

# CENÁRIO DE CRIMES CIBERNÉTICOS NO BRASIL PÓS PANDEMIA



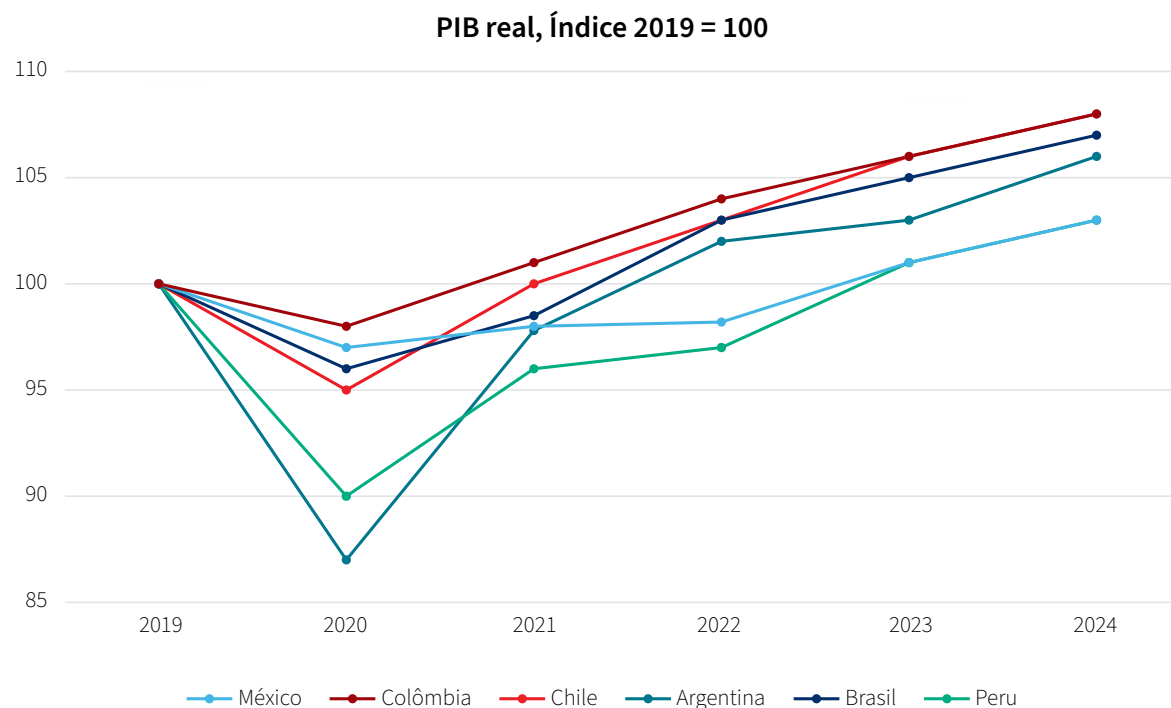
# Fraudes e a recuperação econômica

Conforme a economia vem se recuperando, os níveis de fraude aumentam

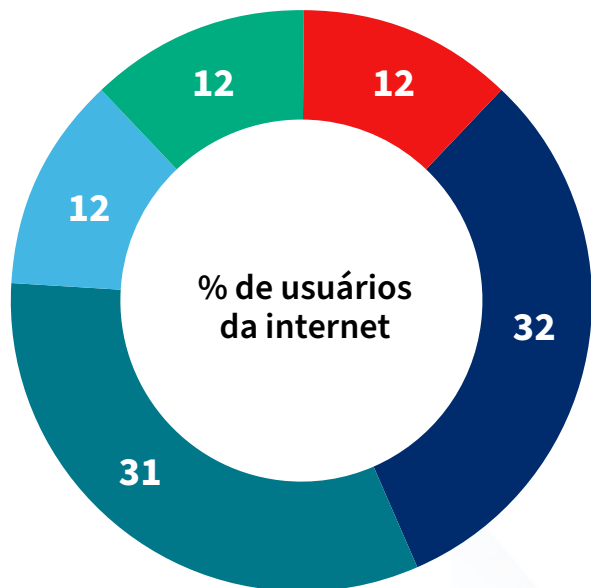
Além das tendências e análises da nossa Digital Identity Network, iremos explorar vários tópicos:

- Como a maior dependência do consumidor do canal móvel alterou os padrões de fraude ao longo do tempo
- As sofisticadas redes de fraude que ligam o sistema financeiro, ecommerce e telecomunicações
- O nível de detalhe e complexidade das fraudes realizadas por cyber fraudadores

Fonte: The World Bank



# Os novos consumidores digitais



- Retratores
- Mantiveram
- Adaptaram
- Disruptivos
- Novatos

Fonte: AMI/Echo survey, N = 2,078



Brasil



México



Colômbia

PERFIL DE CONSUMO	% DE USUÁRIOS DA INTERNET		
	Brasil	México	Colômbia
<b>Retratores</b> — reduziram seu padrão de compras online	9	11	21
<b>Mantiveram</b> — Não alteraram seu padrão de compras	38	28	24
<b>Adaptaram</b> — estão comprando ligeiramente mais	33	32	23
<b>Disruptivos</b> — estão comprando online significativamente mais	18	11	11
<b>Novatos</b> — apenas recentemente fizeram sua primeira compra	3	17	21

# Em 2022, o consumo das famílias alcançará 103% do nível de 2019

**-7%**

Resultado do PIB regional em 2020

**6%**

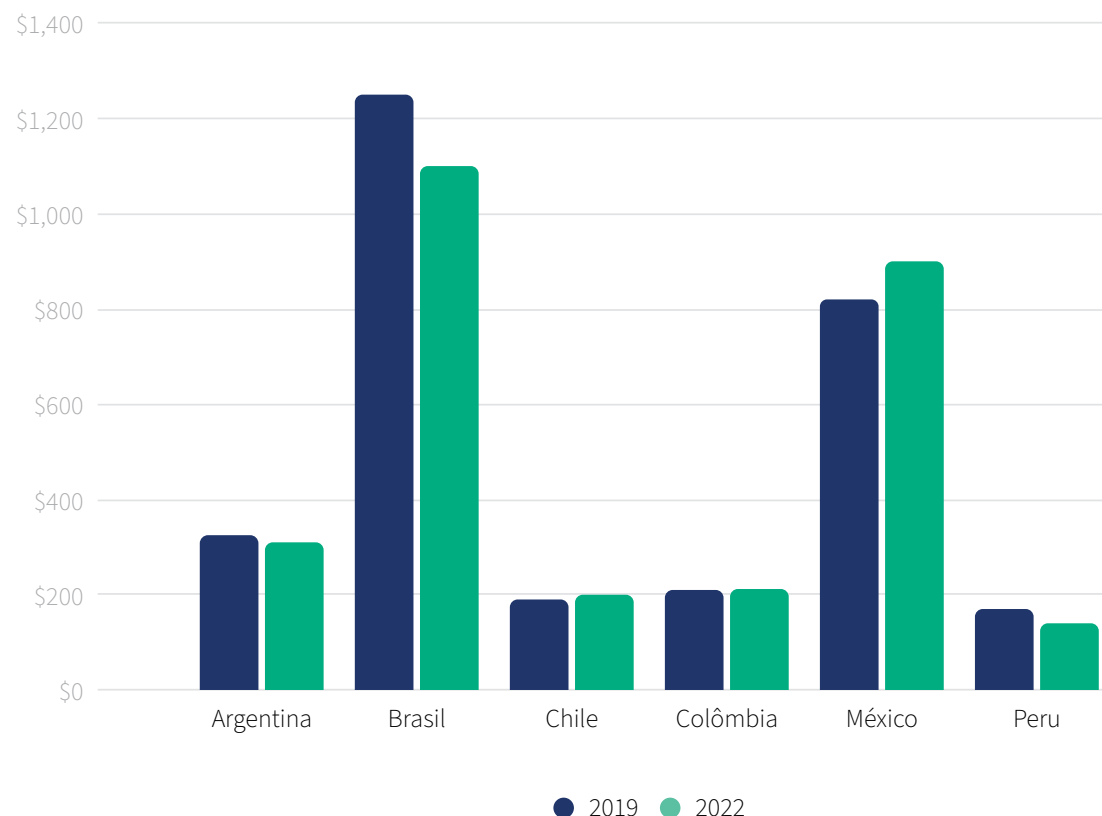
Crescimento do PIB em 2021

**3%**

Previsão de crescimento do PIB em 2022

Fonte: The World Bank

CONSUMO DAS FAMÍLIAS (MILHÕES USD)



# O físico perdeu espaço em definitivo para o digital

Recuperação do consumo das famílias + maior penetração de pagamentos eletrônicos = declínio do dinheiro físico



**US\$ 2,6 Trilhões**

Consumo das famílias em 2021 nos 6 principais mercados latino americanos

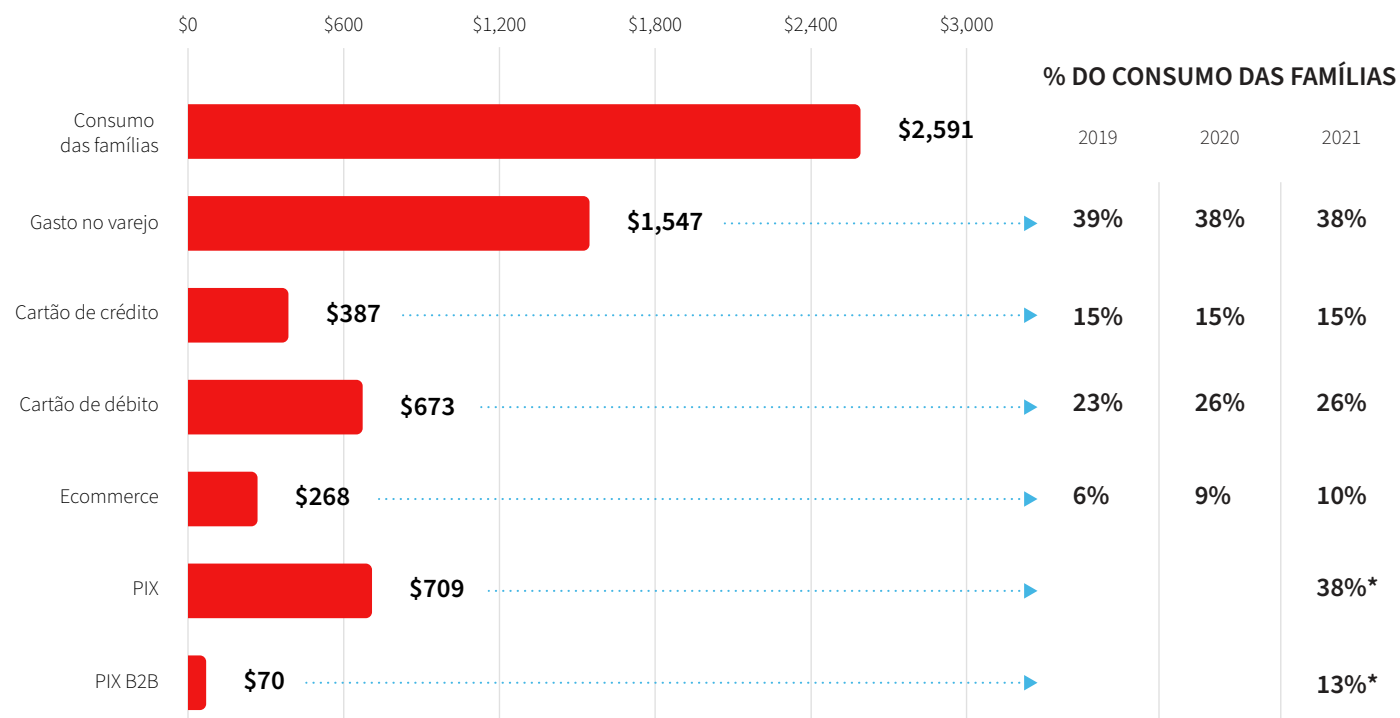


**12%**

de crescimento com relação a 2020

Argentina, Brasil, Chile, Colômbia, México, Peru

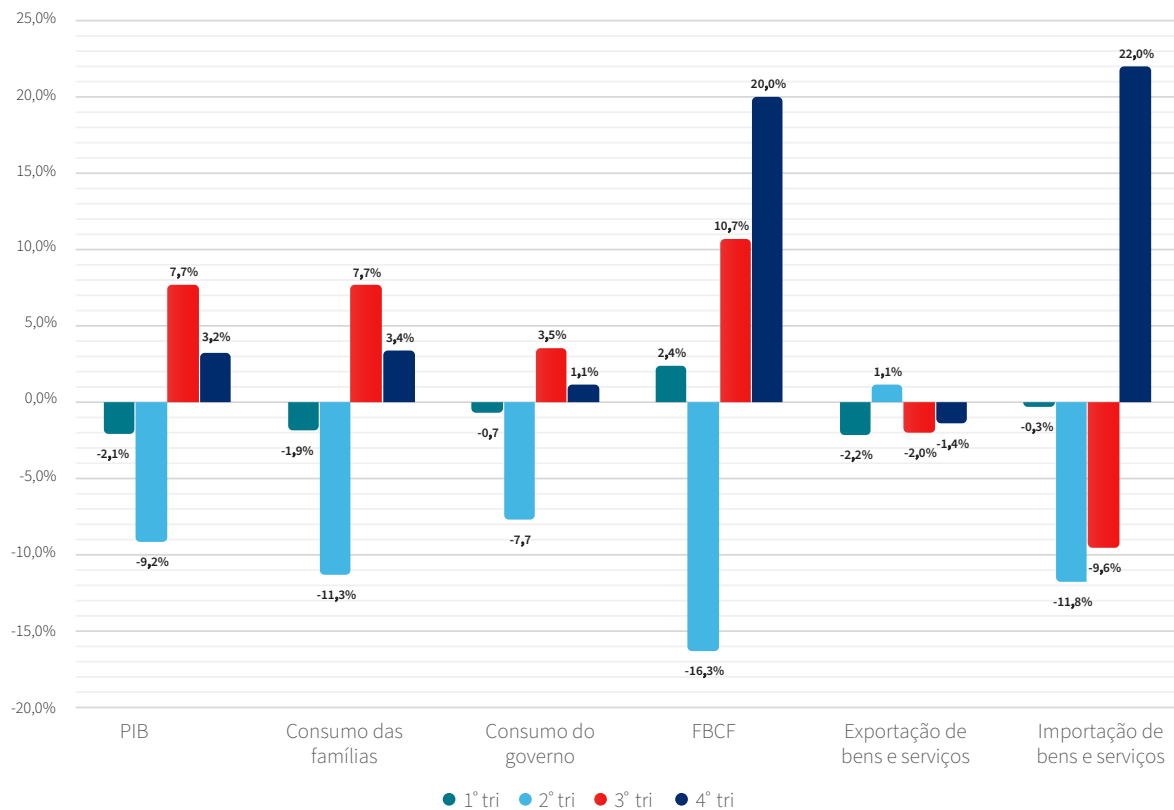
CONSUMO DAS FAMÍLIAS (Milhões)



\* Fonte: Banco Central do Brasil

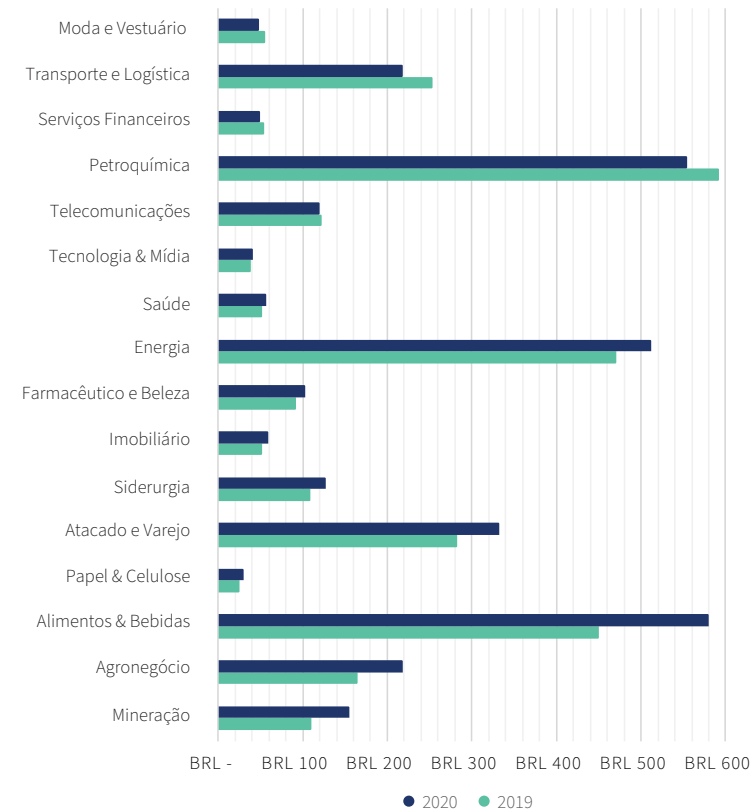
# Componentes da demanda sazonalizada

Taxa do trimestre em relação ao trimestre imediatamente anterior – 2020



Fonte: IBGE

EVOLUÇÃO DA RECEITA POR SETOR (MILHARES BRL)



Fonte: IBGE

# Impacto da pandemia no ambiente digital



**14 MILHÕES**

de brasileiros abriram uma conta bancária pela primeira vez em 2020



**96% DA POPULAÇÃO**

acima de 15 anos possui pelo menos uma conta bancária aberta



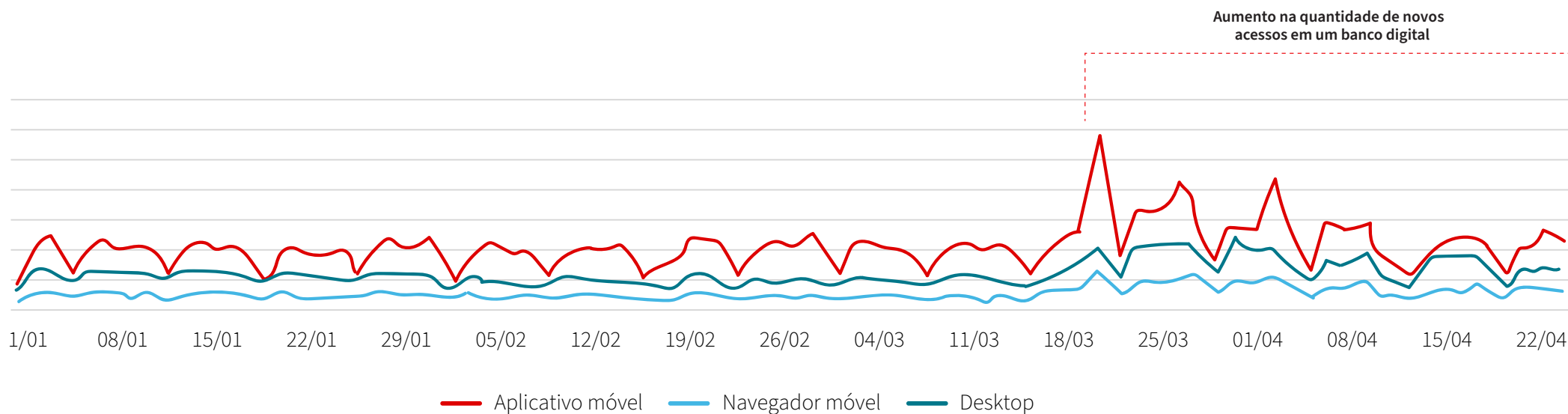
**342 MILHÕES**

de dispositivos portáteis no Brasil ao final de 2021



**1,6 MILHÕES**

dispositivos portáteis por habitante, em média, no Brasil. Considerando Smartphones, Tablets e Notebooks



Fonte: LexisNexis Risk Solutions, Banco Central do Brasil e EESP – FGV

# Padrões de transações em números

## TRANSAÇÕES



LATAM

**+473% ▲**

Volume de transações ano a ano

**+138% ▲**

Ataques iniciados por humanos ano a ano

**+455% ▲**

Volume de bots ano a ano



TRANSAÇÕES PROCESSADAS

**5B**

**+473% ▲**  
Crescimento ano a ano

TRANSAÇÕES POR CANAL

Desktop / Móvel



**11%**



**89%**

Navegador móvel / Aplicativo móvel



**7%**



**93%**

## ATAQUES



ATAQUES INICIADOS POR HUMANOS

Crescimento ano a ano

**+138% ▲**

ATAQUES INICIADOS POR HUMANOS POR CANAL

Desktop / Móvel



**28%**



**72%**

Percentual de ataques iniciados em dispositivos móveis **diminuiu ano a ano**

**-5% ▼**



ATAQUES INICIADOS POR BOTS

Crescimento ano a ano

**+455% ▲**

Fonte: Relatório de crimes cibernéticos da LexisNexis® Risk Solutions



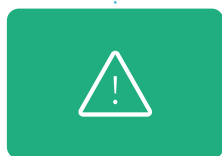
# Transações com base em identidades digitais

Ataques baseados em contas são ainda mais lucrativos para fraudadores do que fraude baseada em transações



## 7 em cada 10

Transações vem de um dispositivo móvel



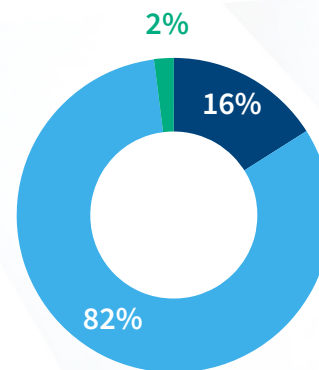
## Ataques

Focados em criação de novas contas continuarão em alta

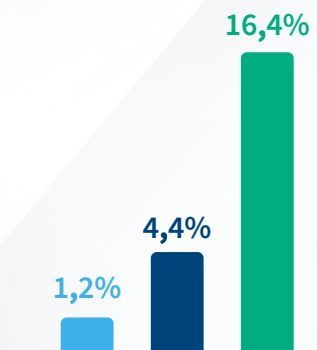


## Logins

Continuarão a ser o tipo de transação proeminente em todos os segmentos digitais, tanto para mobile quanto para web



VOLUME POR TIPO DE TRANSAÇÃO



TAXA DE ATAQUE POR TIPO DE TRANSAÇÃO

● Logins de contas ● Pagamentos ● Novas criações de contas

A taxa de ataque é baseada na porcentagem de transações identificadas como de alto risco e classificadas como ataques, por caso de uso. Eventos identificados como ataques como normalmente bloqueados ou rejeitados automaticamente e em tempo real, dependendo dos casos de uso de cada cliente.

TAXA DE CRESCIMENTO DE ATAQUES EM APPS MOBILE



**4%**  
ano após ano



**144%**  
nos últimos 6 meses

Fonte: Relatório de crimes cibernéticos da LexisNexis® Risk Solutions

# O crescimento dos bancos virtuais

Analizando a mudança no comportamento dos usuários em bancos tradicionais e virtuais

Os bancos virtuais oferecem todos os produtos e serviços online e não possuem rede de agências.

Às vezes, são submarcas de bancos tradicionais, mas geralmente operam de forma completamente independente do modelo bancário tradicional.

Eles estão ajudando cada vez mais a facilitar a inclusão financeira da população não bancarizada e sub-bancarizada em economias de países emergentes, já que muitos priorizam aplicativos móveis em vez de transações de navegador.

Fonte: Relatório de crimes cibernéticos da LexisNexis® Risk Solutions

## CRESCIMENTO NO VOLUME DE TRANSAÇÕES ANO APÓS ANO



**37%**

Bancos Tradicionais

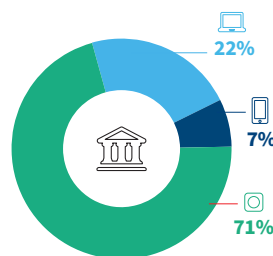


**68%**

Bancos Virtuais

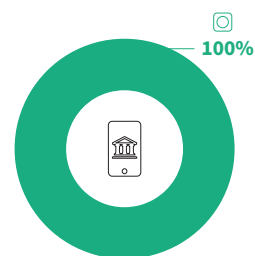
## PREFERÊNCIA DE CANAL

● Aplicativo móvel ● Desktop ● Navegador móvel



**Bancos Tradicionais**

Mix de transações mobile e desktop

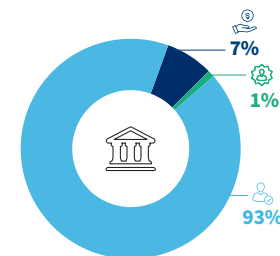


**Bancos Virtuais**

Transações majoritariamente de apps mobile

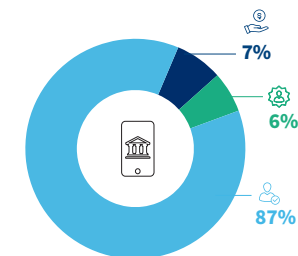
## PERFIL DE TRANSAÇÃO

● Logins de contas ● Pagamentos ● Novas criações de contas



**Bancos Tradicionais**

Menor percentual de criação de conta



**Bancos Virtuais**

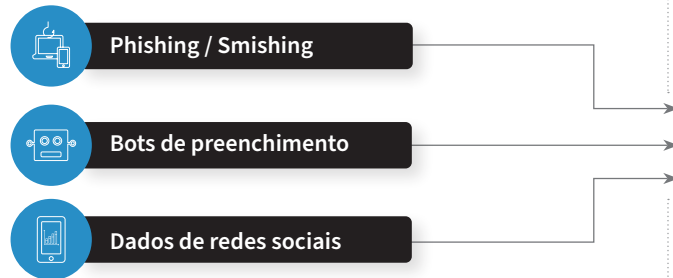
Maior proporção de criação de novas contas, com os usuários que estão migrando para o digital

# A jornada típica do fraudador

Dividir o processo de fraude em três estágios fornece oportunidades para mitigar o risco

Os últimos 12 meses viram diversas tipologias de fraude crescendo em um cenário de pandemia, com governos, instituições financeiras e cidadãos em todo o mundo procurando por soluções.

## COLETA DE INFORMAÇÕES

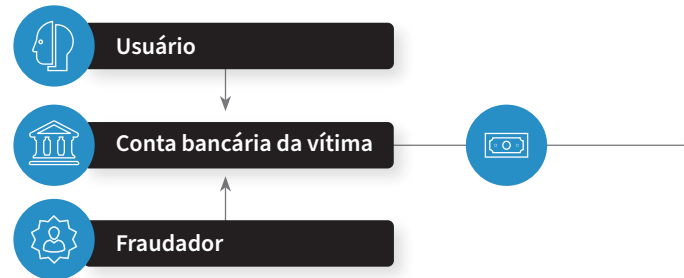


Credenciais de usuários e informações pessoais são roubadas e posteriormente negociadas na dark web. Ataques de phishing e engenharia social voltaram a ganhar força em 2021.

A educação é fundamental, especialmente para novos usuários digitais, para garantir que eles estão cientes dos riscos de clicar em links em e-mails e SMSs.

Fonte: Relatório de crimes cibernéticos da LexisNexis® Risk Solutions

## ACESSO À CONTA



Milhões de transações acontecem diariamente em todo o mundo. Com esse volume é difícil encontrar uma anomalia que identifica um acesso indevido a uma determinada conta.

A chave aqui são os dados – a capacidade de entender os padrões de acesso e comportamento legítimo em combinação com a inteligência artificial que cria links entre dispositivo, localização de acesso e padrões de comportamento em tempo real através de toda a jornada do usuário e não apenas durante seu login.

## JACKPOT



Uma vez que o dinheiro tenha sido transferido de um banco a outro, ou mesmo para outro país, é muito difícil recuperá-lo.

Uma solução robusta de prevenção a fraudes necessita um enfoque pró-ativo para prevenir contas e redes mula.

Uma associação de ferramentas baseadas em modelos analíticos em tempo real com ferramentas de inteligência artificial e uma abordagem colaborativa por meio de consórcios permitirá uma defesa contra essas redes.

# A jornada típica do fraudador

Fraude através da nossa rede a partir de uma única identidade digital

Embora a **Rede de Identidades Digitais** possa revelar a natureza global das redes de fraude, ela é igualmente poderosa para destacar o **comportamento típico** de fraudadores individuais.

## 237%

crescimento de ataques de reset de senha

### DIVISÃO DE ATAQUES POR ORIGEM

Desktop / Móvel








Percentual de ataques com origem em Mobile **creceu** 6% ano após ano



Fonte: Relatório de crimes cibernéticos da LexisNexis® Risk Solutions

# Principais riscos através dos pontos de interação










Risco vem aumentando em todos os principais casos de uso

	 <b>CRIAÇÃO DE NOVAS CONTAS</b>	 <b>LOGINS</b>	 <b>PAGAMENTOS</b>
<b>TENDÊNCIAS DE RISCO</b>	<p>O crescimento no volume de criação de novas contas continua a desacelerar após um crescimento significativo após o início da pandemia.</p> <p>Volumes de ataques automatizados focados em criação de novas contas cresceram 77%.</p>	<p>Consumidores estão acessando uma gama de serviços digitais no pós-pandemia, com logins crescendo 51% ano a ano.</p> <p>Fraudadores continuam a migrar suas atenções para o roubo de contas, com o ataque via apps mobile crescendo 138%, enquanto a taxa geral de ataques cresceu 24%.</p>	<p>Fraudes no pagamento permitem que fraudadores monetizem o ataque sacando rapidamente o produto do roubo.</p> <p>Os ataques focados em pagamentos em apps mobile cresceram 57% ano a ano, enquanto a taxa geral cresceu 8%.</p>
<b>TAXAS DE ATAQUE</b>			
 <b>GERAL</b>	9,0%	0,5%	3,2%
 <b>DESKTOP</b>	<b>13,3%</b>	<b>1,0%</b>	<b>3,7%</b>
 <b>NAVEGADOR MÓVEL</b>	9,3%	0,6%	3,4%
 <b>APLICATIVO MÓVEL</b>	3,0%	0,3%	2,6%

Fonte: Relatório de crimes cibernéticos da LexisNexis® Risk Solutions

# Principais riscos através dos pontos de interação

Risco vem aumentando em todos os principais casos de uso

	 <b>RESETS DE SENHA</b>	 <b>MUDANÇAS DE DETALHES</b>	 <b>LISTAS DE ANÚNCIOS</b>	 <b>TRANSFERÊNCIAS</b>	 <b>OUTRO</b>
<b>TENDÊNCIAS DE RISCO</b>	<p>Os resets de senha são o ponto de interação de maior risco pela primeira vez, com as taxas de ataque aumentando acentuadamente no aplicativo móvel e no desktop.</p> <p>Controles fracos de reset de senha podem permitir que um fraudador obtenha acesso rapidamente e bloqueie a vítima de sua conta, permitindo que o fraudador retire dinheiro ou faça compras.</p>	<p>Os fraudadores alteram endereços de e-mail e números de celular para um que eles controlam para contornar métodos de segurança, como uma senha de uso único SMS (OTP).</p> <p>As taxas de ataque em alteração de dados cadastrais diminuíram significativamente em relação ao ano anterior.</p>	<p>As listagens de anúncios permitem que os fraudadores controlem a venda ou promoção de bens e serviços. Isso pode fornecer uma forma de monetizar bens roubados, publicar anúncios falsos de propriedades ou serviços ou criar avaliações falsas para facilitar as vendas.</p> <p>As taxas de ataque permaneceram relativamente estáveis ano após ano.</p>	<p>As transferências permitem que o dinheiro seja movido para uma conta diferente dentro do perfil geral de um cliente. Essa ação às vezes precede um evento de pagamento fraudulento após uma aquisição de conta.</p> <p>As taxas de ataque associadas a transferências caíram significativamente em relação ao ano anterior.</p>	<p>Abrangendo vários outros pontos de contato de alto risco, como registro de novos canais, mandatos de ordem permanente, débitos diretos e modificações de beneficiários.</p> <p>As taxas de ataque associadas a outros pontos de contato caíram significativamente em relação ao ano anterior.</p>
<b>TAXAS DE ATAQUE</b>					
 <b>GERAL</b>	13,5%	14,7%	5,1%	0,4%	3,6%
 <b>DESKTOP</b>	<b>25,6%</b>	6,6%	4,6%	0,2%	<b>7,4%</b>
 <b>NAVEGADOR MÓVEL</b>	2,9%	6,8%	<b>7,4%</b>	<b>0,7%</b>	5,7%
 <b>APLICATIVO MÓVEL</b>	12,2%	<b>18,7%</b>	4,9%	0,4%	2,5%

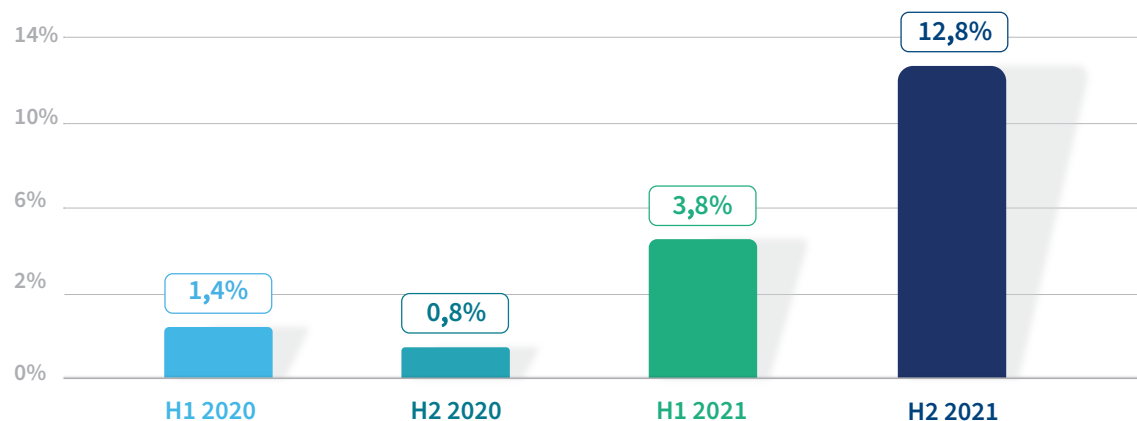
Fonte: Relatório de crimes cibernéticos da LexisNexis® Risk Solutions

# Reset de senhas – um novo ponto focal de fraudes

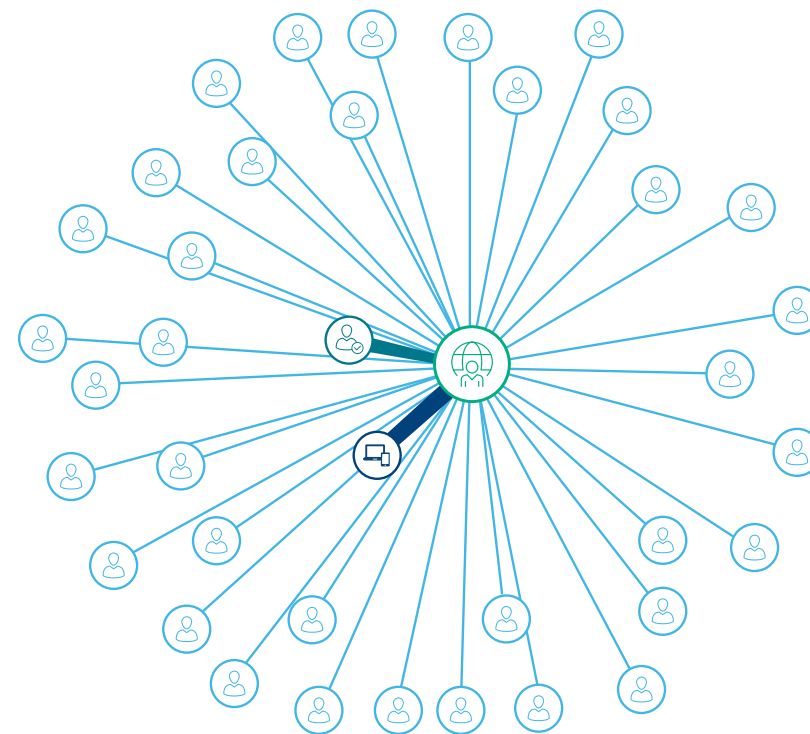
Taxas de ataque saltam a medida que as cotas digitais estão sob ataque

Uma única identidade digital LexID® indica uma origem de resets de senha atacando várias contas. Todos os eventos chegaram via um proxy anônimo, com a identidade simulando estar no Brasil, enquanto estava realmente localizada na China.

TAXA DE ATAQUES DE RESET DE SENHA



Fonte: Relatório de crimes cibernéticos da LexisNexis® Risk Solutions



LexID Digital



ID de dispositivo



Logins de contas










Nome da conta

# Visão geral da indústria financeira

## Overview das taxas e padrões de ataque

### OVERVIEW DA INDÚSTRIA FINANCEIRA

	 CRIAÇÃO DE CONTAS	 LOGINS	 PAGAMENTOS
<b>TENDÊNCIA DE RISCOS</b>	A criação de contas viu o maior crescimento de ataques, 73% ano a ano, com fraudadores focando no onboarding em bancos digitais.	O roubo de contas geralmente tem uma participação pequena considerando o total de logins válidos.  Apesar disso, o volume cresceu 48% ano a ano.	As taxas de ataques aos pagamentos em serviços financeiros são geralmente as maiores em todas as indústrias analisadas. Ataques cresceram 400% ano a ano.
<b>TAXAS DE ATAQUE</b>			
 GERAL	3,0%	1,2%	6,7%
 DESKTOP	4,4%	<b>3,9%</b>	6,8%
 NAVEGADOR MÓVEL	<b>5,2%</b>	0,7%	4,8%
 APLICATIVO MÓVEL	2,7%	1,0%	<b>8,7%</b>

Fonte: Relatório de crimes cibernéticos da  
LexisNexis® Risk Solutions





# Percepção de risco entre os gestores antifraude

Desafios que serão enfrentados pelos gestores nos próximos 24 meses

## DESAFIOS DAS FRAUDES NOS CANAIS DIGITAIS

% classificados entre os 3 principais

	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%

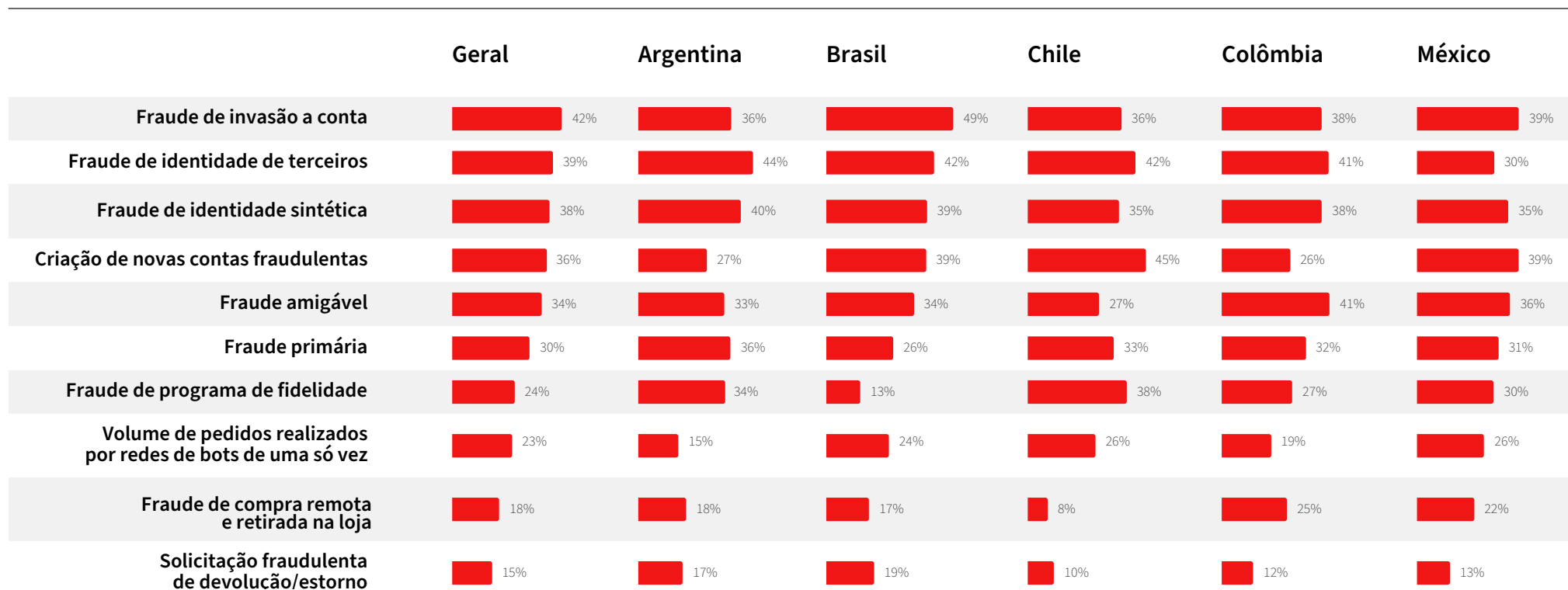
Fonte: LexisNexis® Risk Solutions  
True Cost of Fraud 2021

# Percepção de risco entre os gestores antifraude

Principais ameaças de fraudes nos canais digitais para os próximos 24 meses

## PRINCIPAIS AMEAÇAS ESPERADAS DE FRAUDES (PRÓXIMOS 24 MESES)

*% classificados entre os 3 principais*



Fonte: LexisNexis® Risk Solutions  
True Cost of Fraud 2021



### **Para mais informações**

[risk.lexisnexis.com/fraudes](http://risk.lexisnexis.com/fraudes)

### **Relatório sobre crimes cibernéticos da LexisNexis**

[risk.lexisnexis.com.br/insights-resources/research/cybercrime-report](http://risk.lexisnexis.com.br/insights-resources/research/cybercrime-report)

### **LexisNexis® ThreatMetrix®**

[risk.lexisnexis.com.br/threatmetrix](http://risk.lexisnexis.com.br/threatmetrix)

### **Sobre a LexisNexis® Risk Solutions**

A LexisNexis® Risk Solutions explora o poder dos dados e da análise avançada para fornecer informações a empresas e entidades governamentais com a finalidade de reduzir riscos e auxiliar na tomada de decisões que beneficiem pessoas ao redor do mundo. Fornecemos soluções de dados e tecnologia para uma ampla gama de setores, incluindo seguros, serviços financeiros, assistência médica e governo. Com sede na área metropolitana de Atlanta, Geórgia, temos escritórios em todo o mundo e fazemos parte da RELX (LSE: REL/NYSE: RELX), uma fornecedora global de análises baseadas em informação e ferramentas para tomada de decisões voltada para profissionais e empresas. Para maiores informações, acesse [www.risk.lexisnexis.com](http://www.risk.lexisnexis.com) e [www.relx.com](http://www.relx.com). Nossas soluções ajudam as organizações a prevenir crimes financeiros, assegurar o compliance regulatório, mitigar riscos empresariais, melhorar a eficiência operacional e aumentar a rentabilidade. Este documento é meramente informativo e não garante a funcionalidade de nenhum dos produtos identificados pela LexisNexis® Risk Solutions. A LexisNexis® Risk Solutions não garante que este documento esteja completo ou livre de erros. A LexisNexis e a logomarca Knowledge Burst são marcas registradas da RELX Inc. Outros produtos e serviços podem ser marcas comerciais ou registradas de suas respectivas empresas. Copyright© 2022 LexisNexis® Risk Solutions Group.

NXR15688-00-0922-PT-LA

**Para mais informações, visite [risk.lexisnexis.com.br](http://risk.lexisnexis.com.br), e [relx.com](http://relx.com)**