Servicio Nacional del Consumidor

FACULTAD ECONOMÍA Y NEGOCIOS UNIVERSIDAD DE CHILE

Fraude en Medios de Pago en Chile: Determinantes de la Autoprotección del Consumidor

Subdirección de Consumo Financiero
Coordinación de Economía del Comportamiento

Universidad de Chile
Facultad de Economía y Negocios
Departamento de Administración

Julio de 2025

Resumen ejecutivo

Según el *World Economic Forum*, la ciberseguridad es uno de los riesgos globales críticos a corto plazo (WEF, 2024). El uso de tecnologías avanzadas como la inteligencia artificial y el aprendizaje automático ha incrementado la sofisticación de los ataques fraudulentos, transformando la seguridad en un desafío constante para individuos, organizaciones y gobiernos (Edwards, 2024). En Chile, las estadísticas sobre reclamaciones de fraudes financieros, presentadas por los consumidores a las entidades financieras, muestran un notable incremento en los últimos años. Durante el segundo semestre de 2023, se alcanzó el nivel más alto de reclamaciones. 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

En este contexto, la Ley N° 21.673, publicada en el Diario Oficial el 30 de mayo de 2024, reformuló el marco regulatorio relacionado a la limitación de la responsabilidad de los usuarios de medios de pago con ocasión del fraude, contenido en la Ley N° 20.009. Respecto de la prevención del fraude, la normativa indica 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 y los mecanismos de autenticación asociados, y que las entidades reguladas tienen el deber de proveer información periódica, clara, accesible y actualizada sobre las medidas de seguridad y las instrucciones para un uso seguro, fomentando prácticas responsables en la gestión de los medios de pago.

En este sentido, la reforma destaca el papel fundamental del factor humano en la seguridad informática. Aunque la tecnología es esencial, no basta para prevenir el fraude. Su eficacia es limitada sin la promoción de conductas de autoprotección en los consumidores (Liang & Xue, 2010; Ng Boon-Yuen, et al. 2009). Estudios como el de Jansen y Leukfeldt (2015) confirman que el comportamiento del usuario es un factor crítico en la victimización por fraude bancario online.

Por ello, es imperativo que los consumidores estén preparados para enfrentar las amenazas de fraudes digitales, desarrollando conciencia de riesgos y sabiendo cómo

reaccionar. En este contexto, este estudio se centra en identificar los factores que motivan a los consumidores a adoptar comportamientos preventivos. Comprender estas motivaciones es clave para crear incentivos informativos eficaces que eduquen sobre los riesgos de fraude y fomenten prácticas seguras.

Este estudio evaluó empíricamente las principales teorías conductuales predictivas de la motivación hacia la prevención del fraude. Para ello, se analizaron los resultados de una encuesta realizada a más de 2.000 consumidores, implementada entre los meses de marzo y abril de 2024. Los datos se procesaron utilizando un modelo de ecuaciones estructurales (SEM, por sus siglas en inglés), que integra tanto un Modelo de Medición como un Modelo Estructural.

En concreto, la investigación examinó la aplicabilidad de dos teorías fundamentales en el contexto de la prevención del fraude financiero en línea:

- **La Teoría de la Motivación de Protección (TMP)** (Rogers, 1975; Maddux y Rogers, 1983), conocida por su capacidad predictiva en conductas preventivas (Floyd et al., 2000), se centra en cómo las personas toman decisiones frente al riesgo.
- **La Teoría del Comportamiento Planificado (TCP)** (Ajzen, 1991), que ofrece un marco para entender la influencia de factores internos y externos en las intenciones de comportamiento, siendo una herramienta valiosa para diseñar intervenciones de cambio (Yousafzai et al., 2010; Brown et al., 2016).

Los hallazgos de este estudio demuestran que la integración de ambas teorías proporciona una comprensión significativamente más completa de los factores que determinan la intención de protegerse contra el fraude en línea, superando la aplicación individual de cada modelo.

La **Teoría de la Motivación de Protección (PMT)**, desarrollada por Rogers (1975) y Maddux & Rogers (1983), es un modelo teórico que explica cómo las personas deciden protegerse ante situaciones de riesgo.

La PMT postula que nuestra respuesta a una amenaza se basa en dos procesos principales:

1. Evaluación de la Amenaza
En esta fase, la persona valora la probabilidad y el impacto de una amenaza. Esto incluye percibir cuán vulnerable se es ante ella y la gravedad del daño potencial. Si una amenaza se percibe como seria y la persona se siente vulnerable, es más probable que se motive a actuar.

2. Evaluación del Afrontamiento
Una vez reconocida y evaluada la amenaza, el individuo analiza las estrategias disponibles para mitigarla. Aquí se consideran la eficacia de la respuesta recomendada, la autoeficacia (la confianza en la propia capacidad para ejecutar la acción) y los costos asociados a esa respuesta (por ejemplo, el tiempo, dinero y/o esfuerzo que requiere

afrontar la amenaza). La combinación de estos factores determina si la persona considera la acción protectora como útil y si se siente capaz de realizarla.

Finalmente, tras estas evaluaciones, las personas adoptan un comportamiento adaptativo (acciones para protegerse) o no adaptativo (decidir no tomar medidas de protección).

Otro marco teórico fundamental para este estudio es la **Teoría del Comportamiento Planificado (TCP)**, desarrollada por Ajzen (1991, 2002). La TCP postula que el comportamiento humano está determinado por tres tipos de creencias esenciales:

- **Creencias Conductuales (Actitud):** Se refieren a la evaluación personal de las posibles consecuencias o atributos de un comportamiento. Esto define la actitud que una persona tiene hacia la acción; es decir, si la percibe como positiva o negativa, basándose en los resultados esperados.
- **Creencias Normativas (Norma Subjetiva):** Estas son las creencias sobre las expectativas de personas significativas en el entorno del individuo. Dan origen a la norma subjetiva, reflejando la presión social percibida para realizar o abstenerse de un comportamiento, influenciada por la opinión de familiares, amigos o grupos de referencia.
- **Creencias de Control (Control Conductual Percibido):** Se centran en la percepción de la presencia de factores que pueden facilitar o dificultar la ejecución de un comportamiento. Esto determina el control conductual percibido, que es la evaluación de cuán fácil o difícil resulta llevar a cabo una acción, basada en experiencias previas y posibles obstáculos. Es un factor clave, ya que puede fortalecer o debilitar la intención de actuar, según la capacidad percibida del individuo.

En conjunto, la actitud hacia el comportamiento, la norma subjetiva y el control conductual percibido forman la intención de comportamiento. La TCP asume que esta intención es el principal antecedente del comportamiento y que, si las condiciones lo permiten, las personas actúan de acuerdo con sus intenciones (Ajzen, 2002).

Los principales resultados del estudio son los siguientes:

1. El factor más importante para motivar la protección contra el fraude es la ***autoeficacia***, es decir, la creencia de una persona sobre su capacidad para realizar la conducta que se le recomienda en materia de seguridad contra el fraude online.
2. En segundo lugar, la **percepción de la *gravedad*** del fraude juega un papel esencial, lo que implica que cuando los consumidores consideran que las consecuencias de ser víctimas de fraude son graves están más dispuestos a adoptar medidas preventivas. Esto sugiere que la comunicación eficaz de los riesgos y consecuencias del fraude puede ser una herramienta para fomentar conductas preventivas.
3. Adicionalmente, los ***costos*** **percibidos de la respuesta**, es decir, el tiempo, dinero y/o esfuerzo que requiere afrontar la amenaza, tienen un impacto negativo en la motivación de protección. Por lo tanto, reducir los costos percibidos mediante la simplificación de las medidas de seguridad y la automatización de procesos de

protección podría aumentar la disposición de los consumidores a seguir las recomendaciones de seguridad.

A continuación, se describen los resultados del análisis de heterogeneidad, es decir, en subgrupos de la muestra. Estos resultados se pueden utilizar como base para la elaboración de campañas focalizadas en subgrupos de la población:

- Al diferenciar por género y edad se confirma que la *autoeficacia* es la variable más robusta, ya que tiene efectos significativos en todos los subgrupos analizados.
- Por otro lado, se encontró que la *gravedad percibida* es particularmente relevante para explicar la motivación de protección en mujeres, mientras que la *eficacia de la respuesta* resulta más influyente en hombres.
- Según nivel educacional e ingreso, se encuentra que los *costos de la respuesta* exhiben un efecto significativo en el grupo de menor nivel educacional, y que la gravedad percibida es relevante en el grupo de menores ingresos.
- Se encontró un efecto positivo y significativo de la *eficacia de la respuesta* en el subgrupo de personas que no sufrieron fraude durante el último año.
- Finalmente, se identifican efectos positivos y significativos de la *gravedad percibida* en el subgrupo de personas poco informadas de los riesgos del fraude; y de los *costos de la respuesta* en el subgrupo de usuarios menos informados y experimentados en el uso de la banca en línea.

Otros resultados relevantes, de tipo descriptivo, se exponen a continuación:

- El 58% de los participantes en la encuesta se considera 'Bastante bien informado' o 'Muy bien informado' de los riesgos del fraude informático.
- El 49% de los participantes evaluó su competencia en el uso del sitio web o la aplicación móvil de su institución financiera como 'Algo por encima del promedio' o 'Muy por encima del promedio'.
- El 73% de los participantes declaró utilizar el sitio web o la aplicación móvil de su institución financiera 'Casi todos los días' o 'Todos los días'.
- El 69% de los encuestados declaró no haber sido víctima de fraude. Sin embargo, el 75% señaló conocer a una o más personas que fueron víctima de fraude informático durante el último año.
- Durante el último año las mujeres experimentaron fraude con mayor frecuencia que los hombres: 34% vs 28%, respectivamente.
- Los participantes que autoevaluaron su nivel de conocimiento de los riesgos del fraude informático como 'nada informados' o 'no muy bien informados' fueron quienes sufrieron fraude con mayor frecuencia (54%).
- Los encuestados que se describieron como poco competentes en el uso del sitio web o aplicación de su institución financiera, respondiendo 'algo por debajo' o 'muy por debajo de la media', fueron más afectados por el fraude informático (51%).
- Al tomar en cuenta el efecto de todas las variables simultáneamente (mediante una regresión), se encontró que la identificación con el género femenino incrementa en un 4% la probabilidad de haber sufrido fraude, mientras que un alto nivel de

experiencia con la banca en línea (evaluada como algo o muy por encima del promedio) disminuye dicha probabilidad en un 8%.

- Respecto a la intención de seguir las recomendaciones de seguridad, se encontró que los hombres reportaron una mayor disposición de seguir las recomendaciones de seguridad, lo cual podría contribuir a explicar la mayor incidencia de fraudes en las mujeres en comparación con los hombres. De igual modo, el nivel promedio de las variables psicológicas provenientes de la "TMP" y "TCP" tiende a ser mayor entre los hombres que entre las mujeres, lo cual podría explicar la mayor motivación de protección observada en los hombres. La única excepción es '*Gravedad*', donde el grado de acuerdo es marginalmente mayor en las mujeres.
- Respecto de las variables psicológicas provenientes de la TMP y TCP, se encontró que aquella con mayor nivel promedio es la '*Gravedad*', es decir, los participantes consideran que sufrir un fraude informático tendría consecuencias graves.

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.