O REAL CUSTO DAS FRAUDES AMÉRICA LATINA

Relatório Regional - 2021

LexisNexis®
RISK SOLUTIONS

HISTÓRICO E METODOLOGIA

A pesquisa True Cost of Fraud™ (O real custo das fraudes) da LexisNexis® Risk Solutions ajuda empresas a expandir os seus negócios de maneira segura, enfrentando o crescente risco de fraudes.

A pesquisa oferece uma síntese das/os:

- Tendências atuais de fraudes nos mercados de varejo, comércio eletrônico, serviços financeiros e de crédito na LATAM.
- Principais pontos críticos relacionados à inclusão de novos mecanismos de pagamento, realizando operações em canais online e móveis, e à expansão internacional.

Impactos da Covid-19:

- Os dados foram coletados entre fevereiro e abril de 2021. Como muitas das perguntas faziam referência aos últimos 12 meses, os achados refletem atividades, riscos de fraudes, desafios e custos que foram impactados pelos temores, mudanças no comportamento e lockdowns forçados causados pela Covid-19.

Definições de fraude:

- Operações fraudulentas decorrentes de fraudes de identidade, que é o uso indevido de formas de pagamento (como cartão de crédito) ou informações pessoais roubadas.
- Solicitações fraudulentas de reembolsos/estornos, cheques devolvidos.
- Mercadorias perdidas ou roubadas, assim como os custos de redistribuição associados ao reenvio de itens comprados.
- Inscrições fraudulentas (ex.: envio proposital de informações incorretas sobre si mesmo, como renda, emprego, etc.).
- Invasão a contas por pessoas não autorizadas.
- Uso de contas para lavagem de dinheiro.

Essa pesquisa cobre métodos de fraudes voltadas ao consumidor:

- **Não** engloba fraudes com uso de informações privilegiadas e nem realizadas por funcionários.

O custo do LexisNexis Fraud Multiplier℠:

- Estima o prejuízo total que uma empresa sofre com base no valor real em dólar de uma operação fraudulenta.

LexisNexis® RISK SOLUTIONS

HISTÓRICO E METODOLOGIA (CONT.)

A pesquisa inclui entrevistas abrangentes com 454 executivos de risco e fraudes em empresas de varejo, comércio eletrônico, serviços financeiros e de crédito na região da LATAM.

	Argentina	Brasil	Chile	Colômbia	México	Geral
Varejo	30	30	30	33	30	153
Comércio Eletrônico	30	31	30	30	30	151
Serviços Financeiros	30	30	30	30	30	150
TOTAL	90	91	90	93	90	454

Entre os setores entrevistados estão:

Varejo

Pode ser omnichannel ou não, fatura menos de 80% da receita nos canais online.

Comércio eletrônico

Fatura 80% ou mais da receita nos canais online.

Serviços financeiros

Gestão de ativos
Bancos / Hipotecas
Crédito ao consumidor
Planejamento financeiro

Em diversas categorias, inclusive:
Vestuário/roupas, autopeças, livros/música, computadores/softwares, produtos digitais, remédios/saúde e beleza, flores/presentes/joias, alimentos e bebidas, mercadorias gerais, hardware/materiais de construção, hotelaria/viagem, aparelhos/mobiliário doméstico, material para escritório, produtos esportivos, brinquedos/hobbies.

LexisNexis® RISK SOLUTIONS

**No relatório, a frase "setores entrevistados" significa varejo, comércio eletrônico e serviços financeiros.*

RESUMOS DAS PRINCIPAIS DESCOBERTAS

01 **O custo das fraudes apresentou forte alta para os setores entrevistados na LATAM. Em média, cada operação fraudulenta custou 3,68 vezes o valor da operação perdida, em comparação a 3,64 em 2019.** Isso foi impulsionado pelas instituições financeiras e pelo comércio eletrônico, por conta da migração das operações para canais mais digitais/remotos durante a Covid-19.

02 **Houve um volume maior de atividades realizadas em canais móveis/online, o que aumentou os riscos e os custos de fraudes.** Mais operações remotas foram sendo realizadas à medida que a pandemia de Covid-19 causava o fechamento de oportunidades presenciais. Os riscos dos canais móveis foram dominantes nos aplicativos e pagamentos com carteiras móveis, já que formas de pagamento sem contato começaram a ser usadas com mais frequência pelos clientes. Fraudes de identidades foram uma fonte de preocupação, especialmente para as instituições financeiras.

03 **Fraudes relacionadas a identidades representaram ameaça e desafio significantes para as empresas de varejo/comércio eletrônico e as instituições financeiras na LATAM.** Isso se deu, principalmente, em canais remotos de operações envolvendo novas formas de pagamento e desafios de avaliação dos atributos digitais do dispositivo e do risco da operação. Além disso, houve preocupações sobre como equilibrar os esforços de detecção e prevenção de fraudes ao atrito com os clientes, pois o abandono foi comum quando o esforço destes aumentava.

04 **Os comerciantes e as empresas de serviços financeiros na LATAM podem reduzir custos e riscos de fraudes com a melhor prática de integração de segurança cibernética, experiência digital do cliente e operações de fraudes através de uma abordagem de solução em multicamadas.** Muitas empresas não otimizam os seus esforços de prevenção a fraudes através dessa melhor prática. As que o fazem, enfrentam menos desafios relacionados a verificação de identidade, lidando com novas formas de pagamento móveis e equilibrando a prevenção a fraudes ao atrito com o cliente. Elas também sofrem menores custos de fraudes em comparação às outras.

LexisNexis® RISK SOLUTIONS

DESCOBERTA PRINCIPAL 01

O custo das fraudes apresentou forte alta para os setores entrevistados na LATAM. Em média, cada operação fraudulenta custou 3,68 vezes o valor da operação perdida, em comparação a 3,64 em 2019.

O custo das fraudes foi 4,78 vezes o valor da operação perdida para as instituições de serviços financeiros e 3,40 para o comércio eletrônico, em comparação a 2,97 para o varejo.

As empresas financeiras da LATAM sofreram ataques de fraudes digitais, tendo a conta bancária das pessoas como alvo. Muitas organizações do comércio eletrônico não estavam preparadas para o aumento no volume das operações digitais no que diz respeito a se armarem com soluções de proteção contra fraudes. E a mudança para mais formas de pagamento digitais e operações móveis tem aumentado os riscos de fraudes.

O custo das fraudes apresentou forte crescimento para os comerciantes e as instituições financeiras da LATAM.

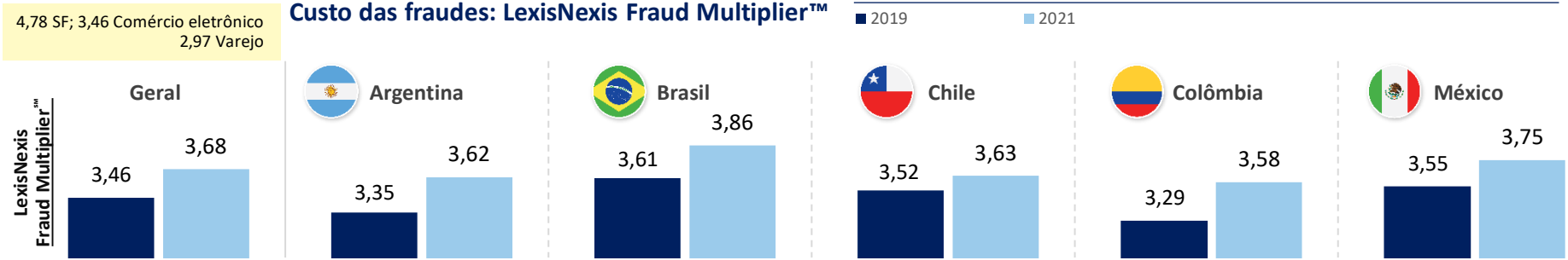
Para cada operação fraudulenta, o custo para as empresas na LATAM foi, na verdade, 3,68 vezes o valor da operação perdida, aumento considerável dos 3,46 em 2019. Tanto o setor de serviços financeiros como o de comércio eletrônico sofreram elevações acentuadas nos custos de fraudes devido ao impulso para o ambiente online.

Vários fatores influenciaram isso, inclusive maior atenção dada pelas empresas financeiras a invasão a contas e clonagem de cartão[1], consumidores usando formas de pagamento digitais e com contato com mais frequência, o que se traduziu em perdas maiores por fraudes e aumento das operações em canais móveis, criando problemas de fraudes de identidade e relacionados à conta.

Além disso, os achados indicam que diversas empresas de comércio eletrônico não estavam preparadas para a investida digital por conta da Covid-19, com uso limitado de soluções que avaliam identidades digitais e riscos de operações que podem desmascarar identidades sintéticas e proteger contra crimes cibernéticos.

4,78 SF; 3,46 Comércio eletrônico
2,97 Varejo

Custo das fraudes: LexisNexis Fraud Multiplier™



* ATENÇÃO: pequeno número de casos, os dados devem ser somente usados direccionalmente

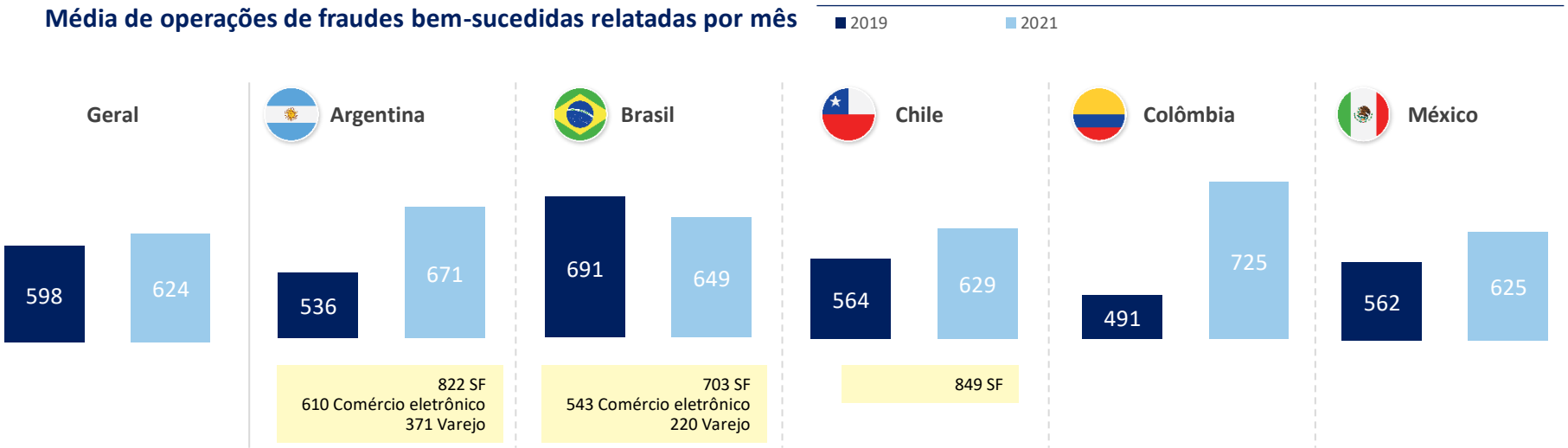
[1] https://www.globenewswire.com/fr/news-release/2021/05/03/2221375/0/en/Latin-America-Fraud-Detection-and-Prevention-Market-to-Reach-USD-2-945-3-Million-by-2028-Increasing-Incidence-of-Data-Fraud-to-Stimulate-Growth-Fortune-Business-Insights.html

Perguntas da pesquisa:
P16a: Pensando no prejuízo total por fraudes sofrido pela sua empresa, mostre a distribuição de vários custos diretos de fraude nos últimos 12 meses.
P10: Qual o valor aproximado do total do prejuízo por fraudes da sua empresa nos últimos 12 meses, como % da receita total?

LexisNexis® RISK SOLUTIONS

A média mensal de ataque de fraudes bem sucedidos aumentou, especialmente na Argentina e na Colômbia. O comércio eletrônico e os serviços financeiros impulsionaram, em grande parte, esse aumento, à medida que as lojas fechavam.

Média de operações de fraudes bem-sucedidas relatadas por mês



P22/24: Em um mês normal, quantas operações fraudulentas, aproximadamente, são impedidas/concluídas com sucesso pela sua empresa?

DESCOBERTA PRINCIPAL 02

Houve um volume maior de atividades em canais móveis/online, o que aumentou os riscos e os custos de fraudes.

Não é de surpreender que tenha havido uma migração em direção a operações online/em navegadores de internet e canais móveis desde o começo da pandemia de Covid-19.

O comércio móvel cresceu na LATAM nesse período, acelerado pela Covid-19, assim como o volume de operações com carteira digital/móvel e formas de pagamento por aproximação.

As operações móveis contribuíram para o aumento das fraudes, com o comércio eletrônico sendo especialmente afetado por isso.

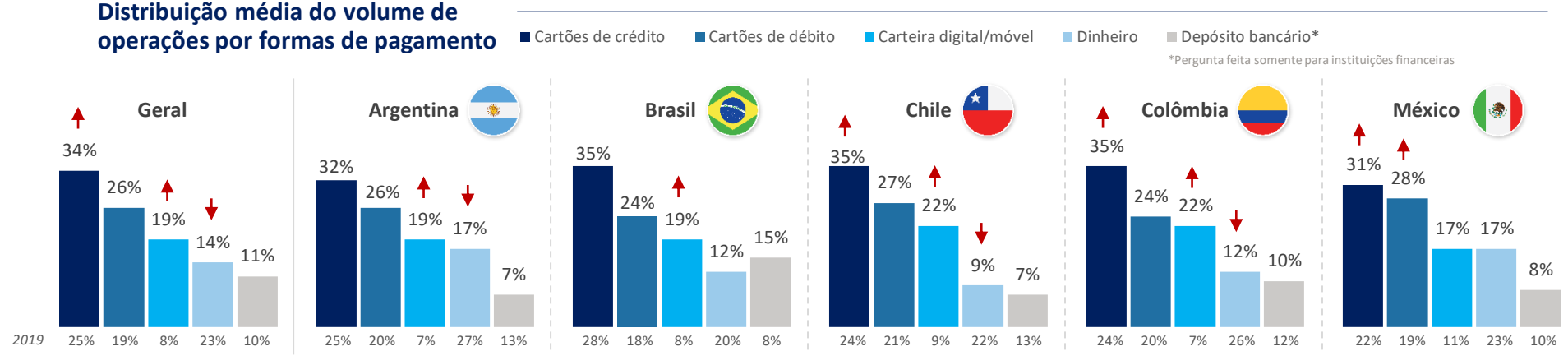
- A taxa de custos de fraudes atribuída aos canais móveis subiu em alguns mercados (Argentina, Colômbia e México) e foi alta para empresas de comércio eletrônico, em particular no Brasil, no Chile e na Colômbia.
- O uso mais frequente de carteiras digitais/móveis e de pagamento sem contato se alinhou com o crescimento da parcela de custos de fraudes atribuída a essas formas de pagamento.

Não é de surpreender que fraudes relacionadas à identidade e à conta sejam particularmente problemáticas para as instituições financeiras e as organizações que fornecem comércio móvel.

Com o impacto geral da Covid-19 nos últimos 12 meses, mais operações foram realizadas com formas de pagamento digital em vez de dinheiro.

As operações com cartão de crédito foram o método mais utilizado, embora o volume de carteiras móveis/digitais tenha aumentado significativamente na maioria dos mercados, ficando bastante próximo dos cartões de débito. Ao mesmo tempo, as operações em dinheiro caíram, apesar de continuarem sendo a principal forma de pagamento em áreas com menos infraestrutura bancária. O crescimento do volume de cartão de crédito provavelmente envolve cartões locais para operações locais, por meio de redes locais de pagamento. Poucos têm acesso a cartões emitidos por provedores globais para realizar operações internacionais. Esse pode ser um dos motivos para o aumento do uso de carteiras móveis, uma vez que a penetração de smartphones é alta e os grandes varejistas aceitam essa forma de pagamento. As operações de carteira móvel através de serviços como Apple Pay, AliPay, Google Pay e Samsung Pay podem ser usadas principalmente para operações internacionais[2], além de serem também uma maneira de promover a inclusão financeira, em função da grande quantidade da população não bancarizada.[3]

Distribuição média do volume de operações por formas de pagamento



[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

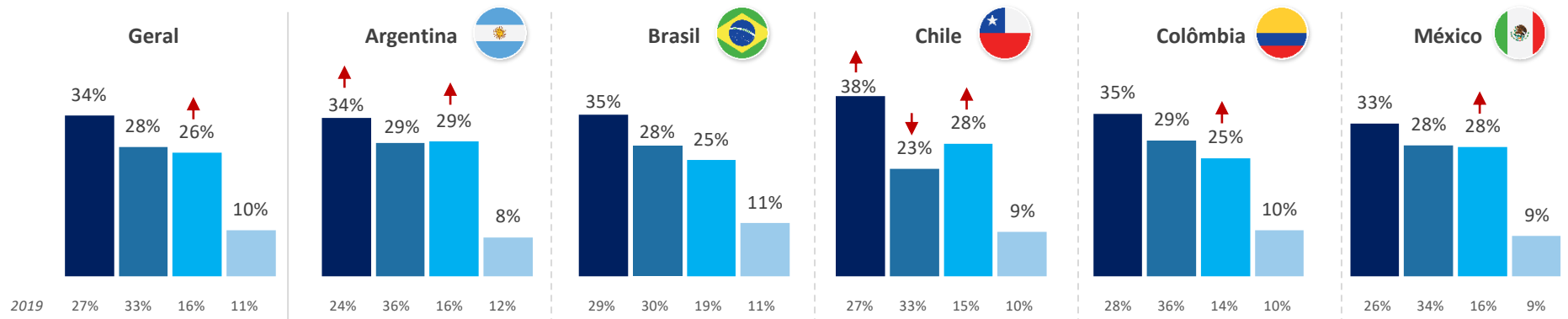
Perguntas da pesquisa:
P3: Indique a taxa de operações concluídas (nos últimos 12 meses) para cada um das formas de pagamento a seguir aceitas pela sua empresa.

= bastante ou direccionalmente mais baixo/alto do que em 2019

Não é de se surpreender que uma maioria significativa das operações tenham ocorrido através de canais remotos durante a pandemia, com o volume dos canais móveis aumentando na maioria dos mercados da LATAM.

Embora a distribuição média de operações realizadas em canais móveis tenha sido significativamente maior em comparação a 2019 na maioria dos mercados, o volume médio relatado de operações presenciais caiu somente moderada/direccionalmente. Mesmo com os consumidores da LATAM realizando mais compras em canais remotos, ainda há uma preferência em adquirir certos itens pessoalmente.[4] O aumento do uso de pagamento sem contato tem fornecido algum apoio àqueles que desejam evitar o manuseio de dinheiro durante uma compra em loja. [5]

Distribuição média do volume de operações por todos os canais



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

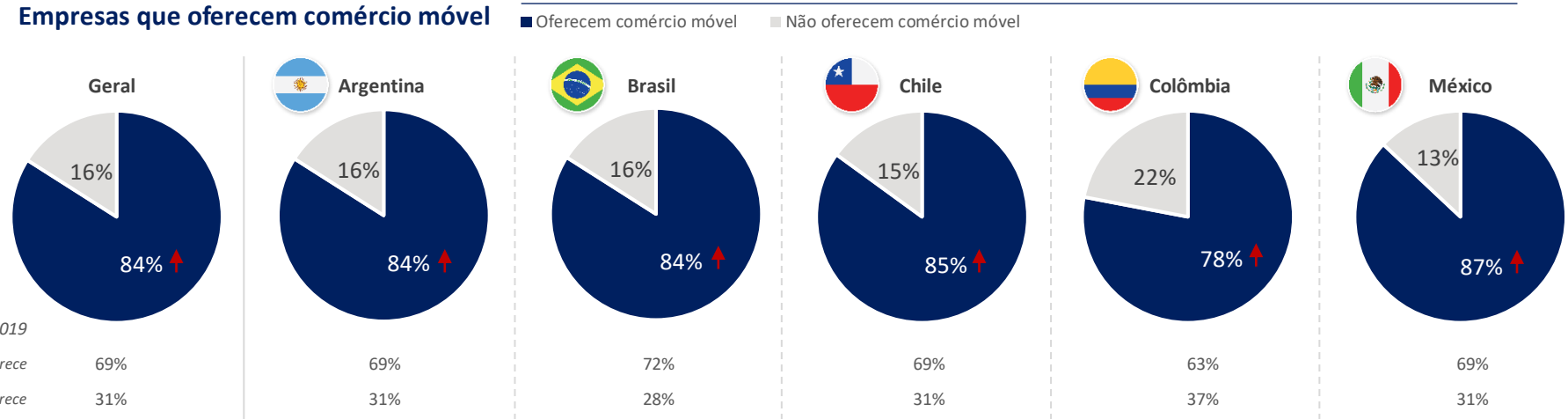
Perguntas da pesquisa:
P2: Indique a taxa de operações concluídas (nos últimos 12 meses) para cada um dos seguintes canais aceitos atualmente pela sua empresa.

↑↓ = bastante ou direccionalmente mais baixo/alto do que em 2019

A LATAM é um dos mercados móveis de crescimento mais rápido, onde os dispositivos móveis são para muitos a principal forma de conexão à Internet. Desde 2019, tem havido um crescimento significativo no número de comerciantes e instituições financeiras que oferecem comércio móvel.

Considerando que a LATAM apresentou crescimento nas operações móveis antes da Covid-19[6], a maior adoção por parte das empresas parece não ser uma resposta rápida à pandemia, pois leva-se tempo para implementar e otimizar um processo de canal móvel. No entanto, a Covid-19 provavelmente acelerou os planos que já estavam em andamento.

Empresas que oferecem comércio móvel



	Geral	Argentina	Brasil	Chile	Colômbia	México
2019						
Oferece	69%	69%	72%	69%	63%	69%
Não oferece	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-itFNlqB4ulliK

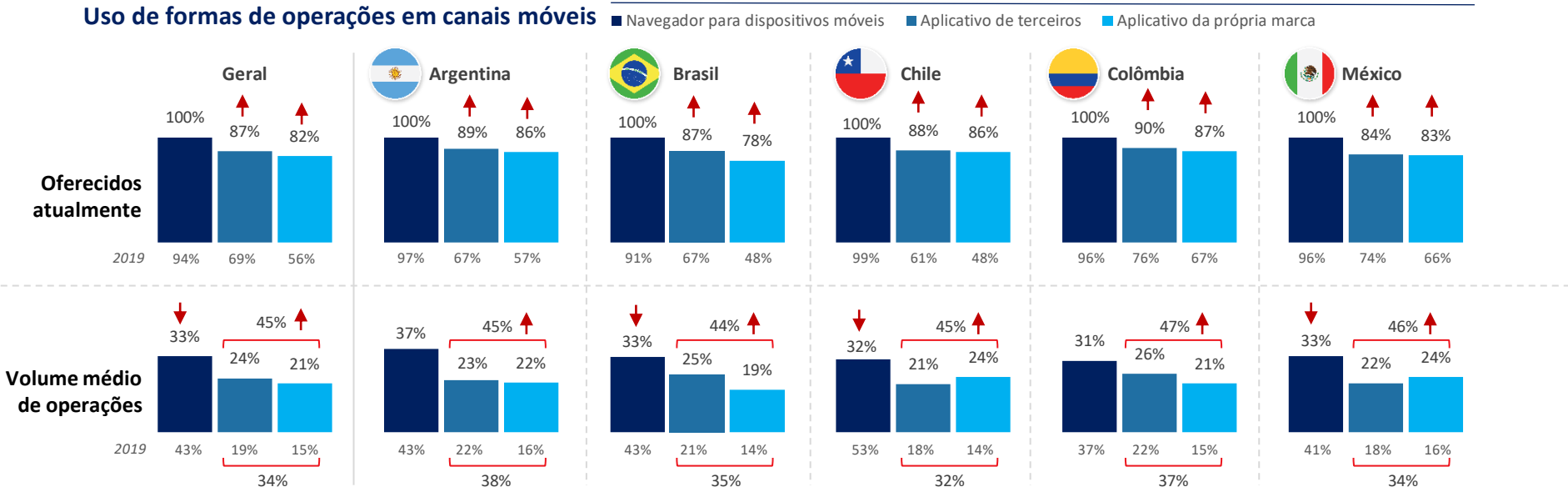
Perguntas da pesquisa:
P4: Indique a taxa de operações concluídas (nos últimos 12 meses) para cada um dos canais de pagamento atualmente aceitos pela sua empresa.

↑↓ = bastante ou direccionalmente mais baixo/alto do que em 2019

Houve um aumento significativo no número de comerciantes e instituições financeiras na LATAM que oferecem operações em aplicativos móveis, o que resultou em volume maior.

O uso de aplicativos para dispositivos móveis cresceu rapidamente no México e no Brasil no começo da pandemia de Covid-19, embora os dados abaixo mostrem que os outros mercados os alcançaram rapidamente.[7]

Uso de formas de operações em canais móveis



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

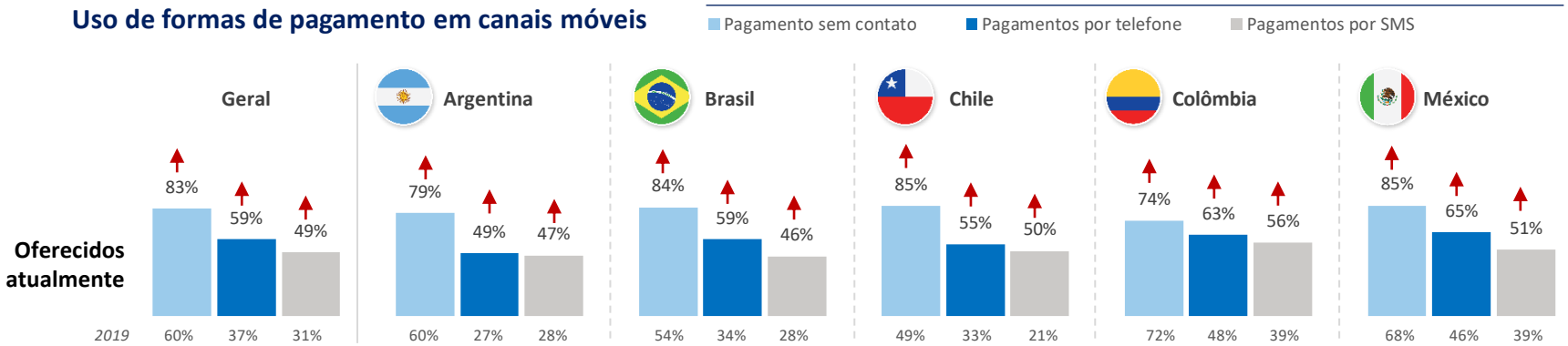
Perguntas da pesquisa:
P4: Indique a taxa de operações concluídas (nos últimos 12 meses) para cada um dos canais de pagamento atualmente aceitos pela sua empresa.

↑↓ = bastante ou direccionalmente mais baixo/alto do que em 2019

Em comparação a 2019, uma parcela significativamente maior de empresas na LATAM oferecem pagamento sem contato, com o medo de transmissão da Covid-19 alimentando as preocupações sobre manuseio de dinheiro em compras presenciais.

Como mostrado anteriormente, a média do volume de operações através de canais presenciais permanece o mesmo do período anterior à Covid-19. Pelo menos alguns consumidores da LATAM têm usado o pagamento sem contato como uma forma de continuar realizando operações presenciais, mas evitando as formas de pagamento comumente usadas.

Uso de formas de pagamento em canais móveis



= bastante ou direccionalmente mais baixo/alto do que em 2019

Perguntas da pesquisa:
P4: Indique a taxa de operações concluídas (nos últimos 12 meses) para cada um dos canais de pagamento atualmente aceitos pela sua empresa.

As fraudes estão se tornando mais sofisticadas e complexas.

Os pontos de verificação tradicional, que usam atributos físicos (endereço físico, data de nascimento, número do seguro social, etc.), são menos eficazes na detecção e na prevenção desses tipos de fraudes organizadas. Isso é um grande desafio, especialmente para as operações realizadas online ou por comércio móvel.

Os métodos sofisticados mostrados abaixo não afetam apenas a avaliação de risco de identidade, mas também do risco das operações. Um desses impactos é a capacidade limitada de determinar a origem/localização da operação.

Redes de fraudes globalmente organizadas e conectadas que compartilham informações de identidade roubadas e colaboram com vários ataques de fraudes. *Exemplos de casos de uso: ataques de bot realizados além de fronteiras, aproveitamento de desafios apresentados por provedores/gateways de pagamento terceiros, uso de vários dispositivos para confundir o rastro da fraude.*

Identidades criadas contendo informações pessoais reais e/ou falsas, combinação real + falsa faz com que a identidade pareça legítima e mais difícil de ser detectada com os métodos de verificação tradicionais baseados em atributos físicos. *Exemplo de casos de uso: trabalha para estabelecer uma boa posição de crédito, alcança capacidade de passar nos pontos tradicionais de verificação e, em seguida, começa a cometer fraudes com itens de valor mais alto.*

Dispositivo fraudulento vinculado a vários outros por meio de um endereço de compra exclusivo. *Exemplo de caso de uso: compra pelo celular e retirada na loja.*

Vários dispositivos associados a vários endereços de e-mail e localizações. *Exemplo de casos de uso: criação de novas contas fraudulentas, invasão a conta e programas de fidelidade usando endereços de IP de proxy.*

Ataques de redes de bots móveis. *Exemplo de casos de uso: malware infecta dispositivo sem o conhecimento do consumidor, rouba identidade, invade contas, faz compras fraudulentas.*

Uso de identidades e credenciais roubadas. *Exemplo de casos de uso: testes das informações do cartão de crédito roubado com bens/serviços de valor baixo (**típicos de bens/serviços digitais**) tendem a despertar menos suspeitas; testes contínuos de credenciais de identidade para encontrar as que passam pelas verificações de identidade dos varejistas.*

LexisNexis® RISK SOLUTIONS

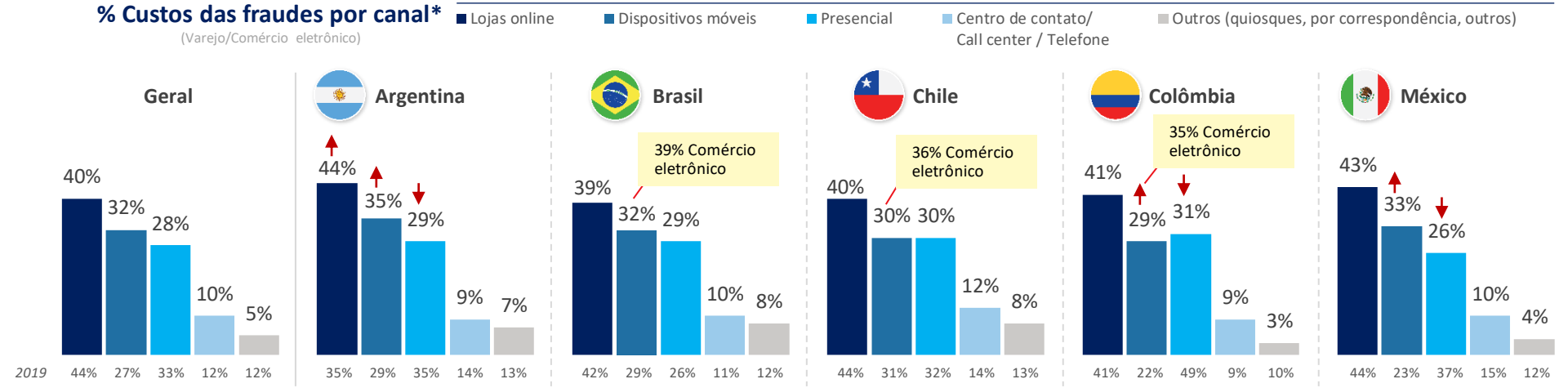
Os canais online apresentaram a maior taxa de custos de fraudes para varejistas/comércio eletrônico, embora estes últimos também percebam um grau considerável de fraudes no canais móveis.

As organizações de comércio eletrônico foram menos propensas a usar certas soluções que aprimoram a detecção de fraudes em operações móveis, como ID de dispositivo, localização geográfica, autenticação através de biometria e classificação de operação em tempo real. Como será mostrado adiante, elas sofreram mais fraudes de carteiras móveis que são varejistas.

É bem interessante que o canal presencial também tenha continuado gerando grande volume de fraudes, mesmo com um nível baixo em alguns mercados.

% Custos das fraudes por canal*

(Varejo/Comércio eletrônico)



*% Pode somar mais de 100% já que as respostas são baseadas em uso de canal.

Perguntas da pesquisa:
P15: Indique a taxa de custo das fraudes gerada por cada um dos seguintes canais de operação usados pela sua empresa.

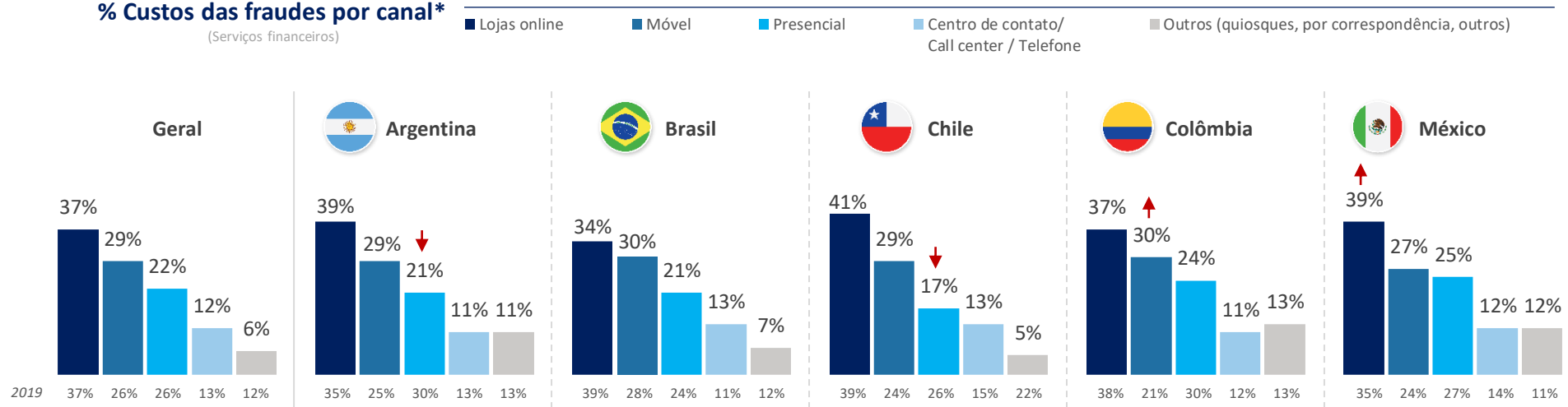
↑↓ = bastante ou direccionalmente mais baixo/alto do que em 2019

O canal online também foi o maior para custos de fraudes entre as empresas de serviços financeiros

Houve um aumento direcional nos custos de fraudes nos canais móveis, embora não tão significante quando comparado ao comércio eletrônico.

% Custos das fraudes por canal*

(Serviços financeiros)



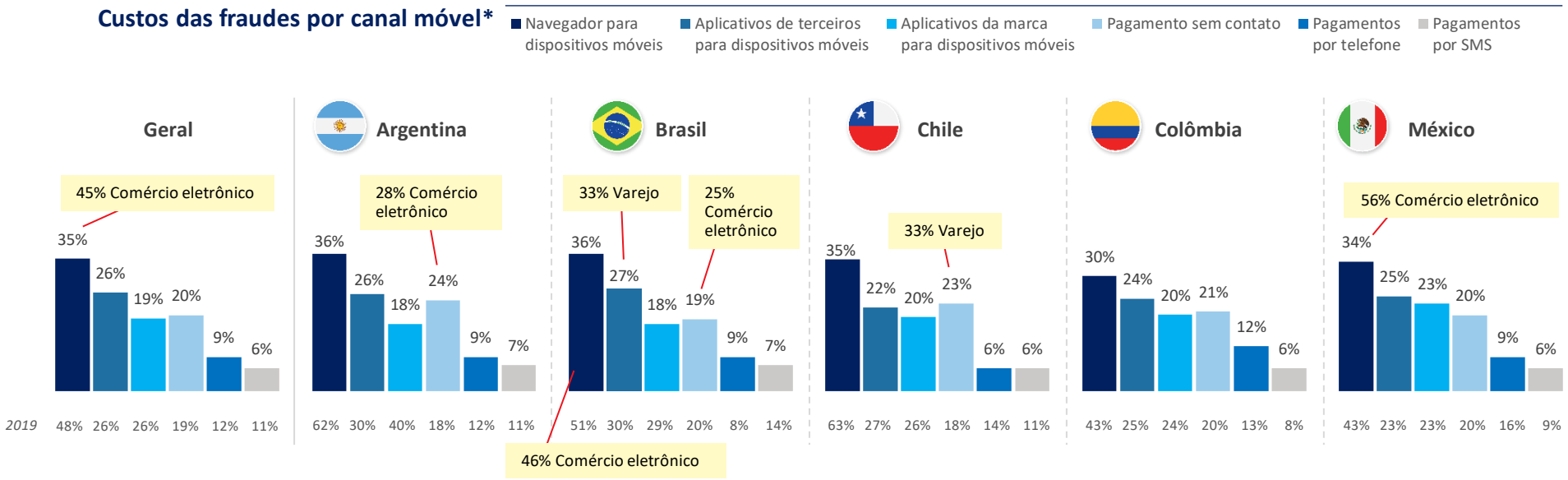
= bastante ou direccionalmente mais baixo/alto do que em 2019

*% Pode somar mais de 100% já que as respostas são baseadas em uso de canal.

Perguntas da pesquisa:
P15 Indique a taxa de custo das fraudes gerada por cada um dos seguintes canais de operação usados pela sua empresa.

Enquanto os navegadores para dispositivos móveis continuaram representando uma grande parcela dos custos das fraudes dos canais móveis, os comerciantes começaram a ver mais com origens nas formas de pagamento em contato.

Custos das fraudes por canal móvel*



LexisNexis® RISK SOLUTIONS

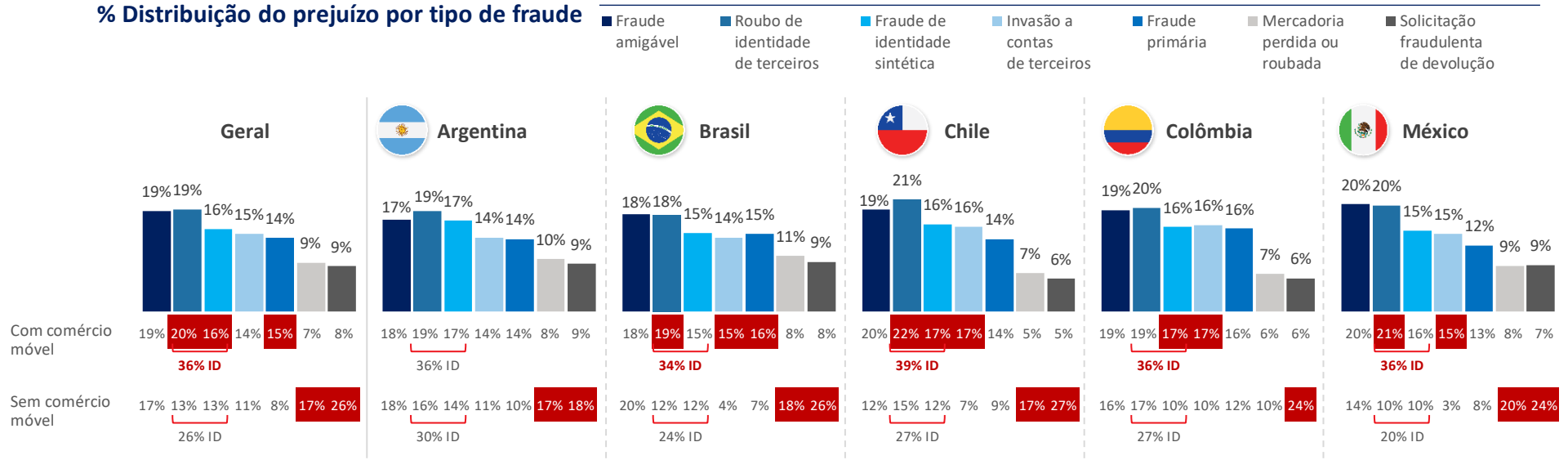
*% Pode somar mais de 100% já que as respostas são baseadas em uso de canal.

Perguntas da pesquisa:
Q17: Indique a distribuição das fraudes pelos diversos canais móveis que você utiliza/aceita.

Com o crescimento do volume nos canais móveis, houve um aumento dos prejuízos associados a fraudes de identidades e de invasão a contas.

Os comerciantes e as instituições financeiras da LATAM que oferecem comércio móvel sofreram muito mais prejuízos com esses tipos de fraudes, inclusive maior exposição a identidades sintéticas.

% Distribuição do prejuízo por tipo de fraude



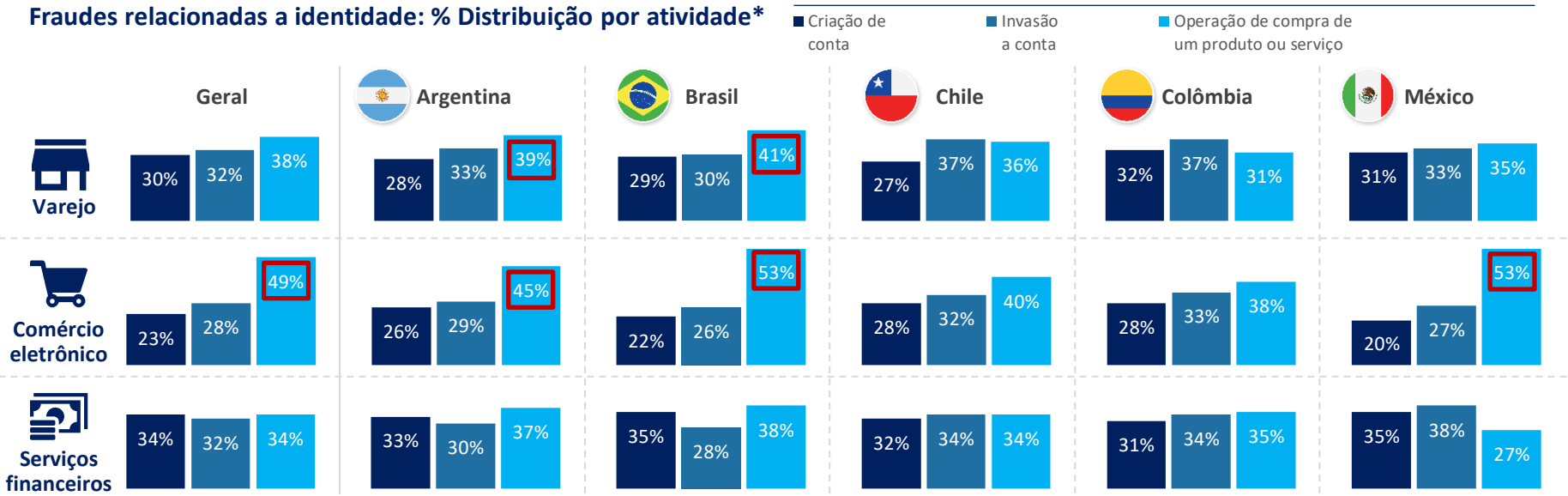
Vermelho = bastante ou direccionalmente mais alto do que outro segmento

LexisNexis® RISK SOLUTIONS

Perguntas da pesquisa:
P12a: Agora pense no seu prejuízo total causado por fraudes nos últimos 12 meses. Indique a taxa de distribuição dos métodos de fraude abaixo, de acordo com a contribuição que tiveram ao prejuízo anual total por fraudes nesse período. Faça uma estimativa com o melhor de seu conhecimento.

Fraudes relacionadas a identidade ocorreram com mais frequência nos pontos de venda dos comerciantes argentinos e brasileiros, especialmente no comércio eletrônico. Em outros mercados, os prejuízos foram distribuídos mais igualmente entre as fraudes de operações e as relacionadas a contas.

Fraudes relacionadas a identidade: % Distribuição por atividade*



= bastante ou direccionalmente mais alto do que fraudes de identidades relacionadas a contas no segmento/mercado do setor

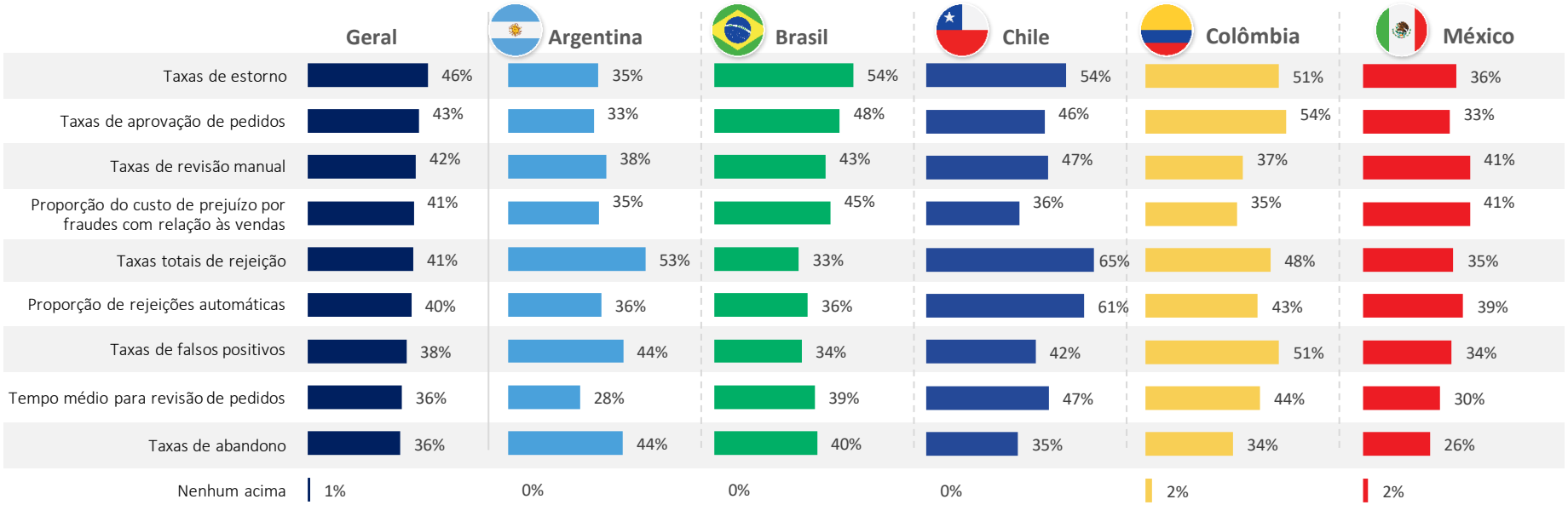
* Cuidado, tamanho de base baixo

P12b: Qual a distribuição de fraudes relacionadas a identidades de acordo com as seguintes atividades?

LexisNexis® RISK SOLUTIONS

As métricas usadas para medir o desempenho das fraudes variaram bastante no mercado da LATAM.

Medição do desempenho de prevenção a fraudes

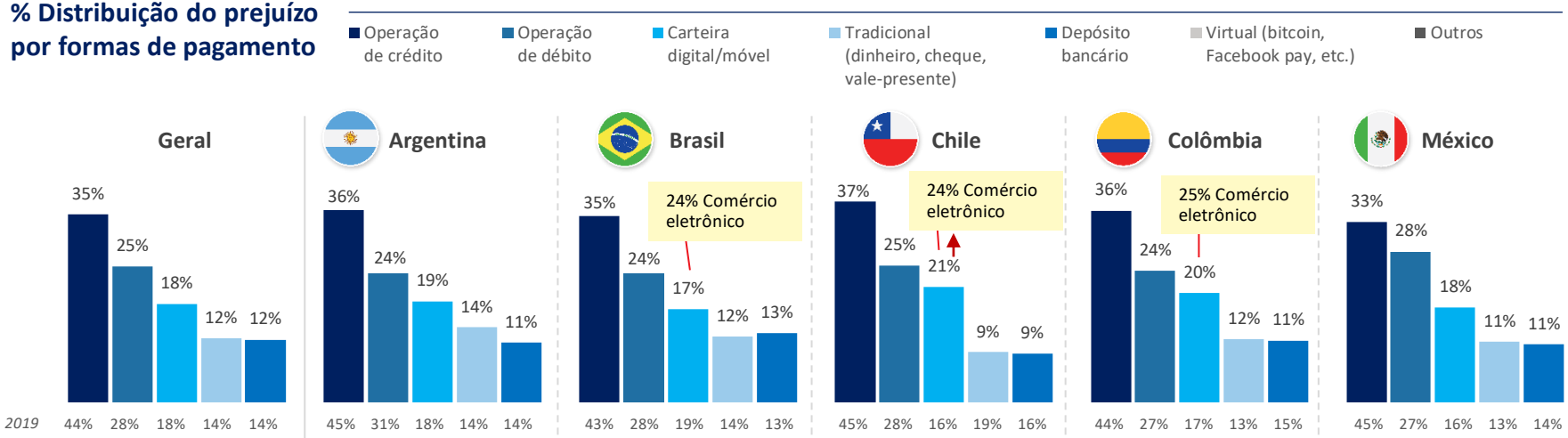


Perguntas da pesquisa:
P12c: Quais das métricas a seguir são usadas pela sua empresa para medir o seu desempenho de prevenção a fraudes (Pergunta não feita em 2019)

Embora as operações de crédito tenham sido responsáveis pela maior parte do prejuízo por fraudes por forma de pagamento, as carteiras móveis/digitais representaram uma parte considerável (quase um quinto).

Como mencionado anteriormente, a pandemia da Covid-19 acelerou o uso de formas de pagamento sem contato como um meio de fornecer uma atividade segura e sem contato na loja, sendo também um método usado em operações remotas. As organizações de comércio eletrônico indicaram direccionalmente mais perdas por meio de carteiras móveis, em comparação ao varejo e aos serviços financeiros. Essa forma de pagamento pode representar riscos de fraudes para os comerciantes, caso dados violados de cartões forem usados durante o processo de inscrição destes. Por isso, a necessidade de fortes ferramentas e processos de autenticação.[8]

% Distribuição do prejuízo por formas de pagamento



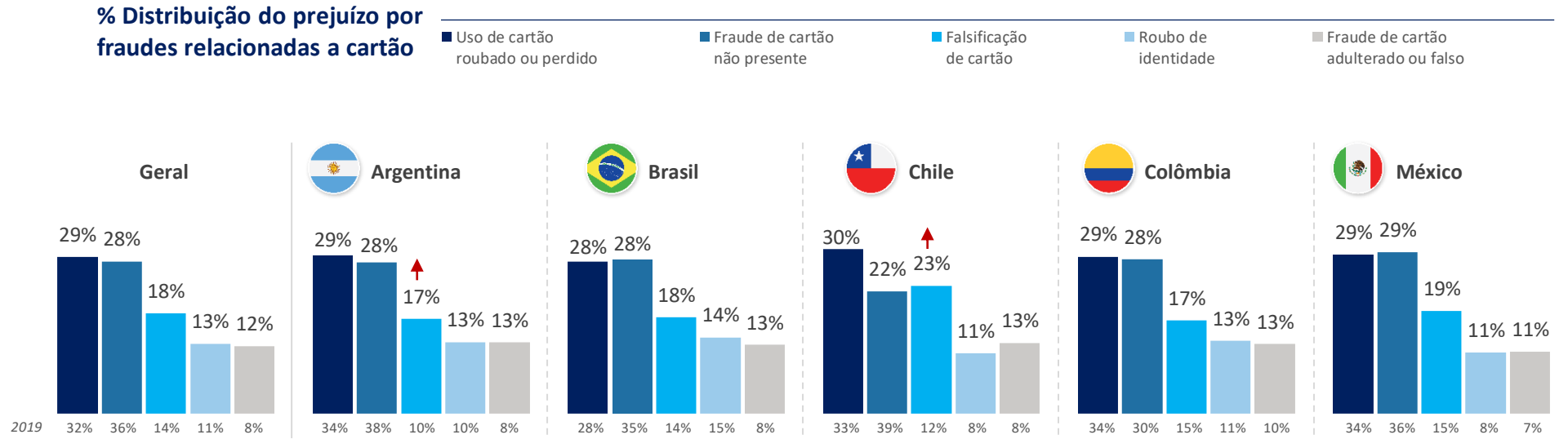
[8] https://www.pindrop.com/blog/mobile-wallets-present-new-opportunities-for-fraud/

Perguntas da pesquisa:
P18: Pensando no prejuízo total causado por fraudes sofrido pela sua empresa nos últimos 12 meses, indique a distribuição dos custos das fraudes para cada forma de pagamento .

↑↓ = bastante ou direccionalmente mais baixo/alto do que em 2019

Cartão não presente (CNP) e cartões perdidos/roubados continuaram sendo os maiores responsáveis pelo prejuízo por fraudes, embora as fraudes por falsificação de cartão tenham aumentado na Argentina e no Chile.

% Distribuição do prejuízo por fraudes relacionadas a cartão



= bastante ou direccionalmente mais baixo/alto do que em 2019

Perguntas da pesquisa:
P18e: Indique a distribuição do prejuízo causado por fraudes relacionadas a cartão de crédito/débito nos seguintes tipos de fraude de cartão.

LexisNexis® RISK SOLUTIONS

DESCOBERTA PRINCIPAL 03

Fraudes relacionadas a identidades representam grande ameaça e desafio para as empresas de varejo/comércio eletrônico e as instituições financeiras na LATAM.

As fraudes relacionadas a identidades são um grande desafio para as operações online/realizadas em navegadores e canais móveis, com novas formas de pagamento online contribuindo para isso, sendo especialmente complicado para o comércio eletrônico.

Esses desafios relacionados a identidades incluem os associados a atributos digitais que avaliam o dispositivo e o risco da operação.

Os comerciantes e as instituições financeiras na LATAM também relataram aumento dos ataques de bots no ano passado, o que não é surpresa, dado o aumento no tráfego digital.

O equilíbrio entre a detecção/prevenção de fraudes com atrito mínimo com o cliente também aumentou, especialmente nos canais online.

Espera-se que os desafios acima persistam pelo menos no curto prazo (próximos 24 meses), provavelmente impactados pelas incertezas sobre o novo normal pós-Covid-19.

A verificação de identidade subiu para o topo da lista dos desafios dos canais online, com a de telefone e de endereço sendo parte do problema, especialmente para o varejo. Novas formas de pagamento são uma questão mais pertinente ao comércio eletrônico do que a outros setores.

Desafios das fraudes por canais online
(% Classificados entre os 3 principais)

Denota estar entre os maiores desafios dos canais online no mercado

↑↓ = bastante ou direccionalmente mais alto/baixo do que em 2019

□ = bastante ou direccionalmente mais alto do que o mesmo desafio em outros mercados

	Geral		Argentina		Brasil		Chile		Colômbia		México	
	2019	2021	2019	2021	2019	2021	2019	2021	2019	2021	2019	2021
Verificação da identidade do cliente	21%	44% ↑	22%	42% ↑	20%	51% ↑	24%	22% ↑	24%	44% ↑	22%	42% ↑
Verificação de endereço	47%	33%	43%	29%	51%	30%	43%	43%	43%	41%	43%	34%
Surgimento de novos e diversos métodos de operação	31%	31%	31%	34%	32%	39%	26%	23%	26%	27%	31%	21%
Verificação de telefone	21%	29%	27%	29%	12%	33% ↑	19%	32% ↑	19%	40% ↑	27%	18%
Equilíbrio da prevenção a fraudes com atrito com o cliente	16%	28% ↑	16%	25%	19%	25%	11%	29% ↑	11%	20% ↑	16%	38% ↑
Verificação de e-mail ou de dispositivo	27%	21%	28%	16%	25%	17%	30%	23%	30%	33%	28%	25%
Incapacidade de determinar fonte/origem da operação	30%	21%	14%	19%	27%	19%	37%	22%	37%	17%	14%	25% ↑
Desafios em aceitar métodos de operação com base internacional	20%	20%	26%	21%	17%	20%	19%	21%	19%	11%	26%	24%
Avaliação de risco de fraude por país/região	22%	19%	21%	18% ↑	21%	11%	35%	30%	35%	22%	21%	28%
Falta de ferramentas especializadas p/ operações/pedidos internacionais	16%	19%	18%	31% ↑	16%	20%	10%	18%	10%	14%	14%	12%
Solicitações em excesso de revisões manuais	17%	18%	14%	24%	23%	16%	16%	21%	16%	20%	14%	15%
Incapacidade de distinção entre humanos e bots	16%	17%	13%	12%	17%	21%	10%	17%	10%	11%	13%	17%

LexisNexis® RISK SOLUTIONS

Perguntas da pesquisa:
P20: Classifique os 3 principais desafios relacionados a fraudes que a sua empresa enfrenta ao atender clientes usando canais móveis/online.

Verificação de identidade permanece um dos principais desafios dos canais móveis, ao lado da verificação de telefone, de endereço e de novas formas de pagamento. Embora poucos tenham classificado a de identidade como um dos principais desafios na Colômbia, as adversidades que causam esse problema foram consideradas altas.

Desafios das fraudes por canais móveis
(% Classificados entre os 3 principais)

Denota estar entre os maiores desafios dos canais online no mercado

= bastante ou direccionalmente mais alto/baixo do que em 2019

= bastante ou direccionalmente mais alto do que o mesmo desafio em outros mercados

	Geral		Argentina		Brasil		Chile		Colômbia		México	
	2019	2021	2019	2021	2019	2021	2019	2021	2019	2021	2019	2021
Verificação da identidade do cliente	47%	37%	45%	48%	50%	39%	43%	21%	56%	25%	43%	41%
Surgimento de novos e diversos métodos de operação	28%	30%	23%	35% ↑	30%	31%	21%	32% ↑	38%	25%	23%	28%
Verificação de endereço	31%	30%	27%	29%	34%	23%	33%	35%	32%	40% ↑	26%	36%
Verificação de telefone	12%	27% ↑	12%	21% ↑	12%	30% ↑	3%	32% ↑	19%	33% ↑	13%	21% ↑
Equilíbrio da prevenção a fraudes com atrito com o cliente	25%	26%	43%	23%	29%	21%	18%	32% ↑	13%	27% ↑	30%	33%
Verificação de e-mail ou de dispositivo	34%	25%	29%	32%	33%	25%	39%	27%	33%	40% ↑	29%	14%
Incapacidade de distinção entre humanos e bots	15%	23%	9%	16%	15%	29%	17%	17%	16%	24% ↑	11%	19%
Solicitações em excesso de revisões manuais	17%	23%	20%	22%	11%	25%	24%	24%	22%	19%	21%	20%
Incapacidade de determinar fonte/origem da operação	18%	22%	19%	22%	18%	28%	25%	17%	20%	13%	20%	20%
Falta de ferramentas especializadas p/ operações/pedidos internacionais	14%	20%	15%	16%	18%	17%	13%	20% ↑	5%	12% ↑	14%	31% ↑
Avaliação de risco de fraude por país/região	19%	18%	16%	17%	22%	15%	21%	27% ↑	14%	21% ↑	18%	19%
Desafios em aceitar métodos de operação com base internacional	18%	18%	24%	19%	10%	16%	24%	19%	24%	20%	26%	18%

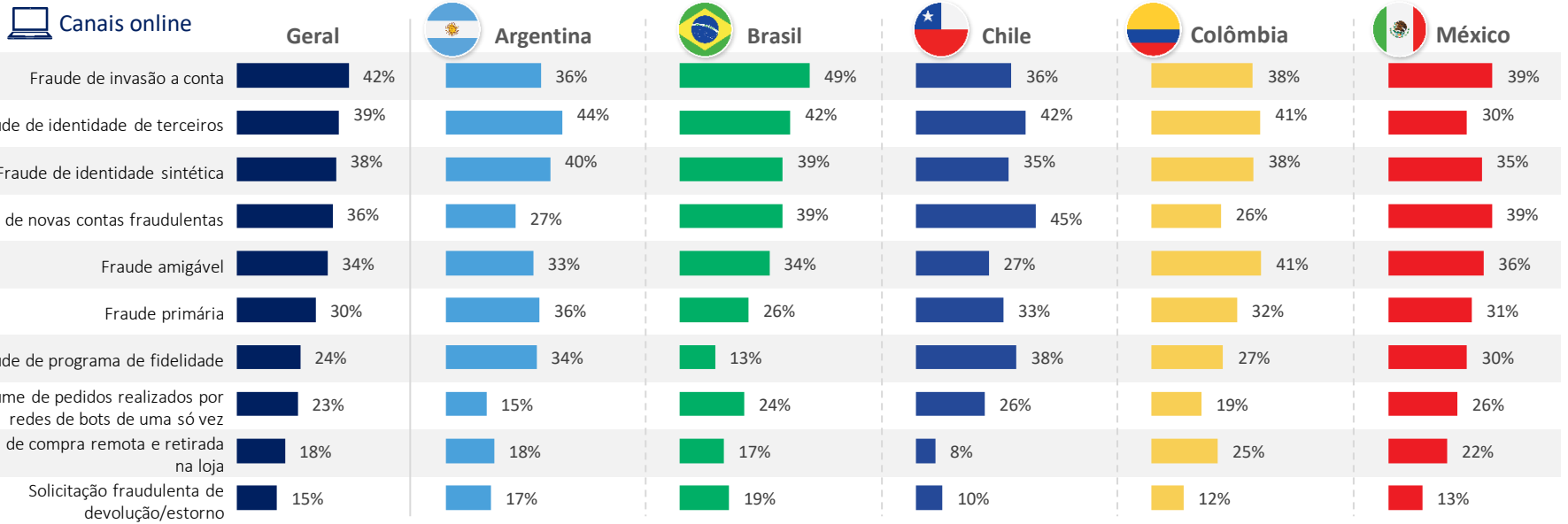
LexisNexis® RISK SOLUTIONS

Perguntas da pesquisa:
P20: Classifique os 3 principais desafios relacionados a fraudes que a sua empresa enfrenta ao atender clientes usando canais móveis/online.

Fraudes de contas e baseadas em identidade são grandes preocupações para os canais online nos próximos 24 meses.

Isso está provavelmente relacionado às incertezas quanto ao "novo normal" após a Covid-19 e ao quanto as operações online continuarão crescendo em preferência.

Principais ameaças esperadas de fraudes (próximos 24 meses) (% Classificados entre os 3 principais)



LexisNexis® RISK SOLUTIONS

Perguntas da pesquisa:
P20e: Classifique as 3 principais ameaças de fraudes que você espera enfrentar nos próximos 24 meses ao atender clientes que usam os seguintes canais: (Pergunta não feita em 2019)

Fraudes primárias e amigáveis se juntam às de identidade como principais preocupações para os canais móveis nos próximos 24 meses.

Fraudes primárias podem envolver membros da família que usam o dispositivo móvel de uma pessoa para realizar compras sem que esta tenha conhecimento. As restrições impostas por conta da Covid aumentaram o risco disso acontecer.

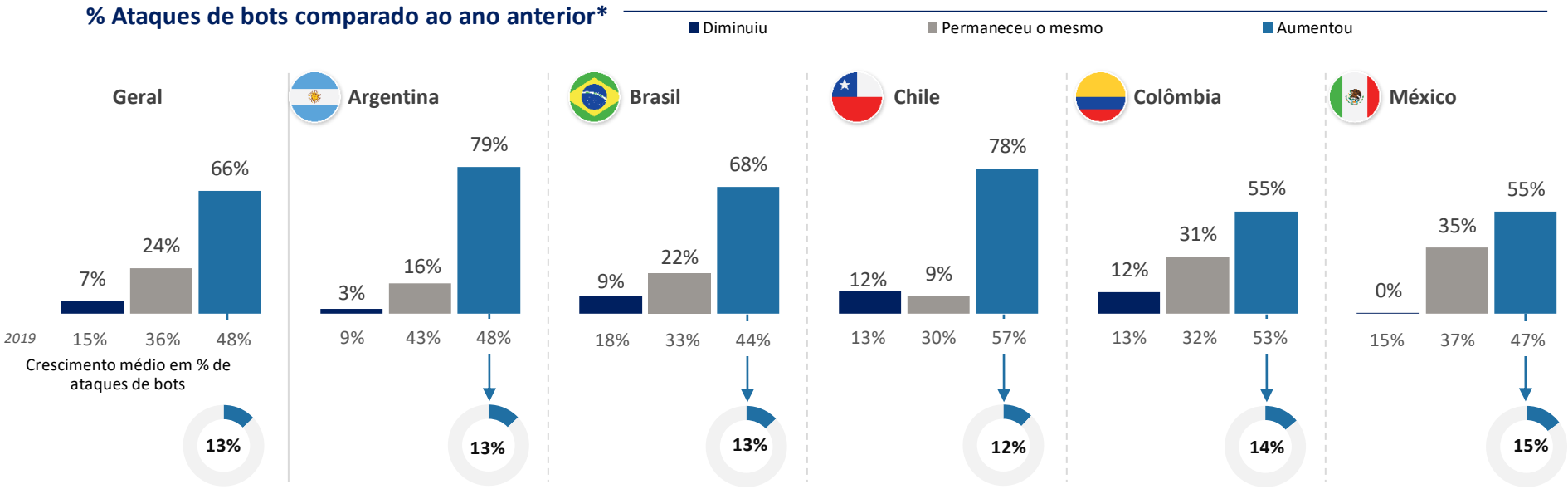
Principais ameaças esperadas de fraudes (próximos 24 meses) (% Classificados entre os 3 principais)

Canais móveis	Geral	Argentina	Brasil	Chile	Colômbia	México
Fraude primária	38%	36%	41%	48%	38%	32%
Fraude amigável	38%	34%	41%	29%	41%	35%
Fraude de identidade de terceiros	37%	38%	39%	28%	35%	37%
Fraude de identidade sintética	37%	35%	42%	33%	39%	30%
Volume de pedidos realizados por redes de bots de uma só vez	32%	22%	27%	38%	28%	45%
Fraude de invasão a conta	29%	30%	24%	35%	25%	36%
Criação de novas contas fraudulentas	27%	33%	31%	27%	34%	15%
Fraude de compra remota e retirada na loja	25%	36%	17%	35%	17%	33%
Fraude de programa de fidelidade	24%	24%	24%	18%	29%	26%
Solicitação fraudulenta de devolução/estorno	13%	14%	14%	10%	14%	12%

LexisNexis® RISK SOLUTIONS

Perguntas da pesquisa:
P20e: Classifique as 3 principais ameaças de fraude que você espera enfrentar nos próximos 24 meses ao atender clientes que usam os seguintes canais: (Pergunta não feita em 2019)

As empresas na LATAM indicaram aumento nos ataques realizados por bots no último ano, principalmente as organizações argentinas, brasileiras e chilenas.



* Exceto os que responderam "Não tenho certeza"

Perguntas da pesquisa:
B1b/c: Como isso fica quando comparado ao mesmo período do ano passado? Em quanto a porcentagem de ataques mensais de bots automatizados nocivos aumentou no ano passado?

DESCOBERTA PRINCIPAL 04

Os comerciantes e as empresas de serviços financeiros na LATAM puderam reduzir custos e riscos de fraudes com melhor prática de integração de segurança cibernética, experiência digital do cliente e operações de fraudes através de uma abordagem de solução em multicamadas.

O atrito com o cliente foi uma preocupação real relacionada ao empenho de prevenção a fraudes, principalmente nos canais online/móveis, onde o abandono é comum por conta dos esforços de clientes e de atrasos nas operações.

Os canais online/móveis estão cada vez mais suscetíveis a fraudes à medida que novas formas de pagamento e de operações oferecem pontos de entrada adicionais para fraudadores sofisticados.

Em média, muitas empresas não otimizaram as suas abordagens de detecção e prevenção de fraudes com base nessa melhor prática. Aquelas que a adotaram, apresentaram maior chance de contarem com os dados necessários para detectar e avaliar os riscos de fraudes. Elas apresentaram:

- Menor probabilidade de classificar verificação de identidade como um dos principais desafios dos canais online ou móveis;
- Menor probabilidade de classificar novas formas de pagamento como um desafio, especialmente no que se refere a fraudes de identidade;
- Maior capacidade de administrar detecção de fraudes e, ao mesmo tempo, minimizar o atrito com o cliente; e
- Maior probabilidade de gastar menos com fraudes em comparação as outras.

As fraudes se tornaram mais complexas, vários riscos podem existir ao mesmo tempo e sem nenhuma solução. As ferramentas de fraudes precisam autenticar tanto os critérios digitais como os físicos, além do risco da identidade e da operação.

QUESTÕES DE FRAUDES

SERVIÇOS DIGITAIS

Operações rápidas, alvos fáceis de identidades sintéticas e botnet. **Necessidade de verificação de velocidade para determinar o risco da operação junto a dados e análises para autenticação do indivíduo.**

FRAUDES RELACIONADAS A CONTAS

Dados violados **exigem nível maior de segurança, além de autenticação da pessoa, diferenciando-a de um bot ou de uma identidade sintética.**

IDENTIDADES SINTÉTICAS

Necessidade de autenticação completa do indivíduo por trás da operação para poder distinguir as identidades falsas com base em dados reais parciais.

ATAQUES DE REDES DE BOTS

Ataques em massa automatizados ou realizados por humanos para testar cartões, senhas/credenciais ou infectar dispositivos.

CANAIS MÓVEIS

Origem da fonte e dispositivos infectados acrescentam risco, *bots* móveis e malwares nocivos dificultam a autenticação, **necessidade de avaliação do dispositivo e do indivíduo.**

OPÇÕES DE SOLUÇÕES

AVALIAÇÃO DO RISCO DA OPERAÇÃO

Verificação de velocidade/classificação da operação: monitoramento dos padrões históricos das operações de um indivíduo em relação às atuais para detectar se o volume do titular do cartão está normal ou se parece haver alguma irregularidade. **Exemplos de solução:** classificação de operação em tempo real, classificação automatizada da operação.

AUTENTICAÇÃO DE PESSOA FÍSICA

Verificação básica: verificação do nome, endereço, data de nascimento ou fornecimento do código CVV associado ao cartão. **Exemplos de solução:** apuração dos serviços de verificação, autenticação do instrumento de pagamento, verificação do nome/endereço/data de nascimento.

Autenticação de identidade ativa: uso dos dados pessoais conhecidos pelo cliente para autenticação ou quando um usuário fornecer dois fatores diferentes de autenticação para a sua verificação. **Exemplos de solução:** autenticação por desafio ou perguntas, autenticação com senha de uso único/de dois fatores.

AUTENTICAÇÃO DE PESSOA DIGITAL

Identidade digital/biometria comportamental: analisa as interações humano-dispositivo e os padrões de comportamento, como a forma com a qual clica-se no mouse e toca-se na tecla, para distinguir entre um real e um impostor ao reconhecer comportamento normal de fraudador. **Exemplos de solução:** autenticação por biometria, avaliação de risco de email/telefone, monitoramento de navegador/malware, ID do dispositivo/ impressão digital.

Avaliação do dispositivo: identifica exclusivamente um dispositivo de computação remoto ou usuário. **Exemplos de solução:** ID do dispositivo/impressão digital, localização geográfica.

LexisNexis® RISK SOLUTIONS

As abordagens de melhores práticas envolvem camadas de diferentes soluções para lidar com os riscos exclusivos aos diferentes canais, formas de pagamento e produtos. E eles vão além, integrando recursos e operações aos seus esforços de prevenção a fraudes.

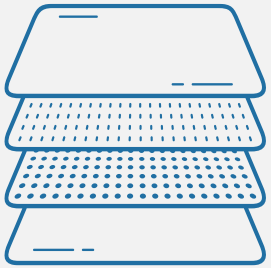
Integração

Ferramentas e recursos com abordagem de prevenção a fraudes

- Alertas de segurança cibernética
- Inteligência de mídias sociais
- Modelos de IA/AM
- Colaboração coletiva
- Operações de segurança cibernética
- Operações de experiência do cliente/digital

Camadas de solução de detecção e prevenção a fraudes

Uma abordagem de solução em multicamadas é essencial para combater as fraudes ao mesmo tempo em que mitiga o atrito do cliente.



- Riscos diferentes quando se vende bens digitais e físicos.
- Redes de bots e malwares podem comprometer os dispositivos móveis. Autenticação do dispositivo e do usuário.
- Abordar tanto os riscos de fraudes de identidade como de operação.
- Diferentes desafios e riscos para o móvel em comparação ao online.

Estratégia e foco

Minimizar o atrito enquanto maximiza a proteção contra fraudes

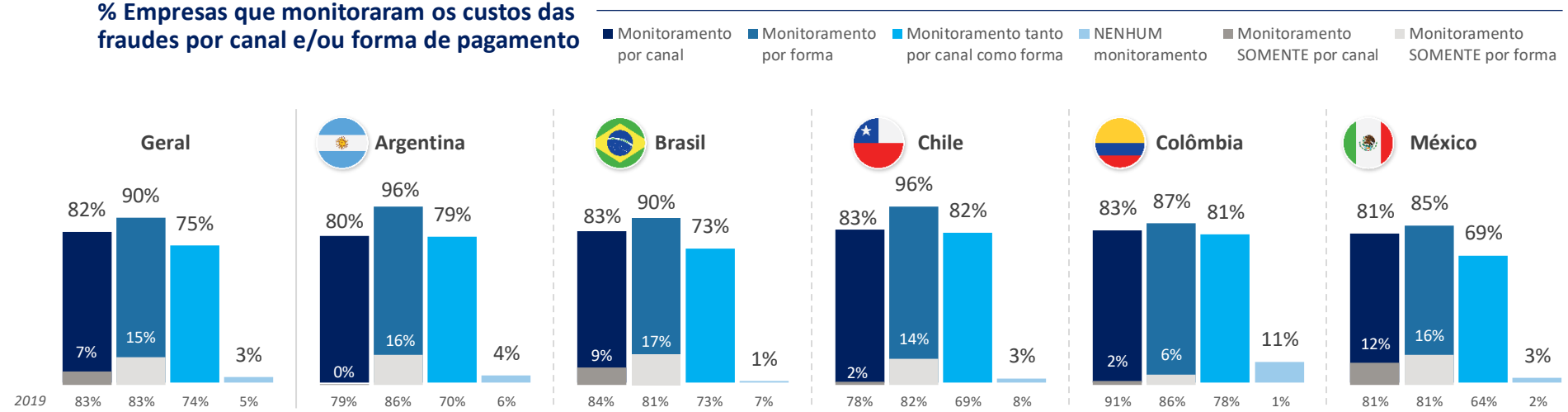
- Monitoramento de fraudes bem-sucedidas e prevenidas por canal de operação e formas de pagamento.
- Uso de soluções de autenticação digital/passiva para diminuir os esforços do cliente (deixa as soluções fazerem o trabalho nos bastidores).
- Avaliação tanto dos riscos individuais como os de operações.

LexisNexis® RISK SOLUTIONS

O monitoramento dos custo das fraudes tanto por canais de operação como por formas de pagamento foi essencial para a prevenção a fraudes. A maioria indica que o fez.

Como as fraudes ocorreram de formas diferentes dependendo se a venda era de bem físico ou digital e se feita por um canal móvel, isso criou diversos endpoints e oportunidades para os fraudadores atacarem. Eles continuaram realizando testes para encontrar os pontos mais fracos onde podem operar sem serem detectados. Saber onde foram bem-sucedidos é importante para "preencher os espaços vazios", mas também conhecer onde tentaram e falharam é igualmente relevante para manter a vigilância.

% Empresas que monitoraram os custos das fraudes por canal e/ou forma de pagamento

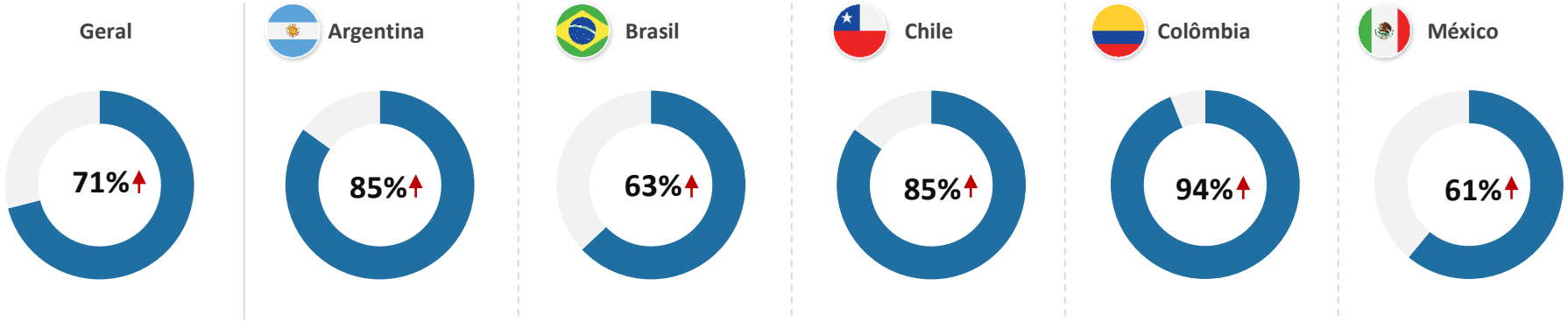


Perguntas da pesquisa:
P14a: A sua empresa monitora o custo de operações fraudulentas por canais e formas de pagamento usados?

A maioria dos comerciantes e das instituições financeiras da LATAM indicaram que monitoram os custos das fraudes por ponto de origem bem mais do que há 2 anos.

É provável que o aumento no volume de operações online e móveis esteja influenciando isso.

% Monitoramento do custo das operações fraudulentas com base no local onde tiveram origem internacionalmente



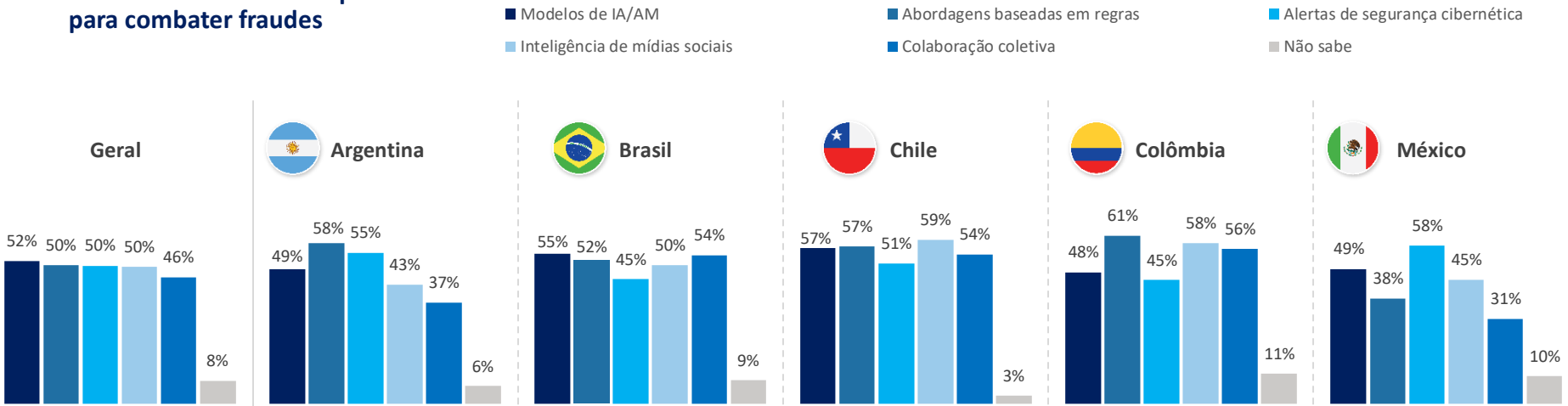
	Geral	Argentina	Brasil	Chile	Colômbia	México
2019	47%	39%	48%	46%	46%	51%

↑ = bastante ou direccionalmente mais alto/baixo do que em 2019

Perguntas da pesquisa:
P14b: A sua empresa monitora o custo das operações fraudulentas com base em onde elas tiveram origem internacionalmente (ex.: vindo de uma região específica)?

Um número considerável de comerciantes e instituições financeiras indicaram o uso de diferentes tipos de recursos de suporte para combater fraudes.

% Uso de recursos de suporte para combater fraudes



*Perguntada àqueles com canais móveis e/ou online traduzidos

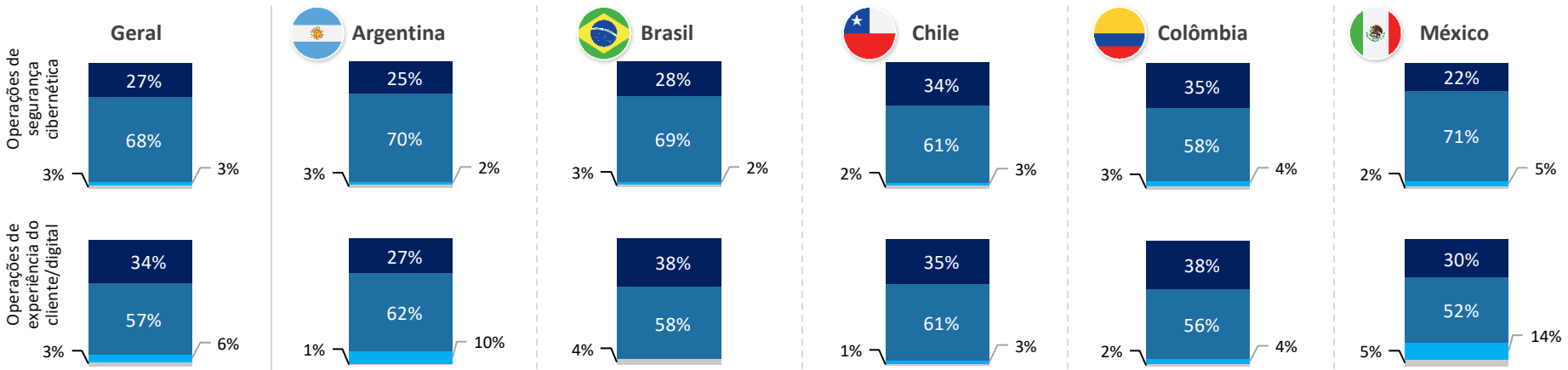
Perguntas da pesquisa:
P28b: Além de soluções, quais recursos de suporte a sua empresa usa para combater fraudes? (Pergunta não feita em 2019)

Entretanto, poucos afirmaram que a sua organização tenha integrado às operações de segurança cibernética e experiência do cliente/digital completamente as abordagens de proteção contra fraudes.

À medida que o volume operacional cresceu através dos canais remotos/digitais, tornou-se fundamental que as empresas integrassem completamente essas operações, tanto em termos de proteção contra fraudes cibernéticas quanto como meio de minimizar o atrito com o cliente ao avaliar os riscos de fraude.

% Uso de melhores práticas de mitigação de fraude

Integração de segurança cibernética e experiência do cliente/digital* Operações c/ prevenção a fraudes



*Perguntada àqueles com canais móveis e/ou online traduzidos

Perguntas da pesquisa:
P29: Até que ponto a sua empresa integrou as suas operações de segurança cibernética aos seus esforços de prevenção a fraudes?
P30b: Até que ponto a sua empresa integrou as suas operações de experiência do cliente/digital aos seus esforços de prevenção a fraudes? (Pergunta não feita em 2019)

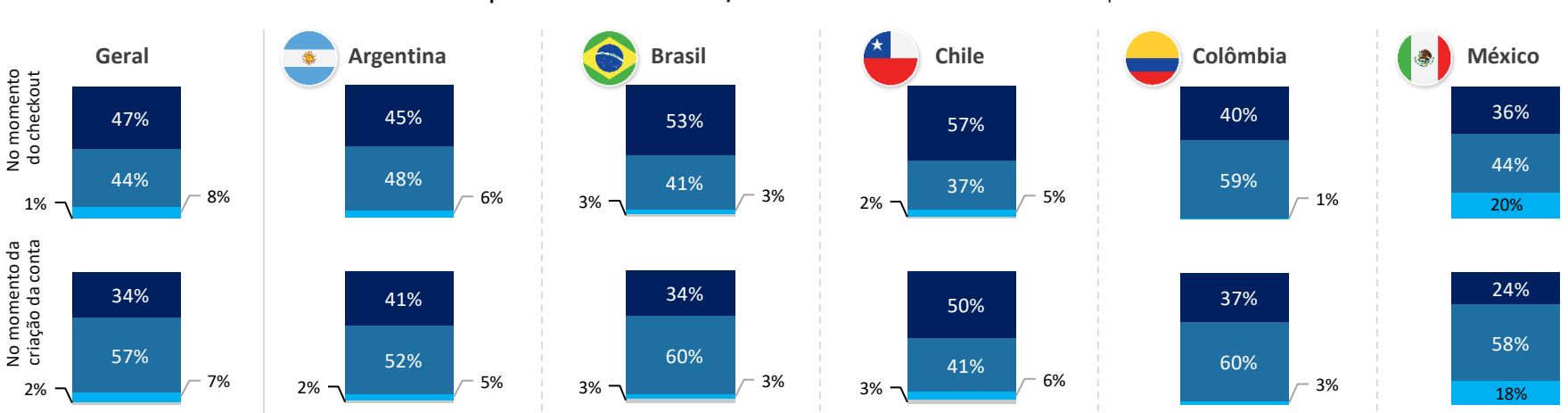
LexisNexis® RISK SOLUTIONS

Aproximadamente metade das empresas argentinas, brasileiras e chilenas afirmaram estar extremamente focadas em minimizar o atrito com o cliente no momento da operação, embora um menor número se concentre nisso quando o assunto é criação de contas. O México e a Colômbia ficam atrás em ambos.

Equilibrar a detecção de fraudes ao atrito com o cliente foi uma preocupação real para as empresas que operam com canais online e móveis. O abandono é comum quando os clientes ficam frustrados por terem que fazer muito esforço. Ao mesmo tempo, esses canais apresentaram altos riscos de fraudes e devem ser abordados.

% Uso de melhores práticas de mitigação de fraude

Grau de foco em minimizar o atrito com o cliente por meio dos canais online/móveis



*Perguntada àqueles com canais móveis e/ou online traduzidos

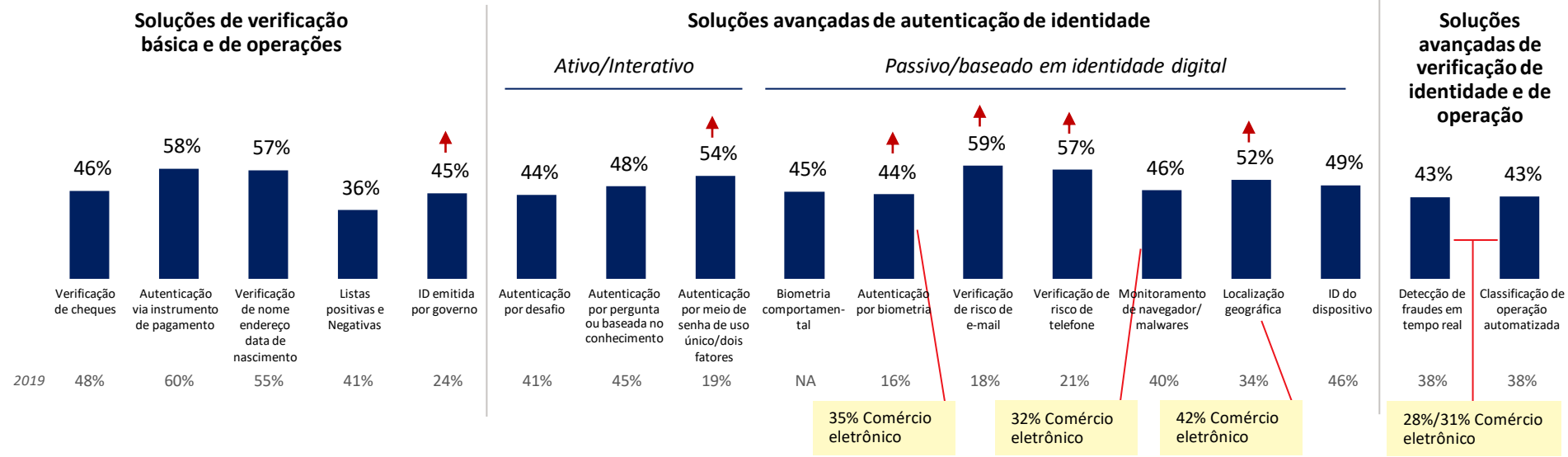
Perguntas da pesquisa:
P30: Até que ponto a sua empresa está focada em minimizar o atrito com o cliente durante o checkout de uma operação nos canais online ou móveis?
P30a: Até que ponto a sua empresa está focada em minimizar o atrito com o cliente quando alguém abre uma nova conta online através de um dispositivo móvel?
(Pergunta não feita em 2019)

LexisNexis® RISK SOLUTIONS

Houve investimentos em autenticação por meio de senha de uso único/dois fatores e soluções passivas/ baseadas em identidade digital

No entanto, menos empresas de comércio eletrônico estão entre as que fizeram esses investimentos, tornando-as mais vulneráveis durante a pandemia, principalmente por usarem menos soluções digitais que fornecem detecção de fraudes mais eficaz contra crimes cibernéticos e identidades sintéticas.

Uso de soluções de mitigação de fraudes (Regional)



= bastante ou direccionalmente mais alto/baixo do que em 2019

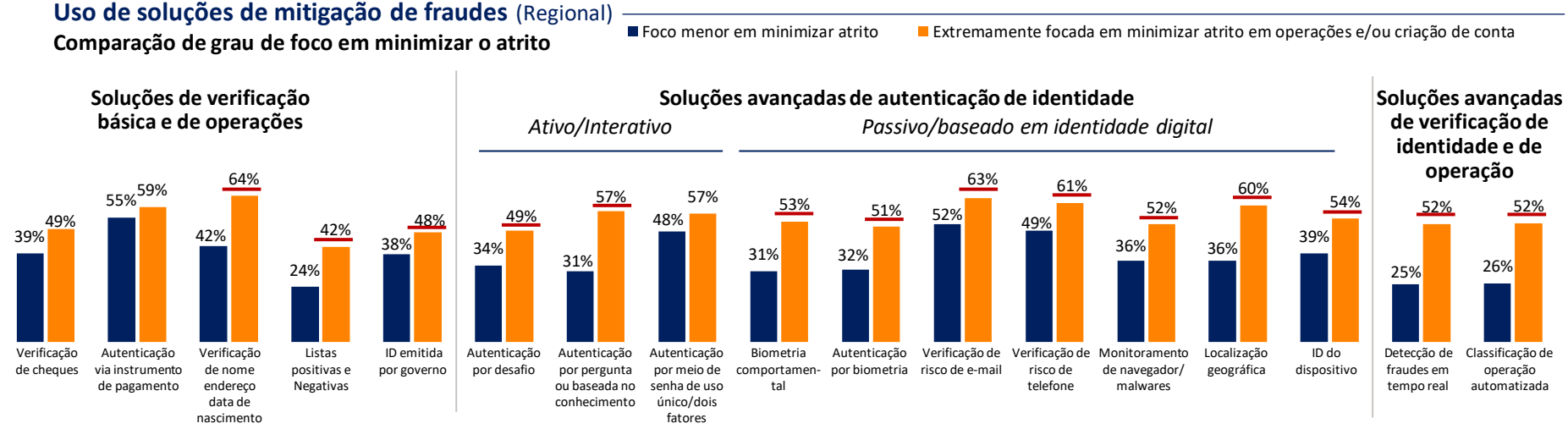
Perguntas da pesquisa:
P27: Quais das soluções de fraudes a seguir a sua empresa utiliza atualmente?

Esses e outros investimentos foram realizados, em grande parte, por comerciantes e instituições financeiras da LATAM que estão focadas em minimizar o atrito com o cliente, inclusive através de soluções digitais que avaliam comportamentos, dispositivos, operações e o indivíduo.

Isso inclui as projetadas para avaliar os riscos individuais e do dispositivo (verificação de risco de e-mail/telefone, localização geográfica, ID do dispositivo, rastreamento de navegador/malware) e, para alguns, risco da operação (classificação de operação automatizada). A localização geográfica e a ID do dispositivo também deram suporte à detecção de fraudes em canais móveis. Todas essas soluções mencionadas oferecem detecção de fraudes rápida, simples e "nos bastidores", reduzindo os esforços dos clientes e os atrasos.

Uso de soluções de mitigação de fraudes (Regional)

Comparação de grau de foco em minimizar o atrito



* Integração de operações de segurança cibernética, experiência digital do cliente e de fraudes, além de estar extremamente focado em minimizar o atrito com o cliente

Perguntas da pesquisa:
P27: Quais das soluções de fraudes a seguir a sua empresa utiliza atualmente?

= bastante ou direccionalmente mais alto do que a mesma solução em **outros** mercados

O custo das fraudes, do atrito com o cliente e dos seus desafios foram menores para as organizações que investiram em soluções de mitigação de risco em multicamadas, que focam em minimizar o atrito com o cliente e têm as suas operações de segurança cibernética e de experiência digital do cliente integradas.

Ao investir em soluções que avaliam os atributos de identidade digital e os riscos da operação, as organizações também reduziram a carga sobre o esforço de clientes legítimos (permitindo a entrada destes) enquanto detectaram e bloquearam fraudadores de maneira mais eficaz. Como resultado, elas enfrentaram um volume significativamente menor de desafios relacionados a autenticação de identidade e para equilibrar prevenção a fraudes a atrito com o cliente, ao mesmo tempo em que reduziram o custo das fraudes.

***Abordagem de melhor prática de solução em multicamadas:** as organizações que seguiram uma abordagem de soluções em multicamadas tenderam a usar alguma combinação de soluções passivas/ baseadas em identidade digital, além de algumas que avaliam atributos de identidade física e o risco da operação.

DADOS REGIONAIS

	Abordagem de melhor prática de solução em multicamadas*	Os que NÃO seguem a abordagem de melhor prática de solução em multicamadas*
Soluções de **verificação de atributos físicos** (ex.: nome, data de nascimento, endereço)		
Soluções de **verificação de atributos digitais** (ex.: risco de e-mail, do número de telefone, biometria)		Limitada ou nenhuma
Soluções de **avaliação de risco de dispositivo e de localização** (ex.: ID do dispositivo, localização geográfica)		Limitado ou nenhum
Soluções de **avaliação de comportamento** (ex.: biometria comportamental, riscos das operações)		Limitada ou nenhuma
	Além de operações de fraudes integradas à segurança cibernética/experiência digital e extremamente focada em minimizar o atrito com o cliente.	Não integrada e focada em minimizar o atrito com o cliente

	Online	Dispositivos Móveis	Online	Dispositivos Móveis
% Ranking de verificação de identidade como um dos principais desafios online/móvel	39%	38%	70%	60%
% Ranking de equilíbrio entre prevenção a fraudes e atrito como um dos principais desafios online/móvel	25%	16%	49%	33%
Novas formas de pagamento móveis como principal desafio móvel	20%		41%	
O custo de cada operação fraudulenta é de . .	3,44 vezes o valor perdido		3,85 vezes o valor perdido	

LexisNexis® RISK SOLUTIONS

RECOMENDAÇÕES

Permaneça atento e preparado para um aumento no volume de fraudes no futuro próximo, combinando isso a um foco em minimizar o atrito com o cliente em um ambiente competitivo de canais online/móveis.

Tecnologia é fundamental. As empresas precisam de uma plataforma de tecnologia robusta de segurança e fraudes que as ajude a se adaptar a um ambiente digital dinâmico.

Conte com uma abordagem de solução em multicamadas. Proteção de ponto único não é mais suficiente e resulta em falhas de ponto único. Uma abordagem de defesa de autenticação em multicamadas forte é necessária.

As operações de segurança cibernética e de experiência digital do cliente devem estar integradas aos processos de fraudes.

Busque alianças no setor para compartilhar conhecimento e informações sobre fraudes. É provável que as empresas estejam enfrentando os mesmos fraudadores.

PERMANEÇA ATENTO E PREPARADO PARA UM AUMENTO NO VOLUME DE FRAUDES ENQUANTO MINIMIZA O ESFORÇO DO CLIENTE

Embora partes da sociedade estejam se abrindo desde o início da pandemia, não está claro como será o futuro no curto prazo em relação ao novo normal. É razoável supor que a migração acelerada em direção a operações e pagamentos online/móveis causada pela pandemia permanecerá sendo uma preferência após a Covid. Portanto, as empresas devem continuar desenvolvendo e aprimorando a experiência digital do cliente ao mesmo tempo em que se protegem contra fraudes.

Os fraudadores adquiriram novas habilidades e conhecimento durante a pandemia, inclusive os pontos fracos de comerciantes e instituições financeiras com relação à detecção de fraudes. Identidade e dados relacionados a contas roubados durante golpes e tentativas de *phishing* no ano passado serão usados com identidades sintéticas e ataques de bot em um nível mais bem-sucedido enquanto as empresas continuarem avaliando apenas os atributos de identidades físicas e não os comportamentos de identidades digitais e riscos das operações.

À medida que mais operações são realizadas nos canais online e móveis, os consumidores passam a ter mais opções, o que inclui abandonar uma operação trabalhosa. Nem toda operação apresenta o mesmo nível de risco. As empresas precisam contar com inteligência para saber quando demandar mais ou menos esforços dos clientes. Os novos podem apreciar as etapas extras para verificar a sua identidade, como perguntas desafio e senhas de uso único, já os recorrentes podem se cansar disso em algum momento, pois esperam que a empresa os conheça.

Uma abordagem bem-sucedida de detecção e prevenção de fraudes envolve integração das operações de tecnologia, segurança cibernética e experiência digital, de forma a abordar os riscos exclusivos aos diferentes canais de operação e formas de pagamento, assim como por indivíduos e tipos de operações.

TECNOLOGIA É FUNDAMENTAL

Para minimizar fraudes, as organizações não podem mais depender de processos manuais com a ajuda de tecnologias limitadas para reduzir as taxas de desafio, revisões manuais e custos.

As empresas precisam de uma plataforma de tecnologia robusta de segurança e fraudes que as ajude a se adaptar a um ambiente digital dinâmico, oferecendo sólida gestão de fraudes e resultando em uma experiência sem atrito para clientes genuínos.

A implantação de tecnologias que conseguem reconhecer clientes, identificar fraudes e construir a base de conhecimento sobre fraudes para agilizar o acolhimento pode evitar invasões a contas e detectar ameaças internas.

Usar atributos de dados valiosos, como login de usuários em vários dispositivos, localizações e canais, é essencial para identificar riscos.

Habilitar perícia integrada, gestão de caso e inteligência de negócios pode ajudar a melhorar a produtividade.

CONTE COM UMA ABORDAGEM DE SOLUÇÃO EM MULTICAMADAS

Proteção de ponto único não é mais suficiente e resulta em falhas de ponto único.

À medida em que os consumidores realizam operações em diferentes localizações, dispositivos e geografias, os comportamentos do usuário, como padrões de operação, valores de pagamentos e beneficiários de pagamentos, estão se tornando mais variados e menos previsíveis.

Isso exige uma abordagem de defesa de autenticação em multicamadas forte, o que inclui uma plataforma única de decisão de autenticação que incorpora dados de eventos em tempo real, sinais de terceiros e inteligência global entre canais.

Também é necessária a capacidade de examinar ameaças de nível de malware, bot e Cavalo de Troia de Acesso Remoto e detecção de falsificação de IP em canais móveis e da internet.

Ao mesmo tempo, é fundamental conseguir fornecer análises comportamentais e reduzir falsos positivos e atritos com o cliente.

AS OPERAÇÕES DE SEGURANÇA CIBERNÉTICA E DE EXPERIÊNCIA DIGITAL DO CLIENTE DEVEM ESTAR INTEGRADAS AOS PROCESSOS DE FRAUDES

Melhore a tomada de decisão e a experiência do cliente com aprendizado de máquina e uma integração de sistemas/recursos que gerenciam o risco em toda a empresa e em todos os *endpoints* - convergência de risco.

Dados aprimorados e recursos analíticos de ferramentas como IA/AM, alertas cibernéticos, inteligência de redes sociais e colaboração coletiva permitem que as empresas prevejam as ameaças em vez de reagir a estas.

A integração dessas ferramentas a soluções baseadas em identidade digital oferece proteção em toda a jornada do cliente, não apenas no ponto da operação. A maioria dos fraudadores prefere invasão/criação relacionadas a contas, pois isso fornece uma fonte contínua de ativos em vez de uma operação única.

Combinados, os itens acima podem prover eficiência e economia de custo, além de garantir uma experiência do cliente otimizada, especialmente onde os riscos de fraude podem ser segmentados para que os controles de segurança possam ser ajustados para cima ou para baixo com base na operação.

BUSQUE ALIANÇAS NO SETOR PARA COMPARTILHAR INFORMAÇÕES

É provável que as organizações estejam enfrentando os mesmos grupos de fraudadores. Na realidade, os padrões de fraudes e riscos apresentam muitas semelhanças entre os setores e localizações geográficas.

Construir uma aliança específica do setor para a troca de informações importantes pode manter os seus membros atualizados sobre os padrões e as táticas de fraudes, complementando a sua própria inteligência e permitindo que identifiquem e rastreiem, com mais precisão, os indivíduos e dispositivos em risco. Tais informações podem incluir:

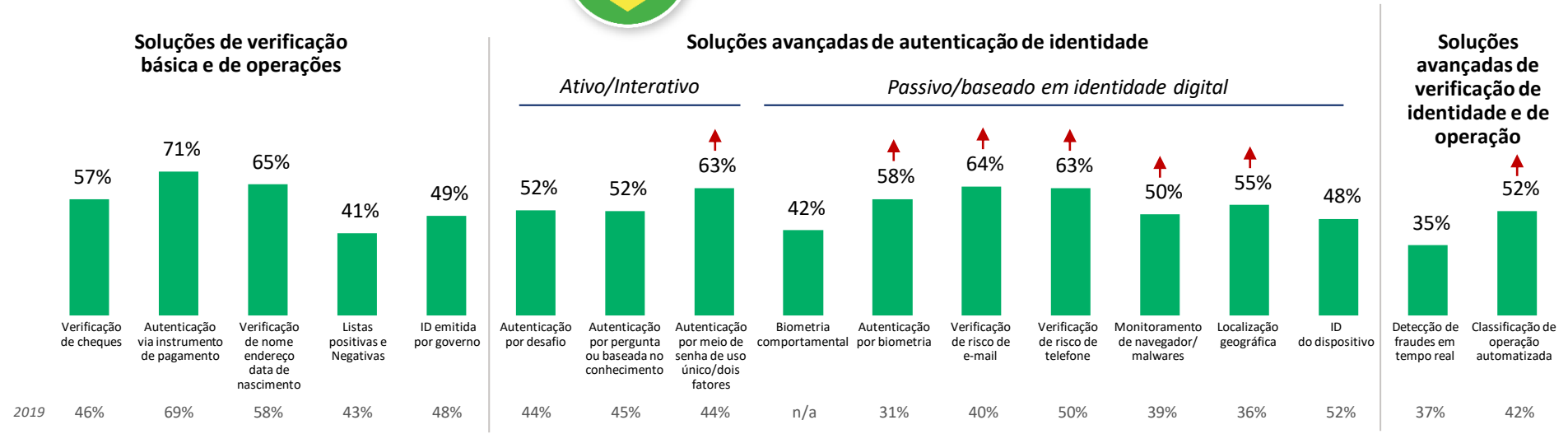
- Dispositivos com histórico de listra negra;
- Contas mula e estratégias associadas a fraudes;
- Riscos específicos pertinentes ao setor/casos de uso/localização geográfica.


A LexisNexis® Risk Solutions
pode ajudar sua empresa
Para mais informações:
risk.lexisnexis.com/fraudes
LexisNexis®
RISK SOLUTIONS

ANEXO

Desde 2019, vários comerciantes e instituições financeiras brasileiros têm investido em soluções baseadas em identidade passiva/digital e em classificação avançada de risco da operação.

Uso de soluções de mitigação de fraudes



↑ = bastante ou direccionalmente mais alto/baixo do que em 2019

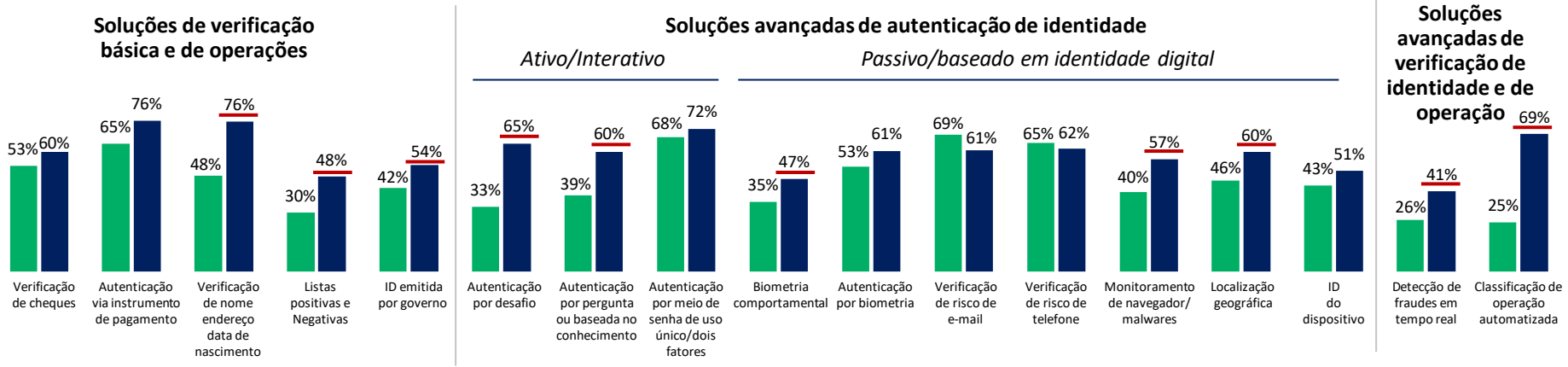
Perguntas da pesquisa:
P27: Quais das soluções de fraudes a seguir a sua empresa utiliza atualmente?

Embora diversas empresas brasileiras tenham investido em verificação de risco de e-mail/telefone, as focadas em minimizar o atrito do cliente o fizeram mais em soluções digitais, inclusive monitoramento de navegador, localização geográfica, ID de dispositivo e biometria.

Elas também apresentaram maior probabilidade de avaliar o risco da operação, não somente do indivíduo. As soluções oferecem detecção de fraudes rápida, simples e "nos bastidores", reduzindo os esforços do cliente e os atrasos. E muitas dessas organizações afirmaram terem tido muito sucesso em administrar detecção de fraudes com atrito.

Uso de soluções de mitigação de fraudes

Comparação de grau de foco em minimizar o atrito — Foco menor em minimizar atrito | Extremamente focada em minimizar atrito em operações e/ou criação de conta

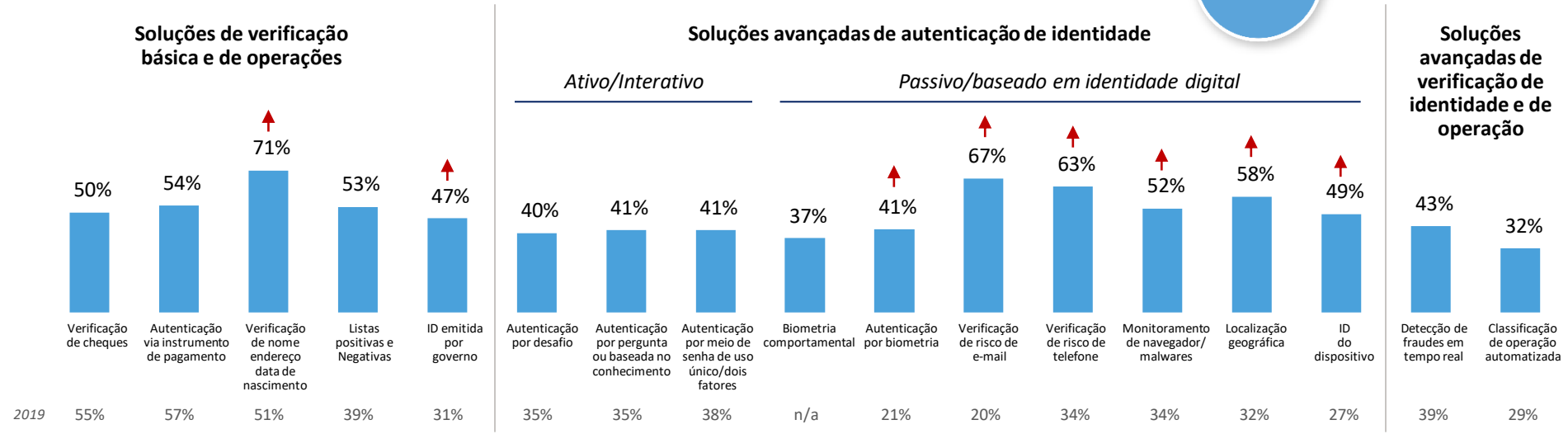


= bastante ou direccionalmente mais alto do que a mesma solução em **outros** segmentos

Perguntas da pesquisa:
P27: Quais das soluções de fraudes a seguir a sua empresa utiliza atualmente no ponto de compra/distribuição de fundos?

Autenticação usando atributos digitais (risco de e-mail, telefone) e físicos (nome, endereço, data de nascimento) são soluções de mitigação de fraudes comumente usadas pelos comerciantes e instituições financeiras argentinos.

Uso de soluções de mitigação de fraudes



= bastante ou direccionalmente mais alto/baixo do que em 2019

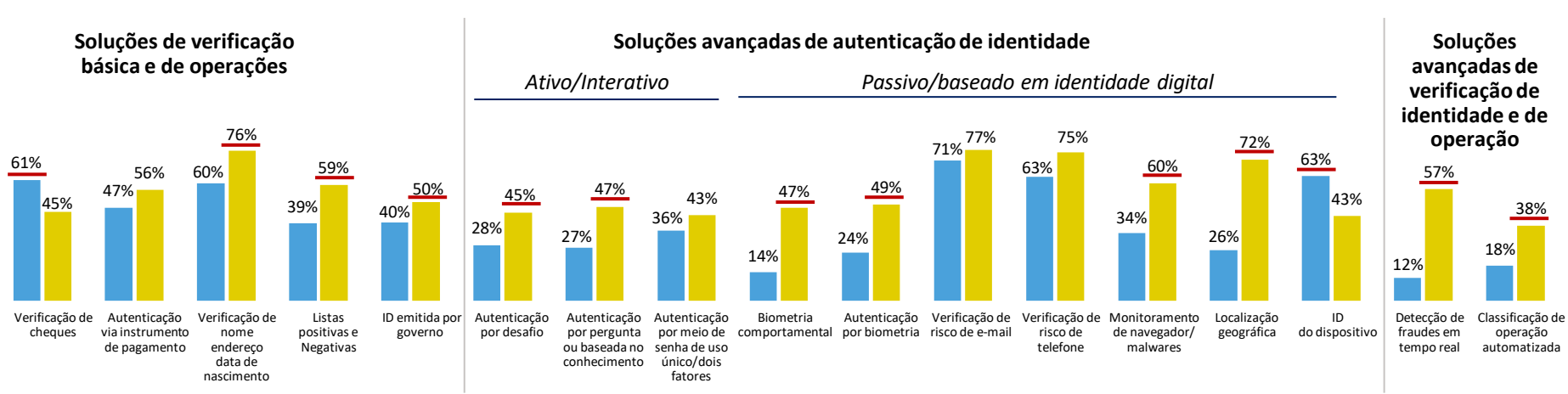
Perguntas da pesquisa:
P27: Quais das soluções de fraudes a seguir a sua empresa utiliza atualmente?

Embora diversas empresas argentinas tenham investido em verificação de risco de e-mail/telefone, as focadas em minimizar o atrito do cliente o fizeram em um conjunto mais amplo de soluções - muitas das quais fornecendo uma avaliação de risco mais profunda e nos bastidores.

Elas também apresentaram maior probabilidade de avaliar o risco da operação, não somente do indivíduo.

Uso de soluções de mitigação de fraudes

Comparação de grau de foco em minimizar o atrito

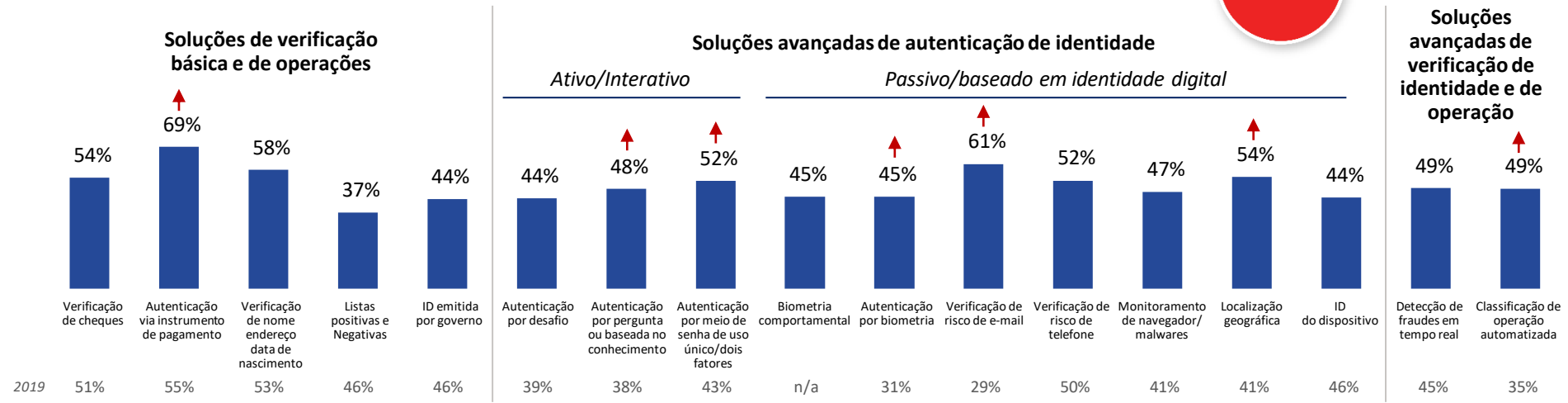


= bastante ou direccionalmente mais alto do que a mesma solução em **outros** segmentos

Perguntas da pesquisa:
P27: Quais das soluções de fraudes a seguir a sua empresa utiliza atualmente no ponto de compra/distribuição de fundos?

Desde 2019, alguns comerciantes e instituições financeiras chilenos têm investido em soluções baseadas em identidade passiva/digital e em classificação avançada de risco de operação. A verificação de risco de e-mail foi o que recebeu mais investimento.

Uso de soluções de mitigação de fraudes



= bastante ou direccionalmente mais alto/baixo do que em 2019

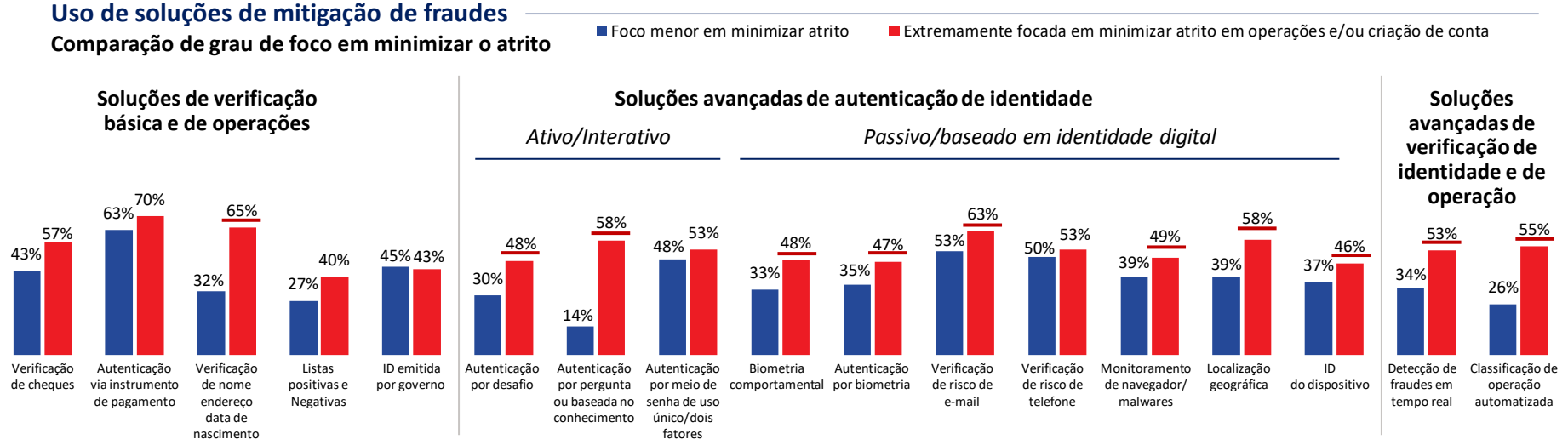
Perguntas da pesquisa:
P27: Quais das soluções de fraudes a seguir a sua empresa utiliza atualmente?

Esses investimentos maiores foram realizados, em grande parte, por comerciantes e instituições financeiras chilenos que estão focados em minimizar o atrito com o cliente através de soluções digitais que avaliam comportamentos, dispositivos, operações e o indivíduo.

As soluções oferecem detecção de fraudes rápida, simples e "nos bastidores", reduzindo os esforços do cliente e os atrasos. E muitas dessas organizações afirmaram terem tido muito sucesso em administrar detecção de fraudes com atrito.

Uso de soluções de mitigação de fraudes

Comparação de grau de foco em minimizar o atrito

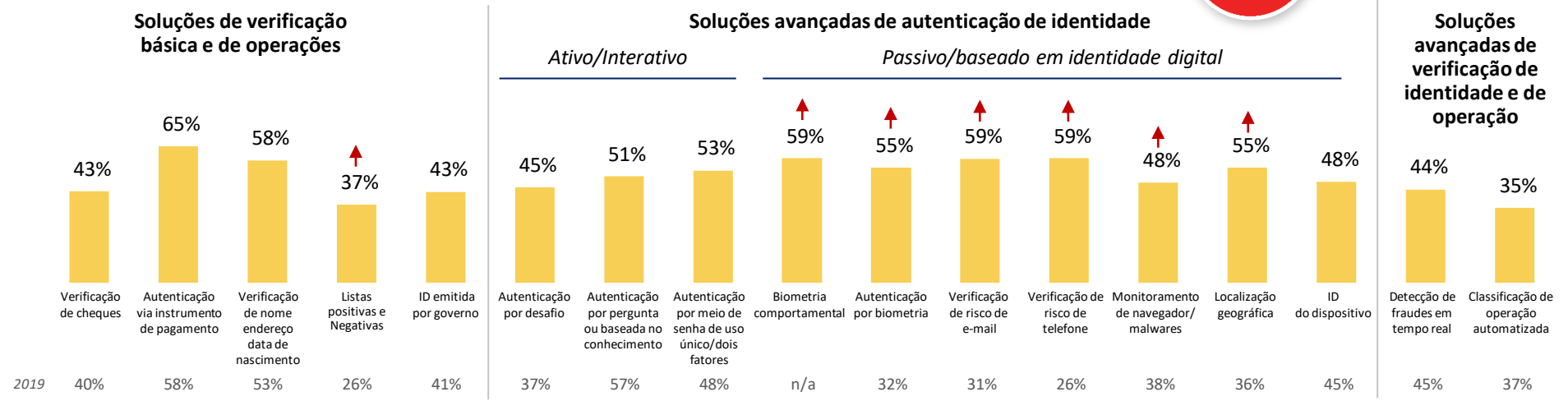


= bastante ou direccionalmente mais alto do que a mesma solução em **outros** segmentos

Perguntas da pesquisa:
P27: Quais das soluções de fraudes a seguir a sua empresa utiliza atualmente no ponto de compra/distribuição de fundos?

Desde 2019, alguns comerciantes e instituições financeiras colombianos têm investido em soluções baseadas em identidade passiva/digital, especialmente biometria, verificação de risco de e-mail/telefone, monitoramento de malwares e localização geográfica.

Uso de soluções de mitigação de fraudes



↑ = bastante ou direccionalmente mais alto/baixo do que em 2019

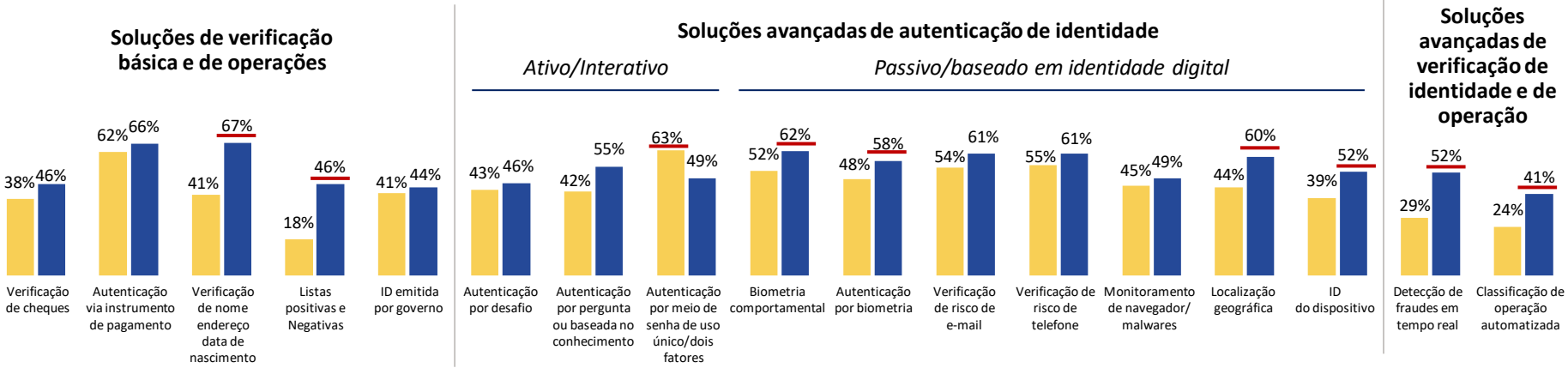
Perguntas da pesquisa:
P27: Quais das soluções de fraudes a seguir a sua empresa utiliza atualmente?

Esses investimentos maiores foram realizados, em grande parte, por comerciantes e instituições financeiras colombianos que estão focados em minimizar o atrito com o cliente através de soluções digitais que avaliam comportamentos, dispositivos, operações e o indivíduo.

As soluções oferecem detecção de fraudes rápida, simples e "nos bastidores", reduzindo os esforços do cliente e os atrasos. E muitas dessas organizações afirmaram terem tido muito sucesso em administrar detecção de fraudes com atrito.

Uso de soluções de mitigação de fraudes

Comparação de grau de foco em minimizar o atrito — Foco menor em minimizar atrito — Extremamente focada em minimizar atrito em operações e/ou criação de conta



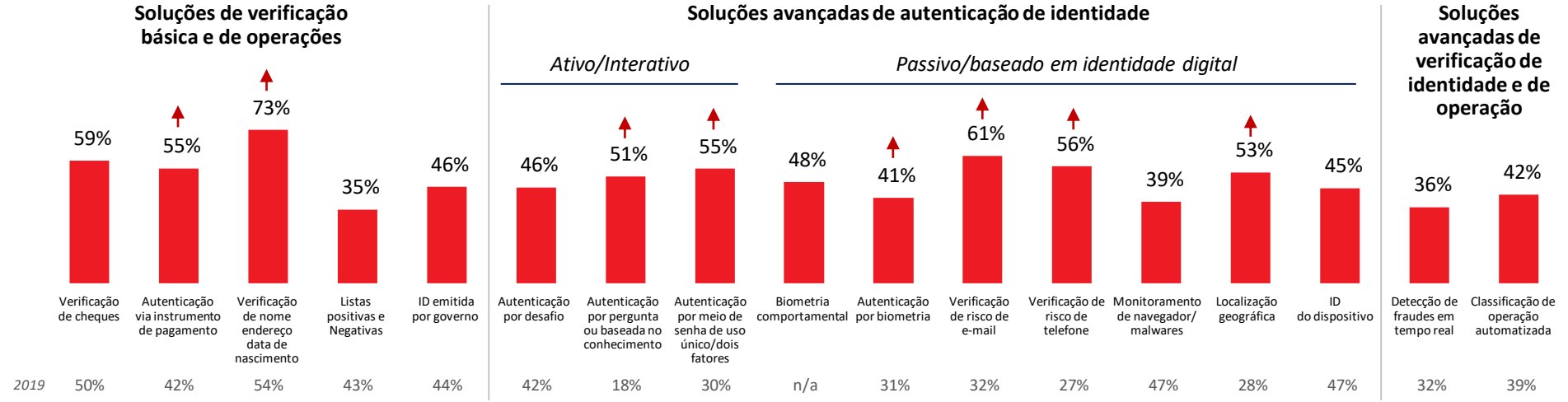
= bastante ou direccionalmente mais alto do que a mesma solução em **outros** segmentos

Perguntas da pesquisa:
P27: Quais das soluções de fraudes a seguir a sua empresa utiliza atualmente no ponto de compra/distribuição de fundos?

Como em outros mercados da LATAM, houve investimento em diversas soluções, inclusive baseadas em identidade passiva/digital, verificação de risco de e-mail/telefone e localização geográfica.

Diversas organizações mexicanas também investiram em soluções de questionário e/ou senha de uso único/autenticação de fatores.

Uso de soluções de mitigação de fraudes



↑ = bastante ou direccionalmente mais alto/baixo do que em 2019

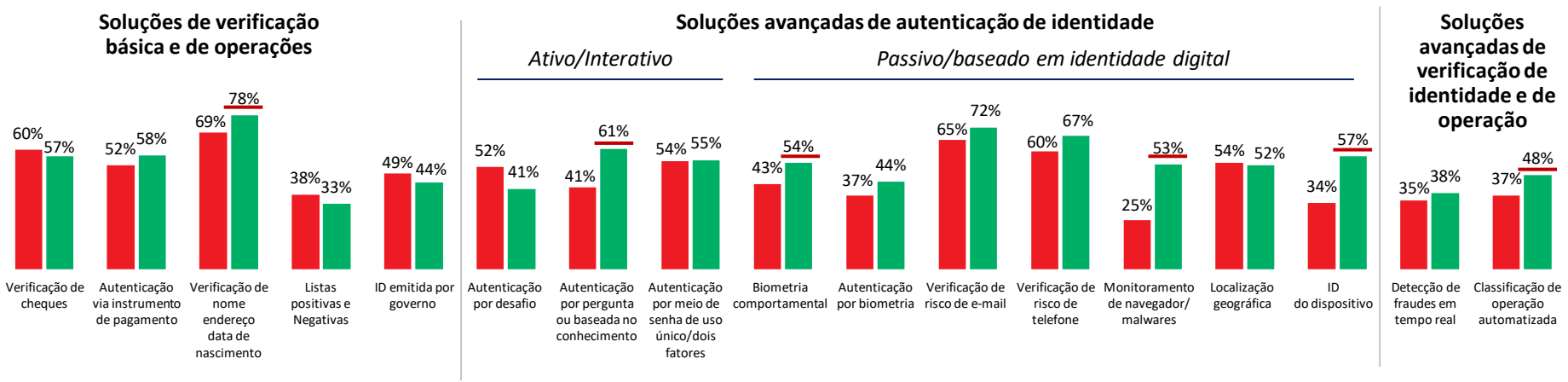
Perguntas da pesquisa:
P27: Quais das soluções de fraudes a seguir a sua empresa utiliza atualmente?

Em muitos casos, esses investimentos maiores foram realizados por comerciantes e instituições financeiras mexicanos focados em minimizar o atrito com o cliente.

As soluções oferecem detecção de fraudes rápida, simples e "nos bastidores", reduzindo os esforços do cliente e os atrasos. E muitas dessas organizações afirmaram terem tido muito sucesso em administrar detecção de fraudes com atrito.

Uso de soluções de mitigação de fraudes

Comparação de grau de foco em minimizar o atrito



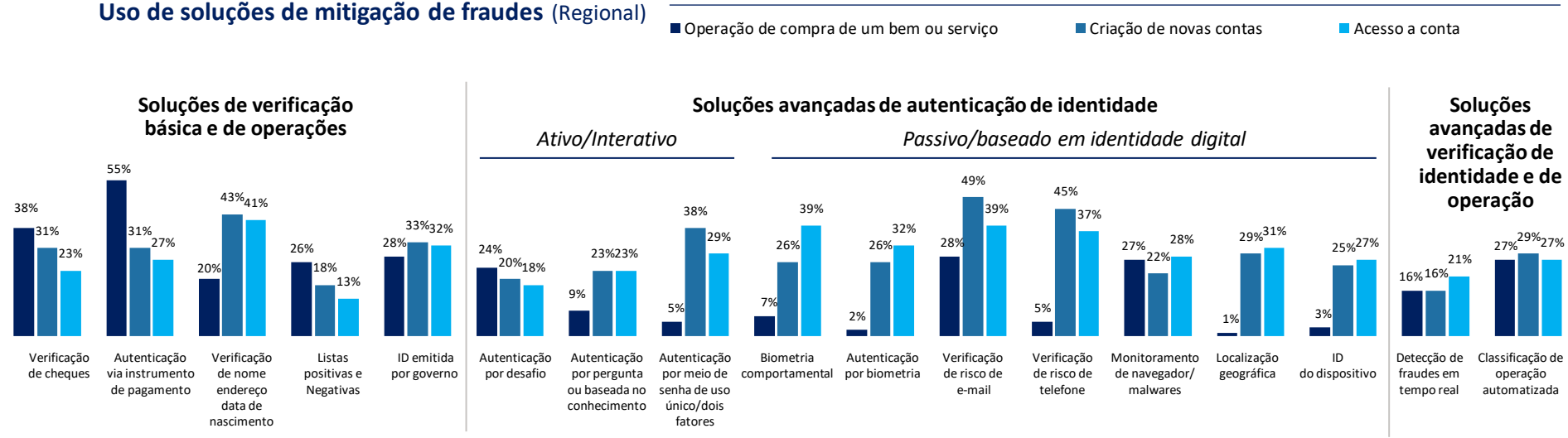
= bastante ou direccionalmente mais alto do que a mesma solução em **outros** segmentos

Perguntas da pesquisa:
P27: Quais das soluções de fraudes a seguir a sua empresa utiliza atualmente no ponto de compra/distribuição de fundos?

USO DE SOLUÇÕES DE FRAUDES POR JORNADA DO CLIENTE/VAREJO

Varejo

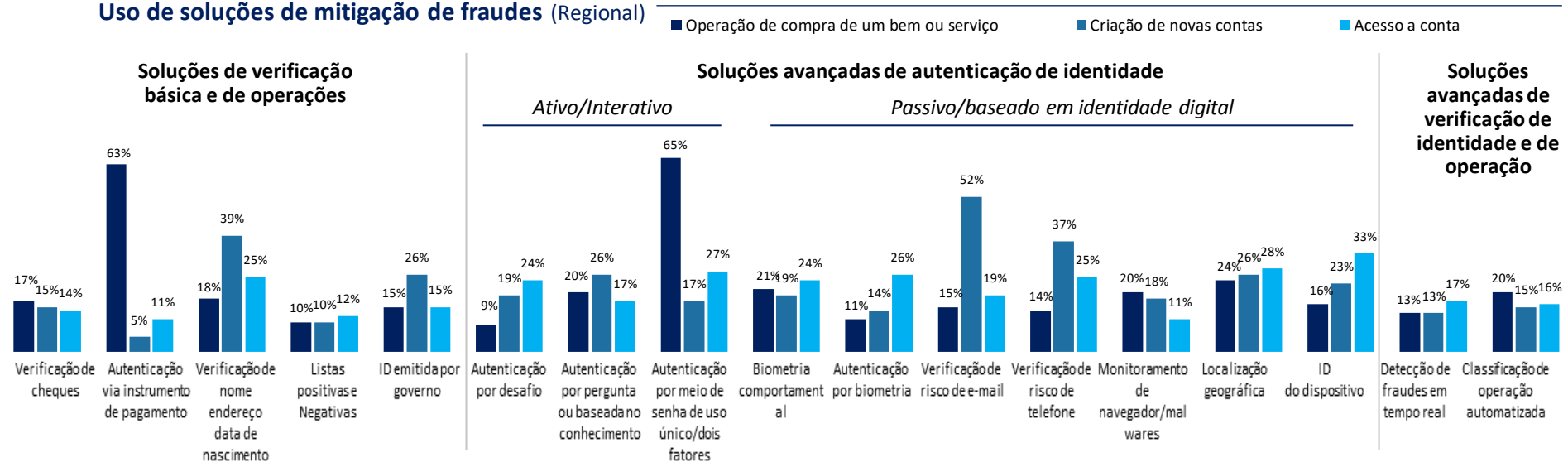
Uso de soluções de mitigação de fraudes (Regional)



Perguntas da pesquisa:
P27: Quais das soluções de fraudes a seguir a sua empresa utiliza atualmente?

Comércio eletrônico

Uso de soluções de mitigação de fraudes (Regional)

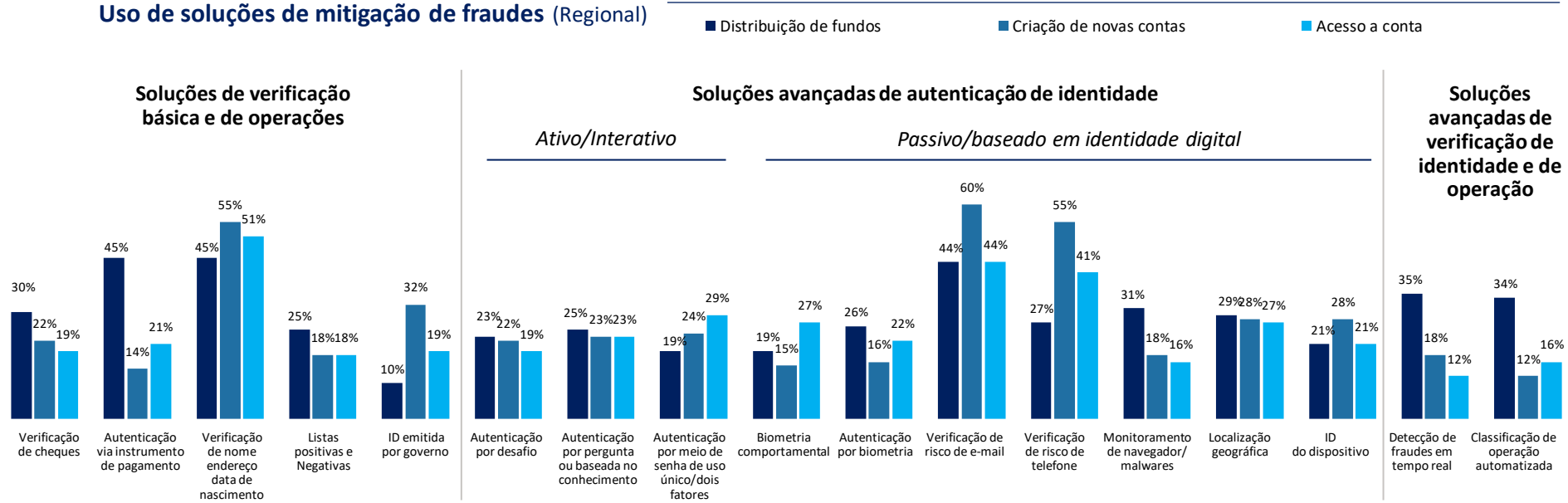


Perguntas da pesquisa:
P27: Quais das soluções de fraudes a seguir a sua empresa utiliza atualmente?

USO DE SOLUÇÕES DE FRAUDES POR JORNADA DO CLIENTE/SERVIÇOS FINANCEIROS

Serviços financeiros

Uso de soluções de mitigação de fraudes (Regional)



Perguntas da pesquisa:
P27: Quais das soluções de fraudes a seguir a sua empresa utiliza atualmente?

Todas as referências monetárias neste relatório são baseadas em dólares americanos. Para o propósito deste estudo, o México está incluído com a América Latina. Este documento é apenas para fins educacionais e não garante a funcionalidade ou características dos produtos LexisNexis identificados, se houver. A LexisNexis não garante que este documento esteja completo ou livre de erros. LexisNexis e o logotipo do Knowledge Burst são marcas registradas da RELX Inc. Outros produtos e serviços podem ser marcas registradas de suas respectivas empresas.

NXR15151-00-1021-PT-LA

LexisNexis® RISK SOLUTIONS