campaña del tipo: "Nunca des tus claves ni contraseñas":
"…me indicó que ingresara un código que él me dio (no era clave personal)…"
"…cabe señalar que di información pero nunca di mis claves…"
"…me solicitaron los datos de la tarjeta, los entregué pero no así claves, confiando plenamente en la información entregada y me habló con tal seguridad no pensé que era una estafa , ya que tenía todo mis datos personales…"
"…ingresé en mi aplicación y autoricé un link… debo recalcar que yo no entregué ningún tipo de información por teléfono…"
"…me pidió digitar mi clave de la aplicación para cancelar las compras que estarían retenidas…"
Respecto al mensaje de campaña del tipo: "No entregar datos personales, bancarios o contraseñas solicitados por medios informales":
"…me pidieron anular las 4 compras que fueron ejecutadas, en donde fueron anulando una compra a la vez, y cada vez que se anulaba se pasaba a una grabación del banco , en donde la grabación decía ingrese dígito ej. e5, d4, d2, y debía eliminar las compras…"
"…también me indicó que ellos no pedirían mi clave de internet y que solo tendría que validar las anulaciones con la app del banco. Se hicieron varias anulaciones…"
"…ingresé en mi aplicación y autoricé un link… debo recalcar que yo no entregué ningún tipo de información por teléfono…"
"…me solicitó solamente digitar en mi teléfono la clave de la aplicación, no me solicitó ningún otro dato, por lo que no sospeché de nada raro ya que tenían todos mis datos personales…"
"...informando una supuesta devolución de cobros excesivos de mantenciones hacia la cuenta bancaria, esta persona me indico que para validar el proceso debía digitar en el teclado de mi teléfono el código de seguridad (token)…"
Respecto al mensaje de campaña del tipo: "Recuerda que las estafas telefónicas son realizadas por personas con habilidad para obtener tus datos personales":
"…yo en ningún momento dudé que era un ejecutivo ya que manejaba todos mis datos personales…"
"…se identificó como ejecutivo del banco en quien confié ya que conocía todos mis datos que debía resguardar dicho banco…"
"…manejaba mucha información mía, tales como: nombre, Rut, número de cuenta, tipo de cuenta, nombre de mi ejecutiva bancaria…"
"…la página ya estaba siendo vulnerada porque la persona que me hablaba conocía toda la información que contiene, incluido el saldo exacto de mi cuenta Rut y ahorro a plazo de vivienda…"
"…el banco está incumpliendo con la privacidad de sus datos, no puede ser posible que ellos tengan información tan detallada con respecto a mis cuentas, montos y accesos. ya que la información que me dieron era la misma que yo veía en línea en mi aplicación…"
"…tenía detalles de mis cuentas, movimientos, montos, valores, solo información que tiene el banco " "... ¿cómo es posible que ellos accedieran a todos mis datos personales si no es a través del banco"
"…todo era confiable ya que tenían todos los numero de mi cuenta y tarjeta…"
"…confirmaron todos los datos conmigo incluyendo el número de tarjeta coordenada en el cual me sentí segura porque el banco y yo somos los únicos que tenemos dicha información…"
"…vulneraron la seguridad del banco ya que indicaron los productos que yo tenía y los cupos de las tarjetas, información que solo la manejan ustedes, por eso yo confié, y la transacción que había realizado yo el día anterior, entonces como no creerles…"

VI. Conclusiones

El presente informe sobre el fraude en medios de pago en Chile subraya la importancia crítica de abordar y mitigar las diversas formas de fraude que afectan a los consumidores. El fraude financiero, especialmente en el entorno digital, representa una amenaza significativa para la seguridad y la confianza de los consumidores. En un contexto global donde la inseguridad cibernética se posiciona como uno de los principales riesgos, Chile no es la excepción. El incremento de los reclamos y los montos involucrados en fraudes financieros reflejan una tendencia alarmante que demanda acciones coordinadas y efectivas por parte de las instituciones financieras y los reguladores.

El análisis cuantitativo y cualitativo de 9.899 reclamos en materia de fraude ingresados por los consumidores al SERNAC durante el año 2023, ha permitido identificar tipologías o *modus operandi* del fraude en medios de pagos, conforme a la descripción provista por los consumidores, y explorar las eventuales vulnerabilidades de seguridad que facilitan la ocurrencia de estos fraudes. Este análisis ha permitido identificar la relevancia del phishing, en sus distintas formas, y la suplantación de identidad, como riesgos de fraude financiero relevantes de ser prevenidos. A la vez, el análisis identifica varias vulnerabilidades explotadas por los delincuentes, como la falta de medidas robustas de verificación de identidad.

En este contexto, la regulación local está avanzando para fortalecer los mecanismos de autenticación reforzada y protección de datos personales. Sin embargo, estas medidas, si no se implementan y supervisan con rigor, corren el riesgo de ser superadas por la creciente sofisticación de los ataques impulsados por inteligencia artificial.

La adopción de autenticación biométrica introduce nuevos desafíos críticos, pues a diferencia de las contraseñas, los datos biométricos como el rostro o la huella dactilar no pueden cambiarse. **Si estos datos biométricos son comprometidos o sus bases de almacenamiento vulneradas, el riesgo de suplantación de identidad y otros usos ilícitos es permanente e irreparable.**

Aunque la biometría ofrece mayor seguridad que los métodos tradicionales, la literatura especializada destaca riesgos significativos. Entre ellos, los ataques potenciados por IA permiten la suplantación de la biometría con huellas sintéticas o imágenes manipuladas, y los deepfakes generan identidades falsas indistinguibles de las reales, aumentando la probabilidad de engaño. Asimismo, los bots con comportamiento humano y la manipulación emocional por IA hacen los intentos de fraude más sutiles y difíciles de detectar. Sumado a esto, el robo masivo de datos biométricos de bases de datos centrales y los desafíos en la precisión de los sistemas (por condiciones como iluminación o vello facial) son vulnerabilidades que deben ser mitigadas.

Para contrarrestar estos riesgos, es esencial una estrategia de seguridad robusta y multifacética. Esto implica reforzar la detección de vida (*liveness detection*) en hardware y software, que integra análisis en tiempo real y *deep learning* para identificar patrones imperceptibles. Además, es recomendable implementar sistemas biométricos multimodales y una autenticación trifactorial que combine biometría con "algo que se tiene" y "algo que se sabe" para una mayor precisión y resistencia a la falsificación. La protección de datos biométricos se refuerza mediante el cifrado y el aislamiento de plantillas en hardware seguro, utilizando criptografía de clave pública y una gestión impecable de claves). Finalmente, se requiere una defensa en profundidad que integre

la analítica de IA, la inteligencia de amenazas y una respuesta orquestada para detectar patrones sospechosos y anticipar riesgos, todo bajo marcos regulatorios proactivos y una gobernanza sólida. La urgencia de estas medidas se subraya por el aumento global del fraude con IA y deepfakes, que ya afectan a casi la mitad de las empresas y representan un creciente porcentaje de los intentos de fraude financiero.

En este escenario, se subraya aún más la necesidad de fortalecer las medidas de seguridad y perfeccionar los mecanismos de educación a los consumidores. Las instituciones financieras deben adoptar prácticas proactivas para proteger a sus usuarios y colaborar estrechamente con los reguladores para implementar políticas efectivas. Solo a través de un enfoque integrado y coordinado será posible mitigar los riesgos de fraude y proteger la integridad del ecosistema financiero en Chile.

La reciente reforma a la Ley 20.009, sobre limitación a la responsabilidad de los usuarios de medios de pago, incorporó el deber de los usuarios de informarse y adoptar todas las medidas necesarias para prevenir el uso indebido, el fraude u otros riesgos afines a la utilización de los medios de pago y los mecanismos de autenticación asociados. Asimismo, la reforma legal incorporó el deber de las entidades emisoras de proporcionar, de manera periódica, clara, accesible y actualizada, toda la información necesaria sobre las medidas de seguridad y las instrucciones de uso seguro a sus usuarios, promoviendo las prácticas responsables en el manejo de los medios de pago. En ese contexto, es conveniente que las campañas de educación y prevención del fraude tengan directa relación con las experiencias de fraude sufridas en el país por los consumidores, como las descritas en el presente informe.

Por lo tanto, en base a los hallazgos anteriores, es posible formular las siguientes recomendaciones:

1. Se recomienda que las campañas de prevención del fraude cubran una variedad más amplia de fraudes, no limitándose únicamente a los casos de phishing. Es también aconsejable medir la efectividad de estas campañas en cuanto a su capacidad para captar la atención de los usuarios, utilizando diversos formatos como texto, video, audio e infografías. Además, estas deben incluir información variada, como la definición del tipo de fraude, su modus operandi, indicadores para su reconocimiento, acciones recomendadas en caso de exposición, medidas preventivas, posibles consecuencias y ejemplos específicos del tipo de fraude abordado.

2. Las instituciones deben evaluar continuamente la claridad con la que los usuarios perciben las recomendaciones proporcionadas. El análisis de los reclamos presentados al SERNAC revela confusiones sobre mensajes largamente expuestos, como no compartir claves. Comúnmente, los usuarios asumían que sólo las claves de cajero no debían compartirse, subestimando las consecuencias de compartir otros tipos de claves y datos personales. En muchos casos, los usuarios no asociaban la recomendación de no compartir claves con prácticas como digitalizarlas en el teclado telefónico, un método frecuentemente utilizado por bancos y otras instituciones para verificar la identidad. Por último, es crucial que las campañas informen que los defraudadores pueden haber tenido acceso a información personal del individuo, disminuyendo el riesgo de ser engañados cuando un estafador se hace pasar por un funcionario bancario o público y cita información personal del usuario.

3. Finalmente, para fortalecer las recomendaciones de las campañas de prevención del fraude, resulta fundamental explorar los factores que motivan a los consumidores a adoptar comportamientos de precaución contra los fraudes en línea. Considerando que la tecnología por sí sola no basta para prevenir el fraude y que el comportamiento humano es crucial, las ciencias conductuales ofrecen contribuciones significativas al diseño de políticas de prevención de fraudes. En este contexto, los consumidores pueden protegerse de los fraudes financieros adoptando comportamientos precautorios, y es posible incentivarlos si se comprenden los factores que influyen en sus decisiones.

4. Adicionalmente, es conveniente evaluar experimentalmente (a) aquellos elementos que permiten informar a los consumidores de manera efectiva sobre el riesgo de fraude, (b) identificar los drivers motivacionales que inciten a las personas a salvaguardarse de fraudes informáticos, y (c) evaluar la efectividad de las campañas informativas para fortalecer las habilidades de los consumidores, particularmente en la detección de intentos reales de Phishing. Esto podría contribuir a una reducción en la incidencia de fraudes en el país.

Implementar estas recomendaciones contribuirá significativamente a mejorar la seguridad de los medios de pago en Chile y protegerá de manera más efectiva a los consumidores frente a las crecientes amenazas del fraude financiero.

VII. Bibliografía

Acquisti, Alessandro, Laura Brandimarte y George Loewenstein. (2015). «Privacy and human behavior in the age of information». *Science, 347*(6221), 509-514. https://doi.org/10.1126/science.aaa1465

Allums, S. (2014). *Designing mobile payment experiences: Principles and best practices for mobile commerce*. O'Reilly Media.

Anderson, Catherine L. y Ritu Agarwal. (2010). Practicing safe computing: A multimedia empirical examination of home-computer-user security behavioral intentions. *MIS Quarterly, 34*(3), 613-643.

Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems* (3.ª ed.). Wiley.

Anguera, S. (2024, 1 dic.). Que no te estafen este Cyber Monday: ¿Cuáles son las estafas más comunes? *Intereconomía.* https://www.intereconomia.com/noticia/finanzas/que-no-te-estafen-este-cyber-monday-cuales-son-las-estafas-mas-comunes-20241201-1111/

APWG. (2024). *Phishing Activity Trends Report* (1Q-2024). https://apwg.org/trendsreports/

Apple. (2025, 19 may.). *Usar Face ID en el iPhone o iPad Pro*. Apple Support. https://support.apple.com/es-lamr/108411

Baker, H. K., G. Filbeck & K. Black (Eds.). (2024). *The Emerald Handbook of Fintech: Reshaping Finance*. Emerald Publishing.

Banco Central Europeo. (2023). *Report on card fraud in 2020 and 2021*. https://www.ecb.europa.eu/pub/pdf/cardfraud/ecb.cardfraudreport202305~5d832d6515.en.pdf

BBVA. (s. f.). *Phishing, vishing, smishing: Qué son y cómo protegerse de estas amenazas*. https://www.bbva.com/es/innovacion/phishing-vishing-smishing-que-son-y-como-protegerse-de-estas-amenazas/

Biblioteca del Congreso Nacional de Chile. (2005). *Historia de la Ley N.º 20.009* (Informe Comisión de Economía). https://www.bcn.cl/historiadelaley/fileadmin/file_ley/5611/HLD_5611_f8ac76fb64482b83f173cc982789c184.pdf

Biblioteca del Congreso Nacional de Chile. (2010). *Ley N.º 20.471. Crea Organismo Implementador para la Portabilidad Numérica*. https://www.bcn.cl/leychile/navegar?idNorma=1020620

Biblioteca del Congreso Nacional de Chile. (2020). *Historia de la Ley N.º 21.234* (Primer Informe Comisión de Economía). https://www.bcn.cl/historiadelaley/fileadmin/file_ley/7752/HLD_7752_f8ac76fb64482b83f173cc982789c184.pdf

BioBioChile. (2022, 27 may.). *CyberDay 2022: Consejos de seguridad para no ser víctima de estafa o suplantación de identidad.* https://www.biobiochile.cl/noticias/economia/tu-bolsillo/2022/05/27/cyberday-2022-consejos-de-seguridad-para-no-ser-victima-de-estafa-o-suplantacion-de-identidad.shtml

BioBioChile. (2024, 30 sep.). *Cyber Monday 2024: 7 recomendaciones para evitar ser víctima de estafas y comprar de forma segura.* https://www.biobiochile.cl/noticias/ciencia-y-tecnologia/pc-e-internet/2024/09/30/cyber-monday-2024-7-recomendaciones-para-evitar-ser-victima-de-estafas-y-comprar-de-forma-segura.shtml

Boulgouris, N. V., K. N. Plataniotis & E. Micheli-Tzanakou (Eds.). (2010). *Biometrics: Theory, methods, and applications*. Wiley-IEEE Press.

Brooks, C. J., C. Grow, P. A. Craig Jr. & D. Short. (2018). *Cybersecurity essentials*. Sybex.

Burt, C. (2025, 13 may.). Data is ammo in biometric authentication's arms race with AI fraud: EIC 2025 panel. *Biometric Update.* https://www.biometricupdate.com/202505/data-is-ammo-in-biometric-authentications-arms-race-with-ai-fraud-eic-2025-panel

Canal 13. (2024, 31 may.). Recomendaciones de la PDI para evitar estafas durante el CyberDay. https://www.t13.cl/noticia/tendencias/recomendaciones-pdi-para-evitar-estafas-cyberday-31-5-2024

Carey. (2024, 12 dic.). *CMF perfecciona regulación sobre prestadores de servicios financieros de la Ley Fintech.* https://www.carey.cl/cmf-perfecciona-regulacion-sobre-prestadores-de-servicios-financieros-de-la-ley-fintech/

Cendrowski, H., L. W. Petro, J. P. Martin & A. A. Wadecki. (2007). *The handbook of fraud deterrence*. John Wiley & Sons. https://doi.org/10.1002/9781119202165

ChicureoHoy. (2025, 27 may.). Brigada de Cibercrimen entrega recomendaciones para un Cyber Day 2025 más seguro. https://www.chicureohoy.cl/actualidad/brigada-de-cibercrimen-entrega-recomendaciones-para-un-cyber-day-2025-mas-seguro/

Chocale. (2024, 3 jun.). Los consejos de la PDI para compras seguras en el CyberDay 2024. https://chocale.cl/2024/06/cyberday-consejos-pdi-para-compras-seguras-en-comercio-electronico/

Cialdini, R. B. (2007). *Influence: The Psychology of Persuasion* (rev. ed.). Harper Business.

CMF. (2025). *Informe Normativo: Normas sobre Medidas Seguridad y Autenticación de Operaciones sometidas a la Ley N.º 20.009.* https://www.cmfchile.cl/institucional/legislacion_normativa/normativa_tramite_ver_archivo.php?id=2025041422&seq=1

CNN Chile. (2024, 3 jun.). ¿Cómo protegerte de estafas durante el CyberDay 2024? https://www.cnnchile.com/pais/protegerte-estafas-cyberday-pdi-recomendaciones-compra-online_20240603/

Committee on Payments and Market Infrastructures (CPMI) & World Bank Group (WBG). (2020). Payment aspects of financial inclusion in the fintech era. Bank for International Settlements. https://www.bis.org/cpmi/publ/d191.htm

Crouse, M. (2024, 11 oct.). Deepfakes can fool facial recognition on crypto exchanges. *TechRepublic.* https://www.techrepublic.com/article/ai-deepfake-video-crypto-accounts/

CSIRT Chile. (s. f.). https://csirt.gob.cl/

Drahanský, M. (Ed.). (2018). *Hand-based biometrics: Methods and technology*. Institution of Engineering and Technology.

Edwards, J. (2025). *A comprehensive guide to the NIST Cybersecurity Framework 2.0: Strategies, implementation, and best practice*. John Wiley & Sons. https://doi.org/10.1002/9781394280391

Engemann, K. J., & Witty, J. A. (Eds.). (2024). Cybersecurity Risk Management: Enhancing Leadership and Expertise. De Gruyter.

European Banking Authority. (2022, 23 jun.). *EBA's response to the call for advice on the review of PSD2* (EBA-Op-2022-06).

European Banking Authority. (2024). *Report on Payment Fraud.* https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.ebaecb202408.en.pdf

Fang, J. (2025, 26 may.). Biometric authentication vs. AI threats: Is mobile security ready? *Biometric Update.* https://www.biometricupdate.com/202505/biometric-authentication-vs-ai-threats-is-mobile-security-ready

FasterCapital. (s. f.). *El efecto de los sesgos cognitivos en el comportamiento online del consumidor.* https://fastercapital.com/es/tema/el-efecto-de-los-sesgos-cognitivos-en-el-comportamiento-online-del-consumidor.html

FasterCapital. (s. f.). *Sesgos cognitivos y su impacto en las decisiones de compra.* https://fastercapital.com/es/tema/sesgos-cognitivos-y-su-impacto-en-las-decisiones-de-compra.html

Federal Bureau of Investigation (FBI). (2023). *Internet Crime Report 2023.* https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

Federal Trade Commission (FTC). (2023). *Consumer Sentinel Network 2023.* https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Annual-Data-Book-2023.pdf

Federal Trade Commission (FTC). (2024). *Consumer Sentinel Network 2024.* https://www.ftc.gov/system/files/ftc_gov/pdf/csn-annual-data-book-2024.pdf

Federal Trade Commission (FTC). (2024 b). *FTC proposes new protections to combat AI impersonation of individuals.* https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-proposes-new-protections-combat-ai-impersonation-individuals

Ferreira, A., L. Coventry & G. Lenzini. (2015). «Principles of persuasion in social engineering and their use in phishing».

Financial Action Task Force (FATF) (2020). Guidance on Digital Identity. FATF. https://www.fatf-gafi.org/publications/documents/digital-identity-guidance.html

Gesprodat. (2023). Cómo evitar el robo de claves mediante lectura de tonos. https://gesprodat.com/2023/11/02/como-evitar-el-robo-de-claves-mediante-lectura-de-tonos/

Ghosh, U., F. Mhlanga & D. B. Rawat (Eds.). (2025). *Secure and smart cyber-physical systems* (1.ª ed.). CRC Press.

Gragg, D. (2003). *A multi-level defense against social engineering.* SANS Institute – InfoSec Reading Room.

Gragido, W. & J. Pirc. (2011). *Cybercrime and espionage: An analysis of subversive multi-vector threats.* Syngress.

Gurrea Martínez, A. & N. Remolina León (Eds.). (2020). *Fintech, Regtech y Legaltech: Fundamentos y desafíos regulatorios.* Tirant lo Blanch.

Irani, D., M. Balduzzi, D. Balzarotti, E. Kirda & C. Pu. (2011). «Reverse social engineering attacks in online social networks». *Lecture Notes in Computer Science, 6739*, 55-74. https://doi.org/10.1007/978-3-642-22424-9_4

Jadhav, A. (2024, 6 ago.). Deepfake detection firms buy, build and buddy-up to combat growing threat. *Biometric Update.* https://www.biometricupdate.com/202408/deepfake-detection-firms-buy-build-and-buddy-up-to-combat-growing-threat

Jain, A. K., A. A. Ross & K. Nandakumar. (2011). *Introduction to biometrics.* Springer.

Jans, J. A. (2024). *Electronic payments in the European market: Creating a level playing field between banks and non-banks.* Palgrave Macmillan.

Jeff, P. (2021). *The new cybersecurity for beginners and dummies: Extensive guide to getting started in cybersecurity.* Independently Published.

Jung, J. & R. Katz. (2022). «Impacto del COVID-19 en la digitalización de América Latina». *Revista CEPAL.* https://repositorio.cepal.org/server/api/core/bitstreams/cf05ce4b-b465-4740-86a1-6b707267e99b/content

Kimery, A. (2024, 25 oct.). AI poses threat to biometric authentication, new report warns; but how soon? *Biometric Update.* https://www.biometricupdate.com/202410/ai-poses-threat-to-biometric-authentication-new-report-warns-but-how-soon

Kimery, A. (2025, 23 may.). Deepfakes are testing the limits of American governance. *Biometric Update.* https://www.biometricupdate.com/202505/deepfakes-are-testing-the-limits-of-american-governance

Kimery, A. (2025 b, 5 may.). Deepfake threats reveal contradictions in Trump administration's AI governance plan. *Biometric Update.*

https://www.biometricupdate.com/202505/deepfake-threats-reveal-contradictions-in-trump-administrations-ai-governance-plan
Kosseff, J. (2020). Cybersecurity law (2nd ed.). Wiley.
Kotler, P., H. Kartajaya & I. Setiawan. (2021). *Marketing 5.0: Technology for humanity.* John Wiley & Sons.
La Tercera. (2024, 31 may.). Las recomendaciones de la PDI para no ser víctima de fraudes en el CyberDay 2024. https://www.latercera.com/nacional/noticia/las-recomendaciones-de-la-pdi-para-no-ser-victima-de-fraudes-en-el-cyberday-2024/
Laudon, K. C. & C. G. Traver. (2022). *E-commerce 2022: Business, technology, society* (17.ª ed.). Pearson.
Macquarie Bank. (s. f.). *How to protect yourself from a phone porting fraud.* https://www.macquarie.com.au/security-and-fraud/fraud/phone-porting.html
Madir, J. (Ed.). (2021). *FinTech: Law and regulation* (Elgar Financial Law and Practice Series). Edward Elgar Publishing.
Martel, D. (2024, 22 ago.). Cómo abrir cuenta MACH: Guía paso a paso y consejos. *Wise.* https://wise.com/cl/blog/como-abrir-cuenta-mach
Mercado Libre. (s. f.). ¿Por qué necesitan validar mi identidad? *Envíos Extra.* https://envios.mercadolibre.cl/envios-extra/ayuda/validar-identidad_20651
Nadotti, L., Porzio, C., & Previati, D. (2022). Economia degli intermediari finanziari (4a ed.). McGraw-Hill Education.
Nicoletti, B. (2021). Banking 5.0: How fintech will change traditional banks in the 'new normal' post pandemic. Palgrave Macmillan.
Nielson, S. J. (2024). *Discovering cybersecurity: A technical introduction for the absolute beginner.* Apress.
Nixon, M. S., T. Tan & R. Chellappa. (2005). *Multimodal biometrics: Human recognition systems.* Springer.
NPR. (2024, 2 dic.). Scared of online scams this Cyber Monday? This expert gives tips on what to avoid. https://www.npr.org/2024/12/02/nx-s1-5210450/scared-of-online-scams-this-cyber-monday-this-expert-gives-tips-on-what-to-avoid
Politou, E., E. Alepis, M. Virvou & C. Patsakis. (2022). *Privacy and data protection challenges in the distributed era* (Learning and Analytics in Intelligent Systems, 26). Springer. https://doi.org/10.1007/978-3-030-85443-0
Portal Innova. (2024, 1 oct.). Las principales estafas a las que estar atentos en el Cyber Monday 2024. https://portalinnova.cl/las-principales-estafas-a-las-que-estar-atentos-en-el-cyber-monday-2024/
Portal Innova. (2025, 28 may.). Cyber Day 2025: Las recomendaciones de los expertos para no caer en estafas. https://portalinnova.cl/cyber-day-2025-las-recomendaciones-de-los-expertos-para-no-caer-en-estafas/
PrestaShop. (2024, 19 feb.). ¿Qué son los sesgos cognitivos y cómo usarlos para vender más en tu e-commerce? https://prestashop.es/blog/marketing-es/sesgos-cognitivos-ecommerce/
Rathgeb, C. & C. Busch (Eds.). (2017). *Iris and periocular biometric recognition.* Institution of Engineering and Technology.
Regula. (2024, 30 sep.). Deepfake fraud surges: 49 percent of businesses hit by audio and video scams. *AiThority.* https://regulaforensics.com/resources/deepfake-trends-2024-report/
Revista Más Seguridad. (2024, jul.). Deepfakes y fraude de identidad, Sumsub. *Revista Más Seguridad.* https://www.revistamasseguridad.com.mx/deepfakes-y-fraude-de-identidad-samsub/
Richard, M. (2023). How scammers bypass face verification and tips for choosing a hacker-resistant liveness solution. https://shuftipro.com/blog/how-scammers-bypass-face-verification-and-tips-for-choosing-a-hacker-resistant-liveness-solution/

Rogers. (s. f.). *Fraud and SIM Swaps.* https://about.rogers.com/stories/port-fraud-and-sim-swaps/

Rogers, Ronald W. (1975). «A protection motivation theory of fear appeals and attitude change». *Journal of Psychology, 91*(1), 93-114. https://doi.org/10.1080/00223980.1975.9915803

Santander. (s. f.). Estafa código QR. https://www.santander.com/es/stories/estafa-codigo-qr

Saporta, G., & Maraney, S. (2022). Practical Fraud Prevention: Fraud and AML Analytics for Fintech and eCommerce, Using SQL and Python. Apress.

Scharcanski, J., H. Proença & E. Du (Eds.). (2014). *Signal and image processing for biometrics* (Lecture Notes in Electrical Engineering, 292). Springer.

Selwal, A., D. Sharma, M. Mann, S. Chakraborty, V. E. Balas & O. E. Lieh (Eds.). (2024). *Leveraging computer vision to biometric applications* (1.ª ed.). Chapman & Hall/CRC.

Sherif, M. H. (2016). *Protocols for secure electronic commerce* (3.ª ed.). CRC Press.

Signicat. (2024, 8 oct.). 42.5 % of fraud attempts are now AI-driven. *Nota de prensa.* https://www.signicat.com/press-releases/42-5-of-fraud-attempts-are-now-ai-driven-financial-institutions-rushing-to-strengthen-defences

Signicat. (2024). *The battle against AI-driven identity fraud* [White paper]. https://5310879.fs1.hubspotusercontent-na1.net/hubfs/5310879/The-Battle-Against-AI-driven-Identity-Fraud-2024-Signicat.pdf

Stajano, F. & P. Wilson. (2011). «Understanding scam victims: Seven principles for systems security». *Communications of the ACM, 54*(3), 70-75.

Statista. (s. f.). Number of unique phishing sites detected worldwide from 3rd quarter 2013 to 1st quarter 2024. https://www.statista.com/statistics/266155/number-of-phishing-domain-names-worldwide/

Subsecretaría de Telecomunicaciones [SUBTEL]. (2025, 4 feb.). Más seguridad y menos estafas: Desde hoy todos tus trámites con empresas de telecomunicaciones deberán utilizar biometría. https://www.subtel.gob.cl/mas-seguridad-y-menos-estafas-desde-hoy-todos-tus-tramites-con-empresas-de-telecomunicaciones-deberan-utilizar-biometria/

Vacca, J. R. (2007). *Biometric technologies and verification systems*. Butterworth-Heinemann.

Wang, L. & X. Geng (Eds.). (2009). *Behavioral biometrics for human identification: Intelligent applications.* IGI Global.

Wirtz, J., & Lovelock, C. (2016). Services marketing: People, technology, strategy (8th ed.). World Scientific.

World Economic Forum (WEF). (2024). *Global Risks Report 2024.* https://www.weforum.org/publications/global-risks-report-2024/

Xu, J. (2022). *The future and FinTech: ABCDI and beyond.* World Scientific Publishing. https://doi.org/10.1142/12686

Zhao, D., & Zhang, W. (2021). Artificial financial intelligence in China. Springer Singapore.