EL VERDADERO COSTO DEL FRAUDE EN AMÉRICA LATINA

Informe Regional - 2021

LexisNexis®
RISK SOLUTIONS

ANTECEDENTES Y METODOLOGÍA

El estudio de LexisNexis® Risk Solutions sobre el Verdadero Costo del Fraude™ ayuda a las compañías a crecer su negocio en forma segura mientras gestionan el creciente riesgo de fraude.

La investigación ofrece una vista rápida de:

- Tendencias actuales de fraude en los mercados minorista, de comercio electrónico, servicios financieros y crediticio de América Latina (LATAM).
- Puntos sensibles claves relacionados con la adición de nuevos mecanismos de pago en transacciones a través de canales en línea y móviles con expansión internacional.

Impacto de COVID-19:

- La recolección de datos se hizo entre febrero y abril de 2021. Muchas de las preguntas de la encuesta se refieren a los 12 meses anteriores; por lo tanto, los hallazgos reflejan actividades, riesgos de fraude, retos y costos que han sido afectados por el miedo a la COVID-19, el cual generó cambios de comportamiento y cierres forzados.

Definiciones de fraude:

- Transacciones fraudulentas debidas a fraude de identidad, mal uso de métodos de pago robados (tales como tarjetas de crédito) o información personal
- Solicitudes fraudulentas de reembolsos/devoluciones, cheques devueltos
- Mercancía perdida o robada, así como costos de redistribución asociados con el reenvío de artículos comprados
- Aplicaciones fraudulentas (p ej., suministro intencional de información personal incorrecta, tal como ingresos, empleo, etc.)
- Apropiación de cuentas por personas no autorizadas
- Utilización de cuentas para lavado de activos

Este estudio cubre métodos de fraude orientados al consumidor

- **No** incluye fraude interno ni de empleados

El costo del LexisNexis Fraud Multiplier™:

- Estima el valor total de las pérdidas incurridas por una firma con base en el valor total en dólares de una transacción fraudulenta

ANTECEDENTES Y METODOLOGÍA (CONT.)

El estudio incluye una encuesta exhaustiva de 454 ejecutivos de riesgo y fraude en compañías de comercio minorista y comercio electrónico así como servicios financieros y crédito, en América Latina (LATAM).

	Argentina	Brasil	Chile	Colombia	México	General
Comercio minorista	30	30	30	33	30	153
Comercio electrónico	30	31	30	30	30	151
Servicios financieros	30	30	30	30	30	150
TOTAL	**90**	**91**	**90**	**93**	**90**	**454**

Los sectores encuestados incluyen*:

Comercio minorista

Puede o no ser omnicanal y recibir menos del 80 % de los ingresos mediante canales en línea

Comercio electrónico

Obtiene el 80 % o más de sus ingresos mediante canales en línea

Servicios financieros

Gestión de activos
Banca/hipotecas
Crédito de consumo
Planeación financiera

En varias categorías, entre ellas:

Vestuario/ropa, partes automotrices, libros/música, computadores/software, artículos digitales, medicamentos/salud y belleza, flores/regalos/joyería, alimentos y bebidas, mercancía general, ferretería y mejoramiento del hogar, hoteles/viajes, artículos para el hogar/mobiliario, suministros de oficina, artículos deportivos, juguetes/pasatiempos

LexisNexis® RISK SOLUTIONS

**La utilización de la frase "sectores encuestados" a lo largo del reporte se refiere a comercio minorista, comercio electrónico y servicios financieros*

RESUMEN DE RESULTADOS PRINCIPALES

01 El costo del fraude para los sectores encuestados de LATAM ha aumentado drásticamente. Hoy en día, cada transacción fraudulenta cuesta en promedio 3,68 veces el valor de la transacción perdida, comparado con 3,46 veces en 2019. Esto está siendo generado por entidades financieras y vendedores de comercio electrónico, como resultado del movimiento hacia más transacciones de canal digital/remoto durante COVID-19.

02 Hay un aumento de actividad en canales móviles/en línea, lo cual aumenta los riesgos y costos de fraude. Se realizan más transacciones remotas ya que la pandemia de COVID-19 cerró muchas oportunidades persona a persona. Los riesgos en el canal móvil prevalecen en aplicaciones móviles y pagos con billetera digital, ya que los métodos de pago sin contacto están siendo utilizados con más frecuencia por los consumidores. El fraude de identidad es una preocupación, especialmente para entidades financieras.

03 El fraude relacionado con identidad es una amenaza y reto clave para minoristas/vendedores de comercio electrónico y entidades financieras de LATAM. Esto tiene que ver específicamente con canales transaccionales remotos que implican nuevos métodos de pago y retos para evaluar los atributos digitales del dispositivo y el riesgo de transacción. Además, hay preocupación por equilibrar el trabajo de detección y prevención de fraude con la fricción para el cliente, ya que cuando aumenta el esfuerzo para el cliente, es frecuente que abandone el carrito de compras.

04 Comerciantes y entidades de servicios financieros de LATAM pueden reducir los costos y riesgos de fraude mediante una buena práctica, que consiste en integrar las operaciones de ciberseguridad, experiencia digital de cliente y fraude por medio de un enfoque de solución multicapa. Muchas empresas no están optimizando sus esfuerzos de prevención de fraude por no utilizar esta buena práctica. Las que sí la utilizan observan menos retos en verificación de identidad, manejo de nuevos métodos de pago móviles y equilibrio entre prevención de fraude y fricción para el cliente. También tienen un costo de fraude menor comparado con las demás.

RESULTADO CLAVE 01

El costo del fraude para los sectores encuestados de LATAM ha aumentado drásticamente. Hoy en día, cada transacción fraudulenta cuesta en promedio 3,68 veces el valor de la transacción perdida, comparado con 3,46 veces en 2019.

El costo del fraude es 4,78 veces el valor de la transacción perdida en entidades de servicios financieros y 3,40 para vendedores de comercio electrónico, en comparación con 2.97 para comercio minorista.

Las entidades financieras de LATAM han estado sometidas a ataques de fraude digital contra las cuentas bancarias de sus clientes. Muchos vendedores de comercio electrónico no estaban preparados para el mayor volumen de transacciones digitales y para proveerse de soluciones de protección contra el fraude. Además, el desplazamiento hacia más métodos de pago digital y transacciones móviles tiene mayores riesgos de fraude.

El costo del fraude ha aumentado drásticamente para comerciantes y entidades financieras de LATAM.

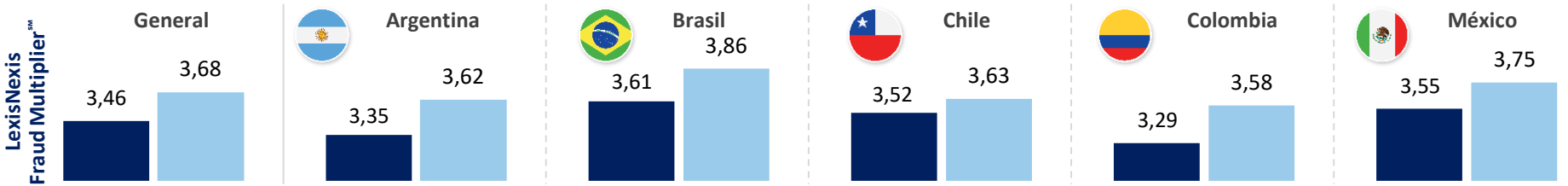
Por cada transacción fraudulenta, el costo para las empresas de LATAM es 3,68 veces el valor de la transacción perdida, un aumento considerable comparado con 3,46 veces el valor perdido en 2019. Tanto el segmento de servicios financieros como el de comercio electrónico observaron fuertes aumentos de costo de fraude dado el impulso hacia lo digital.

Diversos factores están afectando esto, entre ellos la focalización en entidades financieras para apropiación de cuentas y clonación de tarjetas[1], mayor uso de métodos de pago digitales y sin contacto por parte de los consumidores, lo cual se ha traducido en más pérdidas por fraude y por último, el aumento de transacciones en canales móviles, lo cual crea problemas de fraude relacionados con identidad y cuentas.

Los hallazgos indican que varios vendedores de comercio electrónico no estaban preparados para la avalancha digital por COVID-19, con un uso limitado de soluciones que evalúan identidades digitales y riesgo de transacción y pueden desenmascarar identidades sintéticas y proteger contra el delito cibernético.

4,78 Servicios financieros;
3.46 Comercio electrónico
2,97 Comercio minorista

Costo de fraude: LexisNexis Fraud Multiplier™



[1] https://www.globenewswire.com/fr/news-release/2021/05/03/2221375/0/en/Latin-America-Fraud-Detection-and-Prevention-Market-to-Reach-USD-2-945-3-Million-by-2028-Increasing-Incidence-of-Data-Fraud-to-Stimulate-Growth-Fortune-Business-Insights.html

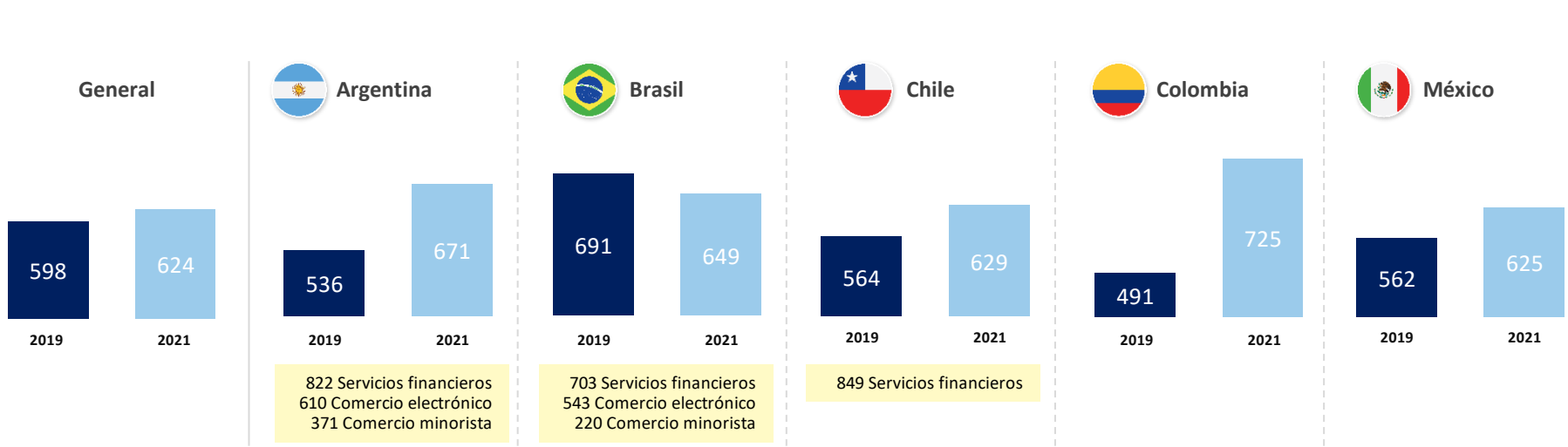
Preguntas de la encuesta:
P16a: Pensando en las pérdidas totales por fraude sufridas por su compañía, indique la distribución de diversos costos directos de fraude en los últimos 12 meses.
P10: ¿Cuál es el valor aproximado del total de pérdidas de su compañía por fraude en los últimos 12 meses, como porcentaje del total de ingresos?

* PRECAUCIÓN: número reducido de casos; los datos deben utilizarse solo direccionalmente

LexisNexis® RISK SOLUTIONS

El promedio mensual de ataques de fraude exitosos ha aumentado, especialmente en Argentina y Colombia. El comercio electrónico y los servicios financieros son los mayores responsables de estos aumentos debido al cierre de las tiendas físicas.

Número promedio de transacciones de fraude exitosas informadas por mes**



P22/24: ¿En un mes típico, aproximadamente cuántas transacciones fraudulentas son prevenidas/completadas exitosamente por su compañía?

RESULTADO CLAVE 02

Hay un aumento de actividad en canales móviles/en línea, lo cual está aumentando los riesgos y costos de fraude.

No sorprende que haya habido un desplazamiento hacia la parte digital/navegadores web y transacciones por canales móviles desde el inicio de la pandemia de COVID-19.

El comercio móvil ha crecido en LATAM, y se ha acelerado por la pandemia. Lo mismo ha pasado con el aumento de transacciones utilizando métodos de pago de billetera electrónica/digital y sin contacto.

Las transacciones móviles contribuyen al aumento de fraude, y los vendedores de comercio electrónico han sido especialmente afectados.

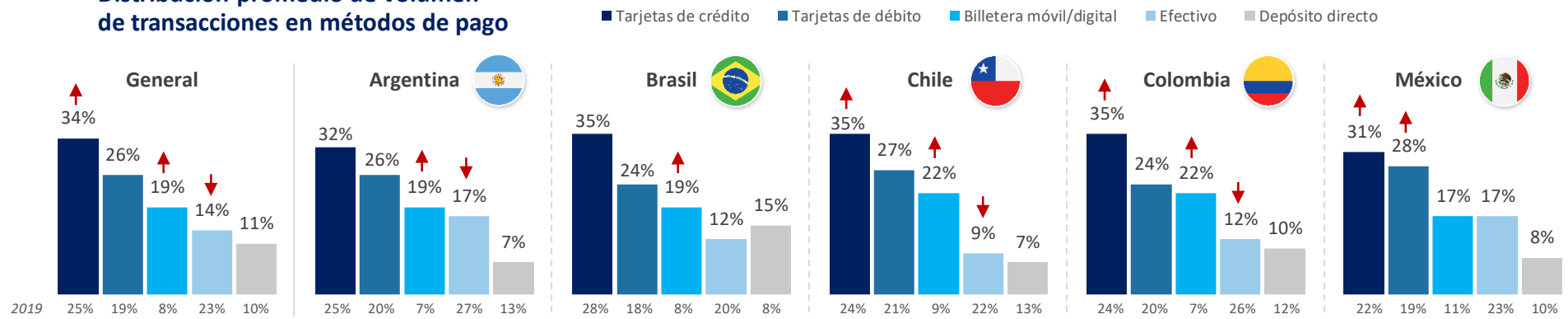
- El porcentaje de costos de fraude atribuido al canal móvil ha aumentado en ciertos mercados (Argentina, Colombia y México), y es alto para vendedores de comercio electrónico especialmente en Brasil, Chile y Colombia.
- El aumento en el uso de billeteras digitales/s móviles y pagos sin contacto se alinea con un aumento en el porcentaje de costos atribuidos a estos métodos de pago.

No sorprende que el fraude relacionado con identidad y cuentas sea especialmente problemático para entidades financieras y comerciantes que permiten el comercio móvil.

Ya que COVID-19 impactó todo en los últimos 12 meses, hay más transacciones con métodos de pago digitales en lugar de efectivo.

Las transacciones con tarjeta de crédito representan el método de pago más grande, a pesar de que el volumen proveniente de billeteras móviles/digitales ha aumentado significativamente en la mayoría de mercados, hasta estar casi a la par con tarjeta de débito. A la vez, aunque las transacciones en efectivo han caído, el efectivo sigue siendo el método principal en áreas con menos infraestructura bancaria. El aumento en el volumen con tarjetas de crédito probablemente está relacionado con tarjetas locales para transacciones locales por medio de redes de pago locales; pocas personas tienen acceso a proveedores globales para transacciones internacionales. Esta podría ser una razón por la que el uso de las billeteras móviles ha aumentado ya que la penetración de los teléfonos inteligentes es alta y los grandes minoristas permiten este método de pago. Las transacciones con billeteras móviles por medio de servicios como Apple Pay, AliPay, Google Pay y Samsung Pay pueden ser utilizadas especialmente para operaciones internacionales[2]. Las billeteras móviles también son un método para aumentar la inclusión financiera dado que hay una población no bancarizada grande[3].

Distribución promedio de volumen de transacciones en métodos de pago



[2]https://cellpointdigital.com/articles/insights/payments-latin-america/

[3] https://techcrunch.com/2020/10/28/current-and-upcoming-trends-in-latin-americas-mobile-growth/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAKl8D2rP3oPZpWhbZpqx-BsI585aNcfc3JH6Spc3ca2KzbLk-jvs09lMiTPvNThrKBhidWkvtcweA94PFO7Inz0cgxW-QgT4oYM0oaPoG4JUgQZeG1IBUcx4R9ZtwMoGhN5vKmlCUYESmjTrdnPUTzbm1crK_r-itFNlqB4ulliK

Preguntas de la encuesta:
P3: Por favor indique el porcentaje de transacciones realizadas (en los últimos 12 meses) para cada uno de los siguientes métodos de pago que son aceptados actualmente por su compañía:

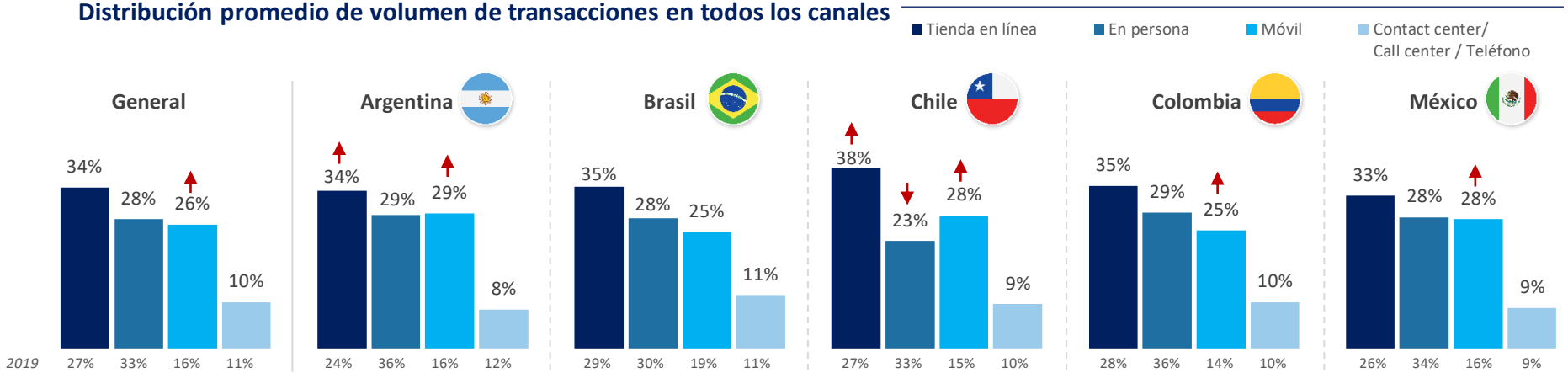
*Pregunta hecha solo a instituciones financieras

↑↓ = significativamente o direccionalmente más alto/más bajo que en 2019

No sorprende que la gran mayoría de transacciones se hicieron por canales remotos durante la pandemia, con un aumento de volumen en el canal móvil en la mayoría de mercados de LATAM.

Aunque la distribución promedio de transacciones por el canal móvil es significativamente más alta comparada con el 2019 en la mayoría de mercados, el volumen promedio reportado de transacciones en persona descendió solo moderada/direccionalmente. Aunque los consumidores de LATAM están haciendo más compras por el canal remoto, sigue habiendo preferencia por la modalidad en persona para ciertos tipos de compras[4]. El aumento de la utilización de pagos sin contacto ha brindado algo de apoyo a aquellos que desean evitar la manipulación de efectivo durante una compra en tienda[5].

Distribución promedio de volumen de transacciones en todos los canales



[4] https://usa.visa.com/visa-everywhere/blog/bdp/2020/10/09/a-covid-silver-1602273015995.html
[5] Ibid

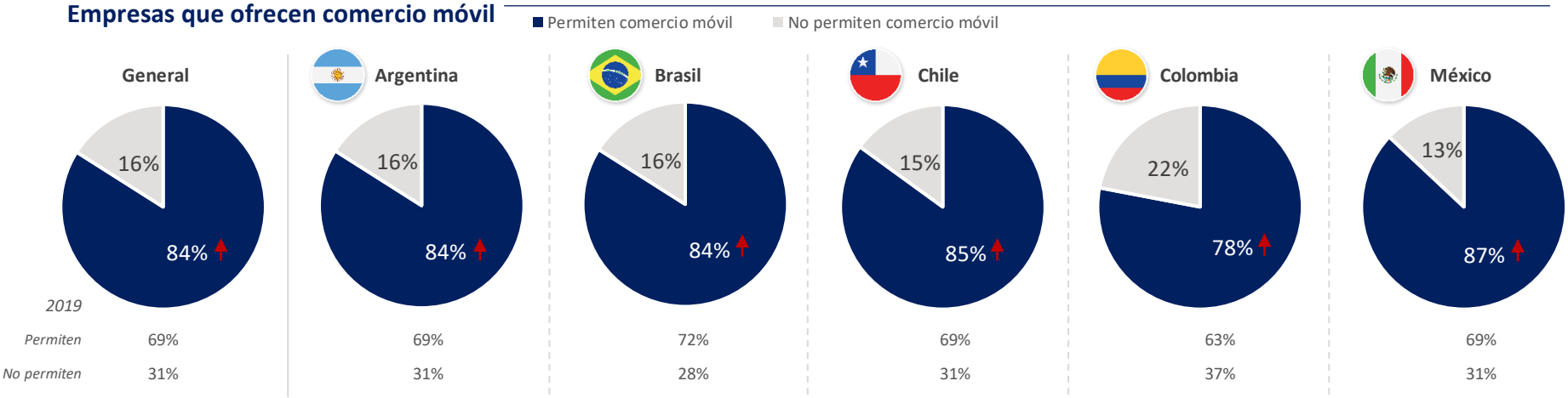
Preguntas de la encuesta:
P2: Por favor indique el porcentaje de transacciones realizadas (en los últimos 12 meses) para cada uno de los siguientes canales utilizados por su compañía:

↑↓ = significativamente o direccionalmente más alto/más bajo que en 2019

LATAM es uno de los mercados móviles de más rápido crecimiento, siendo el móvil principalmente el medio de conectividad a Internet para muchas personas. Hubo crecimiento significativo del número de comerciantes y entidades financieras que ofrecen M-commerce desde 2019.

Dado que en LATAM se observó un crecimiento en transacciones móviles antes de COVID-19[6], es probable que el aumento de su adopción por parte de las empresas no sea una respuesta rápida a la pandemia; se requiere tiempo para implementar y optimizar un proceso de canal móvil. Sin embargo, la COVID-19 probablemente aceleró planes que ya estaban en curso.

Empresas que ofrecen comercio móvil



	General	Argentina	Brasil	Chile	Colombia	México
2019						
Permiten	69%	69%	72%	69%	63%	69%
No permiten	31%	31%	28%	31%	37%	31%

[6] https://techcrunch.com/2020/10/28/current-and-upcoming-trends-in-latin-americas-mobile-growth/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAKl8D2rP3oPZpWhbZpqx-BsI585aNcfc3JH6Spc3ca2KzbLk-jvs09lMiTPvNThrKBhidWkvtcweA94PFO7Inz0cgxW-QgT4oYM0oaPoG4JUgQZeG1IBUcx4R9ZtwMoGhN5vKmlCUYESmjTrdnPUTzbm1crK_r-itFNlqB4uIiK

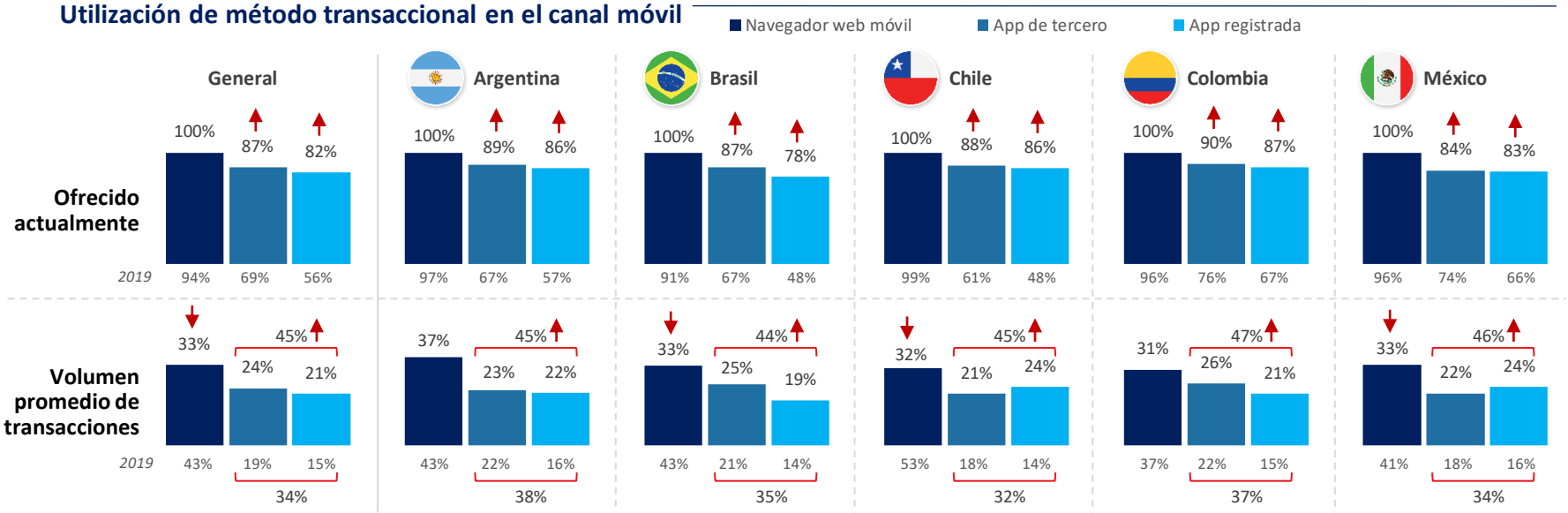
Preguntas de la encuesta:
P4: Por favor indique el porcentaje de transacciones realizadas (en los últimos 12 meses) para cada uno de los siguientes canales de pago que son aceptados actualmente por su compañía:

= significativamente o direccionalmente más alto/más bajo que en 2019

Ha habido un aumento significativo en el número de comerciantes y entidades financieras de LATAM que permiten transacciones con aplicaciones móviles, lo cual se traduce en un aumento de volumen.

La utilización de aplicaciones móviles aumentó rápidamente en México y Brasil al inicio de la pandemia de COVID-19; sin embargo los hallazgos que aparecen abajo muestran que los otros mercados los alcanzaron rápidamente[7].

Utilización de método transaccional en el canal móvil



[7] https://labsnews.com/en/news/business/the-app-economy-surged-in-mexico-and-brazil-during-the-last-few-months/

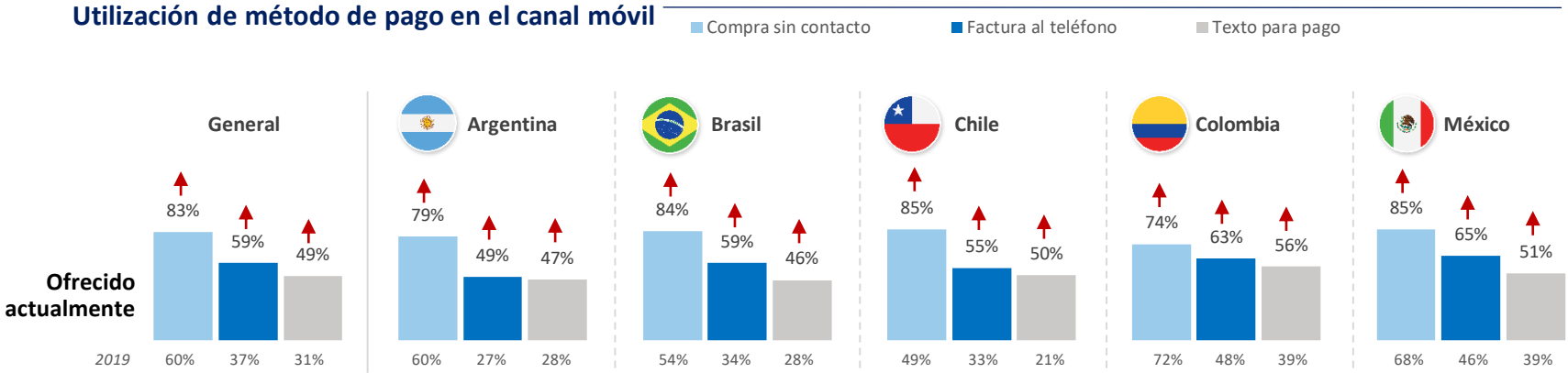
Preguntas de la encuesta:
P4: Por favor indique el porcentaje de transacciones realizadas (en los últimos 12 meses) para cada uno de los siguientes canales de pago que son aceptados actualmente por su compañía:

↑↓ = significativamente o direccionalmente más alto/más bajo que en 2019

El pago sin contacto es ofrecido actualmente por un número significativamente mayor de empresas en LATAM que en 2019, siendo el miedo de contagio de COVID-19 lo que impulsa la preocupación por el manejo de efectivo en persona.

Tal como se dijo antes, el volumen promedio de transacciones en persona se mantiene en niveles de antes de COVID-19. Al menos algunos de los consumidores de LATAM han utilizado los pagos sin contacto como una forma de continuar haciendo transacciones en persona, a la vez que evitan los métodos de pago con contacto comunes.

Utilización de método de pago en el canal móvil



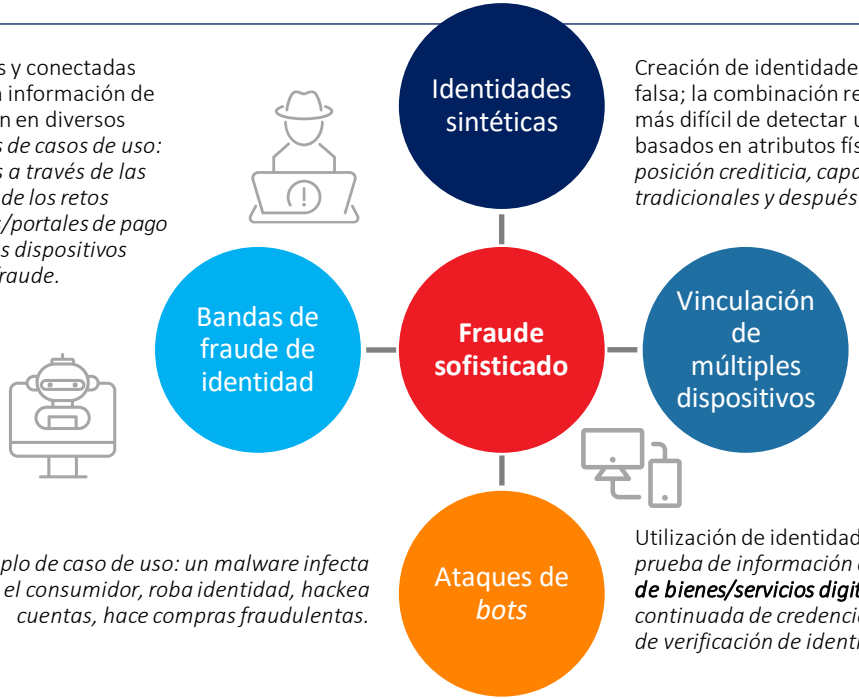
= significativamente o direccionalmente más alto/más bajo que en 2019

Preguntas de la encuesta:
P4: Por favor indique el porcentaje de transacciones realizadas (en los últimos 12 meses) para cada uno de los siguientes canales de pago que son aceptados actualmente por su compañía:

El fraude se está volviendo más sofisticado y complejo.

Los controles de verificación tradicionales utilizando atributos físicos (dirección física, fecha de nacimiento, número de seguridad social, etc.) son menos eficaces para detectar y prevenir estos tipos de fraude organizado. Esto es especialmente difícil para transacciones realizadas en línea o mediante comercio móvil.

Los sofisticados métodos que se muestran abajo impactan no solo la evaluación de riesgo de identidad, sino también el riesgo transaccional. Uno de los impactos es la capacidad limitada para determinar la fuente/ubicación de una transacción.



Redes de fraude organizadas y conectadas globalmente que comparten información de identidad robada y colaboran en diversos ataques de fraude; *ejemplos de casos de uso: ejecución de ataques de bots a través de las fronteras; aprovechamiento de los retos planteados por proveedores/portales de pago externos; utilización de varios dispositivos para confundir el rastro del fraude.*

Creación de identidades que consisten de información personal real y/o falsa; la combinación real+falsa hace que una identidad parezca legítima y más difícil de detectar utilizando métodos de verificación tradicionales basados en atributos físicos; *ejemplos de casos de uso: cultivar una buena posición crediticia, capacidad de superar controles de verificación tradicionales y después salir a cometer fraude con artículos de más alto valor.*

Dispositivo fraudulento vinculado con muchos otros dispositivos por medio de una dirección de compra única; *ejemplo de caso de uso: comprar vía móvil y recoger en tienda.*

Varios dispositivos asociados con múltiples direcciones de correo electrónico y ubicaciones; *ejemplos de casos de uso: creación de cuentas fraudulentas nuevas, apropiación de cuentas y programas de lealtad utilizando direcciones IP de proxies.*

Ataques de redes de *bots*; *ejemplo de caso de uso: un malware infecta dispositivos sin que lo sepa el consumidor, roba identidad, hackea cuentas, hace compras fraudulentas.*

Utilización de identidades y credenciales robadas; *ejemplos de casos de uso: prueba de información de tarjeta de crédito robada con bienes/servicios (**típico de bienes/servicios digitales**) que tiende a generar menos sospechas; prueba continuada de credenciales de identidad para hallar las que pasan los controles de verificación de identidad de los comerciantes.*

LexisNexis® RISK SOLUTIONS

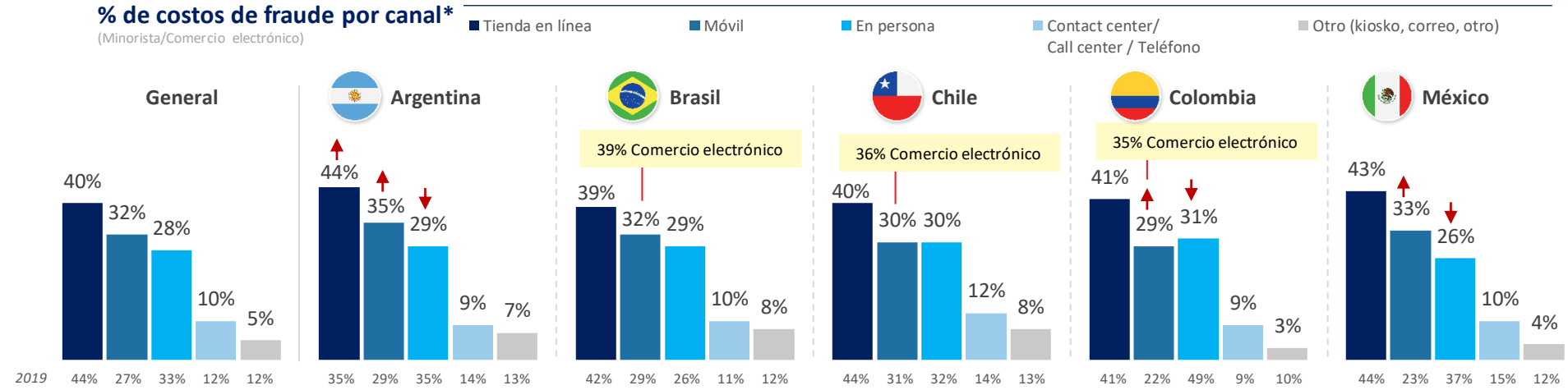
El canal en línea es el canal con el mayor porcentaje de costos de fraude para vendedores minoristas/de comercio electrónico, a pesar de que los vendedores de comercio electrónico también observan un nivel de fraude apreciable en el canal móvil.

Los vendedores de comercio electrónico tienen menos probabilidad que otros de utilizar ciertas soluciones que mejoran la detección de fraude con transacciones móviles, entre ellas identificador de dispositivo, geolocalización, autenticación usando biometría y calificación de transacciones en tiempo real. Tal como se muestra más adelante, los vendedores de comercio electrónico están sufriendo más fraude con billeteras electrónicas que los minoristas.

Es interesante que el canal en persona también continúa generando una cantidad significativa de fraude, aún en ciertos mercados donde el nivel ha bajado.

% de costos de fraude por canal*

(Minorista/Comercio electrónico)



*El porcentaje puede sumar más de 100 % porque las respuestas están basadas en el uso de un canal

Preguntas de la encuesta:
P15: Indique el porcentaje de costos de fraude generados por medio de cada uno de los siguientes canales transaccionales utilizados por su compañía:

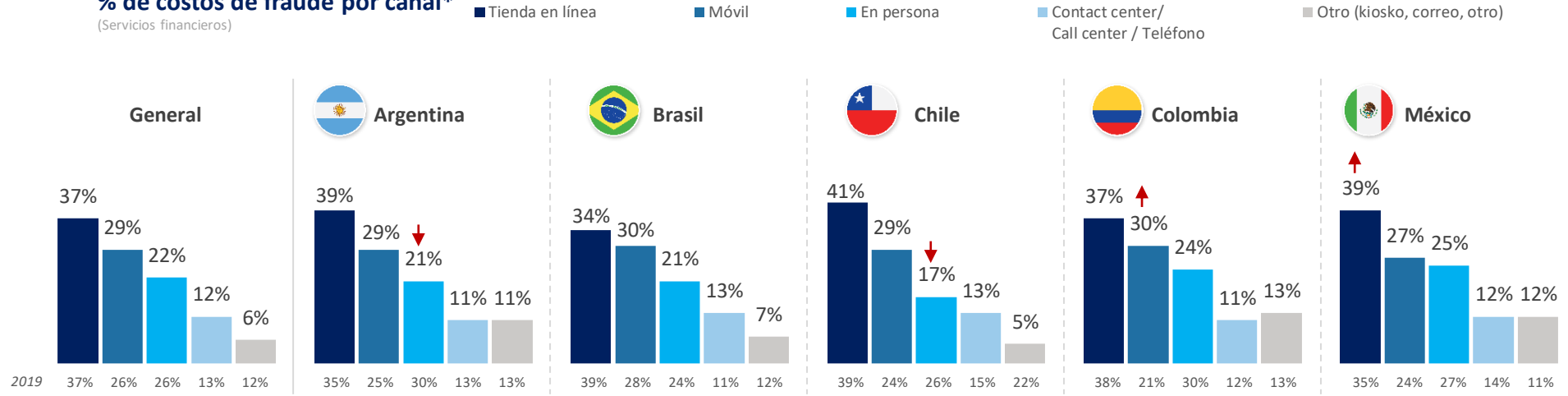
= significativamente o direccionalmente más alto/más bajo que en 2019

El canal digital también es el canal más grande en costos de fraude entre las entidades de servicios financieros

Hay un aumento direccional en costos de fraude en el canal móvil, pero no es tan significativo en comparación con los vendedo res de comercio electrónico.

% de costos de fraude por canal*

(Servicios financieros)



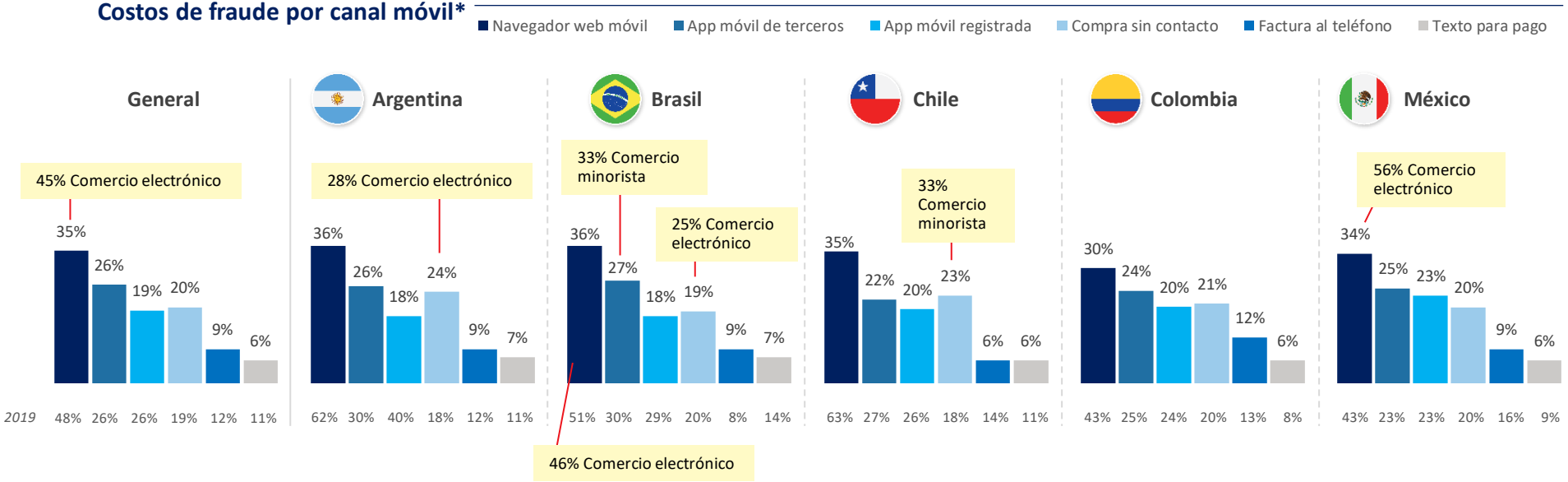
*El porcentaje puede sumar más de 100 % porque las respuestas están basadas en el uso de un canal

Preguntas de la encuesta:
P15: Indique el porcentaje de costos de fraude generados por medio de cada uno de los siguientes canales transaccionales utilizados por su compañía:

= significativamente o direccionalmente más alto/más bajo que en 2019

Aunque los navegadores móviles continúan representando una porción apreciable de los costos de fraude en canales móviles, los comerciantes están empezando a tener más costos desde los métodos de pago sin contacto.

Costos de fraude por canal móvil*



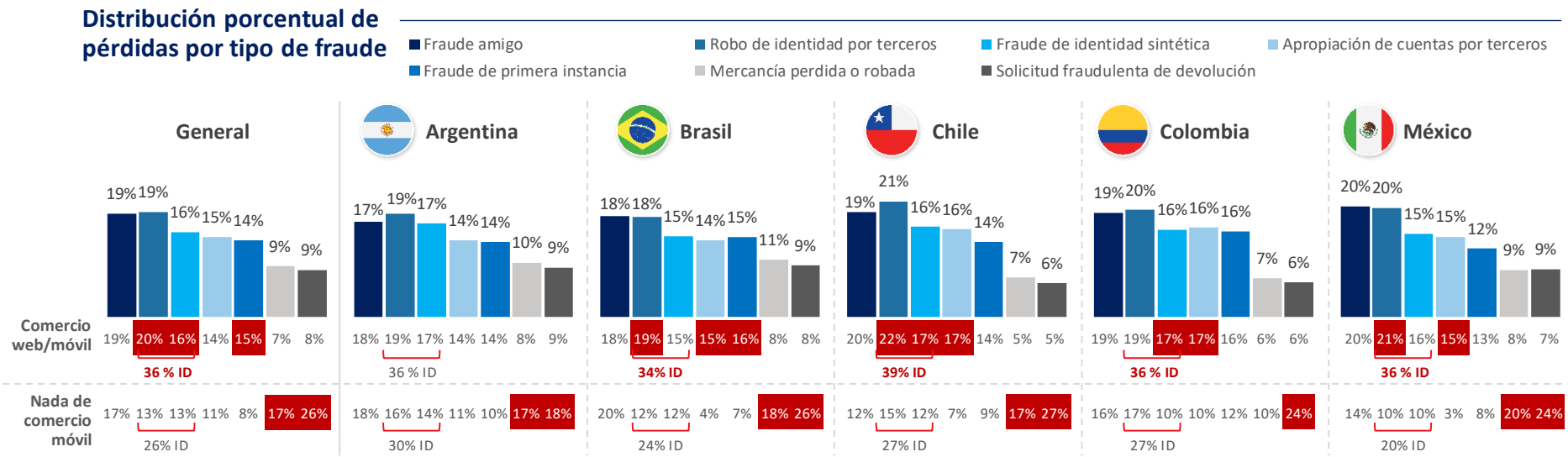
*El porcentaje puede sumar más de 100 % porque las respuestas están basadas en el uso de un canal

Preguntas de la encuesta:
P17: Indique la distribución de fraude en los diversos canales que usted utiliza/acepta.

En la medida que ha aumentado el volumen en canales móviles, también han aumentado las pérdidas asociadas con fraude de identidad y apropiación de cuentas.

Comerciantes y entidades financieras de LATAM que permiten comercio móvil sufren pérdidas significativamente mayores con estos tipos de fraude, incluyendo mayor exposición a identidades sintéticas.

Distribución porcentual de pérdidas por tipo de fraude

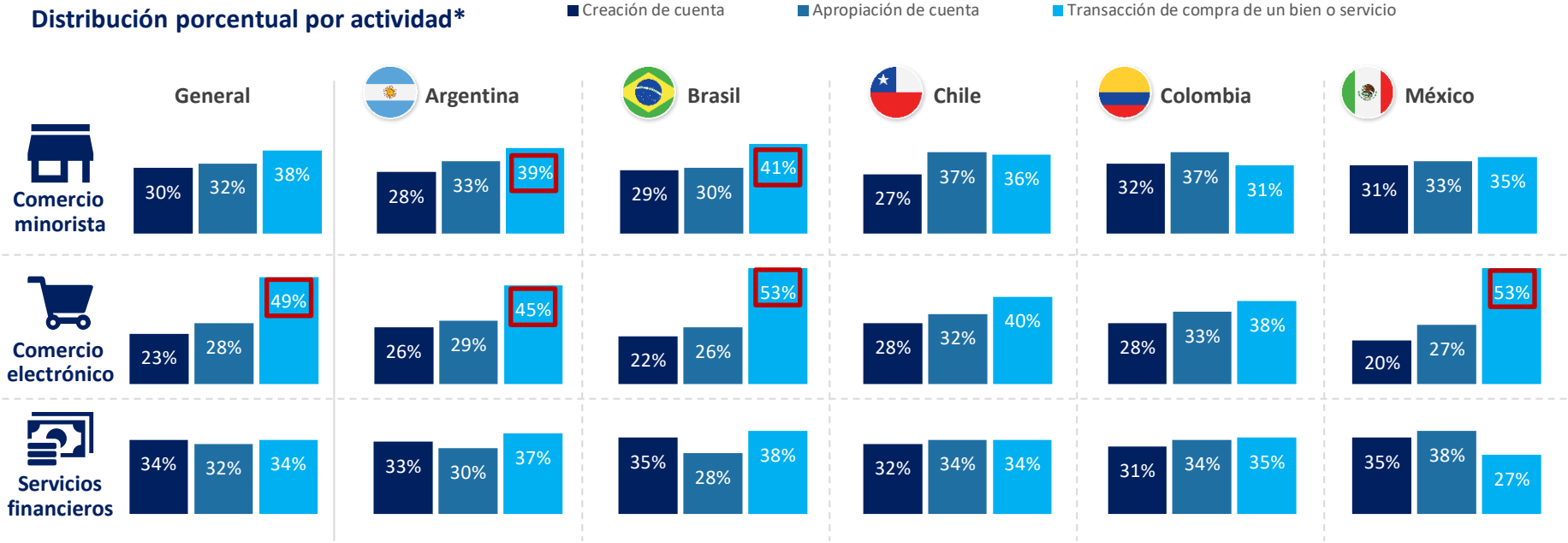


Rojo = significativamente o direccionalmente más alto que otro segmento

Preguntas de la encuesta:
P12a: Piense ahora en sus pérdidas totales por fraude en los últimos 12 meses. Indique la distribución porcentual de los siguientes métodos de fraude, tal como son atribuidos a las pérdidas por fraude que ocurrieron en los últimos 12 meses. Haga su mejor estimación.

El fraude relacionado con identidad ocurre con más frecuencia en el punto de venta de los vendedores argentinos y brasileños, especialmente los de comercio electrónico. En otros mercados, la distribución de pérdidas es similar entre el fraude transaccional y el fraude relacionado con cuentas.

Fraude relacionado con identidad: Distribución porcentual por actividad*



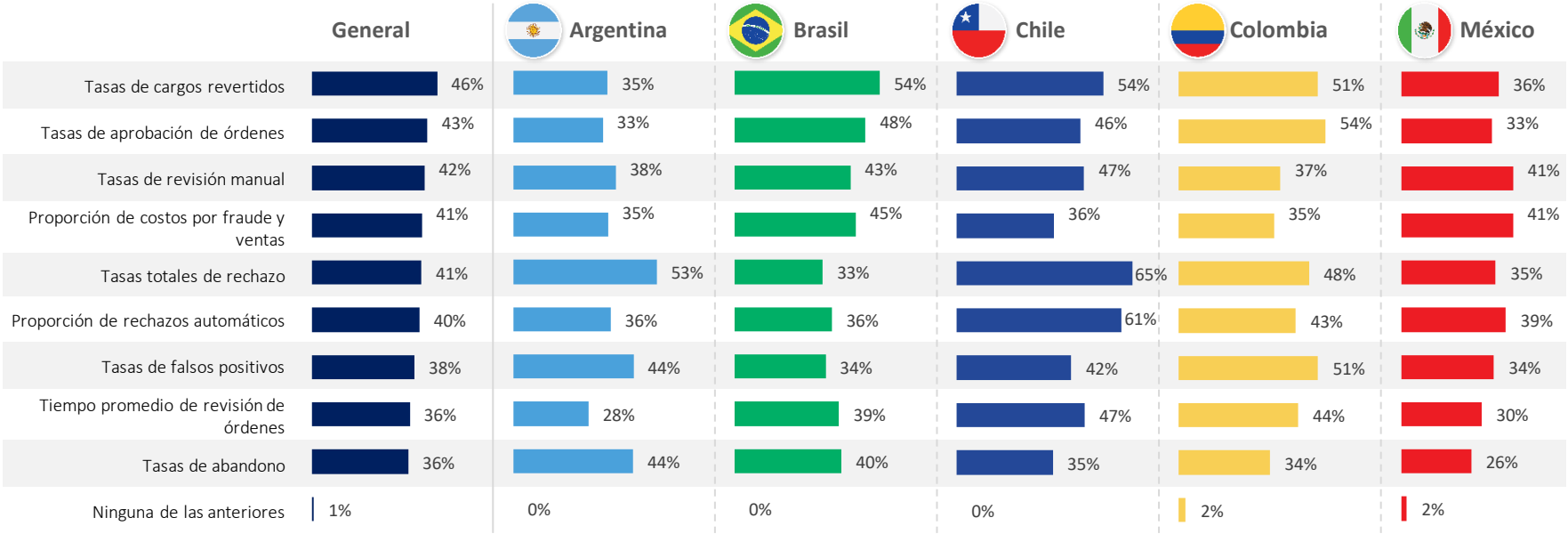
= significativamente o direccionalmente más alto que el fraude de identidad relacionado con cuentas dentro del segmento de industria/mercado

P12b: ¿Para el fraude relacionado con identidad, cuál es la distribución por los siguientes tipos de actividad?

*Precaución: tamaño reducido de la base

Los indicadores utilizados para medir el desempeño contra el fraude varían ampliamente por mercado de LATAM.

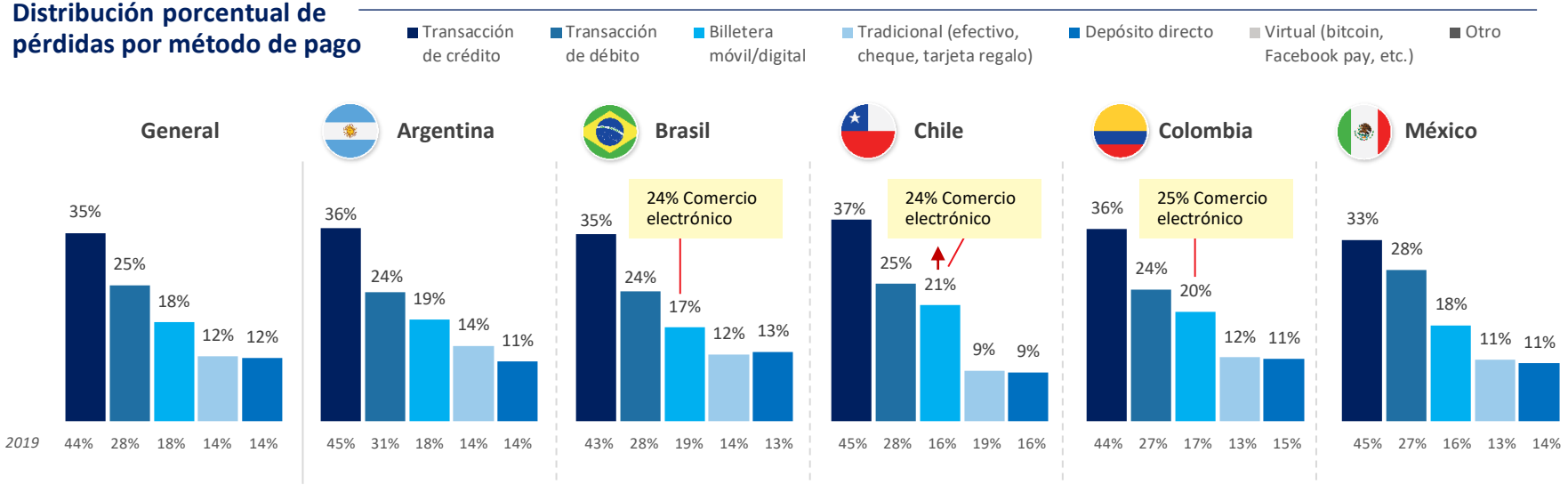
Medición del desempeño en la prevención de fraude



Preguntas de la encuesta:
P12c: ¿Cuáles de los siguientes indicadores utiliza su organización para medir el desempeño en la prevención de fraude? (La pregunta NO se hizo en 2019)

Aunque las transacciones de crédito son el método de pago con las mayores pérdidas por fraude, las billeteras móviles/digitales representan una porción considerable (casi una quinta parte).

Distribución porcentual de pérdidas por método de pago



↑ = significativamente o direccionalmente más alto que en 2019

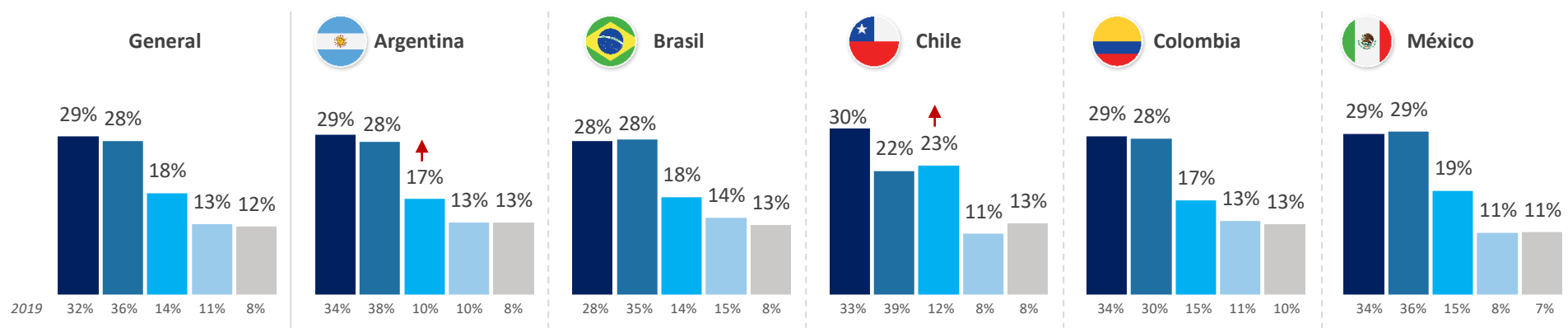
[8] https://www.pindrop.com/blog/mobile-wallets-present-new-opportunities-for-fraud/

Preguntas de la encuesta:
P18: Pensando en las pérdidas totales por fraude sufridas por su compañía en los últimos 12 meses, indique la distribución de costos de fraude para cada método de pago.

LexisNexis® RISK SOLUTIONS

Los casos de tarjeta no presente (CNP) y tarjetas robadas/perdidas siguen siendo los mayores contribuyentes a las pérdidas por fraude relacionado con tarjetas, aunque el fraude con tarjetas falsificadas ha aumentado en Argentina y Chile.

Distribución porcentual de pérdidas relacionadas con fraude de tarjetas



↑↓ = significativamente o direccionalmente más alto/más bajo que en 2019

Preguntas de la encuesta:
P18e: De sus pérdidas por fraude relacionado con tarjetas débito/crédito, indique la distribución de los siguientes tipos de fraude con tarjeta:

RESULTADO CLAVE 03

El fraude relacionado con identidad es una amenaza y reto clave para minoristas/ vendedores de comercio electrónico y entidades financieras en LATAM.

El fraude relacionado con identidad es un reto clave para transacciones con móviles/navegadores y el canal móvil. Los nuevos métodos de pago móviles contribuyen a esto, y es un desafío especialmente para vendedores de comercio electrónico.

Los retos relacionados con identidad incluyen los que tienen que ver con atributos digitales que evalúan el riesgo de dispositivo y transacción.

Comerciantes y entidades financieras de LATAM también reportan un aumento de ataques de *bots* durante el último año, lo cual no sorprende dado el aumento de tráfico digital.

También ha aumentado la búsqueda de equilibrio entre la detección/prevención de fraude y la fricción mínima para el cliente, especialmente en el canal en línea.

Se espera que los retos mencionados arriba continúen al menos en el corto plazo (próximos 24 meses) y probablemente sean impactados por la incertidumbre sobre la nueva normalidad posterior a COVID-19.

La verificación de identidad ha llegado a ser el principal reto del canal digital; la verificación de teléfono y dirección son parte del problema, especialmente para el comercio minorista. Los nuevos métodos de pago son el mayor problema para los vendedores de comercio electrónico.

Retos de fraude por canal digital (clasificados entre los primeros 3)

Significa estar entre los principales retos del canal digital dentro del mercado

= significativamente o direccionalmente más alto/más bajo que en 2019

= significativamente o direccionalmente más alto que el mismo reto en otros mercados

	General		Argentina		Brasil		Chile		Colombia		México	
	2019	2021	2019	2021	2019	2021	2019	2021	2019	2021	2019	2021
Verificación de identidad de cliente	21%	44% ↑	22%	42% ↑	20%	51% ↑	24%	22% ↑	24%	44% ↑	22%	42% ↑
Verificación de dirección	47%	33%	43%	29%	51%	30%	43%	43%	43%	41%	43%	34%
Introducción de nuevos y diversos métodos transaccionales	31%	31%	31%	34%	32%	39%	26%	23%	26%	27%	31%	21%
Verificación de teléfono	21%	29%	27%	29%	12%	33% ↑	19%	32% ↑	19%	40% ↑	27%	18%
Equilibrio entre prevención de fraude y fricción para el cliente	16%	28% ↑	16%	25%	19%	25%	11%	29% ↑	11%	20% ↑	16%	38% ↑
Verificación de correo electrónico o dispositivo	27%	21%	28%	16%	25%	17%	30%	23%	30%	33%	28%	25% ↑
Incapacidad para determinar fuente/origen de la transacción	30%	21%	14%	19%	27%	19%	37%	22%	37%	17%	14%	25%
Retos en la aceptación de métodos transaccionales internacionales	20%	20%	26%	21%	17%	20%	19%	21%	19%	11%	26%	24%
Evaluación de riesgo de fraude por país/región	22%	19%	21%	18%	21%	11%	35%	30%	35%	22%	21%	28%
Falta de herramientas especializadas para pedidos/transacciones internacionales	16%	19%	18%	31% ↑	16%	20%	10%	18%	10%	14%	14%	12%
Excesiva revisión manual de pedidos	17%	18%	14%	24% ↑	23%	16%	16%	21%	16%	20%	14%	15%
Incapacidad de distinguir entre humano y *bot*	16%	17%	13%	12%	17%	21%	10%	17%	10%	11%	13%	17%

LexisNexis® RISK SOLUTIONS

Preguntas de la encuesta:
P20: Clasifique los primeros 3 retos relacionados con fraude que afronta su compañía al atender clientes que utilizan el canal móvil/en línea.

RETOS DE FRAUDE

La verificación de identidad sigue siendo uno de los principales retos del canal móvil, junto con la verificación de teléfono, dirección y nuevos métodos de pago. Aunque menos encuestados indicaron que la verificación de identidad es uno de los principales retos en Colombia, sí dieron una alta importancia a los retos causantes de este problema.

Retos de fraude por canal móvil (clasificados entre los primeros 3)

Significa estar entre los principales retos del canal digital dentro del mercado

= significativamente o direccionalmente más alto/más bajo que en 2019

= significativamente o direccionalmente más alto que el mismo reto en otros mercados

	General		Argentina		Brasil		Chile		Colombia		México	
	2019	2021	2019	2021	2019	2021	2019	2021	2019	2021	2019	2021
Verificación de identidad de cliente	47%	37%	45%	48%	50%	39%	43%	21%	56%	25%	43%	41%
Introducción de nuevos y diversos métodos transaccionales	28%	30%	23%	35% ↑	30%	31%	21%	32% ↑	38%	25%	23%	28%
Verificación de dirección	31%	30%	27%	29%	34%	23%	33%	35%	32%	40% ↑	26%	36%
Verificación de teléfono	12%	27% ↑	12%	21% ↑	12%	30% ↑	3%	32% ↑	19%	33% ↑	13%	21% ↑
Equilibrio entre prevención de fraude y fricción para el cliente	25%	26%	43%	23%	29%	21%	18%	32% ↑	13%	27% ↑	30%	33%
Verificación de correo electrónico o dispositivo	34%	25%	29%	32%	33%	25%	39%	27%	33%	40% ↑	29%	14%
Incapacidad de distinguir entre humano y *bot*	15%	23%	9%	16%	15%	29%	17%	17%	16%	24% ↑	11%	19%
Excesiva revisión manual de pedidos	17%	23%	20%	22%	11%	25%	24%	24%	22%	19%	21%	20%
Incapacidad para determinar fuente/origen de la transacción	18%	22%	19%	22%	18%	28%	25%	17%	20%	13%	20%	20%
Falta de herramientas especializadas para pedidos/transacciones internacionales	14%	20%	15%	16%	18%	17%	13%	20% ↑	5%	12% ↑	14%	31% ↑
Evaluación de riesgo de fraude por país/región	19%	18%	16%	17%	22%	15%	21%	27% ↑	14%	21% ↑	18%	19%
Retos en la aceptación de métodos transaccionales internacionales	18%	18%	24%	19%	10%	16%	24%	19%	24%	20%	26%	18%

LexisNexis® RISK SOLUTIONS

Preguntas de la encuesta:
P20: Clasifique los primeros 3 retos relacionados con fraude que afronta su compañía al atender clientes que utilizan el canal móvil/en línea.

El fraude de cuentas e identidad son las principales preocupaciones para el canal en línea durante los próximos 24 meses.

Esto muy probablemente se relaciona con la incertidumbre por la "nueva normalidad" después de COVID-19 y él grado en que la preferencia por las transacciones en línea continúe creciendo.

Principales amenazas de fraude esperadas (próximos 24 meses) (clasificadas entre las primeras 3)

Canal en línea

	General	Argentina	Brasil	Chile	Colombia	México
Fraude de apropiación de cuenta	42%	36%	49%	36%	38%	39%
Fraude de identidad de tercera parte	39%	44%	42%	42%	41%	30%
Fraude de identidad sintética	38%	40%	39%	35%	38%	35%
Creación fraudulenta de cuentas nuevas	36%	27%	39%	45%	26%	39%
Fraude amigo	34%	33%	34%	27%	41%	36%
Fraude de primera persona	30%	36%	26%	33%	32%	31%
Fraude de programa de lealtad	24%	34%	13%	38%	27%	30%
Volumen de pedidos *Botnet* que se colocan a la vez	23%	15%	24%	26%	19%	26%
Fraude de compra remota y recogida en la tienda	18%	18%	17%	8%	25%	22%
Solicitud fraudulenta de devolución/reembolso	15%	17%	19%	10%	12%	13%

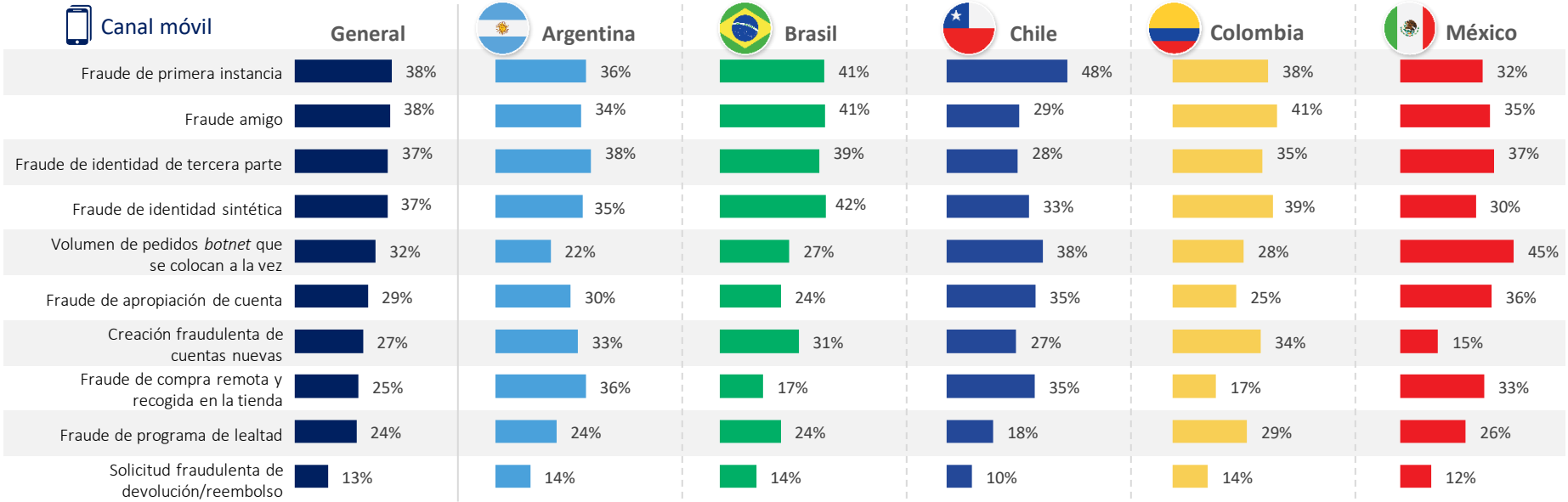
LexisNexis® RISK SOLUTIONS

Preguntas de la encuesta:
P20e: Clasifique las 3 primeras amenazas de fraude que espera enfrentar en los próximos 24 meses al atender clientes utilizando el(los) siguiente(s) canal(es): (La pregunta NO se hizo en 2019)

El fraude de primera instancia (o de primera persona) y el fraude amigo se unen al fraude de identidad como la preocupación importante para el canal móvil en los próximos 24 meses.

El fraude de primera instancia puede consistir en que los miembros de un hogar utilicen el dispositivo móvil de alguien para hacer compras sin que lo sepa el dueño del dispositivo. Las restricciones por COVID han aumentado este riesgo.

Principales amenazas de fraude esperadas (próximos 24 meses) (clasificadas entre las primeras 3)

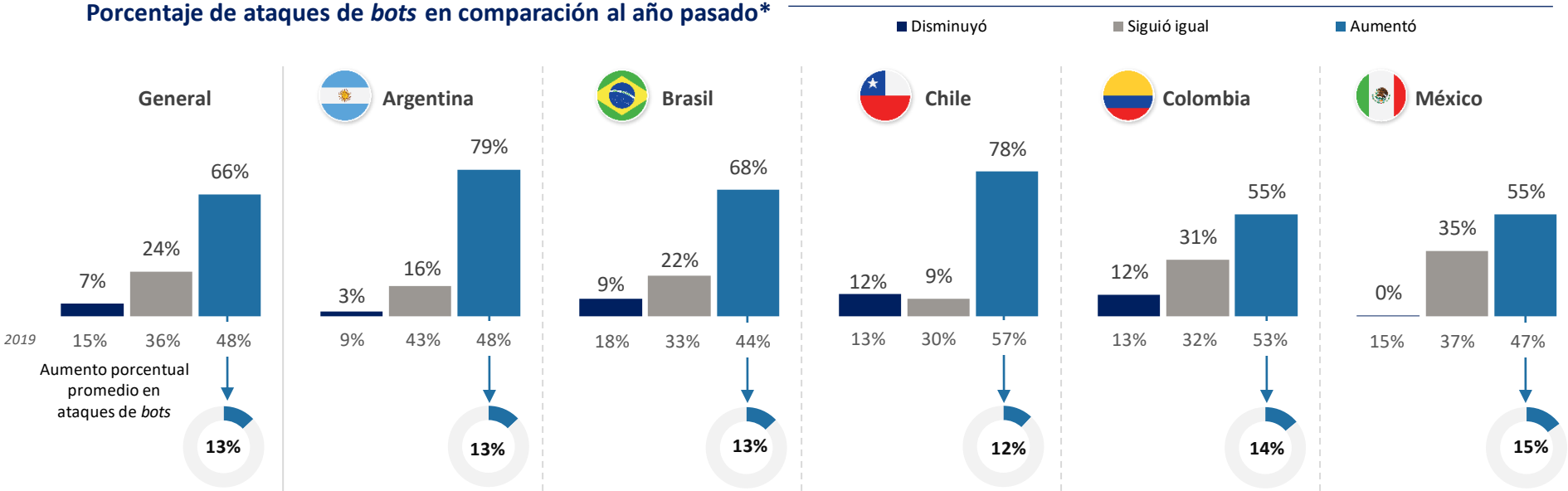


LexisNexis® RISK SOLUTIONS

Preguntas de la encuesta:
P20e: Clasifique las 3 primeras amenazas de fraude que espera enfrentar en los próximos 24 meses al atender clientes utilizando el(los) siguiente(s) canal(es): (La pregunta NO se hizo en 2019)

Las empresas de LATAM, especialmente las argentinas, brasileñas y chilenas, señalan un aumento de ataques de *bots* durante el último año.

Porcentaje de ataques de *bots* en comparación al año pasado*



* Excluye a aquellos que dijeron "No estoy seguro"

Preguntas de la encuesta:
P1b/c: ¿Cómo se compara esto con la misma época del año pasado? ¿En cuánto se ha incrementado el porcentaje de ataques automatizados maliciosos de *bots* durante el último año?

RESULTADO CLAVE 04

Comerciantes y entidades de servicios financieros de LATAM pueden reducir los costos y riesgos de fraude mediante una buena práctica, que consiste en integrar las operaciones de ciberseguridad, experiencia digital de cliente y fraude por medio de un enfoque de solución multicapa.

La fricción para el cliente es una preocupación real en la labor de prevención de fraude, especialmente en los canales móviles/en línea, en los cuales es común que haya abandono cuando el cliente debe esforzarse y hay demoras transaccionales.

Los canales móviles/en línea tienen riesgo creciente de fraude en la medida que nuevos métodos de pagos y transacciones ofrecen puntos de acceso adicionales a defraudadores sofisticados.

En promedio, muchas empresas no están optimizando sus estrategias de detección y prevención de fraude basadas en esta buena práctica. Aquellas que la acogen tienen más probabilidad de tener los datos necesarios para detectar y evaluar riesgos de fraude. Ellas tienen:

- menos probabilidad de clasificar la verificación de identidad como reto móvil/en línea clave;
- menos probabilidad de clasificar como reto los nuevos métodos de pago móviles, especialmente en lo relacionado con fraude de identidad;
- más capacidad de gestionar la detección de fraude a la vez que minimizan la fricción para el cliente; y
- tienen más probabilidad de incurrir un costo de fraude menor comparado con las demás.

ESTRATEGIAS DE DETECCIÓN Y PREVENCIÓN DE FRAUDE

El fraude se ha vuelto más complejo; puede haber diversos riesgos a la vez sin que haya una solución única. Las herramientas contra el fraude deben autenticar los criterios tanto digitales como físicos, así como el riesgo de identidad y transacción.

PROBLEMAS DE FRAUDE

SERVICIOS DIGITALES

transacciones rápidas, identidad fácil sintética y objetivos de botnets; se necesita verificación de velocidad para determinar el riesgo de transacción junto con datos y analítica para autenticar al individuo

FRAUDE RELACIONADO CON CUENTAS

datos vulnerados requieren más niveles de seguridad, así como la autenticación de la persona desde un bot o identidad sintética

IDENTIDADES SINTÉTICAS

necesitan autenticar todo el individuo detrás de la transacción con el fin de distinguir de una identidad falsa basada en datos reales parciales

ATAQUES DE BOTNETS

ataques humanos masivos o automatizados a menudo para probar tarjetas, contraseñas/ credenciales o infectar dispositivos

CANAL MÓVIL

el origen de la fuente y dispositivos infectados añaden riesgo; bots móviles y malware malicioso hacen difícil la autenticación; necesidad de evaluar el dispositivo y el individuo

OPCIONES DE SOLUCIONES

▶ EVALUACIÓN DEL RIESGO DE TRANSACCIÓN

Verificaciones de velocidad/calificación de transacciones: Monitorea patrones transaccionales históricos de un individuo contra sus transacciones actuales para detectar si el volumen del titular de la tarjeta coincide o si parece haber algunairregularidad. **Ejemplos de soluciones:** calificación de transacciones en tiempo real; calificación automatizada de transacciones

▶ AUTENTICACIÓN DE LA PERSONA FÍSICA

Verificación básica: Verificación de nombre, dirección, fecha de nac. o suministro de un código CVV asociado con una tarjeta. **Ejemplos de soluciones:** servicios de verificación de cheques; autenticación de instrumento de pago; verificación de nombre/dirección/fecha de nac.

Autenticación de Active ID: uso de datos personales conocidos por el cliente para autenticación; o cuando un usuario suministra dos factores de autenticación diferentes parasu propia verificación. **Ejemplos de soluciones:** autenticación por reto o quiz; autenticación utilizando factor OTP/ 2

▶ AUTENTICACIÓN DE LA PERSONA DIGITAL

Identidad digital/biometría conductual: Analiza interacciones humano-dispositivo y patrones comportamentales, tales como clics de ratón y teclazos, para distinguir entre un usuario real y un impostor al reconocer el comportamiento de un usuario normal y un defraudador. **Ejemplos de soluciones:** autenticación por biometría; evaluación de riesgo de correo/teléfono; rastreo de navegador/malware; identificador / huella de dispositivo

Evaluación de dispositivos: identificar con certeza un dispositivo computacional remoto o un usuario. **Ejemplos de soluciones:** identificador/huella de dispositivo; geolocalización

LexisNexis® RISK SOLUTIONS

Las buenas prácticas incluyen poner diversas soluciones en capas para abordar riesgos específicos de diferentes canales, métodos de pago y productos. Además, van más allá al integrar capacidades y operaciones con sus esfuerzos de prevención de fraude.

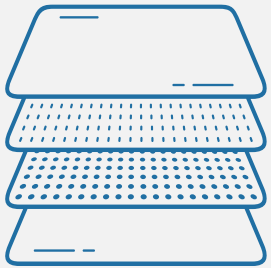
Integración

Herramientas y capacidades con enfoque de prevención de fraude

- Alertas de ciberseguridad
- Inteligencia de medios sociales
- Modelos IA/ML
- *Crowdsourcing*
- Operaciones de ciberseguridad
- Operaciones digitales/de experiencia de cliente

Capas de soluciones de detección y prevención de fraude

Un enfoque de solución multicapa es esencial para combatir el fraude y a la vez, mitigar la fricción para el cliente.



- Abordar riesgos de fraude de identidad y de transacción
- Riesgos diferentes al vender bienes digitales y físicos
- Diferentes riesgos y retos para móvil versus en línea
- *Botnets* y *malware* pueden comprometer dispositivos móviles. Autenticar tanto el usuario como el dispositivo

Estrategia y foco

Minimizar la fricción y a la vez, maximizar la protección contra el fraude

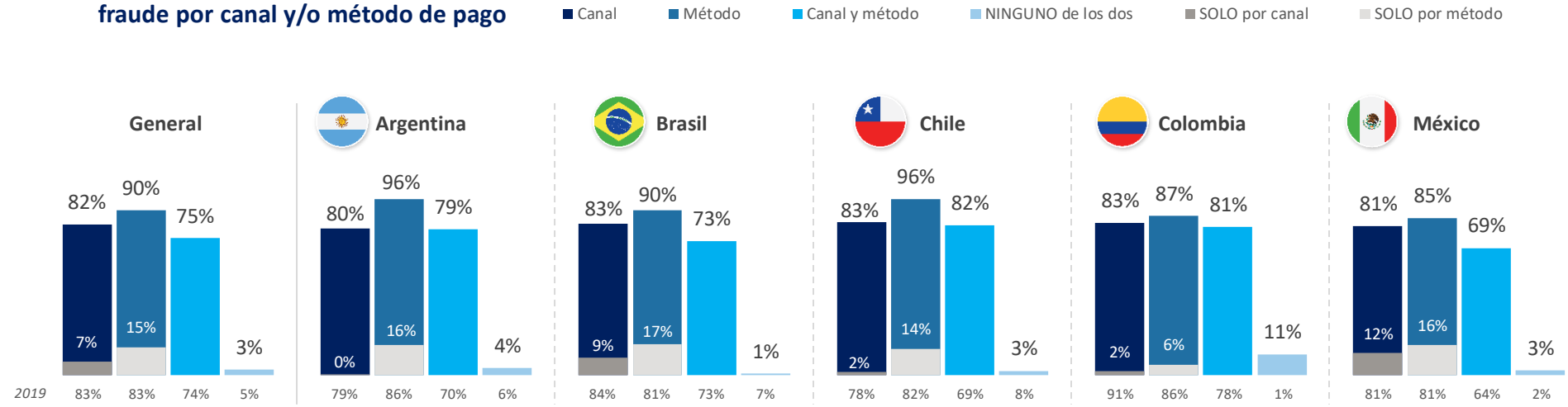
- Rastreo exitoso y prevención de fraude por canal transaccional y método de pago
- Uso de soluciones de autenticación digitales/pasivas para reducir el esfuerzo del cliente (dejar que las soluciones hagan el trabajo tras bambalinas)
- Evaluación de riesgo individual y transaccional

LexisNexis® RISK SOLUTIONS

Rastrear los costos del fraude tanto por canal transaccional como por método de pago es esencial para la prevención del fraude. La mayoría de los encuestados indican que lo hacen.

Ya que el fraude ocurre de diferentes maneras dependiendo de si se venden bienes físicos o digitales y si se utiliza el canal móvil, esto crea múltiples puntos y formas en que pueden atacar los defraudadores. Ellos continúan buscando los eslabones más débiles donde puedan operar sin ser detectados. Saber dónde han sido exitosos los defraudadores es importante para "cerrar las brechas", pero saber también dónde lo intentaron y fallaron es importante con el fin de mantener la vigilancia.

% de negocios que rastrean costos de fraude por canal y/o método de pago

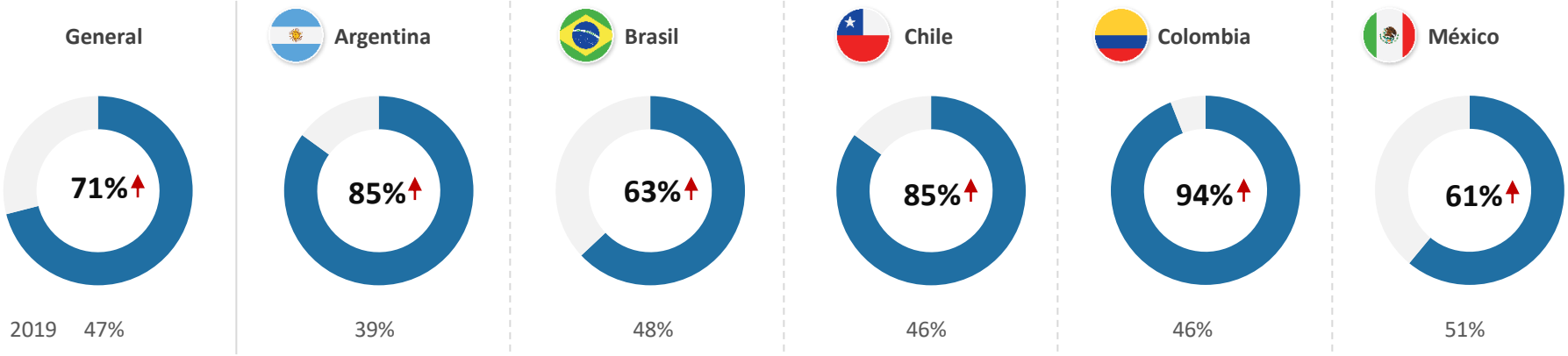


Preguntas de la encuesta:
P14a: ¿Su compañía rastrea el uso de transacciones fraudulentas según el canal o método de pago utilizado?

La mayoría de comerciantes y entidades financieras de LATAM indican que le dan seguimiento a los costos del fraude por punto de origen, mucho más de lo que lo hacían incluso hace 2 años.

El aumento del volumen de transacciones en línea y móviles probablemente influye sobre esto.

% que rastrea el costo de transacciones fraudulentas por punto de origen internacional



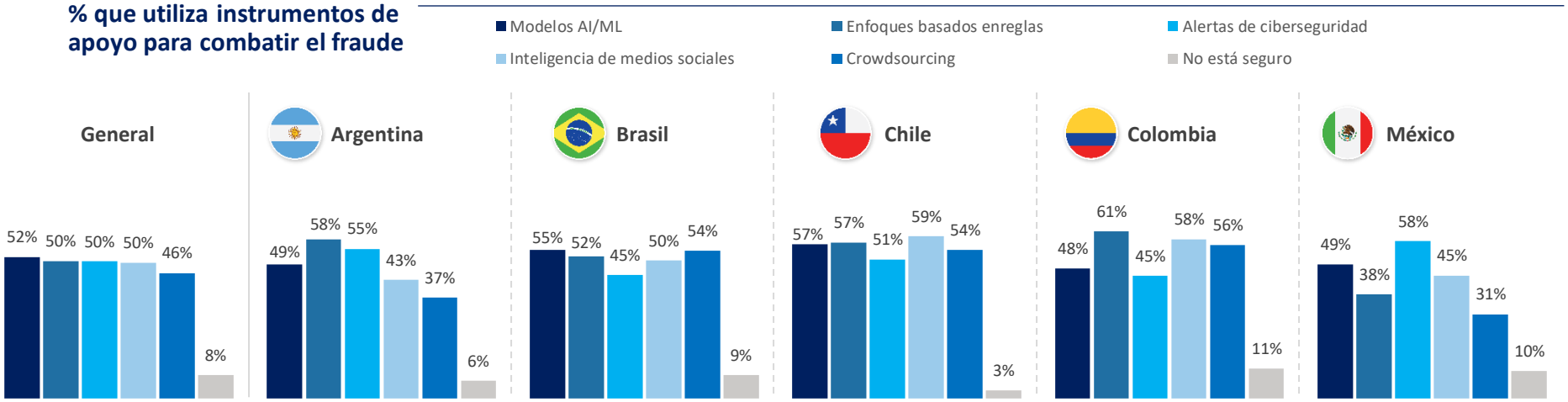
↑ = significativamente o direccionalmente más alto/más bajo que en 2019

Preguntas de la encuesta:
P14b: ¿Su compañía rastrea el costo de transacciones fraudulentas según el sitio donde se originan a nivel internacional (es decir, provenientes de regiones específicas)?

LexisNexis® RISK SOLUTIONS

Una cantidad considerable de comerciantes y entidades financieras indican que utilizan diferentes tipos de instrumentos de apoyo para combatir el fraude.

% que utiliza instrumentos de apoyo para combatir el fraude



*se preguntó a aquellas con transacciones en línea y/o por canal móvil

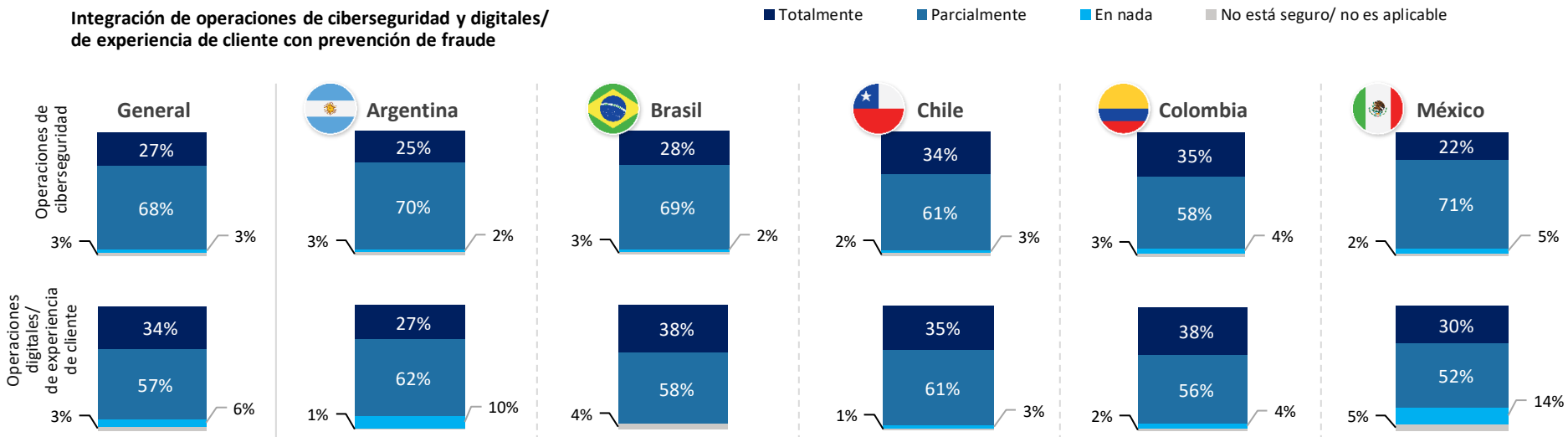
Preguntas de la encuesta:
P28b: Además de soluciones, ¿qué instrumentos de apoyo utiliza su compañía para ayudar a combatir el fraude?
(La pregunta NO se hizo en 2019)

Sin embargo, pocos indican que su organización ha integrado plenamente sus operaciones de ciberseguridad y digitales/de experiencia de cliente con estrategias de protección contra el fraude.

A medida que crece el volumen transaccional a través de canales remotos/digitales, será un imperativo para las empresas integrar plenamente estas operaciones, en términos de protección contra el ciberfraude y como forma de minimizar la fricción para el cliente cuando evalúen los riesgos de fraude.

% que utiliza las mejores prácticas de mitigación de fraude

Integración de operaciones de ciberseguridad y digitales/ de experiencia de cliente con prevención de fraude



*se preguntó a aquellas con transacciones en línea y/o por canal móvil

Preguntas de la encuesta:
P29: ¿Hasta qué punto su compañía ha integrado sus operaciones de ciberseguridad con los esfuerzos de prevención de fraude?
P30b: ¿Hasta qué punto su compañía ha integrado sus operaciones digitales/de experiencia de cliente con los esfuerzos de prevención de fraude? (Las preguntas NO se hicieron en 2019)

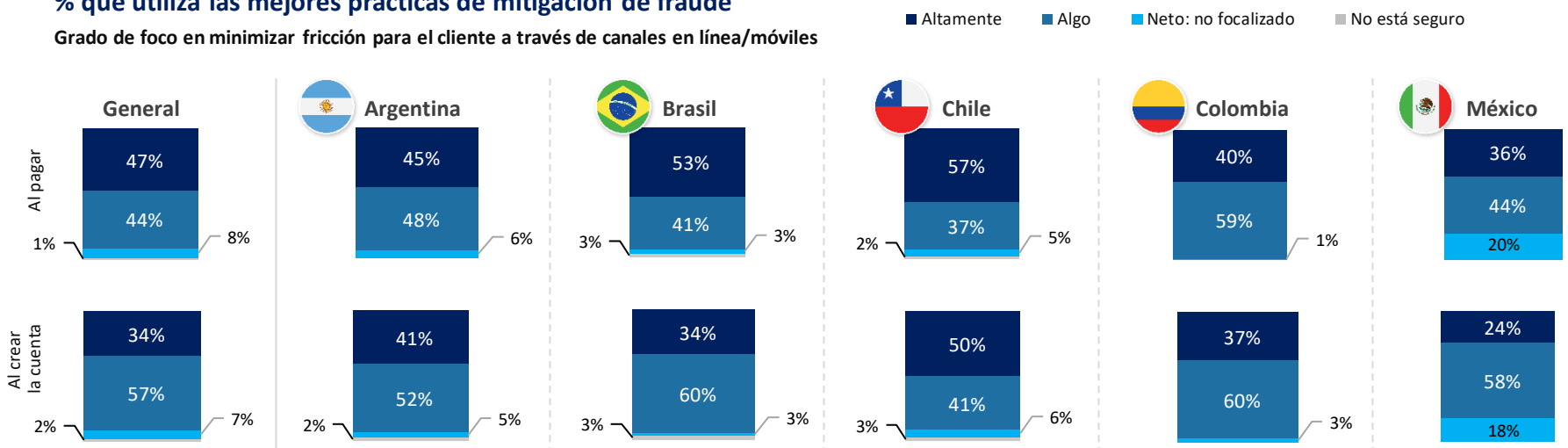
ESTRATEGIAS DE DETECCIÓN Y PREVENCIÓN DE FRAUDE

Más o menos la mitad de las empresas argentinas, brasileñas y chilenas dicen que están muy enfocadas en minimizar la fricción para el cliente en el punto de transacción, pero no todas están enfocadas en lo mismo al crear la cuenta. México y Colombia están rezagados en ambos aspectos.

Equilibrar la detección de fraude con la fricción para el cliente es una preocupación real para empresas que hacen transaccio nes vía los canales en línea y móviles. Es común que los clientes abandonen el carrito de compras cuando se frustran por tanto esfuerzo; a la vez, estos son canales con alto riesgo de fraude que debe ser abordado.

% que utiliza las mejores prácticas de mitigación de fraude

Grado de foco en minimizar fricción para el cliente a través de canales en línea/móviles



*se preguntó a aquellas con transacciones en línea y/o por canal móvil

Preguntas de la encuesta:

P30: ¿Hasta qué punto su compañía está enfocada en minimizar la fricción para el cliente en el momento de pago de una transacción de canal en línea o móvil?

P30a: ¿Hasta qué punto su compañía está enfocada en minimizar la fricción para el cliente cuando alguien abre una nueva en cuenta en línea o mediante un dispositivo móvil? (Las preguntas NO se hicieron en 2019)

LexisNexis® RISK SOLUTIONS

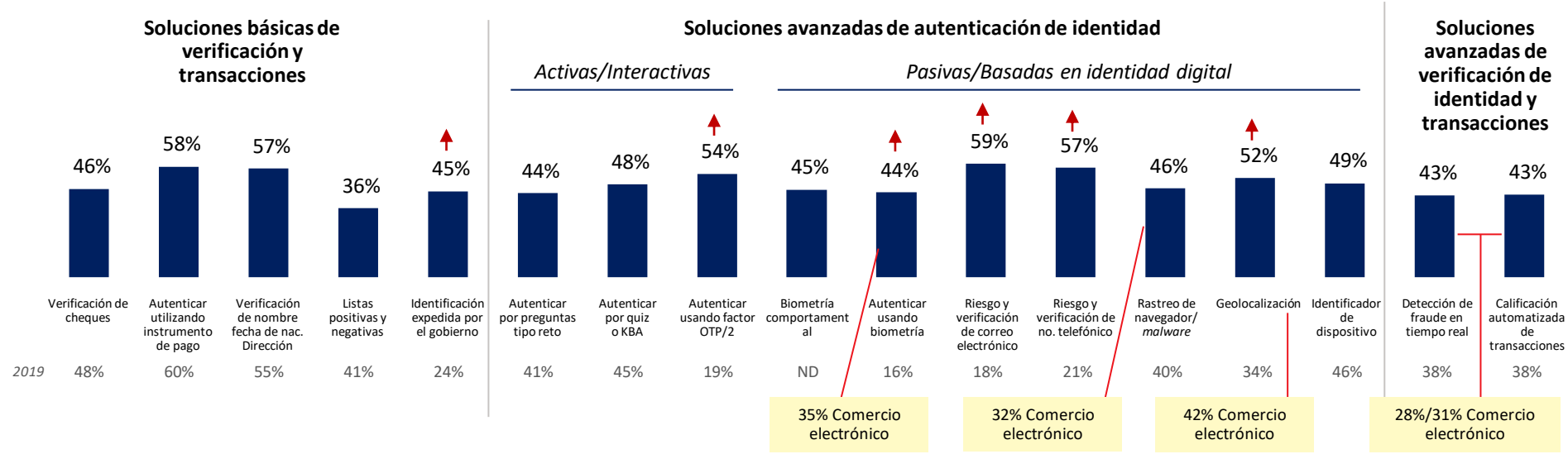
Resultado clave 04

ESTRATEGIAS DE DETECCIÓN Y PREVENCIÓN DE FRAUDE

Han existido inversiones en autenticación utilizando soluciones factor OTP/2 y pasivas/digitales basadas en identidad.

Sin embargo, hay menos vendedores de comercio electrónico entre las empresas que han hecho esas inversiones, lo cual las hace más vulnerables durante la pandemia - especialmente por el uso menos frecuente de soluciones digitales que ofrecen detección de fraude más eficaz contra el ciberdelito y las identidades sintéticas.

Utilización de soluciones de mitigación de fraude (regional)



↑ = significativamente o direccionalmente más alto/más bajo que en 2019

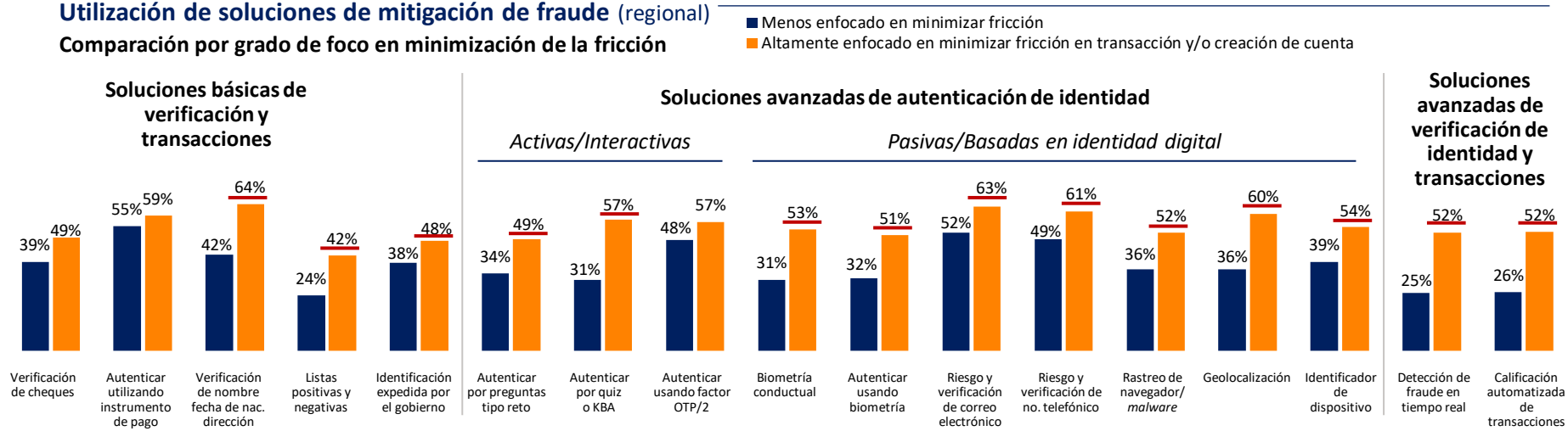
Preguntas de la encuesta:
P27: ¿Cuáles de las siguientes soluciones contra fraude utiliza su empresa hoy en día?

Estas y otras inversiones se han centrado en comerciantes y entidades financieras de LATAM que están enfocadas en minimizar la fricción para el cliente, incluyendo soluciones digitales que evalúan los comportamientos, el dispositivo, la transacción y el individuo.

Incluyen aquellas diseñadas para evaluar riesgos tanto de individuos como dispositivos (riesgo y verificación de correo electrónico/teléfono, geolocalización, identificador de dispositivo, rastreo de navegador/*malware*) y para algunos, riesgo de transacción (calificación automatizada de transacción). Geolocalización e identificador de dispositivo también soportan detección de fraude en canal móvil. Todas las soluciones mencionadas ofrecen detección de fraude rápida, fluída y "detrás de bambalinas" que reduce esfuerzos y demoras para el cliente.

Utilización de soluciones de mitigación de fraude (regional)

Comparación por grado de foco en minimización de la fricción



* integración de operaciones de ciberseguridad, experiencia digital de cliente y fraude, además de estar altamente enfocada en minimizar la fricción para el cliente

= significativamente o direccionalmente más alto que la misma solución en el **otro** segmento

Preguntas de la encuesta:
P27: ¿Cuáles de las siguientes soluciones contra fraude utiliza su empresa hoy en día?

LexisNexis® RISK SOLUTIONS

El costo del fraude, la fricción para el cliente y sus retos se reducen para las organizaciones que invierten en soluciones multicapa de mitigación de riesgo que se enfocan en la integración con las operaciones de ciberseguridad y experiencia digital de cliente.

A la vez que invierten en soluciones que evalúan atributos de identidad y riesgos de transacciones digitales, las organizaciones también están reduciendo la carga sobre clientes legítimos (dejándolos entrar) y también detectando y bloqueando defraudadores en forma más eficaz. El resultado es que observan muchos menos retos con la autenticación de identidad y el equilibrio entre prevención de fraude y fricción para el cliente a la vez que reducen el costo del fraude.

***Enfoque de solución multicapa como mejor práctica:** Aquellos que siguen un enfoque de soluciones multicapa tienden a utilizar alguna combinación de soluciones pasivas/basadas en identidad digital así como algunas que evalúan atributos físicos de identidad y riesgo transaccional.

DATOS A NIVEL REGIONAL

	Enfoque de solución multicapa como mejor práctica	Aquellos que NO siguen el enfoque de solución multicapa como mejor práctica
Soluciones para **verificar atributos físicos** (p.ej., nombre, fecha de nacimiento, dirección)		
+ Soluciones para **verificar atributos digitales** (p.ej., riesgo de correo electrónico y teléfono, biometría)		Limitadas o ningunas
+ Soluciones para **evaluar riesgo de dispositivo, ubicación** (p.ej., identificador de dispositivo, geolocalización)		Limitadas o ningunas
+ Soluciones para **evaluar comportamiento** (p.ej., biometría comportamental, riesgo de transacción)		Limitadas o ningunas
Además, operaciones antifraude integradas con ciberseguridad/experiencia digital y altamente enfocadas en minimizar la fricción para el cliente		No integradas y enfocadas en minimizar fricción para el cliente
	En línea Móvil	En línea Móvil
% que considera la verificación de identidad como un importante reto en línea/móvil	**39% / 38%**	**70% / 60%**
% que considera el equilibrio entre la prevención de fraude y la fricción como un importante reto en línea/móvil	**25% / 16%**	**49% / 33%**
Nuevos métodos de pago móviles como un importante reto móvil	**20%**	**41%**
Por cada transacción fraudulenta, el costo es. . .	**3,44 veces el valor perdido**	**3,85 veces el valor perdido**

LexisNexis® RISK SOLUTIONS

RECOMENDACIONES

Manténgase atento y preparado para un aumento del fraude en el futuro cercano; unido a esto, enfóquese en minimizar la fricción para el cliente en el competitivo entorno de canal móvil/en línea.

La tecnología es clave. Los negocios necesitan una robusta plataforma de fraude y seguridad que les ayude a adaptarse a un entorno digital cambiante.

Se requiere un enfoque de solución multicapa. La protección en un solo punto dejó de ser suficiente y se convirtió en punto único de falla. Se necesita una fuerte estrategia de defensa multicapa.

Las operaciones de ciberseguridad y experiencia digital de cliente deben estar integradas con procesos de fraude.

Busque alianzas en su industria para compartir perspectivas de fraude e información. Es probable que otras empresas estén combatiendo a los mismos defraudadores.

MANTÉNGASE ATENTO Y PREPARADO PARA UN AUMENTO DEL FRAUDE A LA VEZ QUE MINIMIZA EL ESFUERZO DEL CLIENTE

Aunque hay partes de la sociedad que se están reabriendo tras el inicio de la pandemia, el futuro previsible no es claro respecto a la nueva normalidad. Es razonable asumir que el desplazamiento acelerado hacia transacciones en línea/móviles y pagos causado por la pandemia seguirá siendo preferido después de COVID-19; por lo tanto, las empresas deben continuar con el desarrollo y la mejora de la experiencia digital del cliente a la vez que se protegen contra el fraude.

Los defraudadores desarrollaron nuevas habilidades y aprendizajes, incluso sobre los puntos débiles de comerciantes y entidades financieras en detección de fraude. Los datos relacionados con identidad y cuentas que fueron robados durante intentos de fraude y *phishing* el año pasado serán utilizados con identidades sintéticas y ataques de *bot* en forma más exitosa en los casos en que las empresas sigan evaluando solo los atributos de identidad físicos y no los comportamientos de identidad digital y los riesgos transaccionales

A medida que se mueven más transacciones a los canales en línea y móviles, los consumidores tienen más opciones, entre ellas abandonar una transacción que es onerosa. No toda transacción conlleva el mismo nivel de riesgo; las empresas necesitan inteligencia para saber cuándo aplicar más o menos esfuerzo con los clientes. Los clientes nuevos podrían valorar las medidas adicionales tomadas para verificar su identidad, tales como preguntas tipo reto o claves de acceso de uso único. Los clientes que retornan podrían cansarse de esto en algún momento, basándose en la expectativa de que la empresa debería conocerlos.

Una estrategia exitosa de detección y prevención de fraude implica la integración de operaciones de tecnología, ciberseguridad y experiencia digital, de forma que aborde los singulares riesgos provenientes de diferentes canales transaccionales y métodos de pago, así como de individuos y tipos de transacciones.

LA TECNOLOGÍA ES CLAVE

Para minimizar el fraude, las organizaciones ya no pueden seguir dependiendo de procesos manuales asistidos por tecnologías limitadas para reducir tasas de rechazo, revisiones manuales y costos.

Las empresas necesitan una robusta plataforma tecnológica para fraude y seguridad que les ayude a adaptarse a un entorno digital cambiante, que ofrezca una sólida gestión de fraude y genere una experiencia sin fricción para clientes legítimos.

Desplegar tecnologías que pueden reconocer clientes, ubicar el fraude y desarrollar la base de conocimiento de fraude para optimizar la incorporación, puede prevenir la apropiación de cuentas y detectar amenazas internas.

La utilización de valiosos atributos de datos como los datos de ingreso de usuarios desde múltiples dispositivos, ubicaciones y canales es esencial para identificar riesgos.

El habilitar capacidades forenses, gestión de casos e inteligencia de negocios puede ayudar a mejorar la productividad.

SE REQUIERE UN ENFOQUE DE SOLUCIÓN MULTICAPA

La protección en un solo punto dejó de ser suficiente y se convirtió en punto único de falla.

En la medida que los consumidores hacen transacciones en muchos sitios, dispositivos y geografías, los comportamientos de usuario, tales como patrones de transacciones, sumas pagadas y beneficiarios de pagos, se están volviendo más diversos y menos predecibles.

Se necesita una sólida estrategia de defensa multicapa. Incluye una plataforma de decisiones de autenticación única que incorpore datos de eventos en tiempo real, señales de terceros e inteligencia global entre canales.

También se requiere la capacidad de examinar amenazas de nivel de *malware* así como detección de *bots*, troyanos de acceso remoto y suplantación de IP en canales web y móviles.

A la vez, es clave la capacidad de ofrecer analítica conductual y reducir falsos positivos y fricción para el cliente.

LAS OPERACIONES DE CIBERSEGURIDAD Y EXPERIENCIA DIGITAL DE CLIENTE DEBEN ESTAR INTEGRADAS CON LOS PROCESOS DE FRAUDE

Mejore las decisiones y la experiencia de cliente con aprendizaje automatizado e integración de sistemas/recursos que gestionan el riesgo en todo el negocio y todos los extremos - convergencia de riesgo.

Capacidades analíticas y de datos ampliadas, de herramientas tales como IA/ML, ciberalertas, inteligencia de medios sociales y *crowdsourcing,* permiten a las empresas predecir amenazas en lugar de reaccionar a ellas.

La integración de estas herramientas con soluciones basadas en identidad digital brinda protección a lo largo de la jornada del cliente, no solo en el punto de transacción; la mayoría de defraudadores prefieren la apropiación/creación de cuentas porque les provee una fuente continuada de activos en lugar de una transacción por una sola vez.

La combinación mencionada puede generar eficiencias y ahorro de costos, así como la garantía de una experiencia de cliente optimizada, en particular cuando los riesgos de fraude se pueden segmentar de tal forma que los controles de seguridad se pueden ajustar hacia arriba o hacia abajo según la transacción.

BUSCAR ALIANZAS DENTRO DE LA MISMA INDUSTRIA (CONSORCIOS) PARA COMPARTIR INFORMACIÓN

Es probable que las empresas estén combatiendo al mismo grupo de defraudadores. De hecho, los patrones y riesgos de fraude comparten muchas similitudes en diversos sectores y geografías.

La construcción de una alianza específica a un sector para que haya intercambio de información importante puede mantener a los miembros al día sobre patrones y tácticas de fraude en dicho sector, complementando así la inteligencia que poseen los miembros y permitiéndoles identificar y rastrear individuos y dispositivos riesgosos con mayor precisión. Tal información puede incluir:

- Histórico de dispositivos en lista negra
- Cuentas mula y estrategias de fraude asociadas
- Riesgos específicos relacionados con sector/caso de uso/geografía

LexisNexis® Risk Solutions puede ayudar

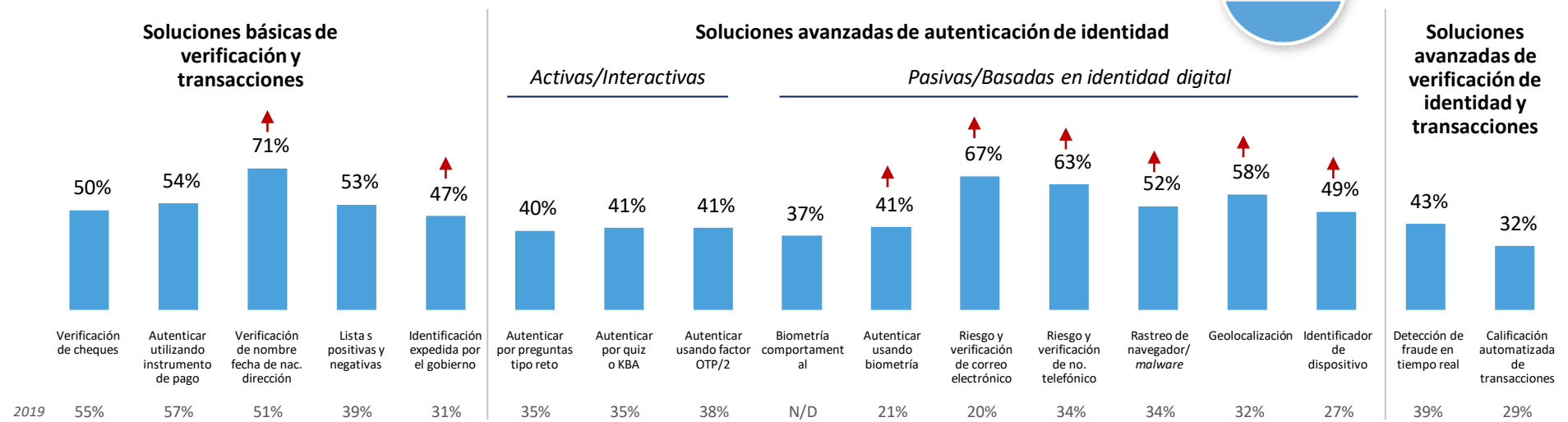
Para más información:
risk.lexisnexis.com/fraude

LexisNexis®
RISK SOLUTIONS

APÉNDICE

La autenticación utilizando atributos digitales (riesgo de correo electrónico y teléfono) y atributos físicos (nombre, dirección, fecha de nac.) son soluciones de mitigación de fraude utilizadas comúnmente por comerciantes y entidades financieras argentinas.

Utilización de soluciones de mitigación de fraude



= significativamente o direccionalmente más alto/más bajo que en 2019

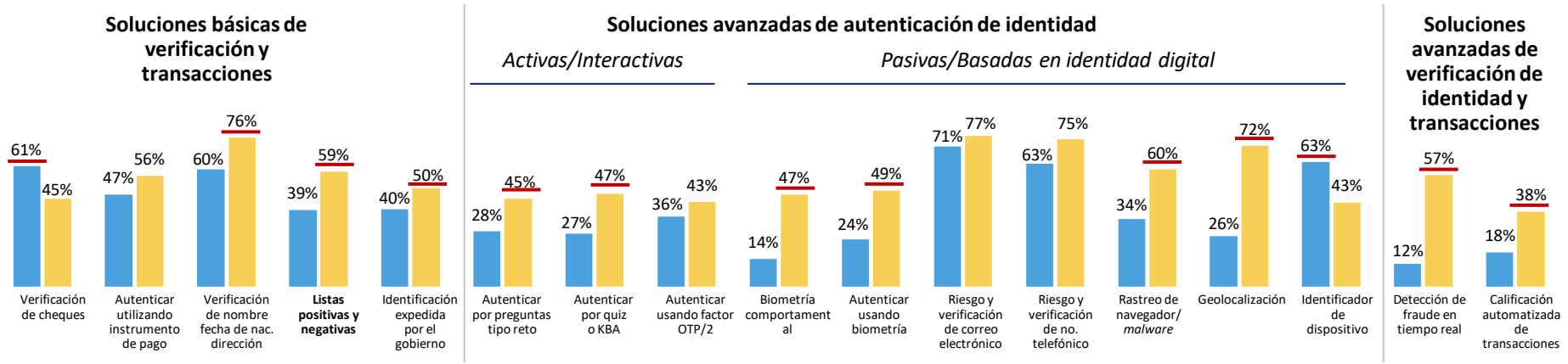
Preguntas de la encuesta:
P27: ¿Cuáles de las siguientes soluciones contra fraude utiliza su empresa hoy en día?

Aunque algunas empresas argentinas han invertido en la verificación de riesgo de correo electrónico/teléfono, aquellas focalizadas en minimizar la fricción para el cliente han invertido en una serie de soluciones más amplias, de las cuales brindarán una evaluación de riesgo más profunda confidencialmente.

Es más probable que también evalúen el riesgo de la transacción, no solo del individuo.

Utilización de soluciones de mitigación de fraude

Comparación por grado de foco en minimización de la fricción

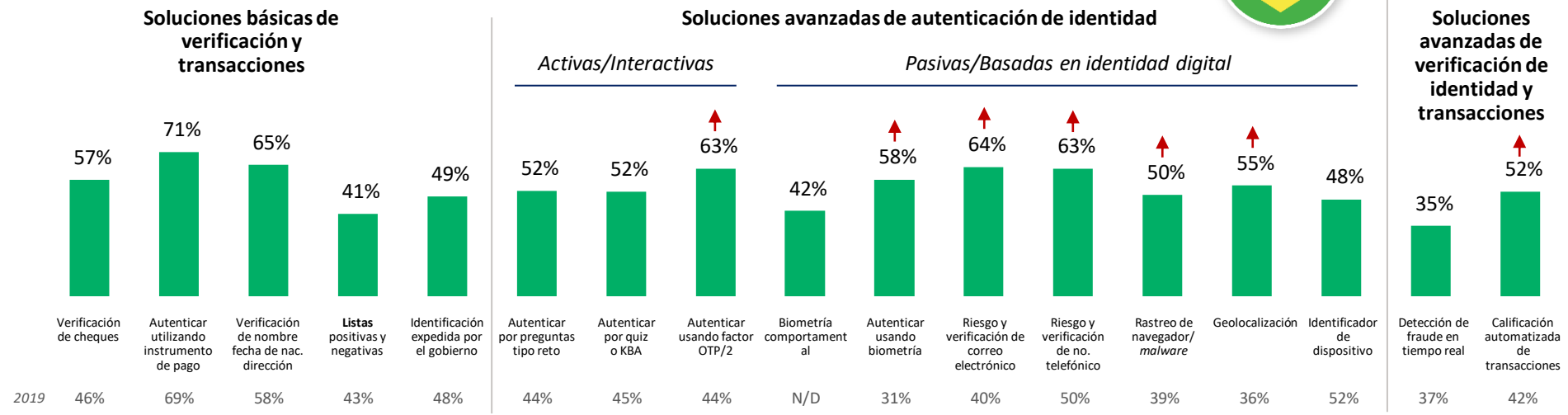


= significativamente o direccionalmente más alto que la misma solución en el **otro** segmento

Preguntas de la encuesta:
P27: ¿Cuáles de las siguientes soluciones contra fraude utiliza su empresa hoy en día en el punto de compra/distribución de fondos?

Varios comerciantes y entidades financieras brasileñas han invertido en soluciones pasivas/basadas en identidad digital desde 2019, así como en calificación avanzada de riesgo de transacción.

Utilización de soluciones de mitigación de fraude



= significativamente o direccionalmente más alto/más bajo que en 2019

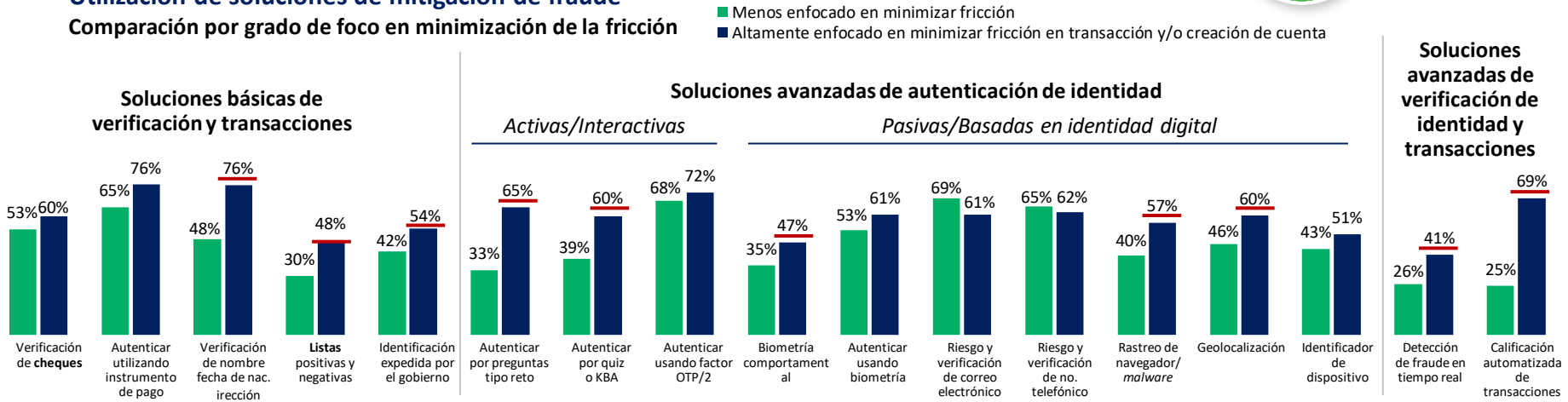
Preguntas de la encuesta:
P27: ¿Cuáles de las siguientes soluciones contra fraude utiliza su empresa hoy en día?

Aunque algunas empresas brasileñas han invertido en la verificación de riesgo de correo electrónico/teléfono, aquellas focalizadas en minimizar la fricción para el cliente han invertido en otras soluciones digitales, entre ellas rastreo de navegador, geolocalización, identificador de dispositivo y biometría.

Es más probable que también evalúen el riesgo de la transacción, no solo del individuo. Las soluciones ofrecen detección de fraude rápida, fluída y "detrás de bambalinas" que reduce esfuerzos y demoras para el cliente. Muchas de estas organizaciones dicen que les ha ido muy bien gestionando la detección de fraude y la fricción.

Utilización de soluciones de mitigación de fraude

Comparación por grado de foco en minimización de la fricción

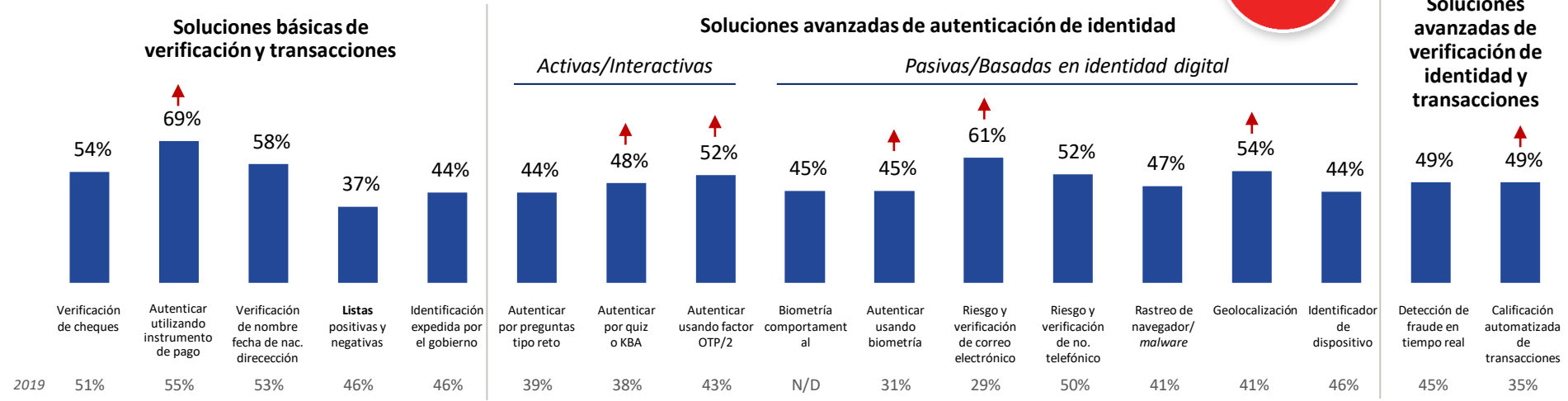


= significativamente o direccionalmente más alto que la misma solución en el **otro** segmento

Preguntas de la encuesta:
P27: ¿Cuáles de las siguientes soluciones contra fraude utiliza su empresa hoy en día en el punto de compra/distribución de fondos?

Han existido inversiones de algunos comerciantes y entidades financieras chilenas en soluciones pasivas/basadas en identidad digital desde 2019, así como en calificación avanzada de riesgo de transacción. La mayor inversión ha sido en verificación de riesgo de correo electrónico.

Utilización de soluciones de mitigación de fraude



= significativamente o direccionalmente más alto/más bajo que en 2019

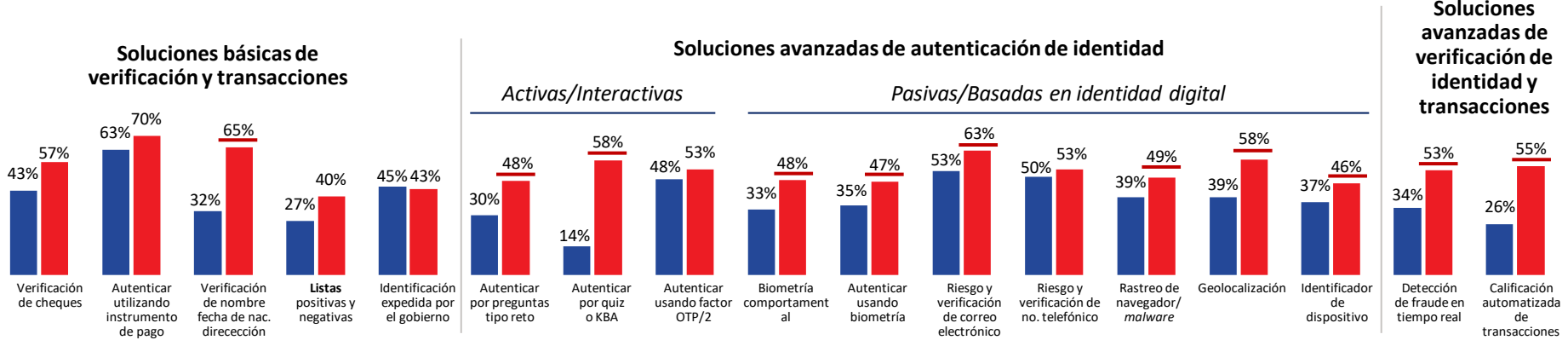
Preguntas de la encuesta:
P27: ¿Cuáles de las siguientes soluciones contra fraude utiliza su empresa hoy en día?

Este aumento de inversiones ha sido más que todo de comerciantes y entidades financieras chilenas que están focalizadas en minimizar la fricción para el cliente mediante soluciones digitales que evalúan los comportamientos, el dispositivo, la transacción y el individuo.

Las soluciones ofrecen detección de fraude rápida, fluída y "detrás de bambalinas" que reduce esfuerzos y demoras para el cliente. Muchas de estas organizaciones dicen que les ha ido muy bien gestionando la detección de fraude y la fricción.

Utilización de soluciones de mitigación de fraude

Comparación por grado de foco en minimización de la fricción

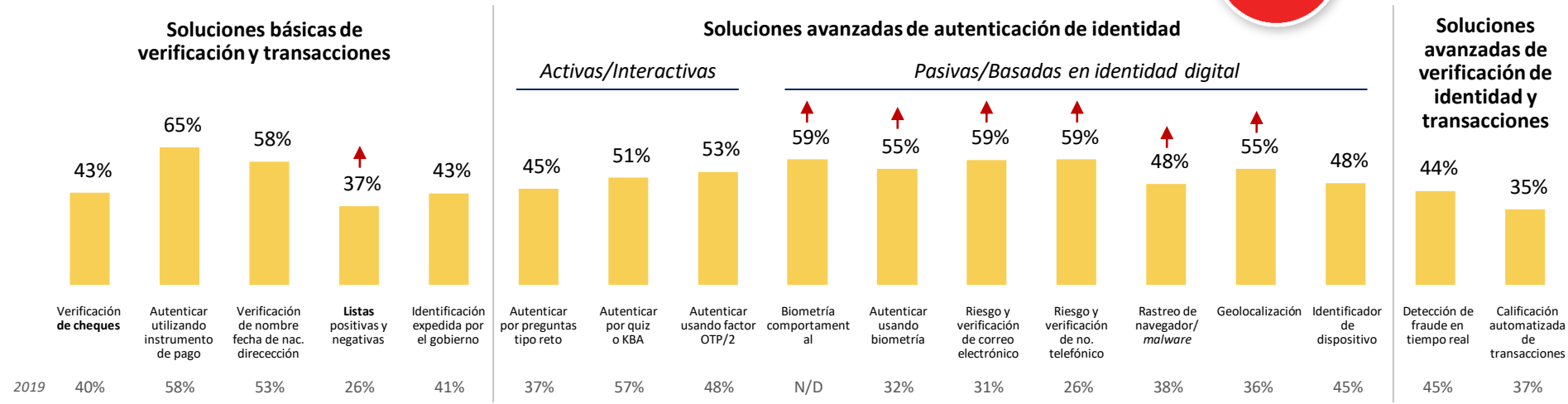


= significativamente o direccionalmente más alto que la misma solución en el **otro** segmento

Preguntas de la encuesta:
P27: ¿Cuáles de las siguientes soluciones contra fraude utiliza su empresa hoy en día en el punto de compra/distribución de fondos?

También ha habido inversiones de algunos comerciantes y entidades financieras colombianas en soluciones pasivas/basadas en identidad digital desde 2019, especialmente en biometría, verificación de riesgo de correo electrónico/teléfono, rastreo de *malware* y geolocalización.

Utilización de soluciones de mitigación de fraude



↑ = significativamente o direccionalmente más alto/más bajo que en 2019

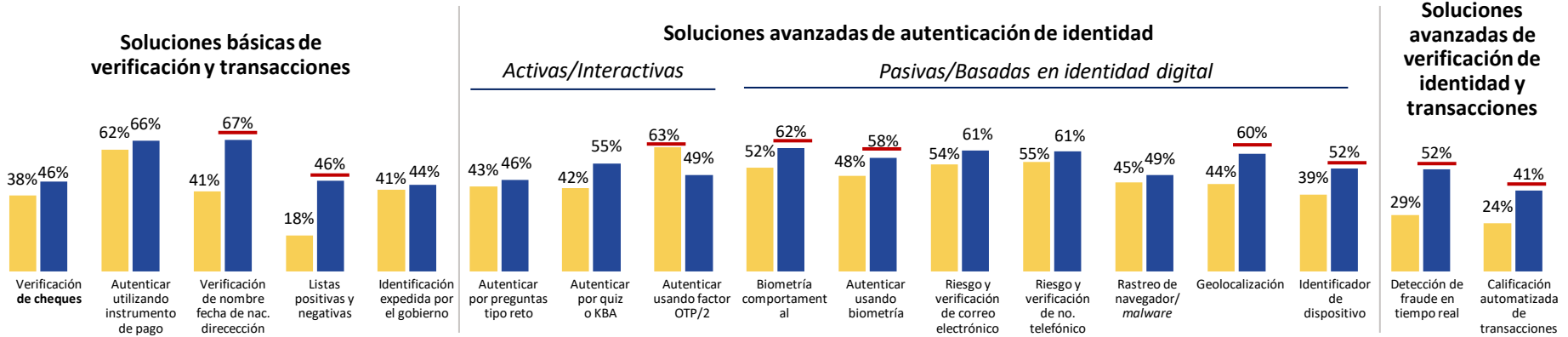
Preguntas de la encuesta:
P27: ¿Cuáles de las siguientes soluciones contra fraude utiliza su empresa hoy en día?

Este aumento de inversiones ha sido en su mayoría de comerciantes y entidades financieras colombianas que están focalizadas en minimizar la fricción para el cliente mediante soluciones digitales que evalúan los comportamientos, el dispositivo, la transacción y el individuo.

Las soluciones ofrecen detección de fraude rápida, fluída y "detrás de bambalinas" que reduce esfuerzos y demoras para el cliente. Muchas de estas organizaciones dicen que les ha ido muy bien gestionando la detección de fraude y la fricción.

Utilización de soluciones de mitigación de fraude

Comparación por grado de foco en minimización de la fricción



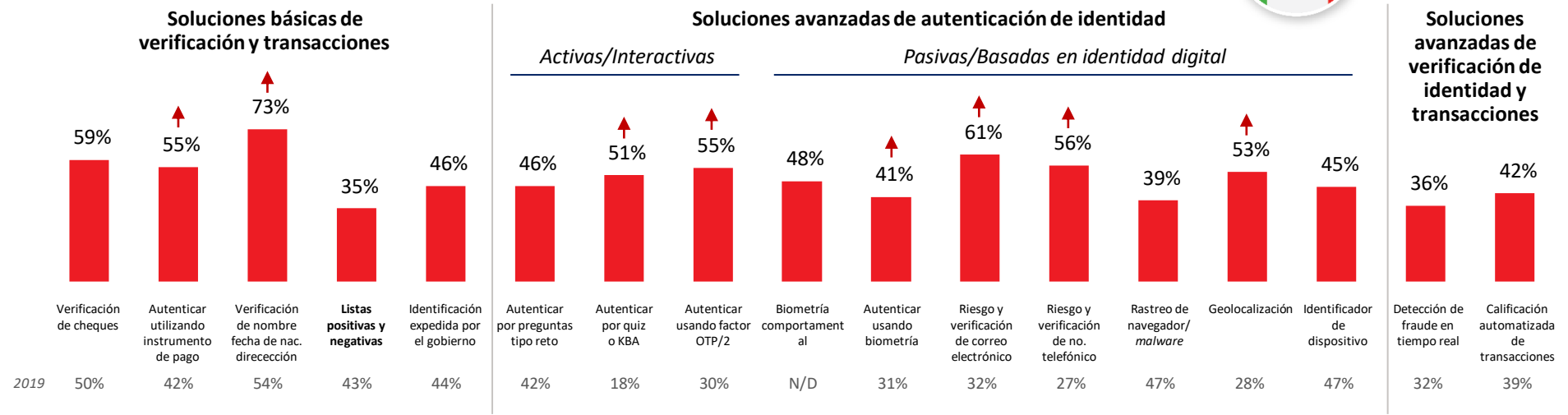
= significativamente o direccionalmente más alto que la misma solución en el **otro** segmento

Preguntas de la encuesta:
P27: ¿Cuáles de las siguientes soluciones contra fraude utiliza su empresa hoy en día en el punto de compra/distribución de fondos?

Al igual que en otros mercados de LATAM, ha habido inversión en varias soluciones, entre ellas las pasivas/basadas en identidad digital, especialmente biometría, verificación de riesgo de correo electrónico/teléfono y geolocalización.

Varias empresas mexicanas también han invertido en soluciones de autenticación de Quiz y/o factor OTP/2.

Utilización de soluciones de mitigación de fraude



= significativamente o direccionalmente más alto/más bajo que en 2019

Preguntas de la encuesta:
P27: ¿Cuáles de las siguientes soluciones contra fraude utiliza su empresa hoy en día?

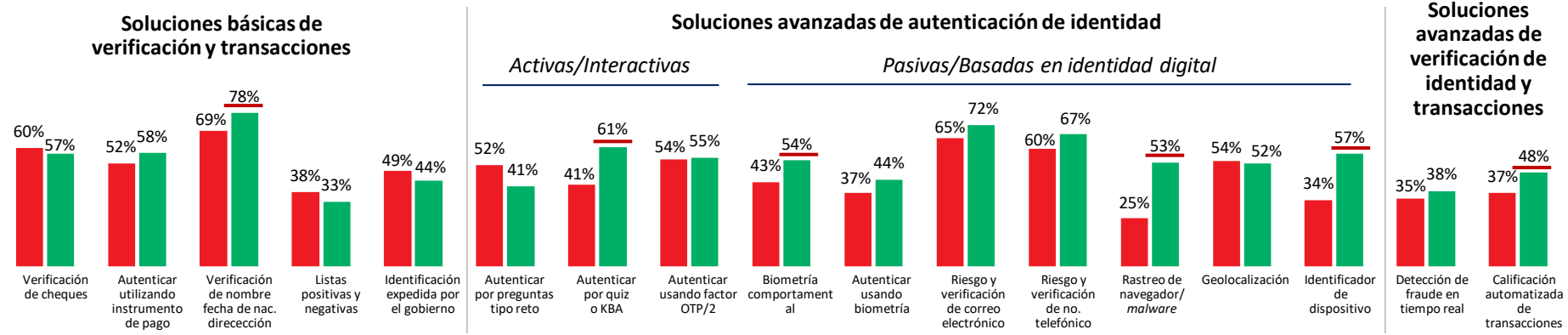
En muchos casos, este aumento de inversiones ha sido de comerciantes y entidades financieras mexicanas que están focalizadas en minimizar la fricción para el cliente

Las soluciones ofrecen detección de fraude rápida, fluída y "detrás de bambalinas" que reduce esfuerzos y demoras para el cliente. Muchas de estas organizaciones dicen que les ha ido muy bien gestionando la detección de fraude y la fricción.

Utilización de soluciones de mitigación de fraude

Comparación por grado de foco en minimización de la fricción

- Menos enfocado en minimizar fricción
- Altamente enfocado en minimizar fricción en transacción y/o creación de cuenta

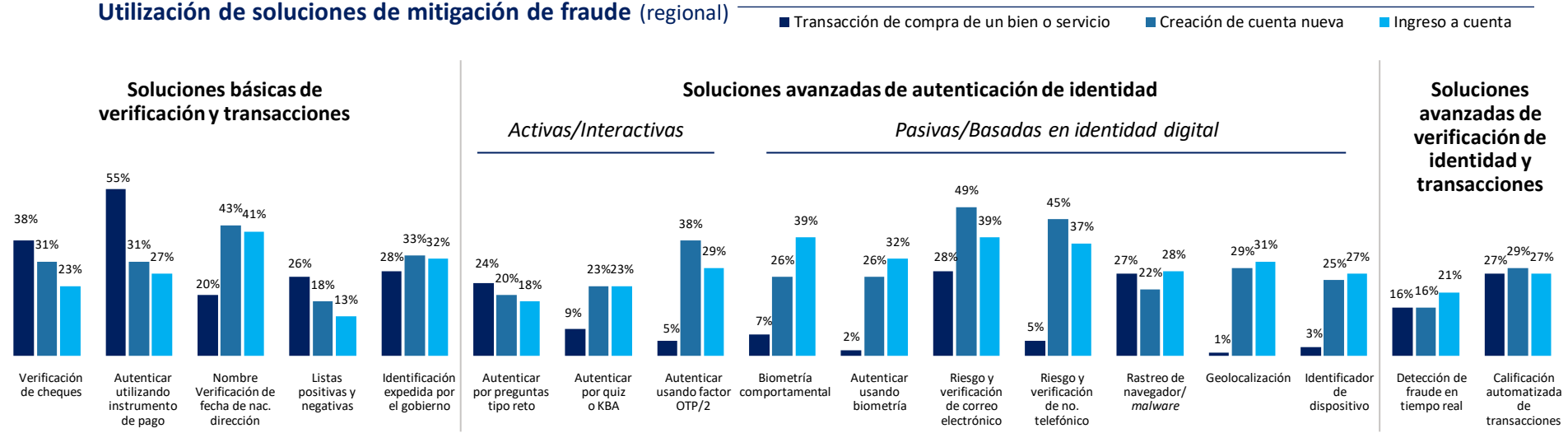


= significativamente o direccionalmente más alto que la misma solución en el **otro** segmento

Preguntas de la encuesta:
P27: ¿Cuáles de las siguientes soluciones contra fraude utiliza su empresa hoy en día en el punto de compra/distribución defondos?

Comercio minorista

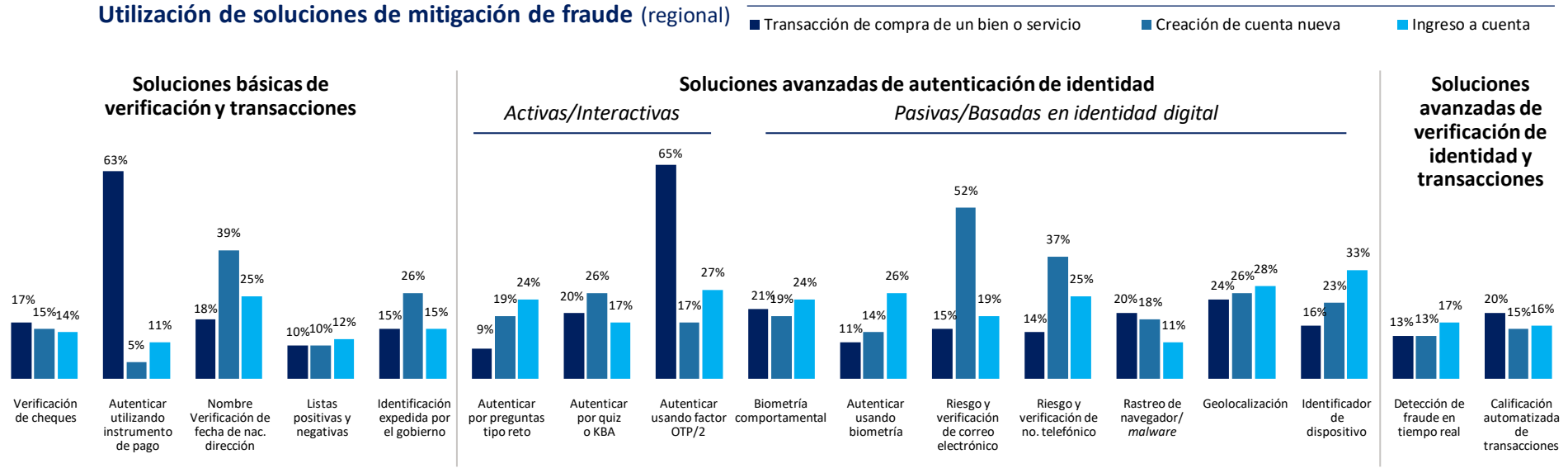
Utilización de soluciones de mitigación de fraude (regional)



Preguntas de la encuesta:
P27: ¿Cuáles de las siguientes soluciones contra fraude utiliza su empresa hoy en día?

Comercio electrónico

Utilización de soluciones de mitigación de fraude (regional)

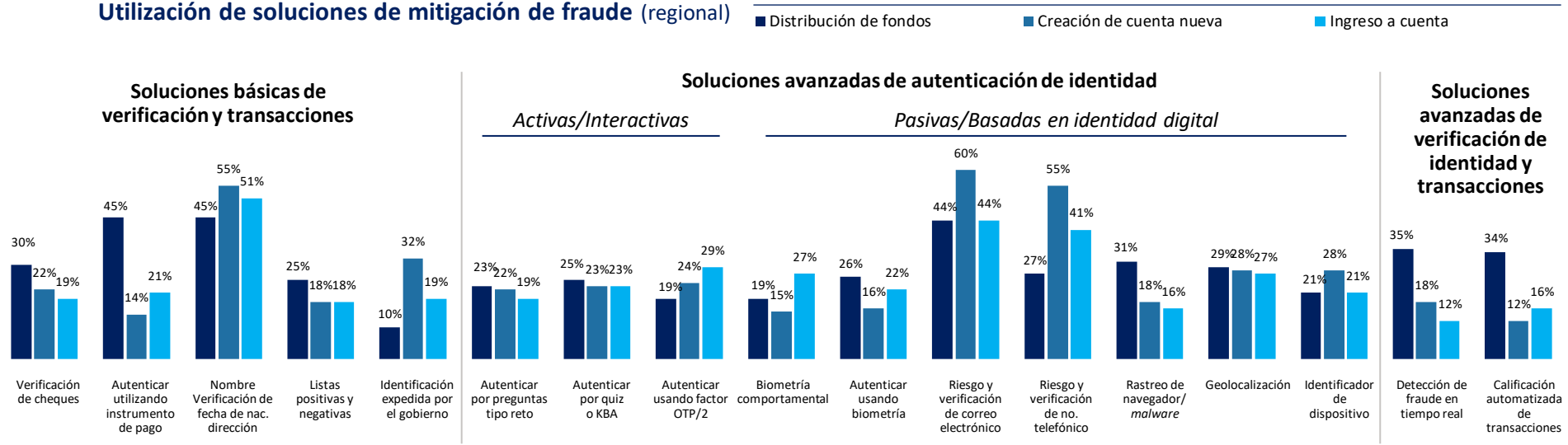


Preguntas de la encuesta:
P27: ¿Cuáles de las siguientes soluciones contra fraude utiliza su empresa hoy en día?

UTILIZACIÓN DE SOLUCIONES DE FRAUDE DURANTE LA JORNADA DIGITAL DEL CLIENTE/SERVICIOS FINANCIEROS

Servicios financieros

Utilización de soluciones de mitigación de fraude (regional)



Preguntas de la encuesta:
P27: ¿Cuáles de las siguientes soluciones contra fraude utiliza su empresa hoy en día?

Todas las referencias a divisas en este informe se basan en dólares americanos. Para el propósito de este estudio, México se incluye con América Latina. Este documento es sólo para fines educativos y no garantiza la funcionalidad o las características de los productos LexisNexis identificados, si los hubiera. LexisNexis no garantiza que este documento esté completo o libre de errores. LexisNexis y el logo de Knowledge Burst son marcas registradas de RELX Inc. Otros productos y servicios pueden ser marcas registradas de sus respectivas compañías.

NXR15094-00-0921-ES-LA