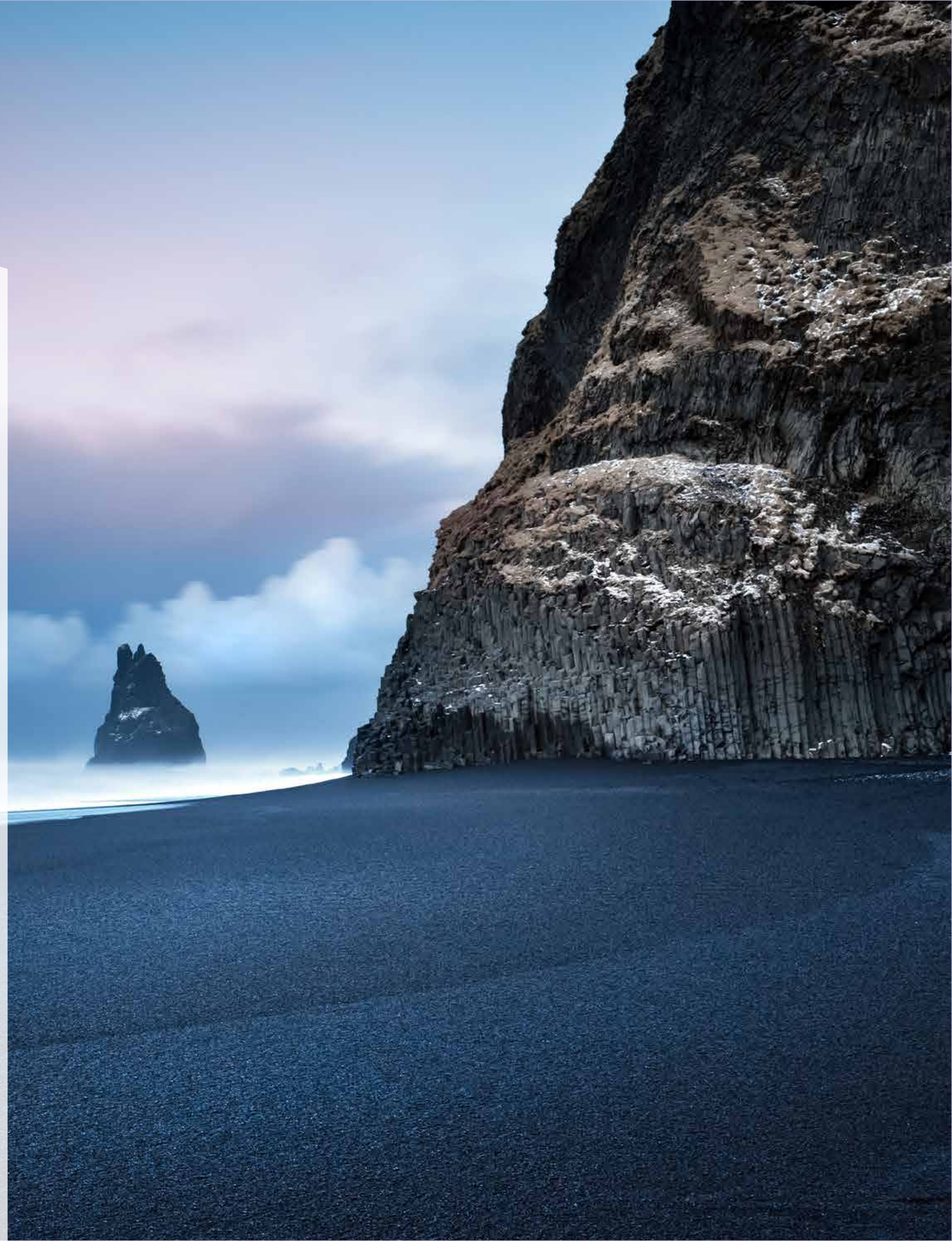
Tendencias

Seguridad en los pagos sin fricciones

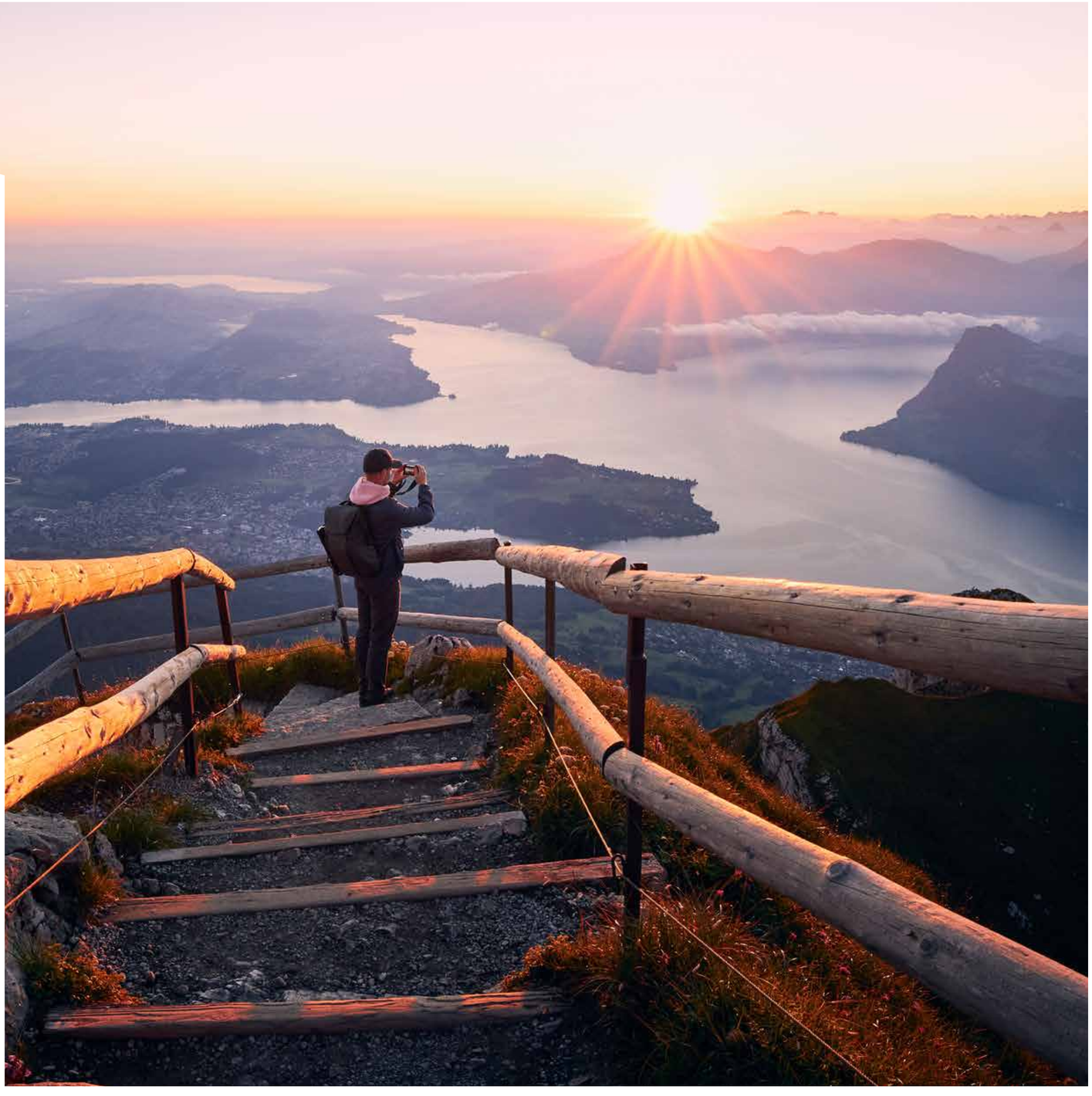
Con la colaboración de Afi



minsait payments

An Indra company

Índice



Principales conclusiones

1.

La seguridad ante fraudes y robos es el principal elemento que motiva la elección del medio de pago.

2.

Casi la mitad de los agentes de la industria consideran que los riesgos cibernéticos son el principal desafío para el ecosistema de los pagos digitales en los próximos cinco años.

3.

El eslabón más débil en términos de fraude y seguridad, que en última instancia determina la fortaleza del conjunto de la cadena de valor de los pagos, se localiza, en opinión del 62% de los agentes de la industria, en las personas usuarias de los medios de pago.

4.

La predisposición a adoptar medidas adicionales de seguridad que faciliten pagos sin fricciones más ágiles y sin contacto es mayor en Latinoamérica, mientras que la población europea es más reacia.

5.

Es casi unánime (88%) la consideración de que es necesario avanzar en la adopción de una identificación digital única e interoperable para la autenticación de los pagos.

6.

La principal aplicación de la IA en el ámbito de los pagos será la seguridad y prevención del fraude. La migración hacia soluciones de pago basadas en la nube es considerada mayoritariamente una opción razonable en términos de seguridad y escalabilidad.

La seguridad es un pilar fundamental de cualquier medio de pago, una condición necesaria para la adopción de innovaciones y nuevas experiencias de pago, y un atributo esencial para garantizar el adecuado funcionamiento de los pagos digitales en entornos de confianza para todas las partes. Es esencial comprender cómo se integra la seguridad en los diferentes contextos de pago.

Las infraestructuras financieras, entre las que se encuentran las de pagos, son infraestructuras críticas y estratégicas que precisan protección especial, máxima responsabilidad de las organizaciones que las administran, normativa y estándares adecuados y actualizados, además de importantes inversiones. En los últimos años se han producido muchos avances en materia regulatoria y supervisora, se han normalizado los necesarios procesos de colaboración entre los agentes de la industria y se ha fortalecido la responsabilidad de los usuarios de practicar medidas de prevención del fraude y de autoprotección adecuadas frente a los riesgos que pueden comprometer la seguridad de los pagos digitales.

En ese contexto, es importante vincular el concepto de seguridad y confianza con el instrumento de pago y con experiencias de pago ágiles y sin fricciones, para lo cual son imprescindibles avances tecnológicos como la tokenización, la biometría y la inteligencia artificial que habilitan nuevas experiencias frictionless sin comprometer la seguridad. También es importante vincular con los agentes no financieros que contribuyen al avance de las finanzas integradas y como proveedores de soluciones robustas en términos de seguridad.

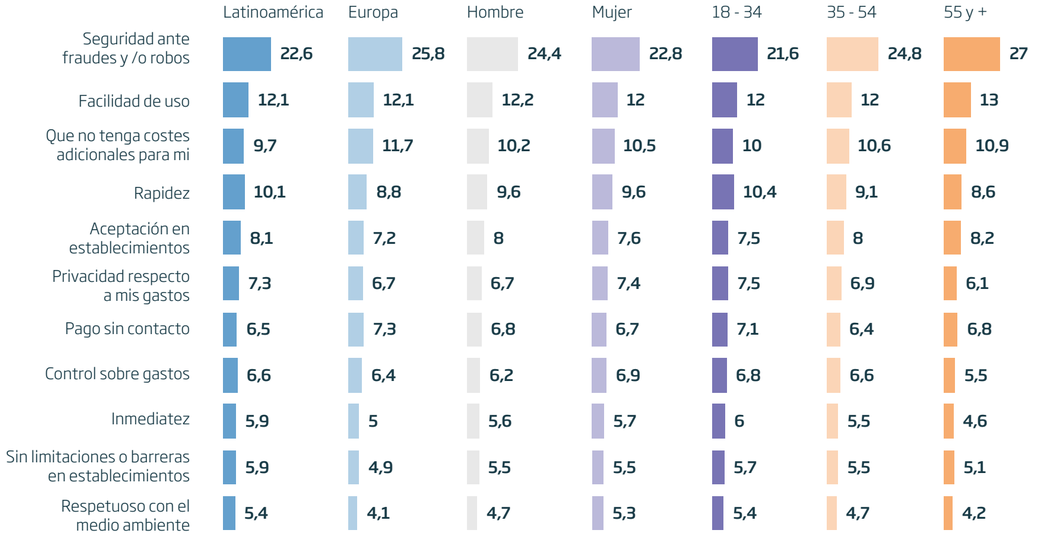
La seguridad, la facilidad de uso, la gratuidad y la rapidez, por ese orden, son los principales motivos que determinan la elección de un medio de pago, atributos deseados todos ellos transversales al conjunto de la población, aunque con pequeños matices: las personas de más de 55 años valoran en mayor medida la seguridad, una cualidad algo menos relevante entre la población más joven.

"Se estima que el coste del fraude mundial en ecommerce en 2023 llegó a los 48.000 millones de dólares, concentrándose en Europa el 26%."

Alicia Escribá
Google, EMEA

Figura 1.
Motivos por los que prefiere un medio de pago.
Porcentaje de población ABI. 2023

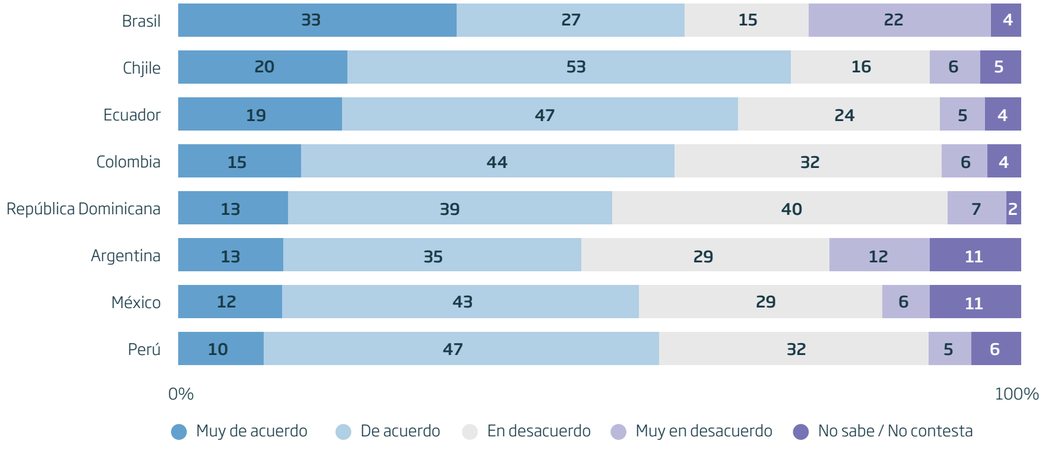
Nota: Responden a la siguiente pregunta: "Supongamos que tienes 100 puntos; asigna estos puntos a los siguientes aspectos relacionados con los distintos medios de pago según sean importante para ti y que te harían decidirte por un medio de pago u otro."



La seguridad de los pagos digitales es asimismo un atributo que las personas consideran mayoritariamente innato al medio de pago. De hecho, el Latinobarómetro 2023 refleja que, para una amplia mayoría de la población de Latinoamérica salvo tímidamente en Argentina, pagar electrónicamente es más confiable que pagar en efectivo. Destacan positivamente los chilenos (72,6%), ecuatorianos (66,4%), brasileños (60,2%) y colombianos (58,8%) en esa mayor percepción de seguridad de los pagos digitales.

Figura 2.
Pagar electrónicamente es más confiable que pagar en efectivo

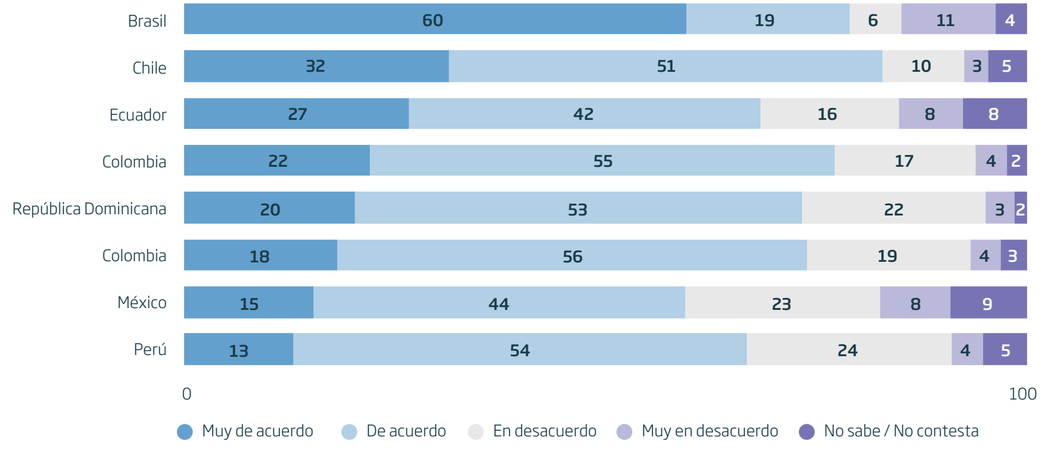
Fuente: Afi, a partir de Latinobarómetro 2023.



La seguridad de los pagos digitales está asociada también a un menor riesgo físico del tenedor del medio de pago. Así, de forma mayoritaria, aunque con mayor intensidad en Brasil, las personas perciben que es más seguro circular por la calle sin dinero en efectivo y pagar todo electrónicamente. México, sin embargo, es el país donde menor prevalencia tiene esta afirmación, con más del 30% de las personas en desacuerdo con la misma.

Figura 3.
Es más seguro circular por la calle sin efectivo y pagar todo electrónicamente

Fuente: Afi, a partir de Latinobarómetro 2023.

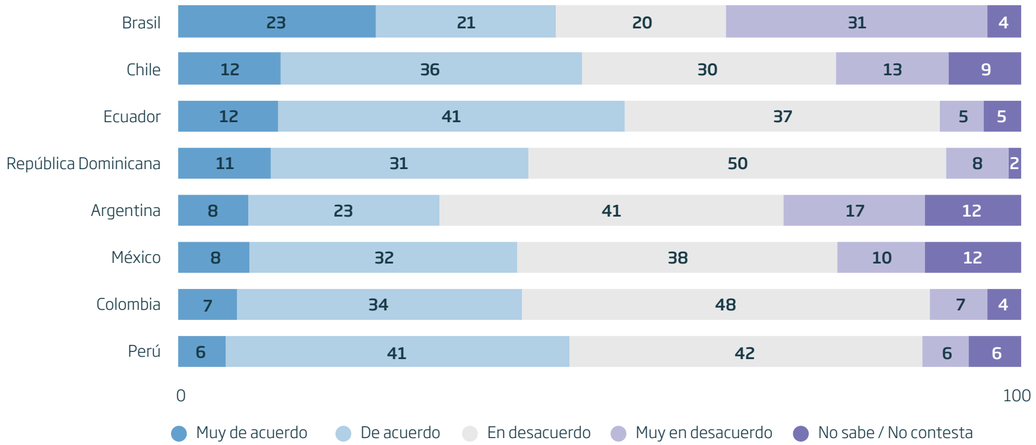


"Siempre buscamos garantizar la mayor seguridad dentro del servicio brindado, pero hay que tener presente que, a mayor seguridad, la UX (user experience) sufre más fricción, por lo que hay que encontrar un balance entre seguridad y UX."

Leonardo González
Sales Director (Europe & Latam), Afterbanks Arcopay

Figura 4.
Mis datos personales están más seguros cuando pago electrónicamente

Fuente: Afi, a partir de Latinobarómetro 2023.



Los expertos que han atendido el Barómetro de Tendencias destacan como principal desafío para el ecosistema de los pagos digitales en los próximos cinco años la amenaza de aumento de los riesgos y vulnerabilidades cibernéticas, señalado como tal por el 44%, siete puntos por encima del desafío de la Interoperabilidad, un atributo también esencial analizado en la Tendencia 1. Una respuesta que se anticipaba mayoritaria y que ha motivado la elección de esta temática relacionada con la seguridad de los pagos en esta Tendencia 3.

El aspirado equilibrio entre seguridad y experiencia de usuario -apuntado como un importante reto entre los agentes de la industria ya que se constata que una mayor seguridad puede complicar los procesos de pago- depende en gran medida del método de pago o de la plataforma en la que se materialicen los pagos, distinguiendo de este modo los pagos con tarjeta de los pagos desde cuenta, y los pagos presenciales de los remotos, fundamentalmente.

"La mejor experiencia de pago es aquella que no recuerdas: ágil, segura y sin fricciones."

Eduardo Prieto
Director general de Visa en España

Figura 5.
¿Cuáles considera los principales desafíos para los pagos digitales en su región en los próximos 5 años?
Respuesta múltiple. Barómetro de tendencias 2023.

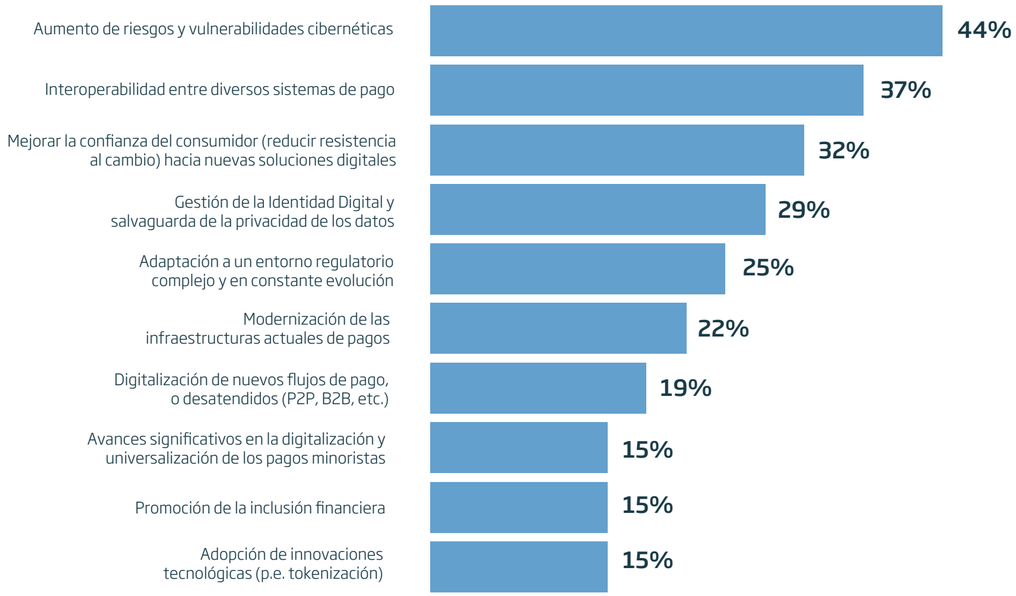
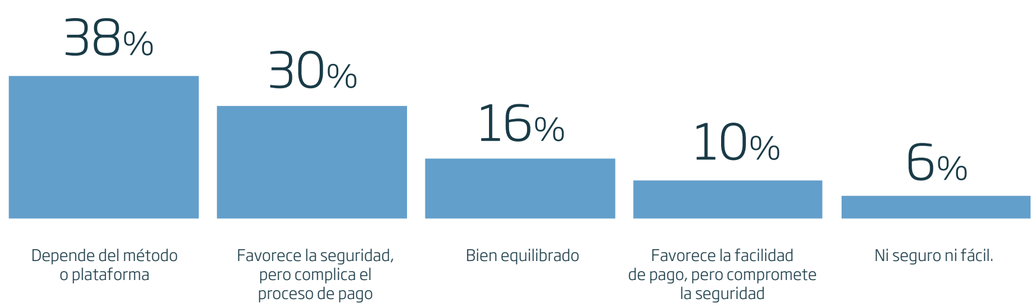


Figura 6.
¿Cómo evaluaría el equilibrio actual entre seguridad y experiencia de pago del usuario?
Respuesta única. Barómetro de tendencias 2023.



Inmediatez, interoperabilidad, apertura, ingeniería social y ubicuidad: elementos que retan a la seguridad

El mundo de los pagos remotos o no presentes, e incluso los pagos físicos que se realizan a través de Internet, impone dos retos: la identificación / autenticación y el traslado de la información, que puede encontrarse comprometida en algunos de los puntos de la cadena de pagos. A ellos se une la mala fe de algunos titulares legítimos de medios de pago, por ejemplo, ejerciendo el denominado **fraude en primera instancia (o first-party fraud en inglés)** que ocurre cuando una persona tergiversa a sabiendas su identidad o da información falsa para obtener ganancias financieras o materiales, pudiendo materializarse de diversas formas. Entre las más habituales está el **fraude de contracargo o fraude amigo,** cuando un cliente solicita el reembolso de una transacción de compra de un artículo o servicio que afirma que no ha recibido o que no es como esperaba. También se producen **fraudes en la solicitud,** cuando un cliente proporciona información falsa sobre sus datos personales, como su nivel de ingresos, para obtener un resultado más favorable.

En términos de identificación, el **Carding** es una modalidad de fraude en la que los delincuentes utilizan información de tarjetas robadas para realizar transacciones no autorizadas.

Interpol[1] señala que el **fraude basado en la ingeniería social,** que ha crecido mucho desde la irrupción de la pandemia, abarca todos los métodos utilizados por los delincuentes para explotar la confianza de una persona con el fin de obtener dinero o información confidencial que les permita acceder a su dinero de forma ilegítima y engañosa. Los medios de comunicación digitales, incluidas las redes sociales, son el canal preferido, aunque también se puede realizar por teléfono o en persona. Destacan en los últimos tiempos las estafas mediante **Phishing, Vishing, SMShing y Spoofing.**

"En la medida en que estamos más digitalizados, la sofisticación de los malhechores es mayor, y por lo tanto los riesgos aumentan."

Ángel Nigorra
CEO de Bizum

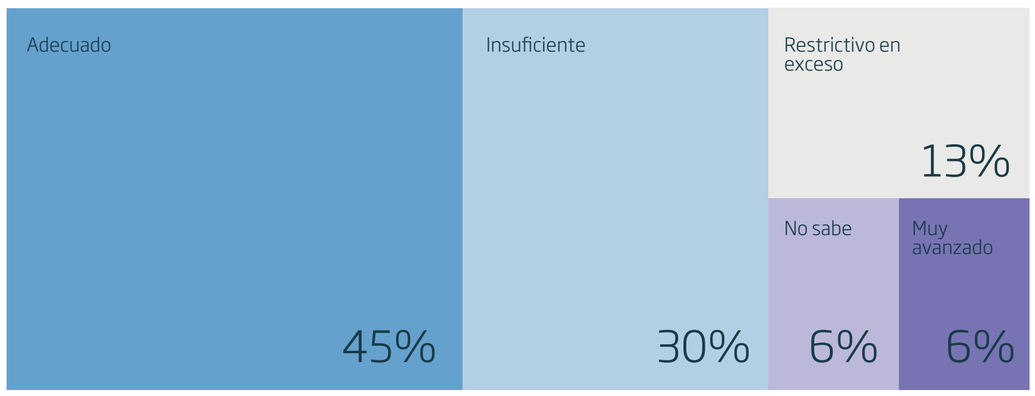
[1] https://www.interpol.int/es/Delitos/Ciberdelincuencia

Las estafas a empresas por e-mail mediante suplantación de identidad obtienen información sobre sistemas de pago corporativos, y engañan a empleados para que realicen pagos a los delincuentes. También son habituales los intentos de estafas románticas, a través de falsas oportunidades de empleo o los fraudes de inversión.

Una vez cometida la estafa u operación ilícita, los delincuentes recurren al blanqueo del dinero para lo que suelen utilizar mulas bancarias, personas que conscientemente o sin saberlo facilitan sus cuentas bancarias (cuentas mula) para recibir y transferir fondos fraudulentos. Cuando esas transferencias se producen en tiempo real -pagos instantáneos-, el margen de maniobra en términos de tiempo disponible para su detección tiende a cero, y obliga a disponer de tecnologías y servicios sofisticadas.

En términos de regulación, una casi mayoría de participantes de la industria (45%) considera que el marco actual en relación con la seguridad es adecuado, pero un 30% lo califica de insuficiente. Las críticas a un excesivo celo regulatorio apenas concentran el 13% de las respuestas, por lo que a priori existiría margen en la predisposición de los agentes para un fortalecimiento de normas, estándares y herramientas de supervisión de su cumplimiento.

Figura 7.
¿Cómo valora el marco regulatorio actual en relación con la seguridad de los pagos digitales?
Respueta única. Barómetro de tendencias 2023.



"El fraude es muy sofisticado y organizado, utiliza tecnologías exponenciales de machine learning e IA para suplantar identidades. Aprovechan vulnerabilidades del ecosistema como las de algunas fintech no vigiladas y sin buenas prácticas de seguridad."

Edwin Zácipa
Latam Fintech

"Se observan de forma creciente intentos de fraude tanto a nivel tecnológico como de ingeniería social, y la industria está acelerando procesos como hacer las tarjetas de pago numberless, sin información visible."

Sebastián Quevedo
Vicepresidente de Produbanco

"El contrapunto de la instantaneidad de los pagos es el fraude. Se trata de un asunto que preocupa mucho en el sector porque dificulta la generalización de los pagos instantáneos y el desarrollo del negocio bancario. La instantaneidad otorga menos margen de maniobra, obligando a actuar ex ante y a utilizar tecnologías muy innovadoras, como la inteligencia artificial y algoritmos de machine learning."

Juan Luis Encinas
CEO de Iberpay

"El fraude no se reduce con más regulación, sino con más tecnología."

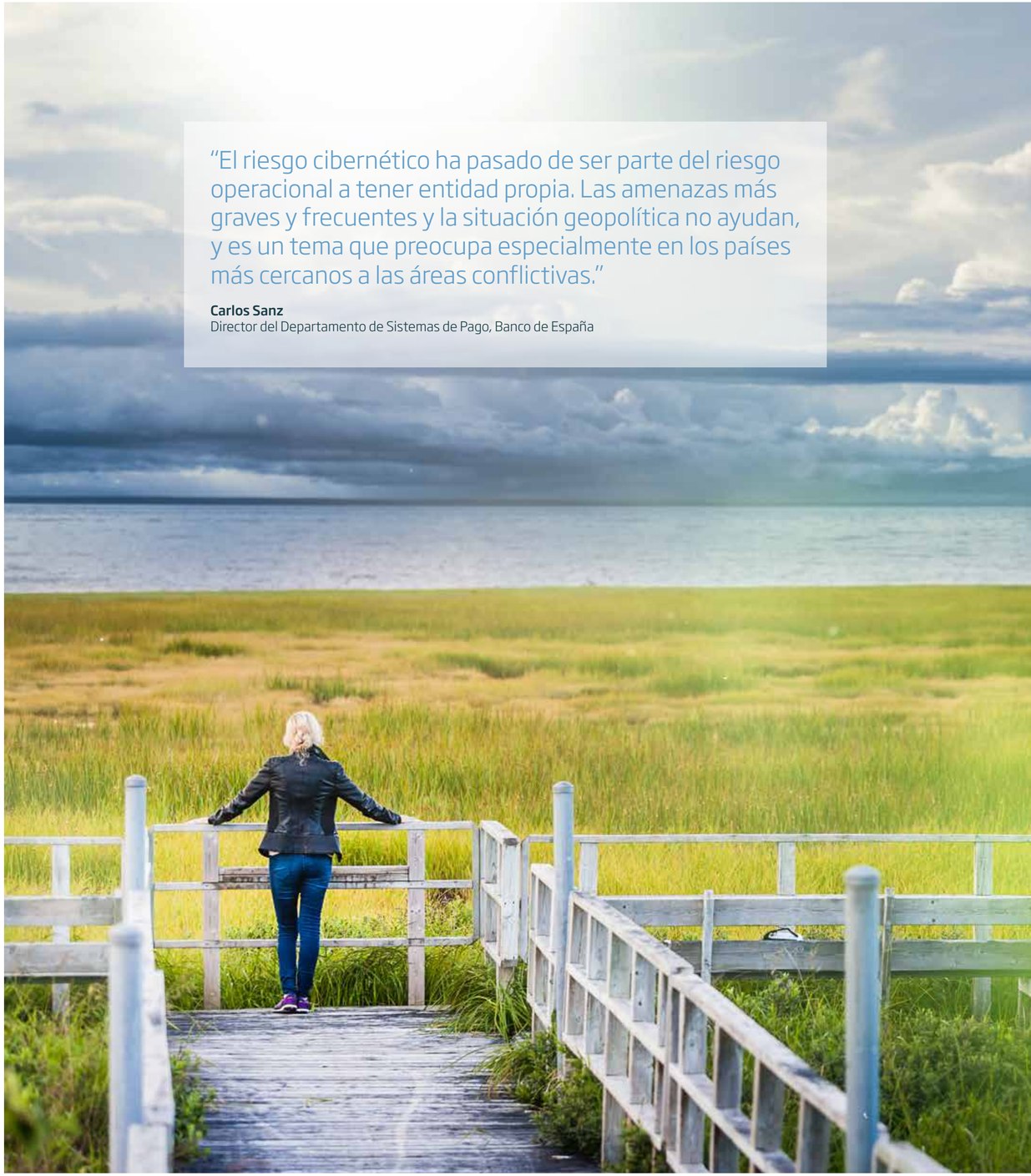
Edwin Zácipa
Latam Fintech

Las infraestructuras de los mercados financieros, entre las que se encuentran las que sustentan los sistemas de pagos, son críticas a efectos de ciberseguridad. Un ciberataque puede provocar eventos de importancia sistémica, de efectos prolongados y con una lenta reversibilidad y recuperación. Las nuevas tecnologías, la inmediatez y la interoperabilidad de las infraestructuras con otras plataformas y con sus participantes (entre los que se encuentra un creciente ecosistema de TPP y fintech) facilitan la propagación y ampliación de los efectos de los ciberataques, así como las vías de acceso de amenazas. Por todo ello, la ciberseguridad de las infraestructuras críticas es (o debe ser) un asunto de seguridad nacional.

En la medida en que la naturaleza de las amenazas cibernéticas es cambiante y está en continua evolución, la regulación, la supervisión, la cooperación y el intercambio de información y de experiencias (cyber intelligence) son elementos clave para lograr una mayor seguridad. Orientaciones como la Guía del Comité de Pagos e Infraestructuras de Mercado del BIS sobre ciberresiliencia[2] de 2016 tienen ese propósito.

Por su parte, el Índice Mundial de Ciberseguridad (GCI, por sus siglas en inglés), inaugurado en 2015 por la Unión Internacional de Telecomunicaciones (UIT) para medir el compromiso de 193 Estados Miembros con la ciberseguridad, contribuye a identificar áreas de mejora y alentar a los países a tomar medidas para que los países mejoren su ciberseguridad. De acuerdo con el GCI más reciente, Reino Unido, España, Portugal, Brasil e Italia se encuentran cercanos a la "perfección" (puntuación por encima de 90 puntos sobre 100). El más rezagado (26 puntos) es Ecuador, mientras que el resto de los países oscilan entre los 50 puntos de Argentina y los 81 de México.

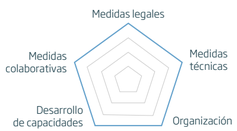
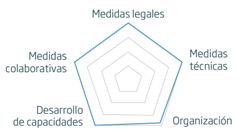
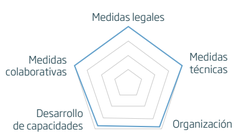
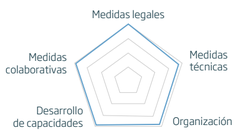
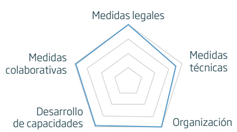
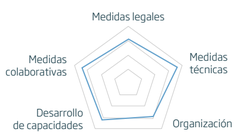
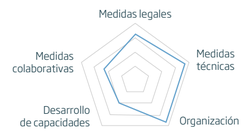
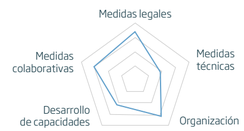
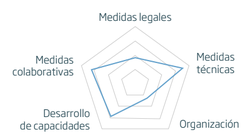
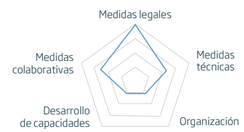
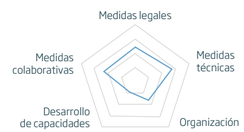
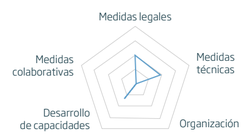
El Informe emite recomendaciones en torno a los aspectos legales, técnicos, organizativos, de desarrollo de capacidades, y de colaboración valorados. De este modo, sugiere acelerar y reforzar la planificación de futuras intervenciones legales en Argentina, Colombia y Ecuador; desplegar CIRT/CERT en Chile, Ecuador y Perú; alinear estrategias en Argentina, Colombia, Ecuador y Perú; desarrollar capacidades en ciberseguridad en Argentina, Chile, Colombia, Ecuador, Perú y República Dominicana; y abordar la acción colectiva en materia de ciberseguridad en Ecuador y República Dominicana.



[2] https://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf

Tabla 1.
Resultados del Global Cibersecurity Index 2020

Fuente: Global Cibersecurity Index 2020[3]

País	Puntuación global	Ranking global	Fortalezas
Reino Unido	99,54	2	
España	98,52	4	
Portugal	97,32	14	
Brasil	96,60	18	
Italia	96,13	20	
México	81,68	52	
República Dominicana	75,07	66	
Chile	68,83	74	
Colombia	63,72	81	
Perú	55,67	86	
Argentina	50,12	91	
Ecuador	26,30	119	

[3] https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

"Las entidades están venciendo la resistencia a compartir información, a pesar de ser información sensible. Entienden que, si se confía en que, por ejemplo, la IA proporcione nuevas herramientas de lucha contra el fraude y otros riesgos de seguridad, hace falta información con la que alimentar los algoritmos."

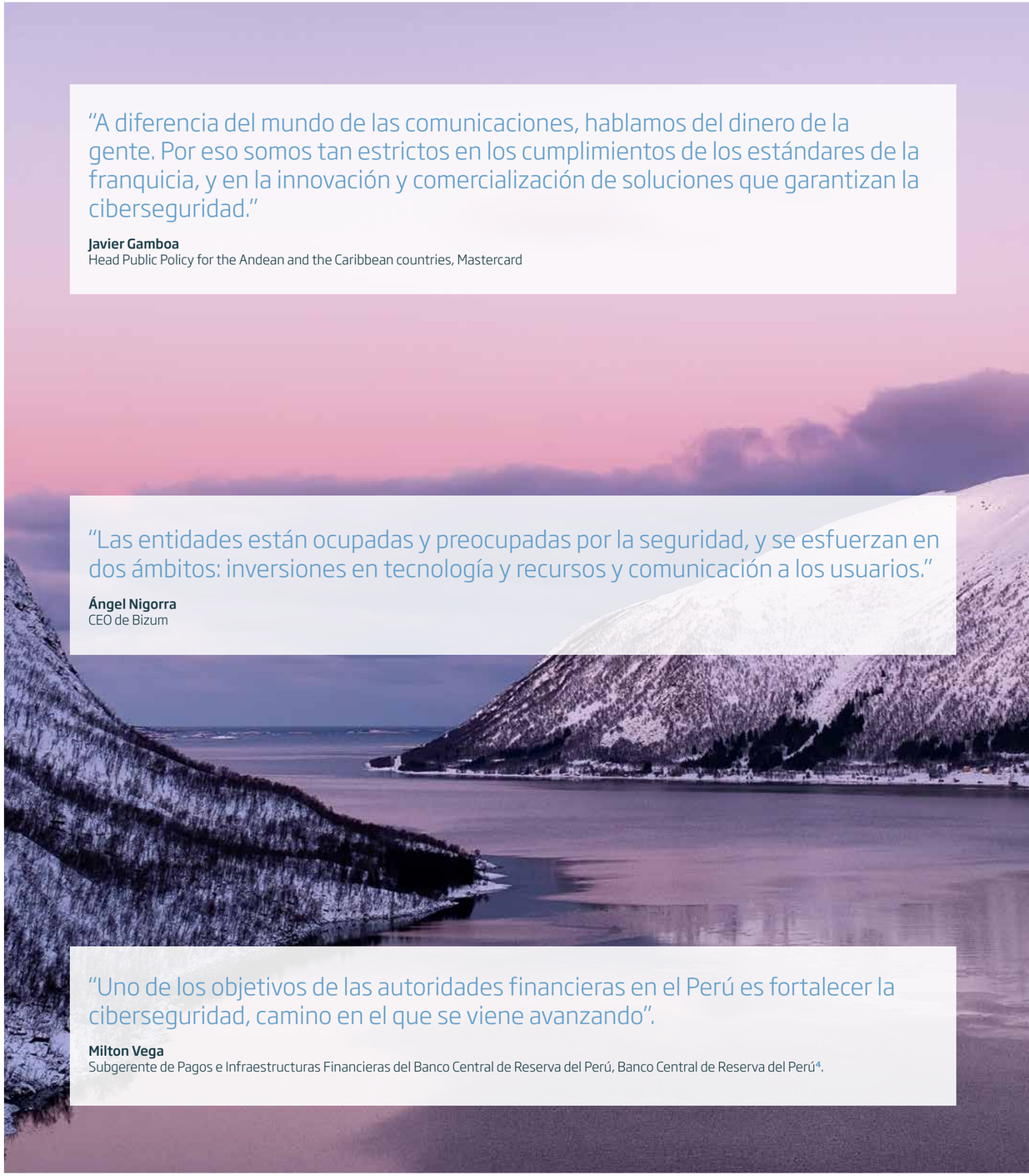
Javier Santamaría
Chair del European Payments Council - Presidente de Iberpay

Como se aprecia, aunque de forma implícita, la inversión en tecnología de prevención del fraude y para el fortalecimiento de la ciberresiliencia es irrenunciable en el actual contexto de inmediatez, interoperabilidad, apertura, ubicuidad y sofisticación de las amenazas de fraude. Y afecta tanto a los agentes proveedores de productos y servicios como al regulador y supervisor.

Pero **el eslabón más débil en términos de fraude seguridad, que en última instancia determina la fortaleza del conjunto de la cadena de valor de los pagos, se localiza, en opinión del 62% de los agentes de la industria, en las personas usuarias de los medios de pago**. El resto de las agentes de la cadena de valor se reparten el 38% restante de las respuestas, ninguno de ellos superando el 10% de las respuestas que transitan desde ese 10% que considera que dicha debilidad se concentra en el punto de venta, el 8% que lo asocia a los proveedores terceros o a los dispositivos, el 6% al personal, el 4% a los emisores y el 2% que lo asocia a las infraestructuras.

"El Banco Central cuenta con un Centro de Respuesta a Incidentes de Seguridad Cibernética y de la Información (CSRIT) orientado al sistema financiero y de pagos, que conjuntamente con otras acciones normativas y del gobierno, ha propiciado el ascender al país muchas posiciones en la evaluación de la ciberseguridad. Este centro ha sido muy bien acogido por los agentes del sistema porque aporta seguridad y permite gestionar mejor los riesgos."

Yilmari Rosario
Consultora del Banco Central de la República Dominicana



"A diferencia del mundo de las comunicaciones, hablamos del dinero de la gente. Por eso somos tan estrictos en los cumplimientos de los estándares de la franquicia, y en la innovación y comercialización de soluciones que garantizan la ciberseguridad."

Javier Gamboa
Head Public Policy for the Andean and the Caribbean countries, Mastercard

"Las entidades están ocupadas y preocupadas por la seguridad, y se esfuerzan en dos ámbitos: inversiones en tecnología y recursos y comunicación a los usuarios."

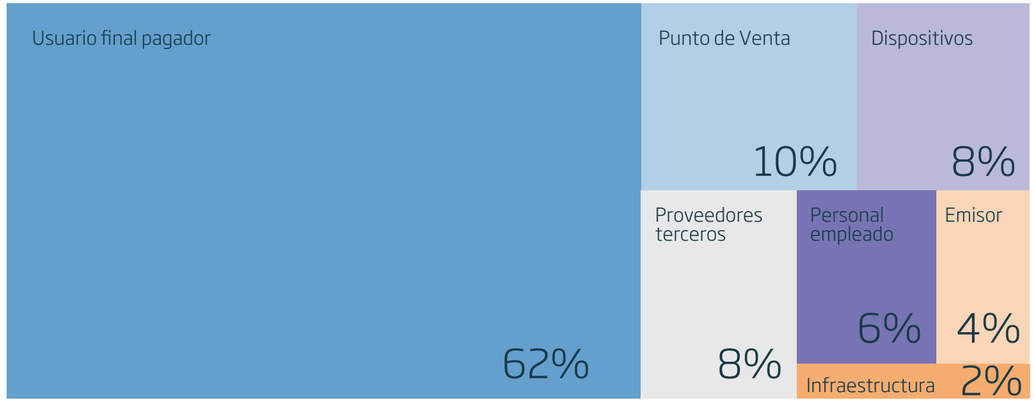
Ángel Nigorra
CEO de Bizum

"Uno de los objetivos de las autoridades financieras en el Perú es fortalecer la ciberseguridad, camino en el que se viene avanzando".

Milton Vega
Subgerente de Pagos e Infraestructuras Financieras del Banco Central de Reserva del Perú, Banco Central de Reserva del Perú[4].

[4] Las opiniones del Sr. Vega no reflejan necesariamente las del Banco Central de Reserva del Perú o de su directorio

Figura 8.
¿Cuál considera que es el eslabón más débil en materia de fraude y seguridad en la cadena de valor de los pagos?
Respuesta única. Barómetro de tendencias 2023



No en vano, los expertos consideran que la estrategia hoy más eficaz para el fortalecimiento de la seguridad de los pagos de bajo valor es la educación financiera y digital de los usuarios, con una valoración de 5,9 sobre 7.

"Hay una punta que es muy difícil del controlar y es el consumidor. Ha de ejercer su parte de corresponsabilidad y autoprotección, y requiere educación financiera y digital."

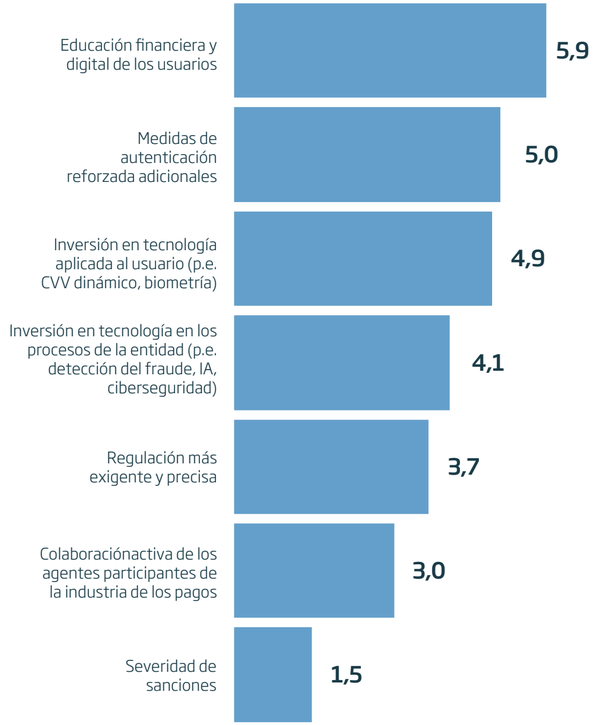
Edwin Zácipa
Latam Fintech

"La normativa PSD2 incorpora la obligatoriedad del segundo factor de autenticación (2FA) para asegurar que todos los pagos sean seguros y que no haya suplantaciones de identidad al momento de ejecutar una operación"

Leonardo González
Sales Director (Europe & Latam), Afterbanks Arcopay

Figura 9.
Orden de eficacia de las estrategias de fortalecimiento de la seguridad en los pagos de bajo valor.
Respuesta múltiple. Barómetro de tendencias 2023.

Nota: La puntuación es la media ponderada invertida una vez ordenadas las opciones de acuerdo con la siguiente valoración: 1 para la estrategia más eficaz; 7 para la estrategia menos eficaz.



"Los bancos tienen una regulación de seguridad muy estricta sobre factores de autenticación. Pero en ausencia de una Política Nacional de Ciberseguridad y en presencia de grandes divergencias regulatorias, el resto de las agentes con los que la banca se conecta no tiene esas obligaciones. Es necesario que las fintech busquen autorregularse."

Ljuvica Vodanovic
Fundadora de Vodanovic

"Sigue faltando educación financiera y autoprotección en la gente. Ya que siguen usando fechas de cumpleaños, direcciones, 1234, claves anotadas en papel, etc. que son fáciles de sustraer. Realizamos constantemente campañas para prevenir estas prácticas y educar al cliente. Llama la atención, la brecha de conocimiento y educación financiera y digital que existe en el país, la cual debemos incorporar como un importante desafío a resolver."

Mauricio Medina
Prepago Los Héroes

Las medidas de autenticación reforzada adicionales se sitúan en segundo lugar en términos de eficacia percibida con una valoración de 5,0, y en tercer y cuarto lugar las inversiones en tecnología aplicada al usuario (tales como el CVV dinámico o la biometría) con un 4,9, y en los procesos de la entidad (detección del fraude, ciberseguridad, IA) con un 4.1, respectivamente.

La Inteligencia artificial se ha erigido como una herramienta revolucionaria de prevención contra el fraude. Es prácticamente unánime (81%) el convencimiento de que la principal aplicación de la IA en el ámbito de los pagos digitales será la seguridad y la prevención del fraude. En el top 5 de aplicaciones de la IA, y treinta puntos por detrás de la seguridad se sitúan el análisis de riesgo (52%), la automatización de procesos (43%), la identidad digital (40%), y la personalización (38%).

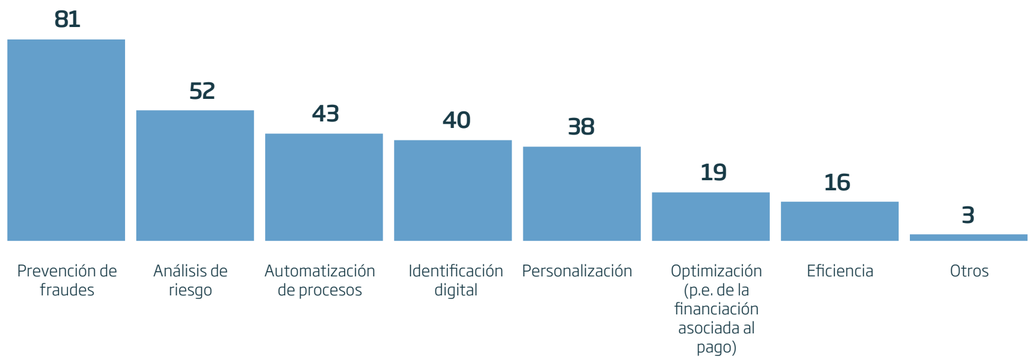
"La normativa de PSD2 incorpora la obligatoriedad del del segundo factor de autenticación (2FA) para asegurar que todos los pagos sean seguros y que no haya suplantaciones de identidad al momento de ejecutar una operación."

Leonardo González
Sales Director (Europe & Latam), Afterbanks Arcopay

"La confianza y la seguridad son fundamentales para el consumidor y también para que el comercio prospere. Por supuesto está en el centro de todo lo que hacemos en Visa. Hemos invertido 9.000 millones en tecnología para prevención del fraude en los últimos cinco años y contamos con más de 1.000 especialistas en ciberseguridad en todo el mundo, lo que nos ha permitido evitar unos 40.000 millones de euros en pérdidas relacionadas con el fraude en el año 2023."

Eduardo Prieto
Director general de Visa en España

Figura 10.
En el contexto de la inteligencia artificial (IA), ¿cuál cree que será su principal aplicación en el ámbito de pagos?
Respuesta múltiple. Barómetro de tendencias 2023



"Con IA el mayor ángulo de desarrollo tradicional en Mastercard es en materia de seguridad. También es una herramienta útil para consolidar datos y en la creación de experiencias y servicios más personalizados."

Javier Gamboa
Head Public Policy for the Andean and the Caribbean countries, Mastercard

"Proveemos a los emisores todos los análisis de datos que realiza Mastercard en tiempo real -más de 200 factores en microsegundos- para confirmar que la compra es segura en todas sus etapas. Adquirimos NuData Security para incorporar la IA en el análisis de biometría del comportamiento en el momento de la autenticación e identificación; disponemos de nuestras soluciones de scoring de riesgo en tiempo real "Decission Intelligence" y "Safety Net" para eliminar el fraude durante la transacción, y vamos a lanzar este año nuestra solución "AML Account Risk" para ayudar a las entidades a identificar los posibles movimientos relacionados con el lavado de capitales."

Alberto López
VP Digital Assets Security Mastercard

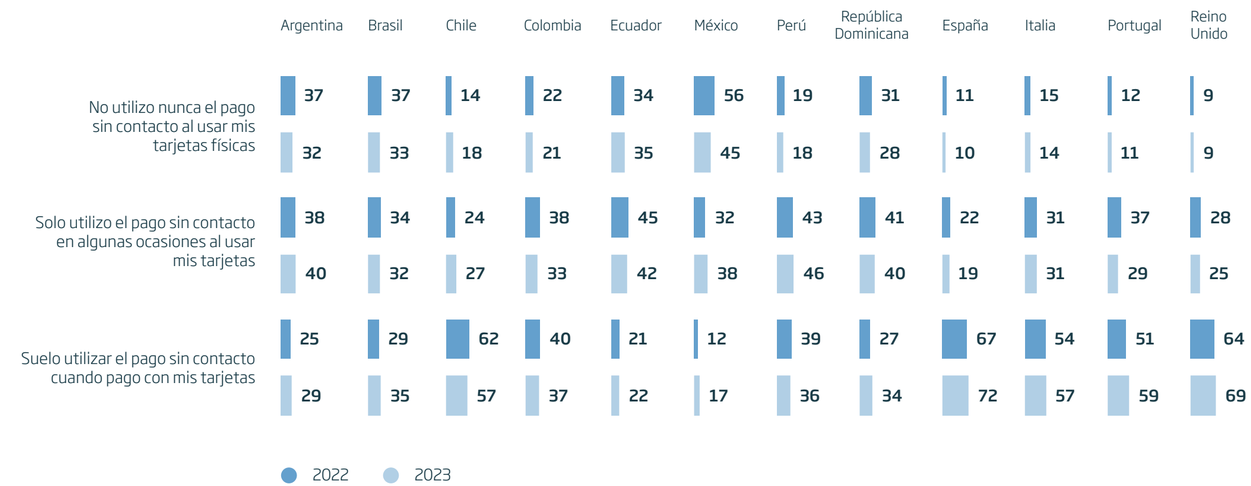
Las personas quieren pagar rápido y de forma segura

La percepción de seguridad que se traslada en este Informe se constata a través de preguntas directas acerca de este atributo, y de la constatación del uso que las personas realizan de sus medios de pago digitales. Y en este contexto, los pagos contactless con tarjeta y con smartphone son, por su mayor recurrencia y cotidianeidad, un buen punto de partida.

El pago contactless con tarjeta física es mayoritario en Europa, pero aún no lo es en Latinoamérica. Salvo en Chile, que presenta un comportamiento parecido al de Italia o Portugal, el pago contactless con tarjeta sólo se usa mayoritariamente de forma ocasional.

La adopción del pago contactless es gradual y también desigual en Latinoamérica. Aunque México sigue siendo el país más reticente al pago contactless con tarjeta, quienes declaran desde allí no usarlo nunca dejan de ser una mayoría (45%). En el extremo opuesto se encuentra Chile, único país de la región donde una mayoría declarada de personas (57%) usan el pago con tarjeta contactless de forma habitual.

Figura 11.
Uso del sistema contactless para el pago con tarjetas físicas.
Población ABI 2023



"Google ofrece su propia API (botón de pagos Google Pay) que permite realizar pagos de forma rápida y sencilla en un solo clic. Cuando el usuario selecciona un método de pago, Google Pay envía el token de pago al proveedor de servicios de pago, un proceso más seguro ya que la información real de la tarjeta no se utiliza ni se almacena."

Alicia Escribá
Google EMEA

En Europa, el uso habitual del pago contactless es mayoritario, especialmente en España, donde el 72% así lo reconoce, seguido de cerca por Reino Unido (69%). Confirmado el pago contactless como una tendencia sólida, existe un amplio margen de progresión en su adopción en Latinoamérica.

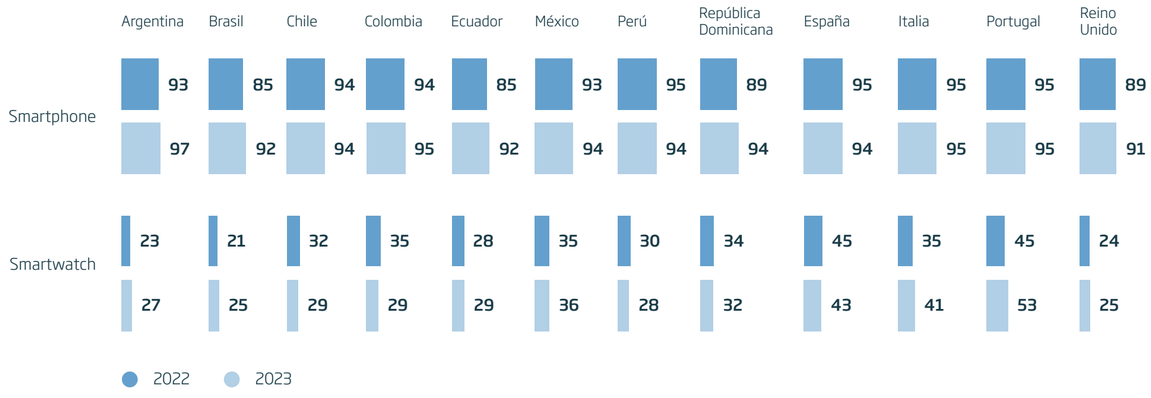
Un aliado imprescindible de esta adopción es el smartphone, que ha incrementado su cuota de mercado y ya supera el noventa por ciento de la población Adulta Bancarizada Internauta (ABI) en todos los países, por lo que puede considerarse ya un dispositivo prácticamente universal. El smartwatch, sin embargo, parece haber alcanzado ya su máximo y sólo supera el 50% de tenencia en Portugal.

El uso del smartphone como dispositivo de pago crece en prácticamente todos los países. La universalización del smartphone va unida a un importante incremento del uso de dicho dispositivo para pagar, tanto de forma habitual como ocasional, salvo en Italia. Simultáneamente, desciende el desconocimiento de esta funcionalidad nativa de los smartphones, que cae a la mitad del registrado el año anterior en Brasil, Chile y todos los países europeos.

Así, la generalización de dispositivos inteligentes con tecnología NFC u otra que permita pagos sin contacto, y su mayor notoriedad pública, hace suponer que sea cada vez empleado por un mayor porcentaje de población, y que esta lo haga más frecuentemente. De hecho, aumentan los dos comportamientos más positivos: el uso habitual y el uso ocasional.

Las medidas de seguridad en los pagos con tarjeta han evolucionado e innovado para aplacar las nuevas amenazas: desde el estándar de banda magnética y firma manuscrita al binomio chip y pin, y ahora, gracias a la tokenización para pagos NFC, 100% contactless.

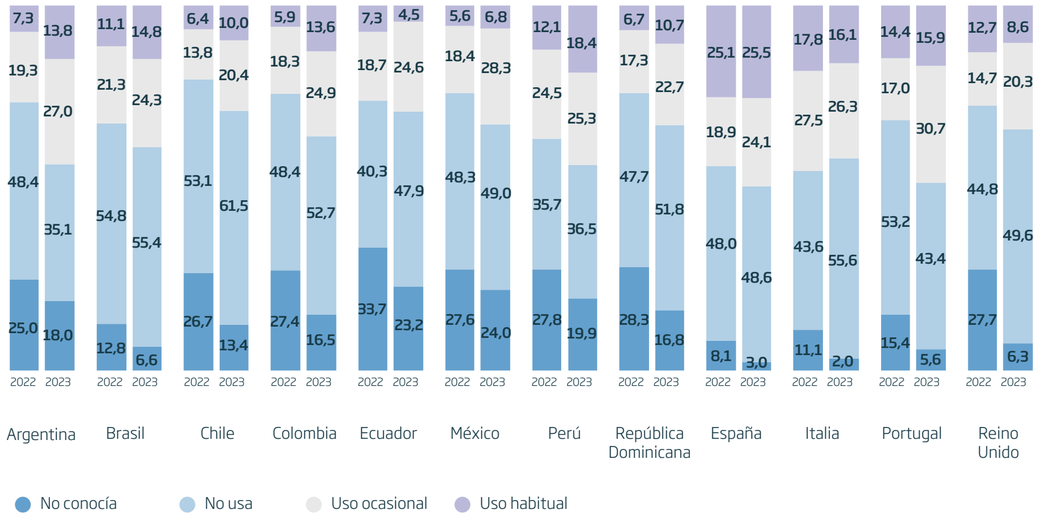
Figura 12.
Porcentaje de población ABI que dispone de teléfono inteligente y/o reloj inteligente.
2023



"En Ecuador se produce la captura de información en comercios porque no hay cultura de acercar el datáfono al cliente, sino que aún se entrega la tarjeta de pago."

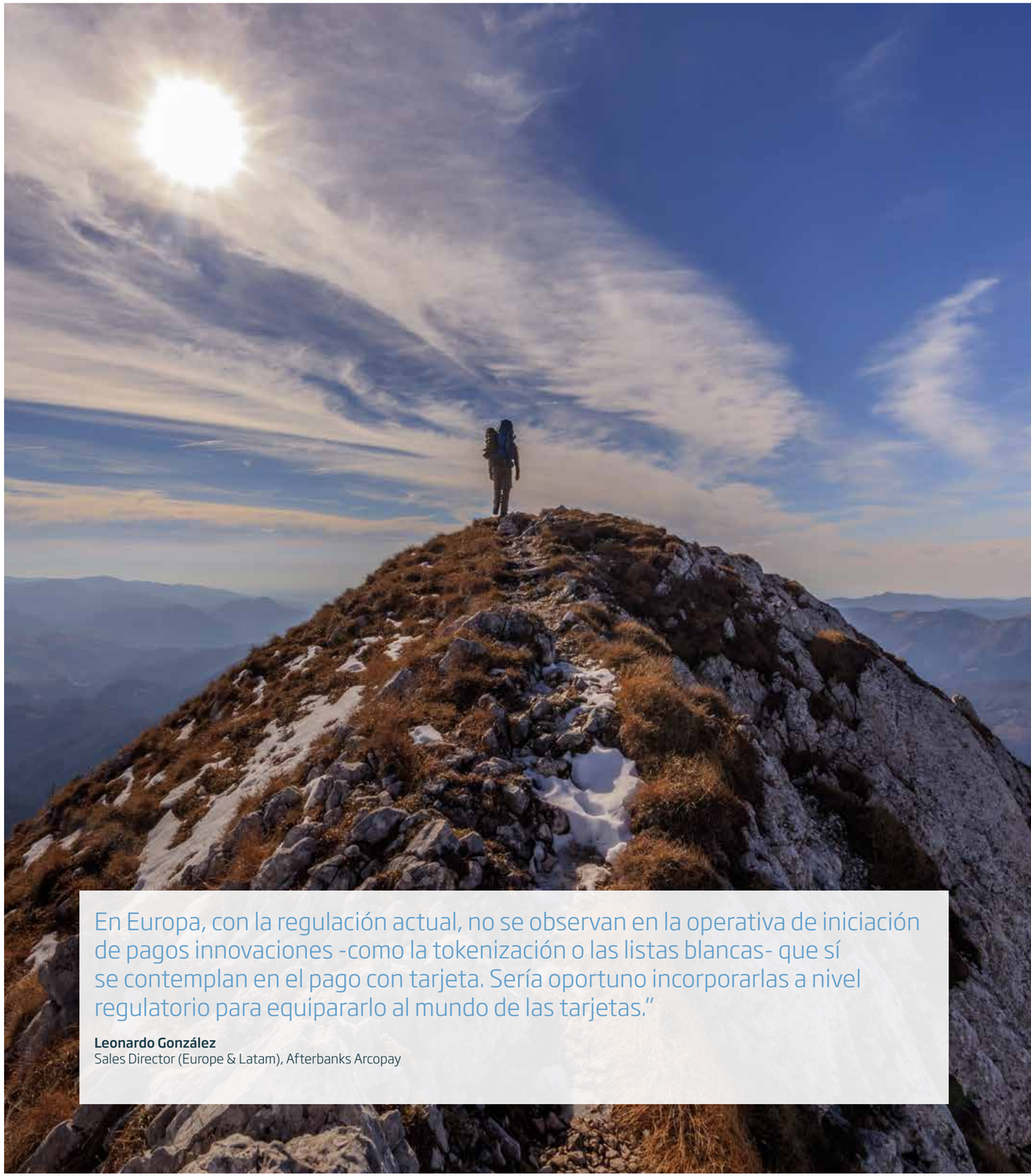
Sebastián Quevedo
Vicepresidente de Produbanco

Figura 13.
Relación de la población ABI con el pago contactless con teléfono o reloj inteligente.
2023



La tokenización, cuando se aplica a la seguridad de los datos, es el proceso de sustitución de un conjunto sensible de datos por un equivalente no sensible (token), sustitución que permite una exposición mínima de datos confidenciales a los dispositivos, aplicaciones, archivos, personas o procesos que los reciben. La conversión a token es un método de protección de los datos sensibles para cumplir con los estándares de la industria de pagos (como el Payment Card Industry Data Security Standard o PCI-DSS) así como regulaciones de protección de privacidad y datos (RGPD o equivalentes) y/o de Open Banking (PSD2 o equivalentes).

Los pagos digitales apalancan el proceso de autenticación del medio de pago en la tecnología que disponen los dispositivos como los smartphones, como la biometría, de la que no disponen de forma generalizada aún, por ejemplo, las tarjetas físicas. Cuando estas se insertan en una billetera digital, el proceso de identificación y autenticación se vincula con la tecnología del dispositivo. En la transacción, esa autentificación viaja de forma encriptada (tokenizada), segura, al no haber credenciales, números de tarjeta o información que quede alojada o inserta en el dispositivo, disminuyendo las posibilidades de fraudes.



En Europa, con la regulación actual, no se observan en la operativa de iniciación de pagos innovaciones -como la tokenización o las listas blancas- que sí se contemplan en el pago con tarjeta. Sería oportuno incorporarlas a nivel regulatorio para equipararlo al mundo de las tarjetas."

Leonardo González
Sales Director (Europe & Latam), Afterbanks Arcopay

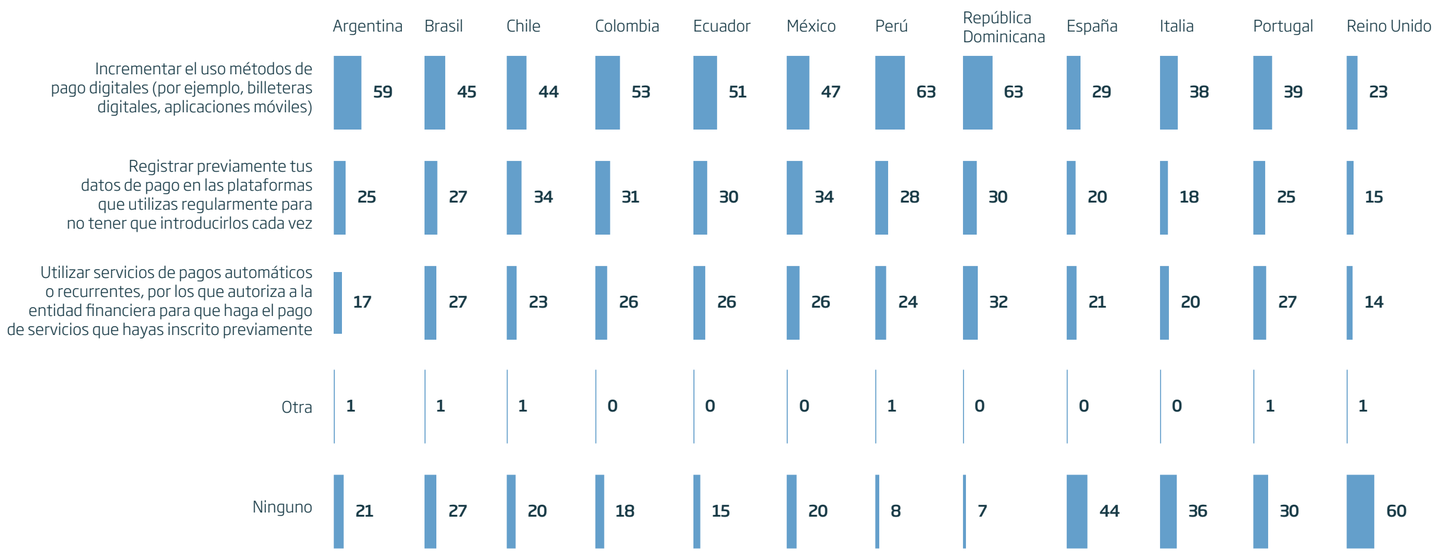
Las personas quieren que la seguridad sea mucha, pero sencilla

La predisposición a adoptar medidas que faciliten pagos sin fricciones más ágiles y sin contacto es mayor en Latinoamérica, mientras que la población europea es más reacia a adoptar acciones para tener experiencias de pago con menos molestias y más rápidas. Estas reticencias alcanzan su máximo en Reino Unido donde el 60% de la población no está dispuesta a adoptar ninguna medida adicional para aumentar la fluidez del pago. En el lado opuesto, República Dominicana (7%) y Perú (8%) apenas muestran reticencias. En parte, la motivación radica en una población ABI europea más envejecida, ya que allí la predisposición a agilizar el pago adoptando acciones adicionales desciende a medida que aumenta la edad.

La propuesta con mayor aceptación es la de fomentar el uso de métodos de pago digitales, mayoritaria en Perú y República Dominicana (63%), Argentina (59%), Colombia (53%) y Ecuador (51%). Aún en los países europeos, donde mayoritariamente se rechazan acciones adicionales, esta propuesta es la más atractiva.

Figura 14.
Predisposición hacia medios de pago sin fricciones.
Población ABI. 2023.

Respuestas a la pregunta: "¿Qué acciones estarías dispuesto/a a tomar para tener experiencias de pago con menos obstáculos o molestias, más rápidas, sencillas, y sin interrupciones?"



"Gracias a PSD2, que introdujo medidas para fortalecer la seguridad de los pagos como la autenticación en dos pasos, el fraude se ha visto reducido. Pero ha venido acompañada de fricciones en el proceso de check-out, y es por ello que la industria busca el equilibrio perfecto entre UX y seguridad."

Alicia Escribá
Google EMEA

Utilizar servicios de pagos automáticos o recurrentes (tipo domiciliación) resultan algo más interesantes que la opción de registrar previamente los datos de pago en las plataformas utilizadas de forma habitual para los europeos (salvo en Reino Unido) y en República Dominicana, mientras que en Brasil las dos opciones resultan equivalentes. En la práctica totalidad de los países de Latinoamérica la preferencia por el registro de credenciales de pago supera a la de la automatización de pagos, preferencia a priori razonable habida cuenta la reducida adopción de los débitos directos.

La predisposición hacia el pago sin fricciones aumentará a medida que las nuevas cohortes de edad se incorporen y aumenten su protagonismo en la sociedad. Sobre todo, en Latinoamérica donde la población más joven muestra una actitud más positiva y favorable, y con la misma prevalencia entre hombres y mujeres.

La decisión de las personas de incorporar o no una verificación adicional en el proceso de pago para fortalecer la seguridad no es ajena al contexto en el que se realiza el pago. Mientras que casi la mitad de la población (46,2%) estaría dispuesta a incluir medidas de verificación adicionales en contextos que no son considerados de confianza, sólo una minoría, que se sitúa alrededor de uno de cada cinco personas, no ve necesario añadir capas de seguridad a los pagos, ya sea porque prefiere la agilidad a la seguridad (10,1%), o porque confía en las medidas de seguridad ya implementadas (9,5%).

Se aprecian algunas diferencias en la predisposición en función de la localización y el perfil sociodemográfico de las personas. La importancia del contexto pesa más en Europa que en Latinoamérica, y en personas más jóvenes. Y resulta llamativo el comportamiento de las personas mayores de 55 años, que polarizan sus posturas: el 21,9% prefiere fluidez en el pago, la cota más alta entre todos los segmentos de edad, mientras que un 37,2% adoptaría la verificación adicional en todos los contextos, también la cota más alta. Anidan en este grupo de edad dos comportamientos distintos: el principal, donde prima la desconfianza hacia los pagos digitales; otro que prefiere que no se le compliquen más las cosas.

Figura 15.
Porcentaje de población que NO está dispuesto a adoptar ninguna medida facilitadora de pagos con menos fricciones.
Población ABI. 2023.

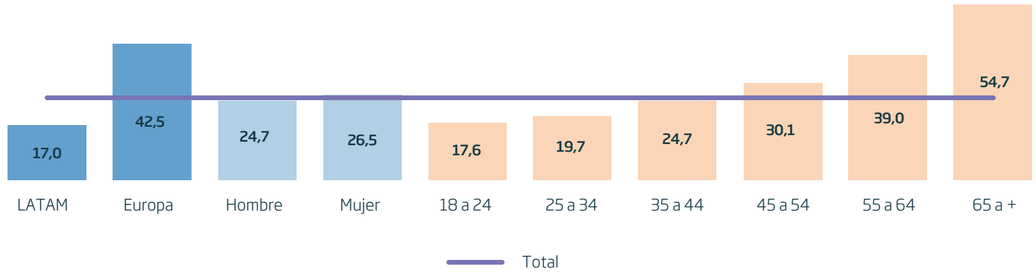
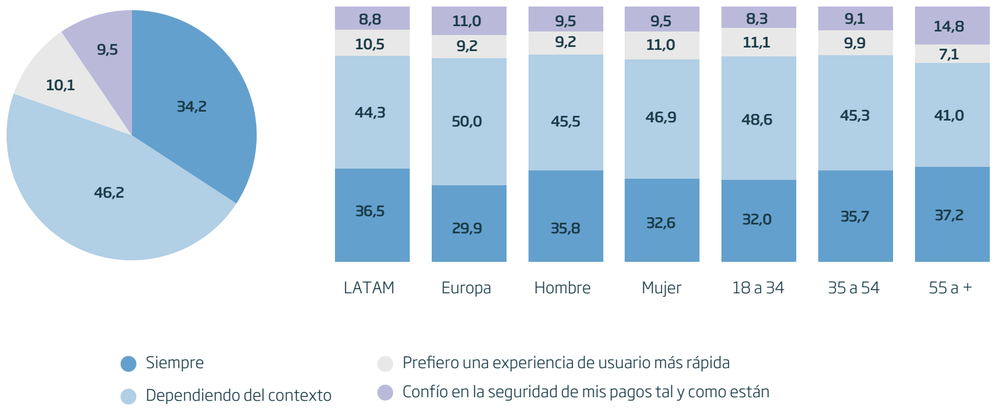


Figura 16.
Predisposición a realizar un proceso de autenticación adicional en transacciones de pago para garantizar mayor seguridad.
Población ABI. 2023.



"Como usuarios, damos la seguridad por hecho, pero seguimos siendo laxos cuidando nuestros datos. Falta una labor de concienciación social al respecto, de cara a mejorar la autoprotección"

Ángel Nigorra
CEO de Bizum

Una forma de "no complicar más las cosas" es considerar el diseño de interfaces intuitivas, fáciles de usar y accesibles a todas las capacidades. Este es de hecho el aspecto reconocido por el 45% de los expertos del Barómetro de Tendencias como más relevante en el despliegue de experiencias de pago fluidas y eficientes.

Le sigue en relevancia la sencillez del proceso de autenticación, como la que habilita la biometría y que concentra el 36% de las respuestas de los expertos. En tercera posición con un 32% se sitúa en términos de relevancia para los pagos sin fricciones la rapidez y claridad en los procesos de confirmación, notificación y de respuesta antes situaciones de errores o problemas técnicos en el momento del pago.

"Es difícil que la seguridad sea apreciada por el consumidor porque que no haya fraude es como estar sano, no se valora salvo cuando se echa de menos."

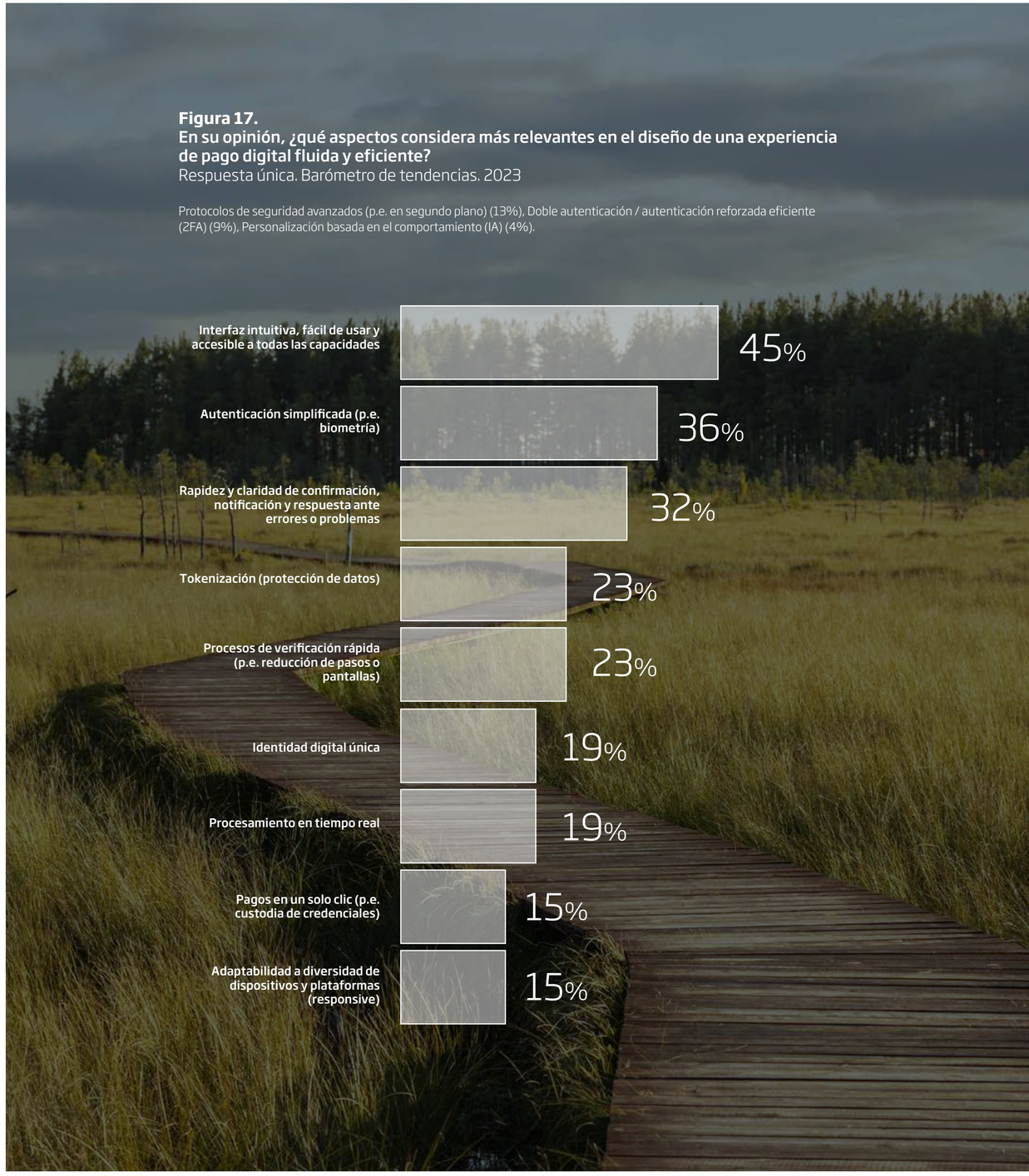
Javier Santamaría
Chair del European Payments Council - Presidente de Iberpay

"Hay que seguir mejorando en seguridad en todos los medios de pago digitales sin perjudicar la usabilidad. Es el equilibrio más difícil. No hacer el pago más complicado; que sea lo más sencillo y fluido posible con seguridad."

Alberto López
VP Digital Assets Security Mastercard

Figura 17.
En su opinión, ¿qué aspectos considera más relevantes en el diseño de una experiencia de pago digital fluida y eficiente?
Respuesta única. Barómetro de tendencias. 2023

Protocolos de seguridad avanzados (p.e. en segundo plano) (13%), Doble autenticación / autenticación reforzada eficiente (2FA) (9%), Personalización basada en el comportamiento (IA) (4%).



La biometría se postula como el método más sencillo para las personas por prescindir de la necesidad de utilizar, memorizar y custodiar contraseñas (passwordless). Junto con el mayor uso del teléfono móvil como dispositivo para realizar pagos, crece el uso de la autenticación biométrica como primera opción frente a los métodos analógicos. La creciente adopción de métodos de autentificación biométrica ilustra la cada vez mayor fiabilidad y asequibilidad de la tecnología.

La adopción de soluciones biométricas de reconocimiento facial comienza a disputar la hegemonía de las de huella dactilar. El crecimiento más destacado de la adopción de la biometría como primera opción se concentra en el último año precisamente en las modalidades de huella dactilar (35,9%) y de reconocimiento facial (23,9%), reduciendo la distancia en más de diez puntos en apenas un año, y ya consolidada esta última como segunda opción.

Los métodos analógicos caen en uso como primera opción de autenticación, aunque son relevantes como segunda opción, en especial el PIN (22,6%) que por primera vez supera al uso de contraseñas (19,0%), cuyo uso se desploma más de cuatro puntos en apenas un año.

Figura 18.
Método de autentificación primario y secundario en pago contactless con teléfono o reloj inteligente.
Población ABI. 2023.

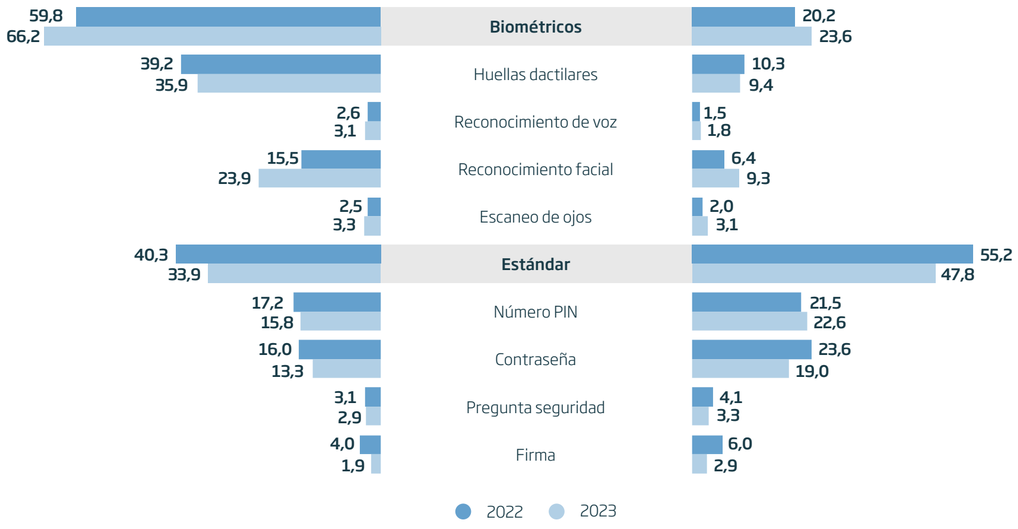
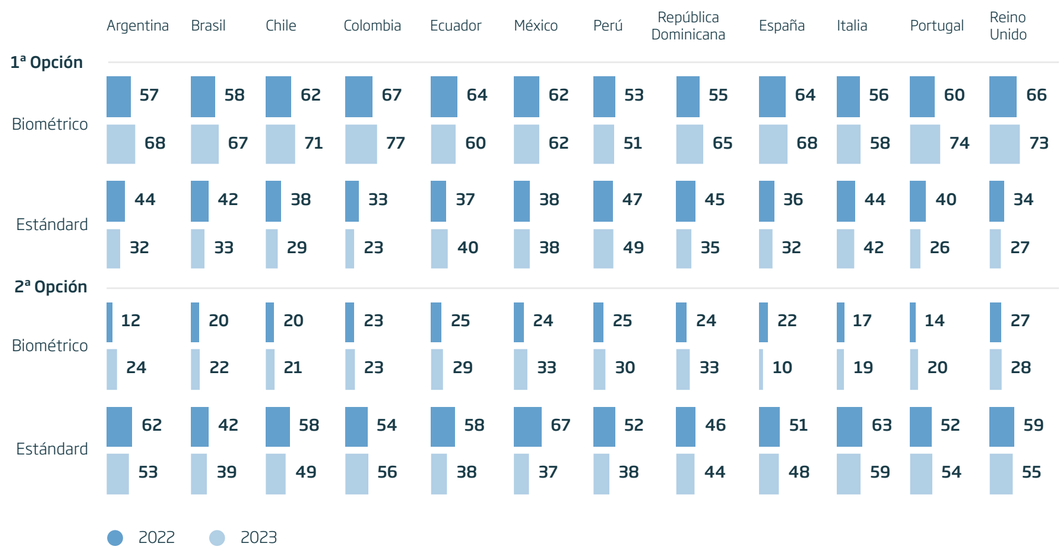


Figura 19.
Método de autentificación primario y secundario en pago contactless con teléfono o reloj inteligente.
Población ABI. 2023.



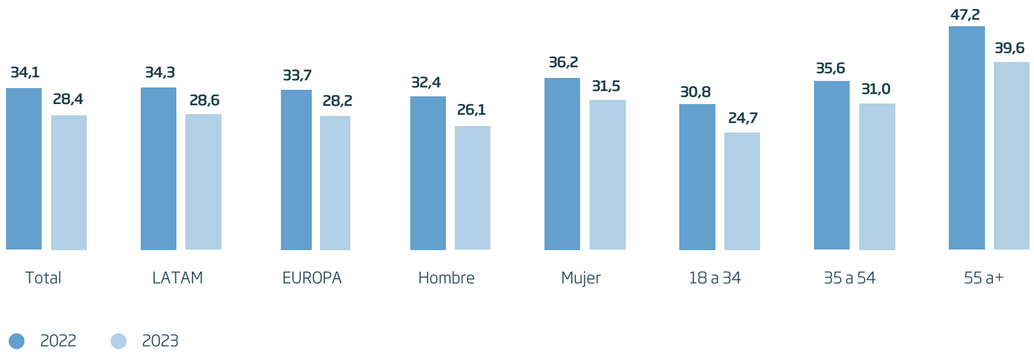
La creciente adopción de métodos de autenticación biométrica en los pagos sucede en casi todos los territorios. Sólo en Perú y Ecuador desciende su uso como primera opción, pero incluso allí aumentan como segunda opción. Entre los países latinoamericanos, el uso de sistemas biométricos ha crecido diez puntos porcentuales y el porcentaje de uso se acerca o incluso supera el 70% (con la salvedad, además de los dos países citados, de México). En Europa, que también aumenta el uso de estos métodos, el crecimiento es más moderado salvo en Portugal, donde crece catorce puntos.

Los métodos analógicos, sin embargo, siguen manteniendo cierta relevancia como primera opción de autenticación en países como Perú (49%) e Italia (42%).

Como contrapartida a este crecimiento, desciende significativamente el porcentaje de personas que no usa sistemas biométricos ni como primera ni como segunda opción, reduciendo aún más el tamaño de un segmento que ya era minoritario. Este descenso es generalizado y sucede en todos los segmentos poblacionales tanto del territorio latinoamericano como europeo, si bien existen brechas de género y etarias.

En parte, el incremento del uso de los métodos biométricos está relacionado con la mayor fiabilidad del servicio. Si bien hace sólo un año la falta de fiabilidad del servicio de autentificación biométrica era la principal razón aducida para no usar este tipo de verificación, la principal razón en la actualidad se asocia con el temor a la pérdida de información personal. Su uso, para una parte de la población que no emplea estos medios de verificación, sigue siendo considerados engorrosos y poco intuitivos.

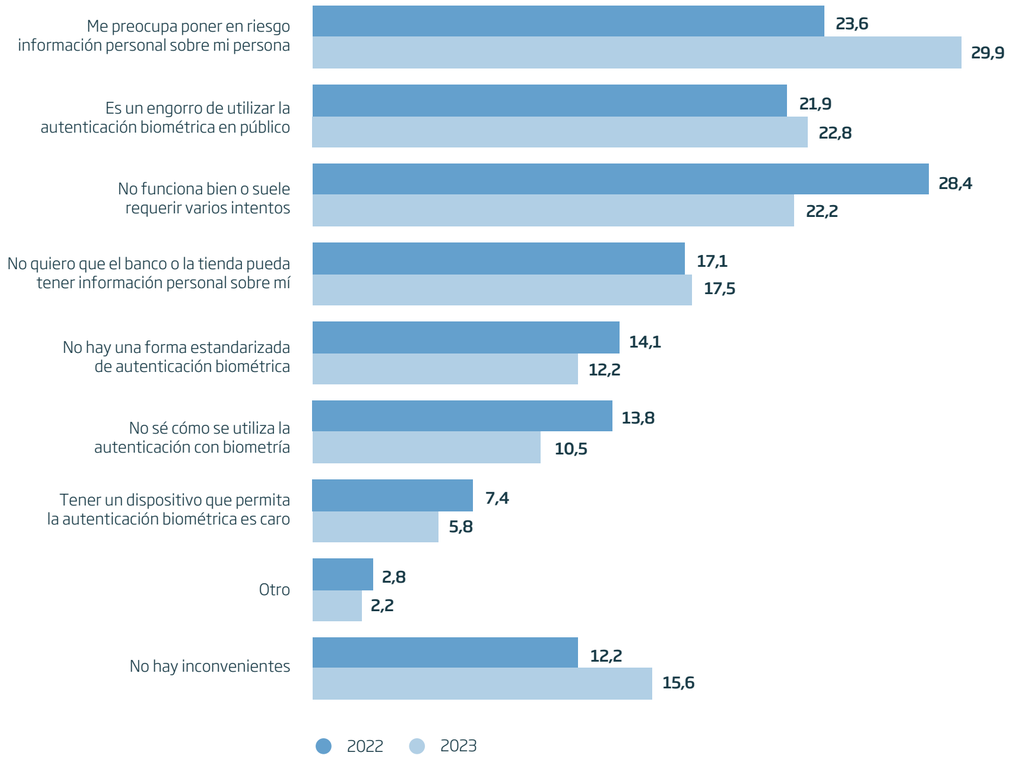
Figura 20.
Porcentaje de personas que NO utilizan sistemas de autenticación biométricos.
Población ABI. 2023.



"Hoy los jóvenes adoptan muy bien la billetera digital, sin embargo, existe una brecha considerable con otras generaciones, principalmente adultos mayores. La aproximación a los medios de pago en los adultos mayores, segmento relevante de nuestra cartera, aún está condicionado a un comportamiento con sistemas de seguridad físicos, tangibles, más analógicos, que les aporta mayor confianza en el uso."

Mauricio Medina
Prepago Los Héroes

Figura 21.
Motivos declarados de NO usan sistemas de autenticación biométricos.
Población ABI. 2023.

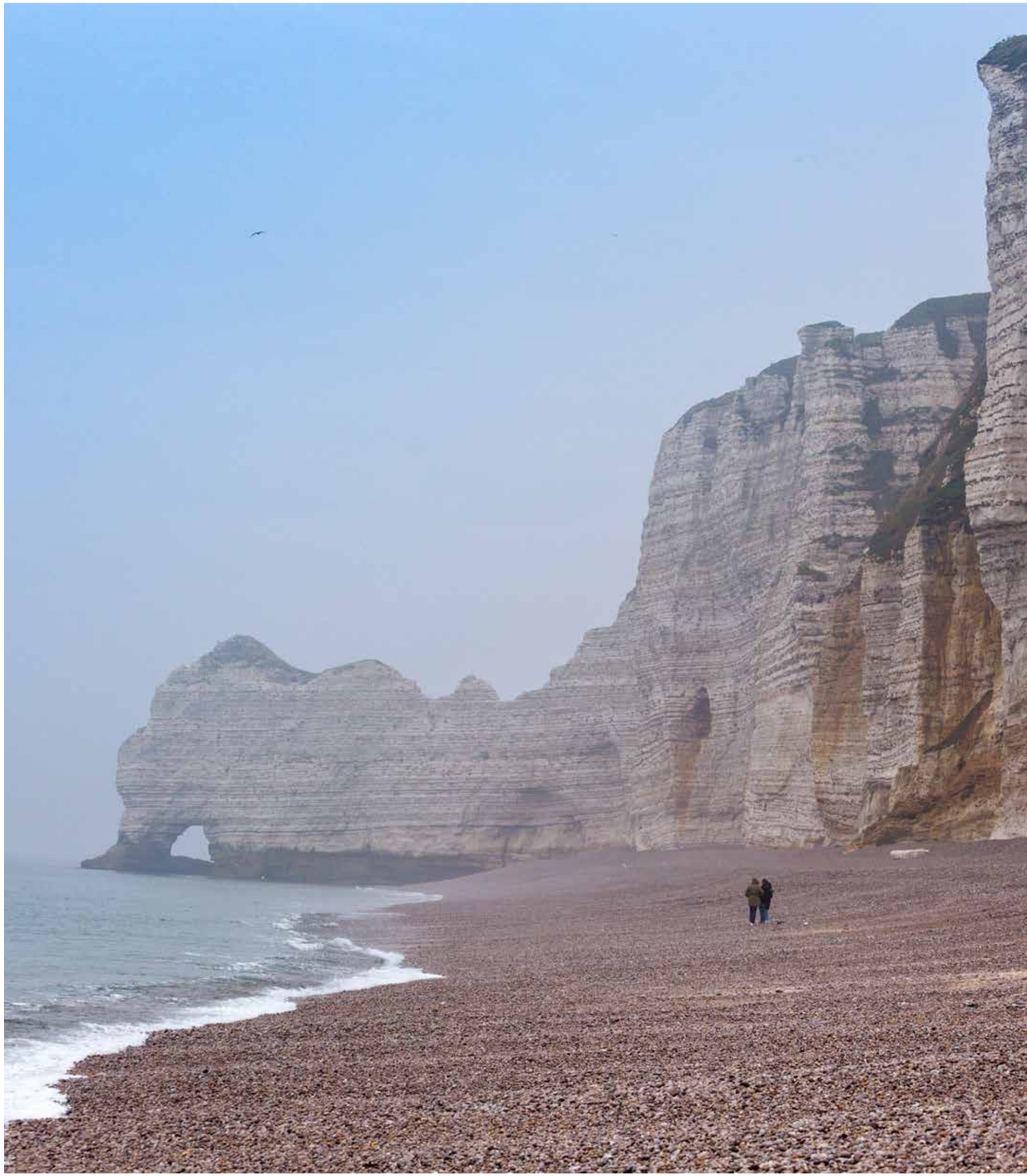


La seguridad de los pagos embebidos está en la nube

Cada vez son más empresas las que habilitan -o facilitan que proveedores terceros habiliten- experiencias de pago sin fricciones a través de la integración de servicios o "microservicios" financieros (embedded finance) buscando agilizar los procesos de pago para los consumidores, y con ello facilitar el acceso y uso de los servicios que necesitan cuando los necesitan.

La integración de servicios financieros y de pagos requiere de grandes capacidades tecnológicas -sofisticadas, flexibles, resilientes y compliant- para competir en un ecosistema diverso de creciente oferta de productos y servicios digitales rápidos, confiables y disponibles 365/24/7. El desarrollo de API que conectan diferentes sistemas y comparten datos para optimizar la entrega de servicios financieros a los consumidores lleva aparejada la condición sine qua non de garantizar que la seguridad se mantiene en lo más alto de la lista de prioridades de los proveedores de servicios.

En este contexto de apertura, conectividad e integración de servicios, las fintech y las entidades financieras tradicionales conviven con diversos elementos que tensionan su operativa cotidiana: los crecientes riesgos de seguridad y privacidad por ser objetivos preferentes de la ciberdelincuencia; la velocidad de la innovación de la tecnología digital que compromete las capacidades autónomas y no colaborativas de prevenir el riesgo de obsolescencia y pérdida de calidad de las soluciones; la creciente y exigente regulación a la que está sometida la industria financiera que exige, entre otros, planes de recuperación ante desastres; y las nuevas infraestructuras y arquitecturas necesarias para el aislamiento, gestión y compartición de los datos que condicionan las capacidades de la innovación aplicada a su análisis, combinación y transformación en información de utilidad para los propósitos de negocio.



Todo ello es posible hoy gracias a la computación en la nube. Las infraestructuras Cloud se caracterizan por ofrecer servicios a través de una red a cambio de un pago por uso y sin necesidad de invertir en infraestructuras propias. Permiten escalar las infraestructuras y adaptarse a las fluctuaciones de la demanda o del uso, además de almacenar y procesar grandes volúmenes de datos; acceder a herramientas y plataformas para el desarrollo de nuevas aplicaciones digitales; y mejorar la ciberseguridad. Los proveedores de Cloud ofrecen seguridad y protección de datos 365/24/7 por diseño, embebida en infraestructuras, datos, identidades y aplicaciones, y dotada de herramientas de autoprotección como la automatización, el machine learning y la inteligencia artificial.

En la nube se encuentran hoy disponibles una enorme y creciente variedad de servicios y soluciones de pago diseñadas por fintech y Bigtech en su condición de Paytech -de emisión, adquirencia, switching, procesamiento, por mencionar algunos- que permiten a los proveedores de servicios de pagos modernizar sus aplicaciones y servicios, unificar fuentes y tipologías de datos, idear y materializar nuevas fuentes de ingresos, testar y escalar soluciones con agilidad, a la vez que optimizan la gestión de los riesgos y previenen el fraude.

No en vano, el 71% de los agentes de la industria valoran positivamente, en términos de seguridad y escalabilidad, la migración hacia soluciones de pagos basadas en la nube. La mitad de ellos (37%), además, la consideran la opción más razonable. Un 21%, sin embargo, aunque positiva, considera que la migración supone también una gran complejidad. Un 13% enfatiza las motivaciones asociadas a la seguridad como mejor atributo.

Es mayoritaria también la opinión de los agentes de la industria de que las soluciones de pago basadas en la nube supondrían una reducción sensible de sus costes operativos (34%), mientras que un 21% aún no se encuentra en capacidad de valorar el sentido y dimensión de dicho impacto. Solo un 6% considera que ese impacto se traduciría en un aumento de costes operativos.

Figura 22.
En términos de seguridad y escalabilidad, ¿cómo valora la migración hacia soluciones de pagos basadas en la nube?
Respuesta única. Barómetro de tendencias. 2023

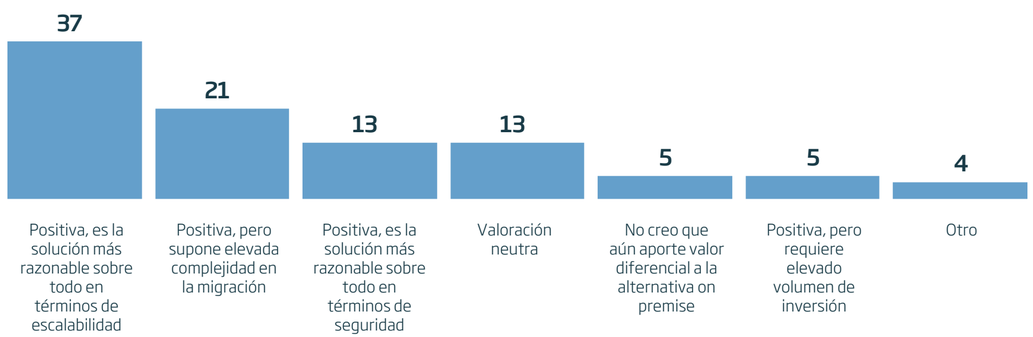
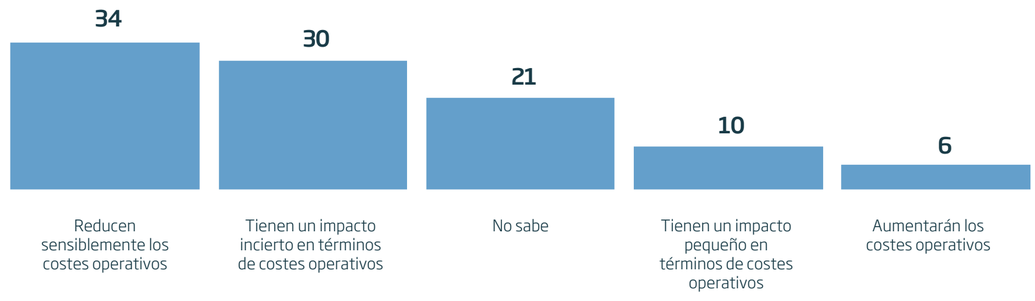


Figura 23.
¿Qué impacto cree que tendrán las soluciones de pagos basadas en la nube en la reducción de costes operativos?
Respuesta única. Barómetro de tendencias. 2023

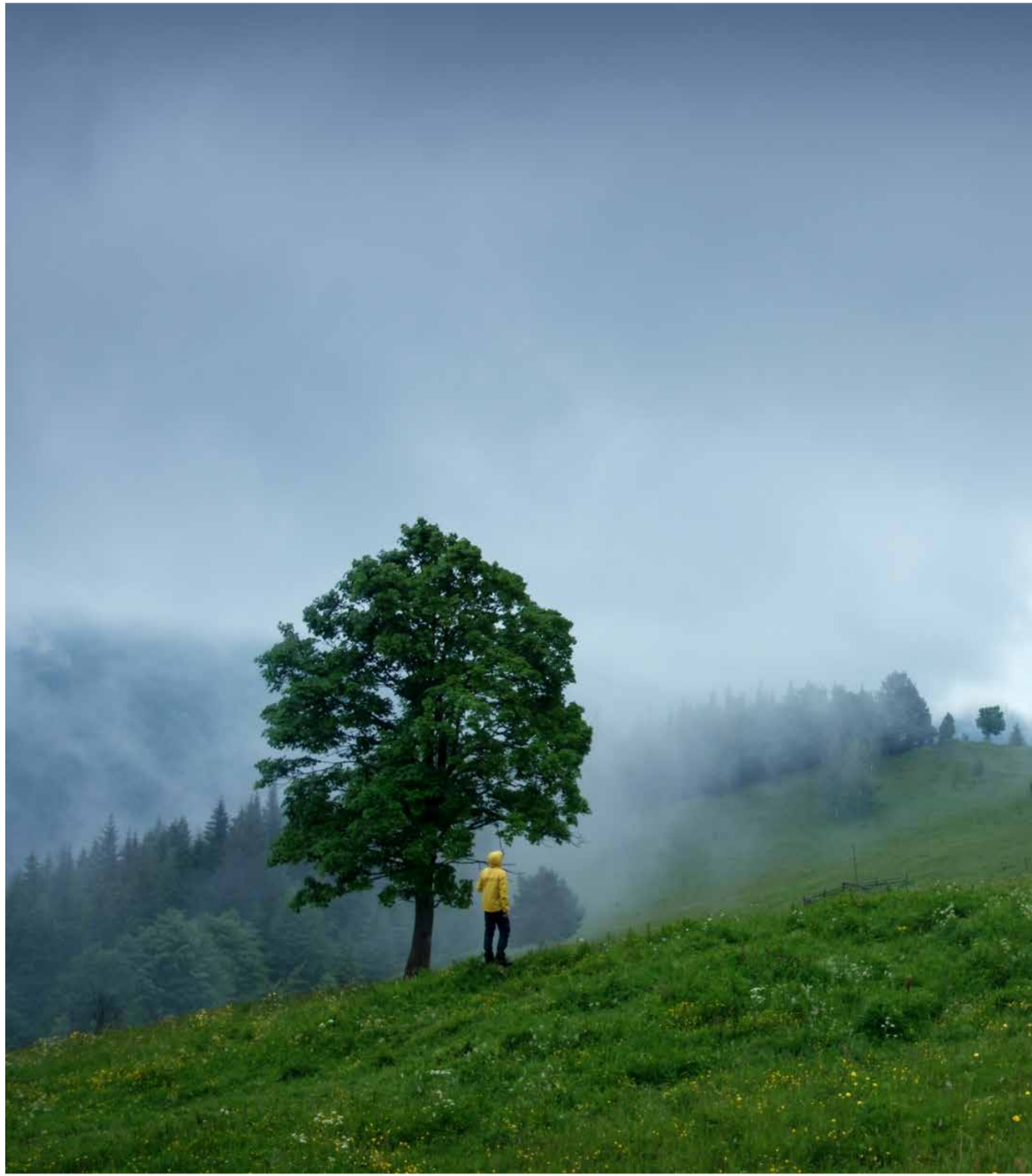


La computación en la nube está satisfaciendo muchas necesidades de la industria financiera en términos de seguridad, servicio, innovación y escalabilidad, evidenciado en la aceleración de su adopción y en la demostración de estar habilitada, lista y probada para acompañar en el despliegue de soluciones innovadoras de pagos digitales de forma segura.

Pero ¿están los países preparados para aprovechar las ventajas que ofrece el Cloud? De acuerdo con el estudio del BID "Computación en la nube: Contribución al desarrollo de ecosistemas digitales en países del Cono Sur" (2019)[5], para poder aprovechar los servicios de la computación en la nube es necesario eliminar algunas barreras aún presentes en muchos países. Desde limitaciones normativas o ausencia de regulación, hasta modelos no adecuados de contratación de servicios TI y los riesgos de "vendor lock-in", pasando por la cualificación de los recursos humanos, la baja conectividad, la preocupación con el cumplimiento normativo sobre datos en otras jurisdicciones e incluso la resistencia cultural y política.

"Dentro del marco de la operativa Open Banking (tanto datos como pagos), el tema de la seguridad está bien cubierto bajo la normativa PSD2. No obstante, las conversaciones sobre Open Finance aún giran en torno a asegurarse de que el Third Party Provider (TPP) es quien debe tener el dato bien resguardado, seguro y encapsulado para evitar posibles vulnerabilidades de la seguridad del dato. Cabe destacar que la mayoría de los TPP tienen bien cubierta esta parte por la infraestructura tecnológica de la que disponen, la autorregulación y auditorías de seguridad a las que se someten de manera periódica"

Leonardo González
Sales Director (Europe & Latam), Afterbanks Arcopay.



[5] Disponible en: https://shorturl.at/fgjR5

Hacia una identidad digital universal

La identificación digital es un requisito de seguridad imprescindible que se ha ido solventando sobre la marcha con el apoyo de proveedores del ámbito privado, generalmente a través de grandes plataformas digitales como Google, Apple o Meta, o bien creando una nueva identidad digital cada vez que se inicia una relación con una aplicación o un sitio web.

En gran medida esto ocurre porque **los sistemas de identificación digital que ofrecen actualmente los gobiernos, cuando disponen de ellos, presentan deficiencias importantes**: no están disponibles para toda la población, a menudo están limitados a los servicios públicos en línea y, en el caso, por ejemplo, de la Unión Europea, no garantizan un acceso transfronterizo ininterrumpido. De acuerdo con el Eurobarómetro 518 sobre derechos y principios digitales[6], el 85% de los ciudadanos de la UE demandan una identificación digital única segura para todos los servicios en línea, públicos y privados. A la fecha, solo el 14% de los proveedores de los principales servicios públicos en los Estados miembros permiten la autenticación transfronteriza con un sistema de identificación electrónica.

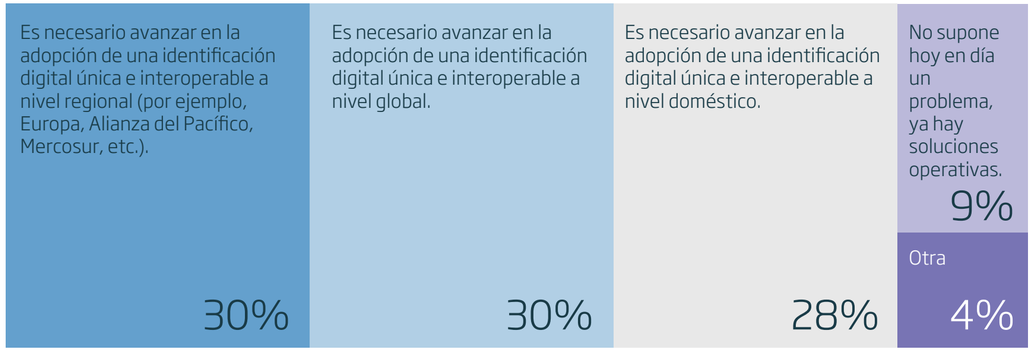
Consultados los expertos de la industria de los pagos a través del Barómetro de tendencias, **es casi unánime (88%) la consideración de que es necesario avanzar en la adopción de una identificación única digital e interoperable para la autenticación de los pagos**, ya sea a nivel doméstico (28%), a nivel regional (30%) o incluso global (30%). Apenas un 9% considera innecesarios dichos atributos porque ya existen soluciones operativas en el mercado.

"La regulación se volvió agnóstica de la tecnología y permite a las entidades utilizar cualquier tecnología para validar la identidad, de la que hay mucha oferta. Solo le importa que gestionen bien los riesgos."

Edwin Zácipa
Latam Fintech

El Reglamento sobre identificación electrónica y servicios de confianza para las transacciones electrónicas en el mercado interior[7] (Reglamento eIDAS) de 2014, en vigor desde 2018 y en revisión desde 2020 (eIDAS 2) va en la dirección señalada por el Barómetro. En su versión primigenia el eIDAS fue ya un hito hacia la construcción de un entorno en el que empresas, ciudadanos y autoridades llevaran a cabo interacciones electrónicas seguras y sin fisuras.
En noviembre de 2023 los legisladores europeos alcanzaron un acuerdo provisional sobre Reglamento eIDAS 2 que supone una evolución y proporcionará a ciudadanos europeos y otros residentes un medio de identidad digital europeo armonizado basado en el concepto de wallet, voluntario y gratuito para las personas físicas que habrá de ser provisto por cada país como parte de un sistema nacional de identificación electrónica. Habilitará, además, un panel de control de transacciones y la posibilidad de denunciar violaciones de la protección de datos.

Figura 24.
Sobre las credenciales de identificación digital para la autenticación en los pagos, ¿considera que...
Respuesta única. Barómetro de tendencias. 2023



"Europa deberá facilitar el onboarding de las personas y ayudar a la autenticación en el momento del pago. La cartera digital europea permitirá que esas credenciales sirvan como factor de autenticación. Confío en que tenga la adopción que no tuvo el eIDAS, que estaba más pensado para el sector público y no tanto para el privado, y los casos de uso eran muy limitados."

Carlos Sanz
Director del Departamento de Sistemas de Pago, Banco de España

[6] https://europa.eu/eurobarometer/surveys/detail/2270
[7] https://shorturl.at/iuFKZ

Los servicios de identificación y confianza con efectos jurídicos en toda la UE que contempla el Reglamento eIDAS 2, algunos de ellos integrados en el wallet, son la firma electrónica; el sello de tiempo; la identificación electrónica; el certificado cualificado de autenticación de sitio web; el sello electrónico y el servicio de entrega electrónica certificada.

La realidad europea dista de la del conjunto de países de la región de Latinoamérica, donde existen proyectos como el SID-Sistema de Identidad Digital[8] de Argentina (sin validez aún efectiva para trámites en los cuales se necesita acreditar identidad), la nueva Ley General de Población de México en la que se incluye una Cédula de Identidad Digital, el proyecto de Cédula Digital de la Registraduría de Colombia y la futura Infraestructura Oficial de Firma Electrónica (IOFE) de Perú, así como realidades como el Certificado Digital "e-CPF", "e-CNPJ" y "NeoID" de Brasil y la firma electrónica (Ley 19799 de 2022) en Chile. De forma generalizada, las entidades financieras han de conectarse con la autoridad electoral o con el registro civil para verificar las credenciales de identidad de sus clientes, u optar por métodos alternativos privados autorizados.

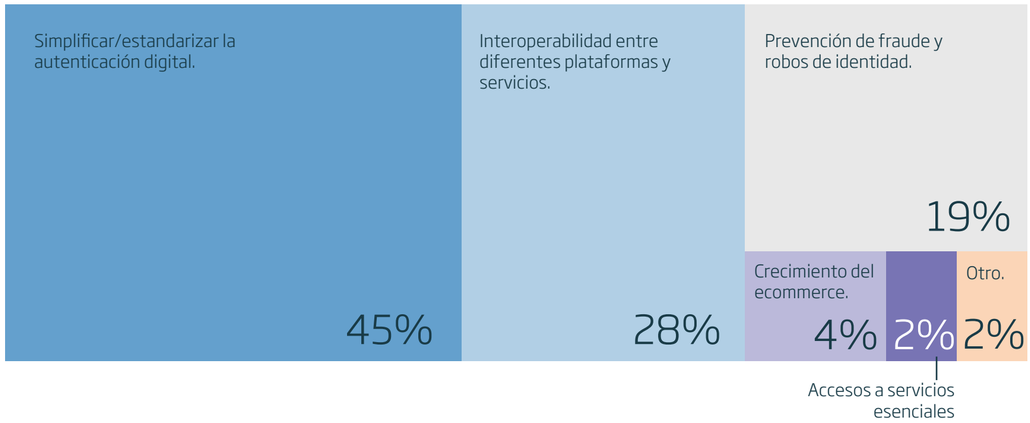
La principal motivación para impulsar una identidad digital única desde la perspectiva de los agentes de la industria está directamente relacionada con la seguridad, y esta a su vez con la sencillez que requieren amplios segmentos de población, como se ha visto anteriormente. Así, **el 45% considera que simplificar y estandarizar la autenticación digital es el principal impulsor de esta innovación.** Le sigue, a distancia (28%), facilitar la interoperabilidad segura entre diferentes plataformas y servicios.

[8] https://shorturl.at/iDGR1

La Superintendencia Bancaria emitió la Circular 011/2022 para el Onboarding digital que permite a las entidades conectarse a una entidad emisora de firma digital para validar la identidad del usuario, además de la habitual conexión a la Junta Central Electoral, el repositorio oficial de la identidad de los dominicanos"

Antonio González Tejada
Director del Departamento de Sistemas Pagos, Banco Central de la República Dominicana

Figura 25.
¿Cuál considera que es el principal impulsor de una eventual identidad digital única?
Respuesta única. Barómetro de tendencias. 2023

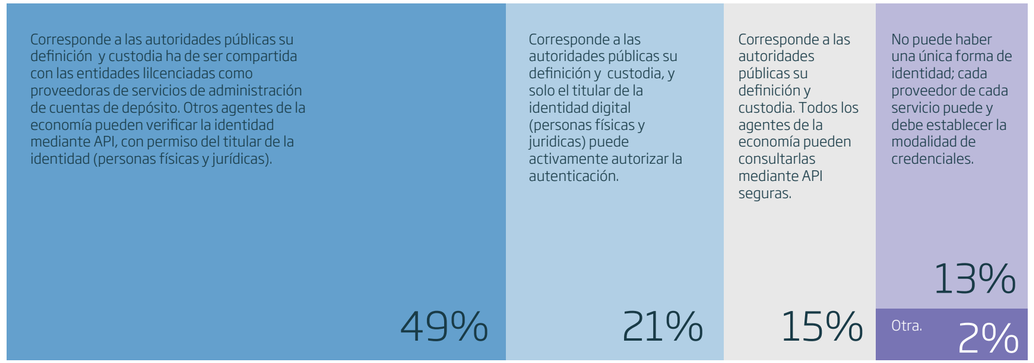


"Perú no dispone de un mecanismo único y estandarizado de identidad digital. Tiene un DNI electrónico que no cumple las funcionalidades para firma y autenticación digital. En su ausencia, los agentes están utilizando biometría y factores de autenticación mediante convenio con RENIEC para validación de la identidad."

Ljuvica Vodanovic
Vodanovic

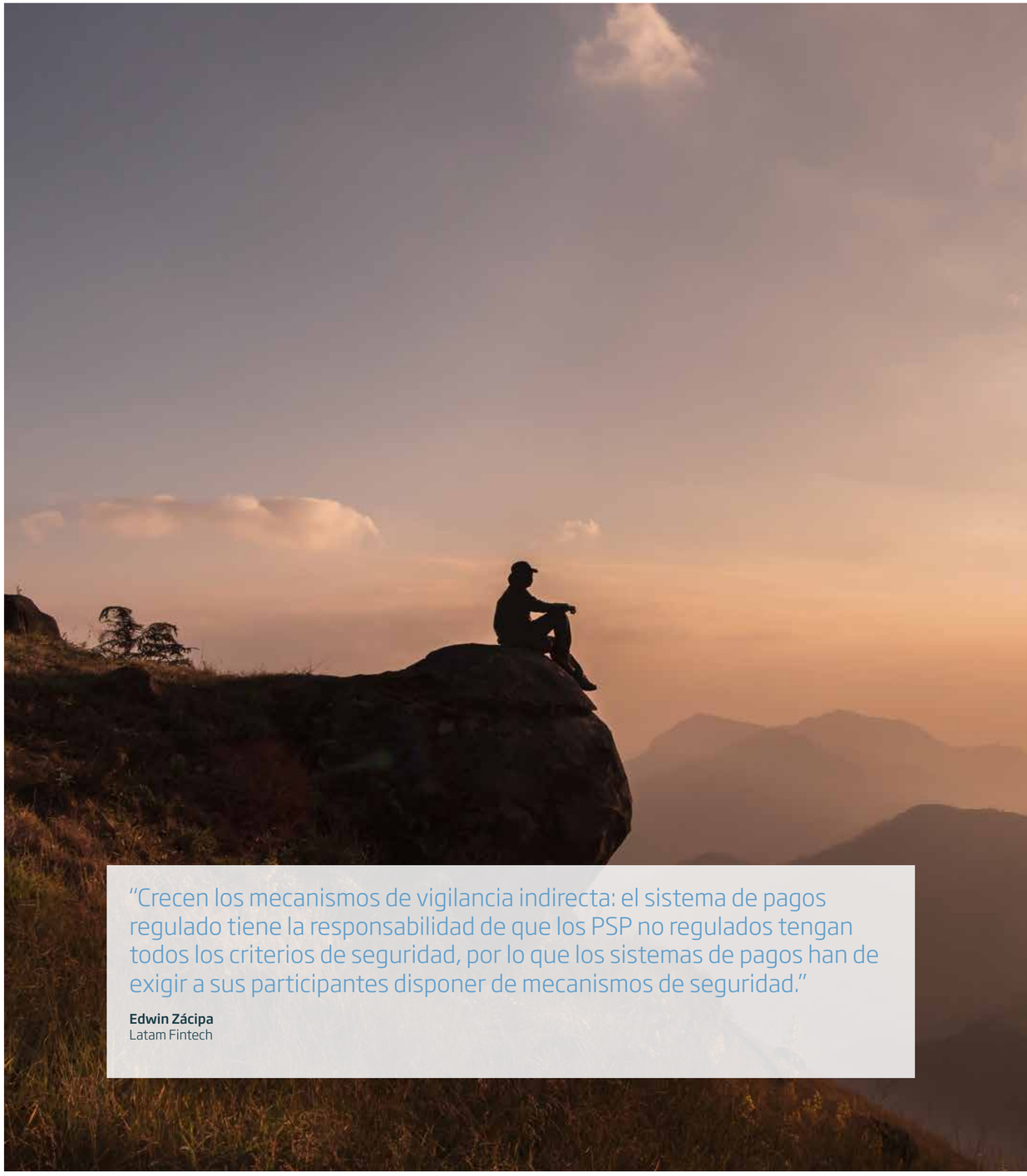
Otro debate está enmarcado en dónde ha de residir la competencia y responsabilidad de definir y custodiar las credenciales de identificación digital de los titulares. En este sentido, **es mayoritaria (49%) la opinión de los agentes que consideran que corresponde a las autoridades su definición, si bien su custodia ha de ser compartida con las entidades licenciadas como proveedoras de servicios de administración de cuentas de depósito (esto es, los bancos)**, mientras que otros agentes terceros estarían habilitados a consultar la verificación de la identidad mediante API, con el consentimiento del titular de la identidad.

Figura 26.
Sobre las credenciales de identificación digital para la autenticación en los pagos, ¿considera que...
Respuesta única. Barómetro de tendencias. 2023



"Están surgiendo iniciativas privadas para crear repositorios de identificación digital como "Soy Yo" de los tres bancos más grandes de Colombia. La Registraduría, que está desarrollando el proyecto de cédula digital, ha sido tradicionalmente la fuente para registrar identidades, pero no es tan eficiente."

Edwin Zácipa
Latam Fintech



"Crecen los mecanismos de vigilancia indirecta: el sistema de pagos regulado tiene la responsabilidad de que los PSP no regulados tengan todos los criterios de seguridad, por lo que los sistemas de pagos han de exigir a sus participantes disponer de mecanismos de seguridad."

Edwin Zácipa
Latam Fintech

Agradecimientos

Brasil

Belline Santana
Banco Central do Brasil

Chile

Álvaro Gonzalez R.
Diana López
Gabriel Aparici
Ivan Abarca V.
María José Meléndez C.
Pablo Furche
Banco Central de Chile
Ignacio Rodríguez del Río
Global66
Mauricio Eduardo Medina
Prepago Los Héroes

Colombia

Dionisio Valdivieso Urbano
Banco de la República
Edwin Zácipa
Latam Fintech Hub
Javier Gamboa
Mastercard

Ecuador

Sebastián Quevedo
Produbanco

España

Alberto López González
Mastercard
Alicia Escribá
Google
Ángel Nigorra
Bizum
Carlos Sanz
Banco de España
Eduardo Prieto
Visa
Juan Luis Encinas
Iberpay
Leonardo González
Afterbanks Arcopay

Italia

Rita Camporeale
Associazione Bancaria Italiana

México

René Centeno
American Express
Sebastián de Lara Gomis
Fintech México

Perú

Ljubica Vodanovic
Vodanovic Legal

Milton Vega
Banco Central de Reserva del Perú

República Dominicana

Ángel González Tejada
Yilmari Rosario
Banco Central de la República Dominicana

Europa

Javier Santamaría
European Payments Council

Latinoamérica

Miguel Díaz
Innovation Hub, Bank of International Settlements

minsait payments

An Indra company