

Comité de Medios de Pago de ChilePay 2023:
Resultados y Conclusiones

Enero 2024

1. INTRODUCCIÓN

ChilePay es la Corporación Chilena para la Digitalización del Efectivo. Fue creada en el año 2021 y cuenta con dos pilares clave en sus estatutos: obtener una mayor inclusión financiera en el país y consolidar una cultura digital en el ámbito del ecosistema de medios de pago. Actualmente son 40 empresas y organizaciones miembros, provenientes de diferentes ámbitos de la economía o rubro empresarial.

El Comité de Medios de Pago inició por primera vez en junio de 2023 y fue conformado por miembros de las siguientes empresas y organizaciones: Asociación Chilena de Gastronomía (Achiga), ACI Worldwide, American Express, Asociación de Emprendedores Chilenos (ASECH), Banco Estado, Barros & Errázuriz Abogados, BM Soluciones, Cajas de Chile A.G., Cámara Nacional de Comercio Servicios y Turismo de Chile (CNC), Continuum, Coopeuch, Coredevx, Dibopay, Edenred, Energy Club, Equifax, Etpay, Evertec, Federación de Empresas de Turismo de Chile (Fedetur), Fortinet, Fundación País Digital, Kuvasz, Logicalis, Mastercard, NCR, Redbanc, Red Mujeres de Alta Dirección (REDMAD), Simetrik, Sodexo Beneficios e Incentivos, Synaptic, Transbank, Verifone y Visa.

Durante julio y agosto de 2023, dispuestos en cuatro mesas de trabajo, los participantes del Comité de Medios de Pago de ChilePay discutieron distintos temas que se consideran claves dentro del ecosistema de pagos local, buscando (i) hacer visibles los retos que previenen u obstaculizan la inclusión financiera y un mayor uso de medios digitales de pago, y (ii) lograr consenso entre las diferentes visiones de los participantes con la intención de que la Corporación pueda posicionar estos retos. El trabajo se inicia en enero del 2023 con entrevistas y cuestionarios a los miembros de la Corporación, que conducen a construir la visión de ChilePay respecto al ecosistema de pago y de los desafíos que éste propone para un mejor desempeño, eficiencia y productividad del país¹.

Los temas principales levantados en el documento inicial “Visión de ChilePay del Ecosistema de medios de pago” y que fueron materia de diálogo por parte de los equipos de trabajo, fueron: **1) Interoperabilidad de los medios de pago, 2) Fraudes, 3) Educación financiera**. Si bien cada uno de estos temas tienen sus matices, en general son convergentes y complementarios.

¹ Ver Anexo 1.

Las cuatro mesas de trabajo estuvieron conformadas por distintos miembros de la Corporación, que trabajaron bajo metodología ágil², guiados por *coaches agile* de Continuum y supervisados por abogados de Barros & Errázuriz, quienes a su vez conformaban estas mesas como “secretarios”.

Los participantes de cada mesa fueron los siguientes:

- En el equipo **IncluPay**: Tomás Crestani, coordinador del equipo (Redbanc); Rodrigo Alegre, coach agile (Continuum); Manuela Ulloa, secretaria (Barros & Errázuriz); Ángel Molina (Simetrik), Bernardita Silva (Cámara Nacional de Comercio), Carolin Morales (AMEX), Claudia Álvarez (REDMAD), Francisco Voss (Verifone), Gonzalo Collarte (Banco Estado), Gonzalo Nazer (Sodexo Beneficios e Incentivos), Jaime Castillo (Energy), Mateo Barbieris (Asech) y Richard Kosche (Equifax).
- En el equipo **CulturaPay**: Juan Beck, coordinador del equipo (ACI Worldwide); Karen Gálvez, coach agile (Continuum); María José Bordalí, secretaria (Barros & Errázuriz); Jean Philippe Cazenave (Mastercard), Elisa Joannon (Sodexo Beneficios e Incentivos), Eduardo Regonesi (Achiga), Manuel Suárez (Synaptic), Marlon Rodríguez (Kuvasz Solutions), Ricardo Blümel (Transbank), Mario Contreras (Asech), Fernando Beya (Evertec), María Dolores Peralta (Banco Estado), Francisco Vial (Barros & Errázuriz), Julio Pardo (NCR) y Diego Castellón (AMEX).
- En el equipo **Los Interoperables**: Paola Ledezma, coordinadora del equipo (Transbank); Carolina Rojas, coach agile (Continuum); Fernanda Irrazabal, secretaria (Barros & Errázuriz); Bernardo Siu (EtPay), Cristian Bertholet (BM Soluciones), Daniel Barba (Evertec), Fernando Muller (Edenred), Gabriel Gutiérrez (Fedetur), Gabriel Moyano (Coopeuch), Jaime Cruzat (Emisora de Tarjetas los Héroe), Juan Pablo Boccardi (Simetrik), Juan Vizcarra (Verifone), María Jesús Urruticoechea (ChilePay) y Rolando Castillo (Synaptic).
- En el equipo **AndesPay**: Gerardo Rivera, coordinador del equipo (ACI Worldwide); Julieta Collino, coach agile (Continuum); Belén Jottar, secretaria (Barros & Errázuriz); Verónica Ibáñez (Visa), Fernando Sánchez (Fundación País Digital), Cristián Briceño (Edenred), Johan Sánchez (Logicalis), Pía Salas (Fortinet), Marco Rivera (Cajas de Chile), María Dolores Lasen (REDMAD), Carolina Flisfisch (Redbanc) y Ricardo Oberpaur (NCR).

² La metodología ágil se implementó en 2001 para potenciar el desarrollo de *softwares*, y se adaptó para ser desarrollada en un contexto como este, que puede no ser tan común, con el objetivo de superar las necesidades de adherencia y foco de los distintos participantes. Sus estrategias incluyen reuniones periódicas, gestión de tareas, trabajo en grupos y el mejoramiento de la eficiencia por medio de la eliminación de elementos prescindibles.

El resumen de los temas de cada mesa es el siguiente:

Mesa de Trabajo	Tema	Descripción
IncluPay	Interoperabilidad Digital (QR) ³	Estandarización en la interoperabilidad con foco actual en QR.
	Pagos Digitales e Informalidad	Informalidad en el comercio desde los pagos digitales.
	Confidencialidad de la información	Relación entre la confidencialidad y la libre competencia.

Mesa de Trabajo	Tema	Descripción
Interoperables	Ley de Fraude	Con la Ley de Fraude actual el cliente no tiene que mostrar evidencias cuando denuncia eventualmente este tipo de delito. La cantidad de fraudes denunciados ha aumentado considerablemente desde la entrada en vigor de la ley, lo que hace sospechar que gran número de estos crímenes, en realidad, pueden ser autofraudes.
	Interoperabilidad y aceptación universal	Actualmente existen distintos medios de pago que no son interoperables entre sí —por ejemplo, en los pagos con QR, cada emisor ha implementado su propio QR—, y algunos medios de pago, por ejemplo, las tarjetas de prepago, no son aceptados en todos los comercios, lo que obstaculiza la masividad de algunas soluciones financieras, además de afectar la experiencia del cliente final. Por otra parte, al no tener estándares de

³ Un QR, o "Código QR" (por sus siglas en inglés, *Quick Response*), es un tipo de código de barras bidimensional que se utiliza para almacenar información de manera codificada. Los códigos QR son cuadrados y consisten en patrones de puntos en blanco y negro dispuestos en una cuadrícula. Para este texto, un QR es una tecnología que se utiliza para captar una intención de compra o de pago en un punto de venta.

		implementación y seguridad, la integración entre los distintos medios de pago es muy costosa en tiempo y esfuerzo para las entidades involucradas, lo que puede afectar la confianza en el sistema de pagos.
--	--	--

Mesa de Trabajo	Tema	Descripción
AndesPay	Educación Financiera & Ciberseguridad	<p>Algunas personas que ya están en el mundo financiero o que recién están ingresando, cuentan con pocos conocimientos y/o herramientas para proteger y cuidar su información financiera digital. Esto genera efectos en dos grupos poblacionales:</p> <ul style="list-style-type: none"> - Los que ya tienen algún producto financiero no necesariamente hacen uso responsable de su información financiera digital, - y aquellos que no tienen productos, cuando ingresan, pueden estar más expuestos y ser víctimas de fraude.
	Ley de Fraudes y autofraude	<p>Los casos de fraude financiero han aumentado, lo que erosiona la confianza de los usuarios y afecta su percepción de seguridad frente al sistema financiero en conjunto.</p> <p>Si bien la Ley de Fraude enmarca las responsabilidades de los diferentes actores, la forma en la que está dispuesta abre la puerta al “autofraude”, que perjudica al usuario, al emisor, al sistema financiero y legal.</p>
	Acceso a Tecnologías y Conectividad	La inclusión financiera y la digitalización del efectivo en Chile se ven limitados por el acceso

		<p>que tenga la población a las tecnologías habilitantes, principalmente redes de comunicación y datos.</p> <p>Disminuir el uso del efectivo se dificulta en sectores cuya población no cuenta con la cobertura mínima básica para hacer uso de productos financieros digitales.</p>
--	--	--

Mesa de Trabajo	Tema	Descripción
Cultura Pay	Fraude Colaborativo	<p>El fraude bancario en Chile se ha duplicado en el primer semestre de 2023. Está siendo combatido de forma individual por cada una de las entidades financieras, sin compartir esfuerzos ni aprendizajes.</p> <p>Cada cual opera con datos históricos propios y a veces insuficientes para la prevención de fraudes.</p>
	Experiencia en pagos y TEF	<p>Chile ha liderado el camino en la adopción de Pagos Inmediatos en América Latina, estableciéndose como un pionero en esta área.</p> <p>Desde 2007, ha desarrollado una infraestructura que posibilita la ejecución de transferencias en tiempo real. A pesar de estos logros, es evidente que la experiencia no ha evolucionado al mismo ritmo que en algunos de nuestros países vecinos.</p>

2. INTEROPERABILIDAD Y EXPERIENCIA DE PAGO

2.1 CONTEXTO Y OBJETIVO

Los participantes de esta mesa se enfocaron en la experiencia de pago y consolidación del modelo de 4 partes (M4P), y en los efectos de potenciar las formas de pago y acelerar la interoperabilidad como parte de las condiciones fundamentales de dicho modelo. El impacto generado podría disminuir las barreras de

entrada tanto de adquirentes como emisores, ofrecer una mayor variedad de opciones y mejores experiencias a los tarjetahabientes, y aumentar la inclusión financiera de comercios más pequeños y personas no bancarizadas.

2.2 EVIDENCIA

Inclupay sostiene que, entendiendo los incentivos de los actores del ecosistema, lo ideal es que la estandarización y camino hacia una autorregulación venga desde el negocio en sí mismo. Desde esta mirada, Yape y Plin, en Perú, son ejemplos válidos. Además, en febrero de 2021 se inició la colaboración entre CCE, Mastercard y ACI Worldwide para modernizar la infraestructura de pagos digitales. Sobre los pagos instantáneos, se comentó su viabilidad basándose en la ISO 20022, tal como PIX, y simplificar la integración de las instituciones.

Desde la mirada del regulador, Pix, en Brasil, es el caso más representativo. Liderado por el Banco Central, la iniciativa que en sólo 1 día procesó 142,4 millones de transacciones (América Retail 2023) se ha convertido en el segundo método de pago instantáneo en el mundo, siendo responsable del 15% de todos los pagos instantáneos en el mundo durante el 2022 (Banco Central do Brasil 2023). Generada el 2020, consideraba tanto a bancos digitales como Fintechs, lo que permitió una gran penetración y popularidad, fortaleciendo la digitalización de los pagos. Desde Pix, se puede aprender muchísimo, y consideramos que el documento *Lesson from Pix* (Abreu y Cunha e Melo 2023) es una base interesante para identificar aprendizajes en torno a la arquitectura, participantes y flujo de pago.

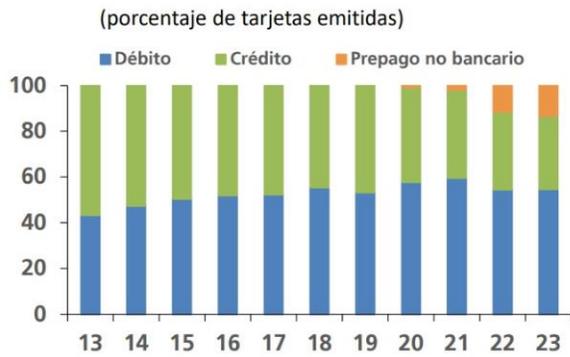
Colombia ha seguido los pasos de Brasil, donde el uso de QR ha sido su inicio; sin embargo, la penetración y adopción no ha sido la esperada por falta de estandarización. En el documento *Diseño de Pagos Inmediatos* (Banco de la República de Colombia 2023) podemos encontrar lineamientos y estándares en el diseño de la interoperabilidad.

En esta misma línea, en Argentina, la adopción del QR ha aumentado significativamente la transaccionalidad en pagos desde cuentas bancarias y virtuales gracias a la interoperabilidad, y en breve se suma la posibilidad de usar QR interoperable para pagar con cualquier tarjeta de crédito aumentando los beneficios para cuentahabientes, tarjetahabientes y comercios.

En Chile, los números de tarjetas de prepago advierten la necesidad de la interoperabilidad. Un producto que ha ido creciendo en número —actualmente es el 13% del universo de tarjetas—, pero en transacciones

representa sólo un 1%, nos lleva a correlacionar que la no universalización en la aceptación de este tipo de producto hace que el uso y adopción sea bajo (Banco Central de Chile 2023).

Participación del número total de tarjetas



Monto de transacciones con tarjeta de prepago

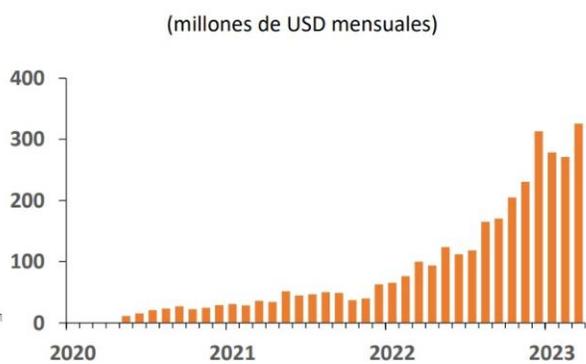


GRÁFICO I.4 USO DE TARJETAS (MONTO) SOBRE CONSUMO DE LOS HOGARES (*) (porcentaje, trimestral)

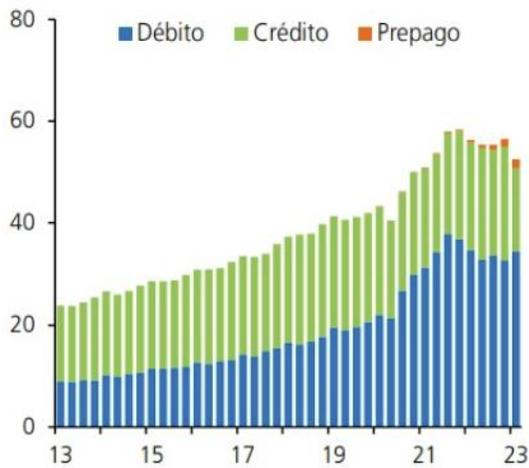
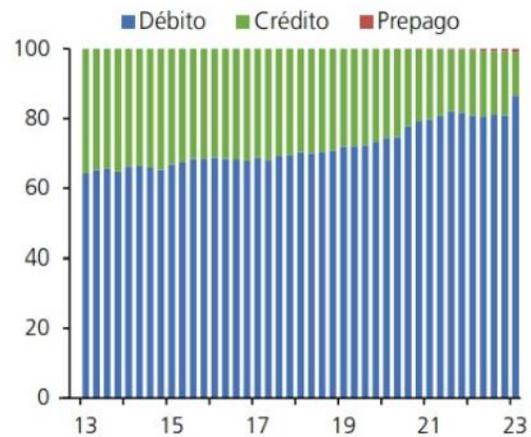


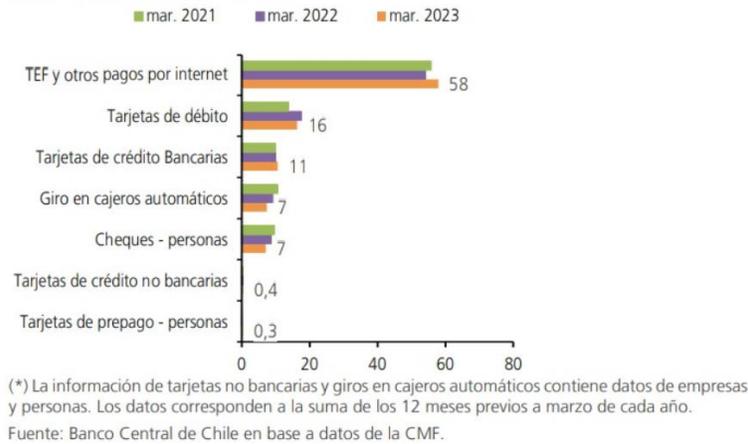
GRÁFICO I.5 PARTICIPACIÓN EN EL NÚMERO DE OPERACIONES POR TIPO DE TARJETAS (*) (porcentaje, trimestral)



(*) Los datos contienen información de empresas y personas.

Fuente: Banco Central de Chile en base a información de la CMF y Banco Centra de Chile.

GRÁFICO I.1 PARTICIPACIÓN DE MEDIOS DE PAGO (*)
(porcentaje de montos transados)



3. FRAUDES

3.1 CONTEXTO

Desde la entrada en vigencia de la nueva Ley de Fraude 21.234 –que limita la responsabilidad de los usuarios de medios de pago y transacciones electrónicas ante casos de fraude, marcando plazos de respuesta y restitución de fondos por parte del Banco al Usuario–, los fraudes han aumentado al doble en el primer semestre de 2023 frente al mismo periodo del año anterior.

Si bien la Ley de Fraude enmarca las responsabilidades de los diferentes actores, la forma en la que está dispuesta abre la puerta al “autofraude”, que perjudica al usuario, al emisor, al sistema financiero y legal. En consecuencia, la confianza de los actores comienza a disminuir y la oferta de servicios financieros para la inclusión digital tiene un sobre costo por el riesgo que implica la protección del dinero y las provisiones de capital por si sucede un fraude.

Se percibe que cada actor del ecosistema combate el fraude de forma individual, sin compartir esfuerzos ni aprendizajes. Cada cual opera con datos históricos propios y a veces insuficientes para la prevención de fraudes.

3.2 EVIDENCIA

Si bien ha sido difícil encontrar estadísticas oficiales desde la Comisión para el Mercado Financiero (CMF), hay artículos en la prensa publicados que hablan del tema, por ejemplo, Ley de Fraude - Cifras Segundo Semestre (Sierralta y Valdés 2023).

“Durante el segundo semestre de 2022 se registraron 201.207 casos de fraudes bancarios relacionados con cobros no reconocidos en cuentas, transferencias y medios de pago de clientes de los 11 principales bancos del país, en el contexto de la Ley de Fraudes que entró en vigencia en 2020, lo que representa un incremento de 92% respecto del mismo periodo de 2021. En comparación con el primer semestre del año pasado, el alza fue de un 83,1%.”.

A pesar de que la Ley 20.009, en su artículo 11, señala que las entidades emisoras deberán informar sobre el número de usuarios afectados por casos de extravío, robo, hurto o fraude publicando esta información en sus portales y compartirla a la CMF, no hay evidencia de la existencia de una base de datos centralizada de fraude, ni el marco jurídico para su creación, operación y uso.

En relación a establecer un enfoque colaborativo, existen estudios que señalan que combatir el fraude de forma colaborativa incrementa la asertividad de fraude en un 10% por sobre las iniciativas individuales de cada entidad financiera (Yang et al., 2019).

En distintos países se están tomando estrategias de prevención de fraude colaborativo, como es el caso de Australia y España. En ambos países, se comparten modelos matemáticos y estrategias de prevención de fraude, no así datos privados.

4. EDUCACIÓN FINANCIERA

4.1 CONTEXTO

Desde las mesas se levantó el tema de la educación financiera y cómo se implementa en el país, desde tres miradas particulares: uso y aceptación de medios de pagos digitales, conocimiento tributario y ciberseguridad.

Chile ha liderado el camino en la adopción de Pagos Inmediatos en América Latina, estableciéndose como un pionero en esta área. Desde 2007, ha desarrollado una infraestructura que posibilita la ejecución de transferencias en tiempo real. A pesar de estos logros, es evidente que la experiencia no ha evolucionado al mismo ritmo que en algunos de nuestros países vecinos, lo que plantea una oportunidad para mejorar y alinearse con las tendencias actuales.

Se desprende de lo anterior, la falta de incentivos y conocimiento sobre temas tributarios. Se percibe que,

si bien la informalidad es una elección de conveniencia, existen pocos incentivos y confusión sobre quién y en qué momento se pagan los diversos impuestos que gravan los pagos digitales, tanto para el pagador como para el aceptador.

En relación con el conocimiento de ciberseguridad, entendemos que algunas personas que ya están en el mundo financiero o que están recién ingresando cuentan con pocos conocimientos y/o herramientas para proteger y cuidar su información financiera digital. Esto genera efectos en dos grupos poblacionales: 1) los que ya tienen algún producto financiero no necesariamente hacen uso responsable de su información financiera digital, y 2) aquellos que no tienen productos, cuando ingresan, pueden estar más expuestos y ser víctimas de fraude.

4.2 EVIDENCIA

Frente a la educación financiera en general, sabemos que el 42% de los chilenos tiene un nivel bajo de conocimiento financiero, el 37%, intermedio, y el 21%, alto, según el *Estudio Educación Financiera (2022)* del Depósito Central de Valores y Cadem. Además, y tomando en cuenta que la CMF tiene un portal de Educación Financiera donde, en el 2021, publicó el “Mes de la educación financiera”, aún se puede percibir una falta de profundización en estas iniciativas. Por otro lado, la CMF divulgó la Carta Circular N°4, donde si bien dicta lineamientos en las Iniciativas y Programas de Educación Financiera para actores del sistema financiero, creemos que aún falta mayor énfasis en su implementación.

Finalmente, la Ley 21.092 incorpora la Educación Financiera dentro de los contenidos del currículum de Enseñanza Media, un paso importante para priorizar el contenido tributario y de seguridad en el plan de estudios.

En relación con la informalidad, la Cámara Nacional de Comercio y ASECH, a través de estudios y conversaciones con emprendedores y comerciantes, han notado el desconocimiento sobre cómo opera la tributación a la hora de pagar. Algunos comercios no tienen claridad si el sistema de pago declara inmediatamente el IVA. A pesar de que ya algunos procesadores lo hacen, no es de común conocimiento cuáles son los procesos ni cómo proceden.

Las cifras que se desprenden de compras informales en canales digitales ascienden a US\$187,6 millones en el primer trimestre del 2023, según la Cámara Nacional de Comercio (*Informalidad en el E-Commerce 2023*).

Conclusiones generales

Durante julio y agosto de 2023, las cuatro mesas de trabajo reunidas por el Comité de Medios de Pago de ChilePay determinaron temas clave dentro del ecosistema de medios de pago, convergentes y complementarios entre sí: Interoperabilidad, Fraudes y Educación financiera.

En cuanto a la interoperabilidad de los medios de pago, las mesas determinaron los siguientes puntos: la falta de un estándar mínimo de infraestructura y nuevas tecnologías, la baja priorización de productos que impulsen la inclusión —como los códigos QR—, y la relación entre confidencialidad y competencia.

Con respecto a los fraudes, los temas giraron en torno a la ley antifraude y los llamados autofraudes, la información cruzada de fraude en la industria, abordar la tendencia del autofraude, y la posibilidad de implementar un enfoque colaborativo para combatirlo.

Finalmente, en relación con la educación financiera, los representantes de la Corporación determinaron la falta de enseñanza en dos temas: ciberseguridad y conocimiento tributario.

Como conclusión, el Comité de Medios de Pago ha señalado temas urgentes en torno a la interoperabilidad de medios de pago, el fraude y la educación en temas financieros. ChilePay, de esta manera, se compromete con la inclusión financiera y el mejor desarrollo de esta realidad contingente que crece día a día: los pagos digitales. A su vez, estos temas ofrecen un espacio para llevar a cabo diversos proyectos dentro del ecosistema financiero, con lo que se presentará un gran desafío que consiste en definir e implementar nuevas iniciativas.

Referencias

- Abreu, J., Cunha e Melo, M. (2023). *Creating the next generation of payment rails: Lessons from Pix*. <https://doi.org/10.59262/swcj93>
- América retail. (9 de agosto de 2023). *Plataforma de pagos brasileña Pix, rompe récord de transacciones*. <https://www.america-retail.com/brasil/plataforma-de-pagos-brasilena-pix-rompe-record-de-transacciones/>
- Banco Central de Chile. (2023). *Informe de Sistemas de Pago*. <https://www.bcentral.cl/web/banco-central/areas/politica-financiera/informe-de-sistemas-de-pago>

- Banco Central do Brasil. (19 de abril de 2023). *Pix is one of the world's most used instant payment systems*.
<https://www.bcb.gov.br/en/pressdetail/2470/nota>
- Banco de la República de Colombia. (18 de abril de 2023). *Sistemas de Pago de Colombia: Diseño del Ecosistema de Pagos Inmediatos*. https://www.banrep.gov.co/sites/default/files/foro-sistemas-pago-etapa-2-interoperabilidad-spi_0.pdf
- Cámara Nacional de Comercio (2023). *Informalidad en el E-Commerce*. <https://www.cnc.cl/wp-content/uploads/2023/06/Informalidad-en-el-Comercio-Electronico-I-Trimestre-2023.pdf>
- Comisión para el Mercado Financiero. (2021). *Mes de la educación financiera*. Rescatado el 07 de noviembre de 2023. <https://www.cmfchile.cl/portal/prensa/615/w3-article-49425.html>
- Depósito Central de Valores, Cadem. (2022). *Estudio Educación financiera*. https://www.dcv.cl/images/avances-de-noticias/2022/011-diciembre/informe-dcv-educacion-financiera-nov_2022.pdf
- Ley N°20.009. Biblioteca del Congreso Nacional de Chile, 17 de agosto de 2023. Recuperado el 07 de noviembre de 2023. <https://www.bcn.cl/leychile/navegar?idNorma=236736>
- Sierralta, B., Valdés, M. (22 de febrero de 2023). *Ley de fraudes: Hubo más de 201 mil casos en el segundo semestre de 2022*. <https://chocale.cl/2023/07/ley-de-fraudes-estadisticas-primer-semestre-2023/>
- Yang, W., Zhang, Y., Ye, K., Li, L., Xu, CZ. (2019). FFD: A Federated Learning Based Method for Credit Card Fraud Detection. In: Chen, K., Seshadri, S., Zhang, LJ. (eds) Big Data – BigData 2019. BIGDATA 2019. Lecture Notes in Computer Science, vol 11514. Springer, Cham. https://doi.org/10.1007/978-3-030-23551-2_2

Anexo 1: Visión inicial de ChilePay del Ecosistema de medios de pago. Marzo 2023.

El presente documento busca resumir la opinión conjunta de la Corporación en torno a los temas de interoperabilidad de medios de pago, fraude y ciberseguridad.

En base a las respuestas otorgadas en marzo de 2023 por distintos miembros de ChilePay en torno a las materias consultadas, fue elaborado el presente texto, que transmite las ideas centrales comunicadas por los miembros⁴.

I. INTEROPERABILIDAD DE MEDIOS DE PAGO

La interoperabilidad de los medios de pago consiste en la capacidad y posibilidad de procesar pagos que cada una de las distintas entidades de la industria financiera tiene con los diversos medios de pago. En ChilePay creemos que existe la necesidad de que cada producto o solución de pago pueda ser aceptado en todos los canales disponibles. La visión de la Corporación es que la interoperabilidad permite ampliar el ecosistema de pago y con ello traer agilidad, seguridad, simplicidad y libertad a la hora de pagar. Además, genera mayor competitividad en el mercado, lo que, a su vez, se traduce en menores costos para el consumidor y una mayor penetración y avance en la inclusión financiera, el cual es uno de los pilares de ChilePay. Creemos en la importancia de la ampliación y aceptación en todos los canales.

En ChilePay vemos la necesidad de que (i) los estándares de calidad de pagos sean cumplidos y aceptados por todos los miembros del ecosistema de pagos, tanto por y en los comercios como por y en los demás actores del referido ecosistema; (ii) la regulación permita dar seguridad al usuario para que este pueda optar por más medios de pago, y (iii) exista una mejor comunicación y acuerdo entre los miembros del ecosistema. La Corporación detecta la necesidad de (i) avanzar y profundizar en torno a la protección de datos y ciberseguridad, (ii) generar una coordinación entre entidades públicas y privadas, (iii) aumentar e implementar las políticas públicas e inclusión financiera en la materia, (iv) desarrollar y buscar una mayor inclusión de tecnologías como NFC y QR, y (v) un mayor desarrollo de nuevas tecnologías, en que el rol de las Bigtech es fundamental. Creemos que esto permitirá que se desarrolle y profundice la interoperabilidad en transferencias bancarias.

⁴ La metodología utilizada para la elaboración del presente texto consistió en respuestas a un cuestionario entregadas por diferentes organizaciones miembros de ChilePay, las cuales fueron fusionadas y resumidas para confeccionar este anexo.

Finalmente, en ChilePay proyectamos que los medios de pago preponderantes para los chilenos en el 2030 serán el teléfono móvil y el uso de aplicaciones digitales (que incluyan el uso de QR y la entrada de nuevos actores “invisibles” al usuario final, tales como billeteras digitales y la tecnología *contactless*.)

II. FRAUDE

El mercado digital nacional tiene un limitado conocimiento de los riesgos asociados a tarjetas no presentes, específicamente a los llamados “contracargos”, que se configuran como reversas de cargos ilícitos de dinero. Esta falta de conocimiento genera una falta de consciencia respecto de la necesidad de contar con soluciones antifraude. Para ChilePay, la existencia de controles de fraude a nivel de emisores que permitan detectar anomalías en transacciones es absolutamente necesaria. Actualmente se reconoce la presencia de transacciones fraudulentas, cuya responsabilidad está definida por la ley y el regulador, sin embargo, muchas veces se trata de vulneraciones a adquirentes o comercios y no está claro el origen o el responsable. Por esto, la Corporación estima necesarios la existencia y aplicación de procesos de verificación de cualquier transacción, y la modernización de las herramientas y soluciones ante estos problemas de ciberseguridad, tomando inspiración a partir de estándares internacionales.

La implementación del “modelo de cuatro partes” modificará los actores que participan en los pagos y el procesamiento de éstos, al incluir nuevos agentes como agregadores (PSPs) e, incluso, adquirentes inéditos. Esto generará la aparición de nuevos cobros tal como el contra cargo, cobros que no son la regla general mundial, puesto que, en la experiencia comparada, los adquirentes transfieren el costo y *fees* asociados a los comercios.

La migración al modelo de cuatro partes plantea la necesidad de que cada actor del nuevo ecosistema tenga un rol importante, y para tales efectos cada actor deberá actualizar sus flujos y procesos respecto a contracargos, representaciones, monitoreo permanente de fraude y responsabilidades, según dictan las marcas de tarjetas.

En ChilePay entendemos que los riesgos antedichos están presentes en el mercado de pago. En el apartado legal, los usuarios se encuentran protegidos por la Ley N°21.234, que limita la responsabilidad de los usuarios de medios de pago y transacciones electrónicas ante el caso de extravío, hurto, robo o fraude. Sin perjuicio del avance que implica tal regulación, la misma puede ocasionar ciertos efectos negativos en el mercado de tarjetas, generando potenciales fricciones en el proceso de pago, ya que el banco o emisor de tarjetas, en la gran mayoría de los casos, será responsable del pago del perjuicio. Como consecuencia de esto, los bancos y emisores buscarán aumentar los estándares de seguridad respecto a este tipo de operaciones, a fin de disminuir su exposición a riesgo, lo que posiblemente elevará las fricciones de los

mencionados procesos. La ley genera, asimismo, un incentivo de efectuar autofraudes. Creemos, que este ambiente y problemáticas presentan una oportunidad para que los emisores de tarjetas creen e implementen medios de autenticación más seguros y que permitan evitar las fricciones.

Identificamos dos fuentes en las que trabajar y evolucionar en pos de la ciberseguridad, ambas se encuentran enmarcadas específicamente en el ámbito no presencial: (i) eliminar la necesidad de declarar el número de la tarjeta, la fecha de vencimiento y el CVC al momento de efectuar un pago; y (ii) modernizar la autenticación del cliente por medio de diferentes opciones, tales como el reconocimiento facial, aspectos biométricos, huella digital, entre otros. Estos objetivos se pueden lograr a través de la protección de datos que otorga la *tokenización* en los dispositivos de los clientes, y las formas modernas de autenticación ya mencionadas.

La entrada de nuevos Proveedores de Servicios de Pago (PSPs) en el mercado potenciará el crecimiento de los canales digitales, billeteras móviles, pasarelas de pagos (y otras subsidiarias relacionadas) de los adquirentes. En ChilePay creemos, como ya se adelantó, que la estandarización es el camino a seguir, como se hizo en Europa, donde se desarrolló un gran trabajo en este ámbito, y se optó por los estándares internacionales de EMVCO. Consideramos que dichos estándares deben aplicar a todos los actores, para así no generar brechas de potenciales lagunas de seguridad, siendo, por tanto, el principal desafío el que estos criterios sean adoptados por los actores a lo largo de toda la cadena de medios de pago. Dicho lo anterior, la implementación e instauración del modelo PSD2 puede traer múltiples beneficios para el mercado nacional, al mejorar la seguridad de los pagos electrónicos y reducir el fraude, dos objetivos a los que apunta el mercado digital de pagos. En cuanto a la seguridad, específicamente, se deberá utilizar tecnología más avanzada y desarrollar nuevos sistemas y procesos para cumplir con las normas y reforzar la seguridad en los pagos electrónicos. Asimismo, es relevante destacar que todo aspecto cuyo objetivo sea generar mayor transparencia, promover la competencia y fomentar la innovación, es beneficioso para cualquier ecosistema, y el mercado digital no es la excepción. Es importante mencionar que, para que la implementación de un sistema como el PSD2 tenga los resultados deseados, resulta importante adecuarse al mercado y realidad nacional.

Junto con lo anterior, PSD2 es una normativa cuyo objetivo es más amplio que la seguridad y fraude. De todas formas, creemos que sería beneficioso establecer una normativa clara con respecto a refuerzos de seguridad y fraude de todos los actores de medios de pago, sean estos bancarios o no bancarios, siendo particularmente necesaria tal normativa en lo que dice relación con la verificación de la identidad del usuario y el cumplimiento de estándares mínimos de gestión de fraude.

En Europa actualmente existe un modelo que permite que los comercios no utilicen Secure 3DS en todas

las transacciones de tarjeta no presente, ahorrando el costo de fricción asociado, siendo necesario al efecto que se apliquen motores antifraude certificados y aprobados por instituciones definidas por los gobiernos. El uso de dichos motores permite un incremento en las ventas y una disminución del fraude, todo a un costo accesible para todo tipo de comercio, permitiendo la democratización de los pagos digitales.

Con la promulgación de la Ley Fintech se potenciarán los sistemas de pago alternativos y digitales, lo que probablemente generará la existencia de formas de pago más inmediatas con menores fricciones. Tal proceso debe aparejarse y darse de la mano con el desarrollo e implementación de elevados estándares de seguridad, impulsados por la nueva ley de protección de datos, que ayudará a crear sistemas más seguros para los clientes y usuarios. Tal proyecto de ley está inspirado en el Reglamento General de Protección de Datos de la Unión Europea, y su promulgación permitirá elevar el estándar en esta materia y convertirnos en un país adecuado para recibir las nuevas formas de pago.

En paralelo a la ley de protección de datos, también se encuentra el proyecto de Ley “Marco de Ciberseguridad”, que busca crear la institucionalidad necesaria para robustecer la ciberseguridad, como indica su nombre, y con ello formar una cultura pública en materia de seguridad digital que permita enfrentar las contingencias en el sector público y privado, y resguardar la seguridad de las personas en el ciberespacio.

En ChilePay estamos convencidos de que ambos cuerpos legales formarán parte del marco normativo aplicable a los Proveedores de Servicios de Pago, lo que contribuirá a un ecosistema digital más seguro y confiable para los usuarios.

En paralelo, se debe esperar la regulación de la CMF, cuya dictación e implementación esperamos pueda ser en el corto plazo de forma tal que sirva como gatillante para la materialización de los cambios.

En general, como Corporación, si bien estamos a la espera de la regulación de la Comisión para el Mercado Financiero, creemos que la entrada del modelo PSD2 será beneficioso para el mercado, pues (i) traerá seguridad en los pagos (que se verá reforzada con la promulgación de leyes); (ii) evitará el fraude, (iii) democratizará los pagos digitales, y (iv) permitirá la estandarización y mayores ventas.

En cuanto al fraude, hoy en día, los métodos de fraude más utilizados son el *pishing* y el *SIM swapping*. El primero consiste en que el delincuente se hace pasar por una persona de confianza para engañar a la víctima y lograr fácil acceso a todo tipo de datos, y, así, poder robárselos. Existe el *Smishing* (por SMS) y el *Vishing* (por voz), además, a través de correo electrónico, software malintencionado, objetivo definido, es decir, datos específicos de una persona previamente investigados; y de altos cargos, cuando el objetivo es alguien en posición influyente. El segundo se trata de un fraude que realizan los ladrones mediante la persuasión para que la víctima traslade los datos de la tarjeta SIM a otra que está en poder de ellos, de esta manera, obtienen acceso a una gran cantidad de datos.

En ChilePay, creemos que las mejores maneras para protegerse contra estos ataques son: (i) la difusión de información sobre enlaces maliciosos y la educación de los usuarios para que se percaten, de manera autónoma, del peligro de fraude; (ii) la exigencia de claves más robustas y eliminar el uso de datos personales, como el RUT, para autenticar, y la implementación de mecanismos de validación con métodos dinámicos; (iii) la *tokenización* de la información, es decir, que esta esté encriptada para evitar que se fugue del comercio; y (iv) la instalación de antivirus, específicamente contra los softwares maliciosos. Como Corporación creemos que todos son importantes, sin embargo, ponemos énfasis en la difusión y educación de los usuarios para que eviten exponerse a situaciones de vulnerabilidad.

III. CIBERSEGURIDAD

El tema de la ciberseguridad se ha ido desarrollando cada vez más, y se espera que continúe por este camino a razón directa con la proliferación de formas de pago digitales, razón por la que debe ser considerada una estrategia de negocio fundamental. En el pasado, considerando tal contexto, la ciberseguridad era solo un recurso, por cuanto la superficie y amplitud de red no tenía la capacidad o no se planteaba la posibilidad de que la misma pudiese extenderse; sin embargo, ahora dicha red se encuentra en constante cambio y expansión, crece conforme el negocio y el mundo lo hace. Si la ciberseguridad es considerada sólo un recurso, entonces no involucra una actualización constante porque se entiende como algo que vemos una vez, lo armamos y queda listo. Sin embargo, si tomamos en cuenta el precepto antes mencionado, la constante evolución de la red, la arquitectura de ciberseguridad debe ser constantemente monitoreada, estudiada y actualizada, debe crecer conforme los activos digitales lo hacen y extenderse a cada capa de la superficie. ChilePay considera que entender la ciberseguridad y tomar un rol activo en torno a la misma la convierte en una estrategia, lo que genera, de manera automática, que sea un activo primordial, en constante transformación y que por lo mismo debe ser atendida, actualizada y tratada como cualquier otra área de negocio que funcione bajo ese mismo principio, especialmente en un panorama creciente y cambiante en cuanto a amenazas y riesgos de ciberseguridad.

Existen varios peligros a los que se enfrentan las plataformas de pago, entre los cuales se encuentran la incapacidad para autenticar correctamente al usuario o tarjetahabiente, el aumento en la capacidad de los delincuentes para generar softwares malignos, el secuestro y robo de los datos, etc. En general, los riesgos en tema de ciberseguridad han ido en aumento con la aparición de las diferentes plataformas de pago; sin embargo, ChilePay considera que al trabajar en colaboración con los distintos actores y a la par con la implementación de políticas públicas, se puede combatir y prevenir los potenciales peligros.

Junto con lo anterior, es importante mencionar que son muchos los miembros de ChilePay que cuentan con un Sistema de Gestión de Seguridad de la Información (SGIS) cuyos lineamientos se encuentran alineados con las mejores prácticas internacionales en este tema. Tales sistemas exigen el cumplimiento de requisitos que acrediten la capacidad de operar bajo los estándares de seguridad. Con esto, miembros de la Corporación realizan auditorías sobre este tema a sus proveedores de servicios críticos, como los de medios de pago.

Contar con una arquitectura de seguridad o ciberseguridad es muy importante para las empresas, ya que están constantemente expuestas a amenazas cibernéticas. El desarrollo de esta arquitectura dependerá, en primer lugar, de la normativa de la CMF en relación con la Ley Fintech, y, en segundo, de las necesidades específicas de la empresa. ChilePay plantea que, para armar una arquitectura de seguridad, se debe (i) identificar los riesgos, tanto internos como externos; (ii) definir los objetivos de seguridad para establecer qué aspectos se deben proteger y el nivel de protección necesarios; (iii) diseñar una estrategia de seguridad basada en los objetivos identificados; (iv) implementar medidas de seguridad tales como *firewalls*, sistemas de detección de intrusiones, sistemas de autenticación, etc.; (v) impulsar una cultura de seguridad para que los usuarios sepan cómo deben comportarse para mantener un ambiente seguro; (vi) monitorear la seguridad para detectar posibles amenazas y ajustar lo que corresponda; (vii) realizar pruebas y auditorías de seguridad, junto con realizar las alianzas necesarias con expertos en el tema. Con todo lo anterior, la Corporación también contempla el beneficio de alinearse con los estándares globales e interoperables para asegurar una operación global y experiencia única al cliente. Las plataformas de pago son blancos muy deseados por los cibercriminales debido a la cantidad de datos bancarios que almacenan, por esta razón, la ciberseguridad es un activo clave para proteger a los usuarios dentro de las plataformas. ChilePay sostiene que contar con una plataforma amplia, integrada y automatizada de ciberseguridad se vuelve vital para mantener cada capa del sistema protegida y para poder monitorear, detectar y mitigar riesgos e incidentes antes de que sucedan.

IV. CONCLUSIÓN GENERAL

En ChilePay apostamos por la digitalización y la inclusión financiera. Para ello, es necesario marcar una hoja de ruta que permita atacar y evitar los posibles riesgos asociados a la proliferación de los medios de pago digitales, aprendiendo tanto de la experiencia de los países extranjeros como la de nosotros mismos para lograr implementar un sistema seguro, libre de fraude y con una interoperabilidad efectiva. Para lograrlo, es necesario colaborar entre todos los actores del ecosistema de medios de pago y el regulador, sin descuidar, no obstante, la educación financiera para que nadie se quede al margen de la digitalización.

