A identidade mobile do futuro

# Métodos de autenticação e recuperação de senhas na jornada do usuário

idwall INCOGNIA™

A porta, a chave, a senha, a foto dos seus documentos e, por fim, você: **seu rosto, digitais, íris, gestos e comportamento.** Todos esses elementos têm um denominador comum: **eles podem servir como meios de acesso a informações pessoais, processos e transações.**

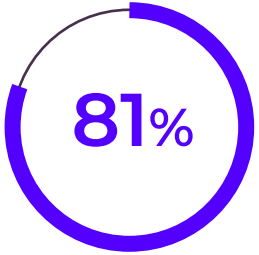
Ou seja, são meios de autenticação de identidade, procedimento essencial para qualquer empresa da atualidade.

Afinal, a digitalização do cotidiano trouxe inúmeras facilidades e possibilidades, mas também abriu caminho para práticas fraudulentas. De um lado **estão as empresas visando não dificultar os processos para usuários legítimos; do outro, o cliente final que exige uma experiência sem fricção em toda a sua jornada**.

Nesse contexto, muitos dos métodos tradicionais de autenticação de identidade não são mais tão efetivos, mesmo quando combinados em um fluxo de verificação em várias etapas. Por outro lado, os avanços da tecnologia mobile oferecem **novas possibilidades e uma otimização do custo-benefício**.

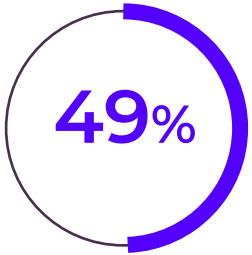
Este relatório traz dados do contexto de adoção de diferentes tecnologias de autenticação de identidade, além de apresentar as tendências de mercado e soluções de ponta que estão liderando um futuro mais tecnológico e prático.

# Contexto atual




dos vazamentos de dados de empresas acontece **devido a senhas inadequadas**

Globalmente, espera-se que até 2025 **95% dos smartphones tenham capacidades de leitura biométrica**, tecnologia considerada pelos usuários **3 vezes mais segura** do que senhas em processos de autenticação.




dos brasileiros acreditam que uma das maiores vantagens da biometria é a **diminuição da necessidade de gerar diversas senhas diferentes para se cadastrar em aplicativos, utilizar serviços mobile e fazer compras.**

Segundo pesquisa da Juniper Research, até 2024 é esperado que **soluções de reconhecimento facial em software estejam integradas em 1,3 bilhões de devices**.


As oportunidades de usos das tecnologias de biometria são muitas e ultrapassam seu uso habitual em procedimentos de cadastro de usuários.. Elas podem ser utilizadas **sempre que o usuário precisar ser identificado e/ autenticado**, ou seja, nos dois momentos essenciais da jornada do cliente — o que inclui login, troca de senhas e recuperação de conta.

**Em nossos testes do processo de recuperação de conta:**

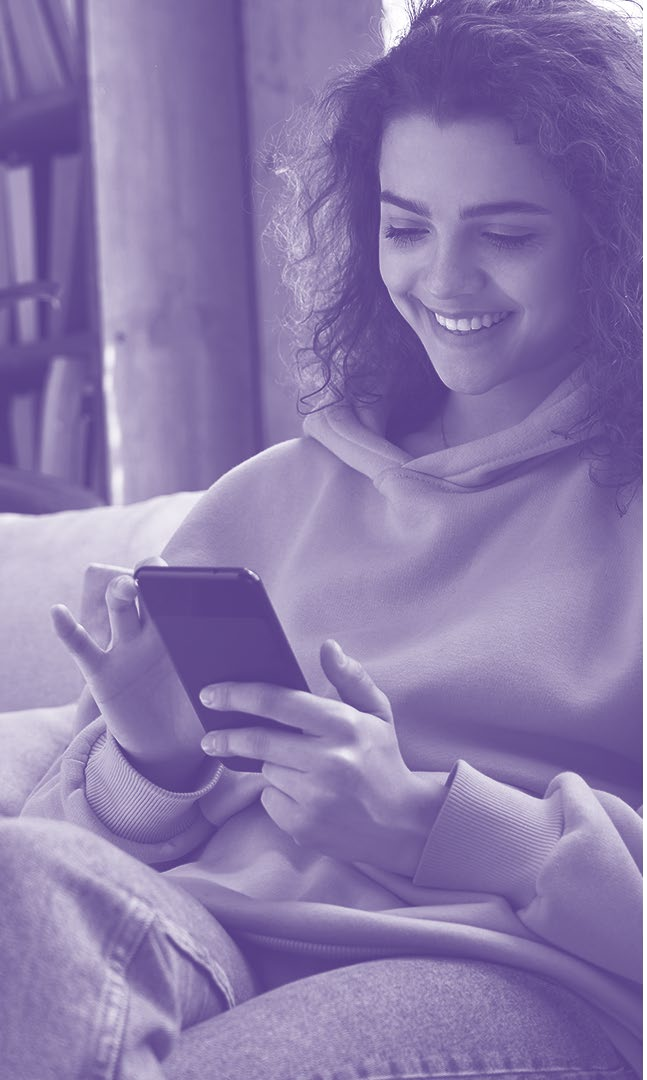
**50%**

**das instituições financeiras analisadas utilizam 2 fatores de autenticação** e 40% utilizam 3 fatores ou mais.

**Dentre os bancos analisados que não são nativos digitais** observamos que eles não utilizam a autenticação do usuário pelo que o indivíduo tem (por exemplo, uma senha de uso único), é ou faz, e sim por métodos de conhecimento.

**Todos os apps de marketplace avaliados possibilitam a recuperação de conta por uma senha de uso único (OTP),** enquanto a maioria dos apps de delivery não aplica essa possibilidade.

Fontes: Verizon 2019 Data Breach Investigations Report, Juniper Research 2021, LastPass 2020,



## Tudo em apenas um clique



Atualmente cerca de **3,8 bilhões de pessoas possuem smartphones, o que representa 49% da população mundial**. Esse número aumentou em **40%** desde 2016.[1] Até 2023, só o número de devices mobile deve chegar a **7,33 bilhões** de pessoas, **92%** da população mundial.[2]

A expansão dos dispositivos móveis transformou quase todos os aspectos de nossas vidas, tanto profissionais quanto pessoais. A possibilidade de acessar praticamente tudo com apenas alguns cliques possibilitou a inclusão digital de milhões de pessoas em relação a serviços financeiros, bens de consumo, informação ou educação.

Só no Brasil, segundo dados do TIC Domicílios, 74% da população tem acesso à internet e **58% das pessoas acessam a internet exclusivamente pelo celular**. Globalmente, até 2025, cerca de **72% de todos os usuários da internet devem acessar a rede somente via mobile**.

Fontes:
bankmycell.com, Statista, DataReportal 2021 e TIC Domicílios 2019, Fundação Alemã para a População Mundial (DSW)/ DW 2019.
[1] Estimativas da ONU indicam que a população atual é de 7,8 bilhões de pessoas.
[2] Segundo dados de 2019 da Fundação Alemã para a População Mundial (DSW), a população do mundo em 2023 será de 8 bilhões de pessoas.

# Tudo em apenas um clique



**Número de usuários de smartphones**
(em bilhões)


Share de tráfego na internet de **Mobile por ano**


Fontes:
bankmycell.com, Statista, DataReportal
* os números de share de tráfego na internet de mobile representam a participação de smartphones para navegadores da web e não incluem dados para outras atividades conectadas (como o uso de aplicativos móveis nativos).

# A força do mobile está na praticidade

Apps de chat, compras e entretenimento são os que mais **se destacam no uso mensal** entre os principais usuários da internet*

**91%** Chat apps

**67%** Apps de entretenimento e vídeo

**39%** Apps de serviços financeiros

**53%** Apps de música

**70%** Apps de shopping

**11%** Relacionamentos

**52%** Apps de games

**29%** Apps de saúde e fitness

**A praticidade está no centro dos principais apps utilizados em smartphones. Entretanto, à medida que os pontos de contato entre empresas e pessoas aumentam, também cresce, a possibilidade de acontecerem interferências indesejadas.**

Nesse contexto digital, pessoas mal intencionadas com acesso a dados pessoais podem conseguir abrir contas bancárias falsas, realizar transações financeiras indevidas e ter acesso a inúmeros serviços. **Com cada vez mais vazamentos de dados massivos acontecendo, principalmente no Brasil, aumenta o volume de informações pessoais que podem cair nas mãos de fraudadores**. Para as empresas, **os usos fraudulentos de dados podem resultar em perdas milionárias**.

Segundo relatório da Axur, houve um **aumento de 815% no vazamento de credenciais de empresas** no primeiro trimestre de 2021 em relação ao mesmo período do ano passado. Para credenciais do gov.br o aumento foi de **530%**.

**E, de acordo com dados da Verizon**, uma empresa média sofre quase um milhão de tentativas de ataques de credential stuffing todos os anos — ou seja, a utilização de listas de credenciais comprometidas com o objetivo de invadir um sistema.

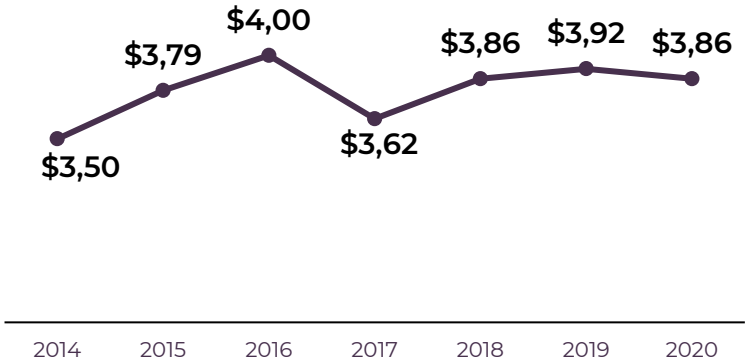
Fontes: DataReportal 2021, Verizon 2020 Data Breach Investigations Report, Axur Q1 2021.
*Indivíduos de 16 a 64 anos

Segundo relatório da IBM em parceria com o Ponemon Institute, **vazamentos de dados geraram um prejuízo total médio de US$ 3,86 milhões somente em 2020**.

**Os setores da saúde, energia e financeiro foram os que sofreram os maiores prejuízos,** estando cerca de 85%, 65,5% e 51% maiores do que a média global, respectivamente.

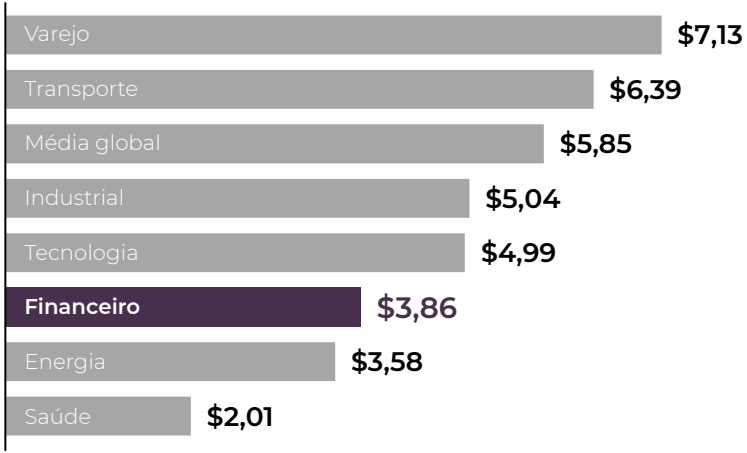
### Prejuízo total médio de um vazamento de dados

Medido em milhões de dólares (US$)




### Prejuízo total médio de um vazamento de dados por setor

Medido em milhões de dólares (US$)




Fontes: IBM e Ponemon Institute



Fraudes ainda
são um **problema bilionário**

**1 em cada**
**5 brasileiros**
já foi vítima de
roubo de identidade
na internet,

o que representa **24,2 milhões** de potenciais vítimas em todo o país.

Entre os dados
**mais fraudados:**

**51,3%**
**Telefone**

**44,3%**
**Credenciais de redes sociais**

**37,1%**
**Credenciais de e-mail**

**26,8%**
**CPF**

**19,3%**
**Cartão de crédito**

Fonte: Psafe, TCU, Javelin, Serasa

Para entender as melhores estratégias de prevenção contra esses riscos, **é necessário entender em quais momentos da jornada do cliente é possível que uma fraude ocorra**.

Para isso, é importante pensar no gerenciamento do ciclo de vida da identidade do usuário, que é constituído por duas fases obrigatórias:

1. **Prova de identidade:** responde à pergunta "quem é você" e conta com os processos de coleta, validação e verificação de informações. É equivalente ao processo de cadastro/onboarding.

2. **Autenticação do usuário:** responde à pergunta "você é quem diz ser?" e conta tradicionalmente com três tipos de categorias de prova:

> **Algo que o usuário sabe:** é tudo aquilo que depende do conhecimento do indivíduo, como senhas, respostas a perguntas pré-selecionadas e PINs;

> **Algo que o usuário tem:** depende da posse de uma conta ou podem ser senhas criptografadas em hardware, senhas de uso único (OTPs) acessadas por aplicativos ou outros dispositivos;

> **Algo que o usuário é ou faz:** se relaciona a suas características físicas (biometria física) e comportamentais (biometria comportamental), como reconhecimento de biometria facial, digital, de voz, além de padrões de localização e de navegação em aplicativos.

**Fator conhecimento**

Algo que o usuário **sabe**


**Fator posse**

Algo que o usuário **tem**

**Fator físico**

Algo que o usuário **é ou faz**

Fontes: Financial Task Force (FATF) 2020

# Processos de autenticação

Os processos de autenticação de identidade são categorizados de acordo com a quantidade de fatores de autenticação utilizados: quanto mais processos forem aplicados, maior o grau de segurança para o usuário e a empresa.

Entretanto, é cada vez mais comum fazer a classificação com base nos efeitos da aplicação dos fatores: em vez de contabilizar o número de fatores, a característica central passa ser o **quão resistente o processo é a ataques comuns**, como phishing ou man-in-the-middle.

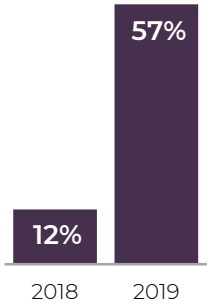
**Os processos mais recorrentes no mercado atual são:**

**Autenticação de um único fator (1FA):** usa somente um fator de autenticação. Por exemplo, solicita somente a senha para conceder acesso a uma conta.

**Autenticação Multi-Fator (MFA):** usa dois ou mais fatores de autenticação de ao menos duas categorias diferentes (o que se sabe, tem e é). Assim, a perda ou roubo de um dos fatores não atrapalha a confiabilidade do outro e não garante acesso à conta.

Um exemplo seria a utilização de uma **senha combinada com o recebimento de um código de acesso por e-mail ou SMS**, ou de uma validação de Face Match.

**Uso de MFA pelas empresas**




Uma pesquisa global feita pelo LastPass mostra que, em 2019, **57% das empresas usavam autenticação multifator** — um aumento de quase 5 vezes em relação ao ano anterior.

Esse relatório também destacou o fato de que pelo menos **62% das organizações já usavam tecnologias de autenticação biométrica**.

Enquanto isso, pesquisas de 2020 mostraram que **19% dos usuários não sabiam dizer o que era autenticação multifator. 54%** declararam usar esse recurso em contas pessoais, enquanto **37%** afirmaram usar nas contas do trabalho.

Fontes: Financial Task Force (FATF) 2020, LastPass 2019 (B2B) e 2020 (B2C).

## Autenticação no ambiente mobile



Há diversas tecnologias disponíveis para autenticação em dispositivos móveis, dentre os três tipos de fatores de autenticação apresentados anteriormente. O fator mais comumente utilizado ainda é a senha, mesmo que sua baixa efetividade e segurança já tenha sido comprovada.

Segundo um estudo global realizado em 2019 pela Verizon, **81% dos vazamentos de dados de empresas acontece devido a senhas inadequadas**.

Opções como a utilização de senhas de uso único (OTPs) enviadas via SMS ou e-mail, tokens e aplicativos de autenticação são outras possibilidades, mas que também oferecem diferentes riscos.

O entendimento dessas e de outras tecnologias, como a biometria biofísica ou comportamental, viabilizam a compreensão desse ecossistema de forma detalhada para a adoção das soluções mais seguras e com maior custo-benefício possível, ao passo que inova processos e a sociedade como um todo.

**A seguir, apresentamos uma análise qualitativa dos prós e contras das principais tecnologias utilizadas em processos de autenticação mobile**.

# Senhas

A senha é o modelo mais tradicional de autenticação — e também um dos mais fracos, já que o nível de segurança da senha depende de cada usuário. Além disso, as senhas estão entre os dados mais frequentemente vazados, ou seja, dos mais fáceis de serem obtidos por fraudadores.

Para fortalecer a segurança desse tipo de autenticação, é preciso adotar senhas altamente complexas (e nada práticas). Em muitos processos, a senha é combinada com outro fator de autenticação.

Em 2016, **estimava-se que uma senha era roubada a cada segundo** . No primeiro trimestre de 2021 só no Brasil foram cerca de **291 credenciais vazadas por segundo**.*

## Prós

Senhas são muito simples de serem usadas, uma vez que basta o indivíduo lembrar ou ter acesso às respostas de desbloqueio.

## Contras

É recomendado que as senhas sejam mudadas regularmente, o que atrapalha a memorização. Além disso, muitos usuários não alteram a senha com frequência.

Dado o número médio de senhas que uma pessoa possui e a necessidade de uma maior complexidade para aumentar a segurança, a praticidade das senhas passa a ser baixa.

As respostas de desbloqueio e senhas podem ser facilmente adivinhadas, roubadas ou esquecidas.

Em junho de 2021, aconteceu o que se estima ser o maior **vazamento de senhas** da história — **8,4 bilhões de senhas foram expostas, número maior do que o de pessoas na Terra**.

**53%**

Não alteraram suas senhas nos últimos 12 meses, mesmo após ouvirem falar de casos de vazamento de dados nas notícias.

**42%**

Afirmaram que ter uma senha fácil de lembrar é mais importante do que ter uma senha segura.

**1 - 20**

Quantas contas online as pessoas acham que têm

**66%**

... Mesmo assim, ao criar senhas, 66% dos participantes sempre ou quase sempre usam a mesma senha ou variações de uma senha

**Quantas contas online as pessoas têm em média**

**≈38**

Fonte: Cybersecurity Ventures, "Psicologia das senhas" de LastPass 2020 e CNN Brasil.
* Número calculado com base no valor total de credenciais vazadas reportado pelo Relatório Q1 de 2021 da Axur.

# Senha de uso único (OTP)

A senha de uso único, ou one-time password (OTP), é **um tipo de token usado para autenticar o usuário somente uma vez**. Nesse caso, é necessário que a pessoa tenha acesso a algo que ela possua, como o celular ou aplicativo, para receber o código ou link via SMS, e-mail ou ligação.

## Prós

- Dificulta o ataque recorrente, uma vez que a o código ou link serve para somente uma tentativa;
- Utiliza meios que são de fácil acesso para o usuário se estiverem protegidos com somente um fator de autenticação, como SMS e e-mail.

## Contras

- O usuário pode não receber o código no momento necessário e acabar perdendo o tempo disponível para a autenticação;
- É uma tecnologia que está sujeita à segurança de outras contas — o cartão SIM pode ser fraudado, as contas de e-mail podem ser hackeadas e o celular pode ser perdido ou roubado.
- Muitas vezes, é necessário que o usuário saia do aplicativo principal para pegar o PIN recebido, o que pode ser um incômodo.
- Nos casos em que um app autenticador é usado, a conta pode acabar se dessincronizado do aplicativo principal.

## Segundo pesquisa da Opinion Box em parceria com a Mobile Time:

**18%**

dos entrevistados consideram o recebimento de token por SMS o meio mais difícil e desconfortável de autenticação, logo depois do escaneamento de íris, com **25%**.

**21%**

acham que esse método é o menos seguro, depois das senhas, com **26%**.

Fonte dos dados: OpinionBox e Mobile Time, 2020.

# Biometria

As tecnologias de biometria utilizam as características físicas e padrões comportamentais para identificar e autenticar o indivíduo. Existem **duas categorias de biometria**:

**Biometria física:**
é uma característica física da pessoa, como as digitais, a íris e a face;

**Biometria comportamental:**
diz respeito a padrões de comportamento do indivíduo, como a forma de segurar o telefone, padrões de localização, como a pessoa digita, etc. É comumente usada no processo de autenticação contínua, ou baseada em risco, e pode detectar anomalias de comportamento durante uma sessão.

Os tipos mais comuns de biometria são:

**Biofísica:**


Digital


Face


Voz


Íris

**Biomecânica:**


Comportamental


Localização

Além de ser universal, a biometria livra o usuário da necessidade de decorar algo ou de ter algo, o que torna o processo de autenticação mais prático e de baixa fricção.

**Há uma diferença importante entres as tecnologias de biometria integradas ao hardware dos smartphones e as habilitadas por software.**

No primeiro caso, o padrão de reconhecimento é armazenado no smartphone em um local protegido.

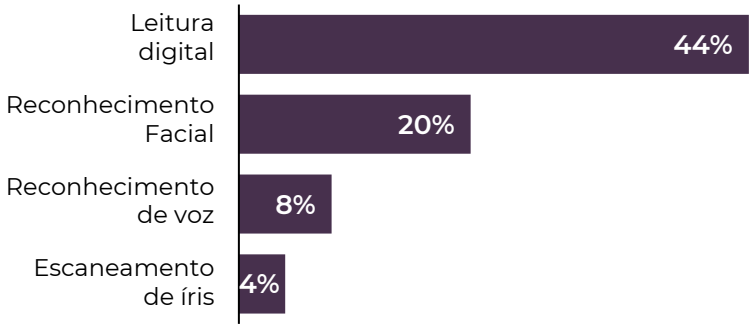
Já no segundo, a captura da biometria é enviada de forma criptografada para um servidor para que o padrão seja comparado a uma base de dados.

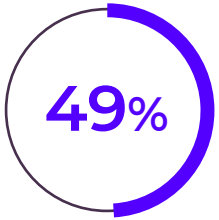
A biometria em hardware permite o bloqueio de acesso somente no dispositivo, enquanto a de software permite o bloqueio a contas em diversos dispositivos. As análises apresentadas neste estudo se concentram no último caso.

Segundo pesquisa realizada em 2021 pela Juniper Research, globalmente espera-se que, **até 2025, 95% dos smartphones tenham capacidade de leitura biométrica e que esse método seja responsável por cerca de US$3 trilhões em autenticação de pagamentos** — muito mais que os US$ 404 bilhões movimentados dessa forma em 2020.

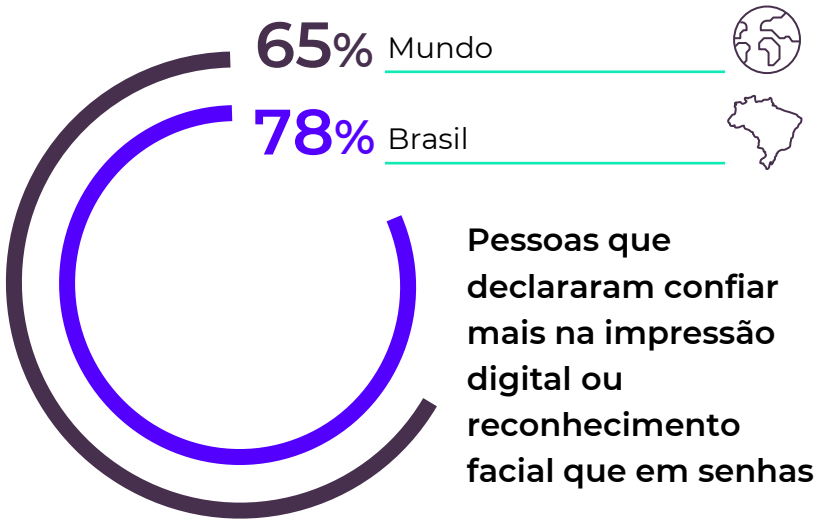
Em outra pesquisa, realizada  em vários países pelo LastPass, **65% das pessoas afirmam confiar mais na impressão digital ou no reconhecimento facial do que nas senhas em texto. No Brasil, esse valor salta para 78%.**

**Quais meios de autenticação biométrica o brasileiro já experimentou para acessar serviços digitais pelo smartphone**




dos brasileiros acreditam que uma das maiores vantagens da biometria é a **diminuição da necessidade de gerar diversas senhas diferentes** para se cadastrar em aplicativos, utilizar serviços mobile e fazer compras.




**Pessoas que declararam confiar mais na impressão digital ou reconhecimento facial que em senhas**

Fontes: Juniper Research 2021, LastPass 2020, OpinionBox e Mobile Time 2020, data2decisions/IDEMIA.

# Biometria Digital

A biometria digital é uma das tecnologias da categoria mais aceitas para a autenticação. Segundo pesquisa da Juniper Research, estima-se que **4,6 bilhões de smartphones serão equipados com sensores de impressão digital até 2024** em todo o mundo.
Nos smartphones há dois tipos de sensores usados: sensor capacitivo e o ultrassônico. O primeiro utiliza capacitores elétricos na identificação dos padrões das digitais, enquanto o segundo envia ondas ultrassônicas que são em parte devolvidas ao sensor, fazendo com que o sensor perceba variações mais detalhadas dos padrões digitais.

## Prós

- É uma tecnologia bem aceita pelo público. Somente 7% considera a biometria digital um meio difícil e desconfortável de autenticação em celulares;
- É fácil de usar, sendo necessário somente posicionar o dedo no sensor;
- Reproduzir a digital de uma pessoa por meio de impressoras 3D, identificação do padrão da digital, etc. - é muito mais complexa que a invasão de uma conta por senhas, por exemplo e, portanto, desencorajador.

## Contras

- Pode apresentar problemas quando os dedos estão molhados ou sujos e, também, por questões de acessibilidade de pessoas que não possuem digitais por alguma razão.

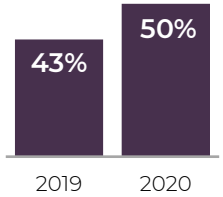
Em pesquisa global de 2019 da IDEMIA, na média global, **74%** dos entrevistados têm **uma percepção positiva sobre o uso de biometria digital**.

**No Brasil, esse percentual é de 90%,** ficando em segundo lugar entre os 11 mercados pesquisados, atrás apenas da Índia (94%).

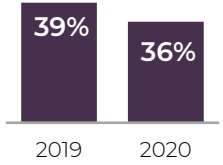

No Brasil, esse percentual fica em segundo lugar entre os **11 mercados pesquisados**, atrás apenas da **Índia (94%)**.


**tem interesse em usar a biometria digital em pagamentos**

**Desbloqueio do celular por digital**




**Método considerado mais seguro de autenticação**




Fonte dos dados: OpinionBox e Mobile Time, 2020.

# Reconhecimento facial

A biometria facial registra a geometria espacial de características distintas do rosto;  o uso do Face Match é recomendado em combinação ao **liveness (ou prova de vida)**.

A validação de liveness  é a capacidade de um sistema detectar se uma forma de biometria (como o rosto) é real ou falsa através da análise de imagens. Um rosto dado como real significa que uma pessoa está presente no momento de captura das imagens, ou seja, fisicamente diante do dispositivo. Em caso contrário, por exemplo,  se uma fotografia for usada, é dada como falsa.

## Prós

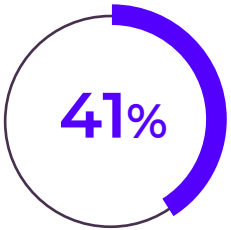
- A tecnologia é fácil de ser compreendida e, em muitos casos, só é necessário que o usuário siga instruções de posicionamento do rosto na câmera.
- Não há necessidade de decorar senhas, tokens ou PIN;
- Não é necessário instalar aplicativos adicionais
- Envolve um processo não intrusivo e sem contato
- Pode ser feito remotamente de qualquer lugar, a qualquer hora
- Não é necessário que o smartphone tenha um sensor especial, só uma câmera

## Contras

- Existem preocupações ligadas à  privacidade do usuário e sobre vieses de algoritmos de reconhecimento facial;
- O usuário pode ter dificuldade para tirar uma foto adequada, por isso é importante trazer instruções no processo;
- A qualidade da câmera do usuário pode atrapalhar na captação da imagem e a identificação do usuário.

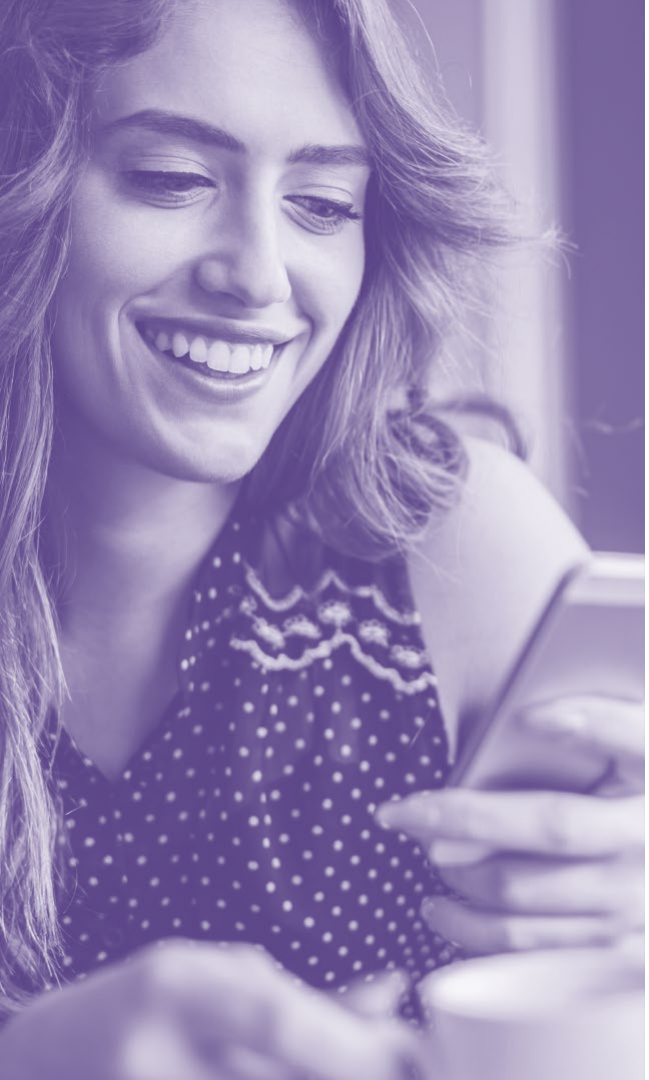
Segundo pesquisa da Juniper Research, **90% dos smartphones devem ter hardware de reconhecimento facial até 2024**.

Enquanto isso**, é esperado que soluções em software sejam integradas em 1,3 bilhões de devices**.




dos usuários têm interesse em usar a **biometria digital para fazer pagamentos mobile**

Fontes: Juniper Research 2021, OpinionBox e Mobile Time 2020, Visa/AYTM Market Research 2017.







# Face Match e Liveness

O liveness é classificado em duas categorias: **liveness passivo e liveness ativo**. Essas duas abordagens podem ser usadas separadamente, mas se mostram ainda mais eficazes quando combinadas.

Fontes: Juniper Research 2021, OpinionBox e Mobile Time 2020, Visa/AYTM Market Research 2017.

### Face Match sem liveness

O Face Match confirma se duas fotos são da mesma pessoa.

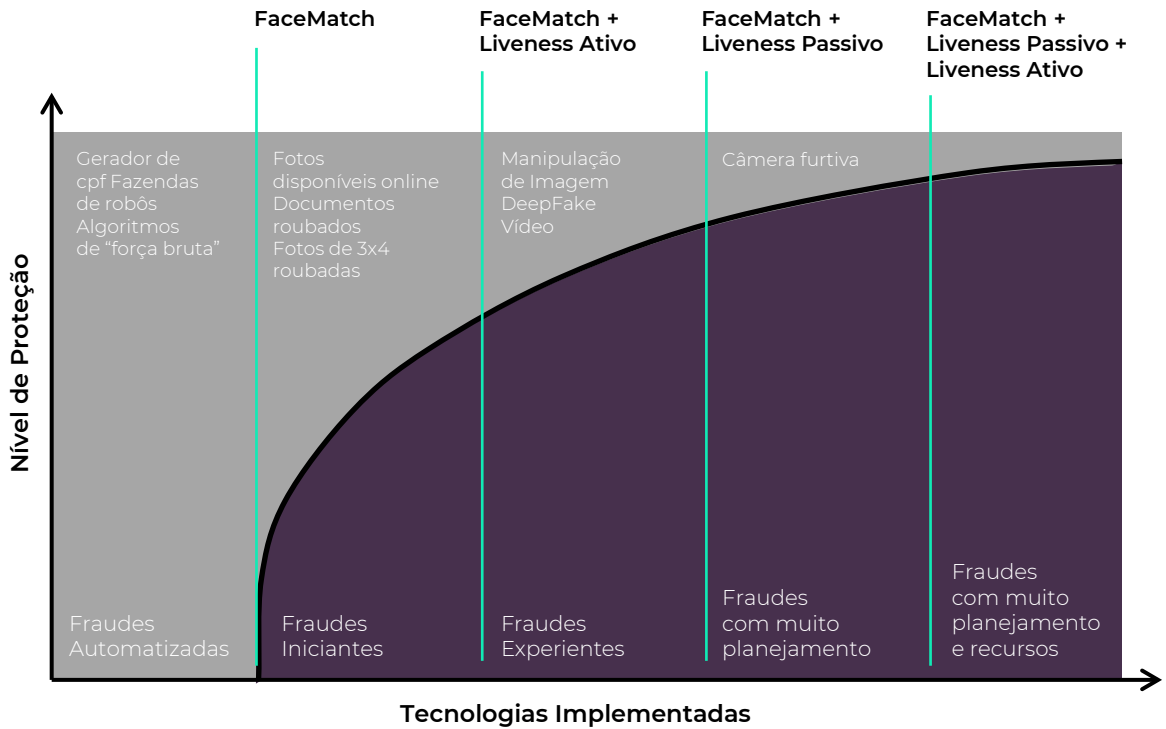
### Face Match com liveness passivo

O liveness passivo não requer uma ação do usuário e garante que a imagem utilizada na validação seja de uma pessoa e não de uma foto por meios passivos de análise de imagem.

### Face Match com liveness ativo

O liveness ativo garante que a imagem utilizada na validação seja de uma pessoa e não de uma foto por meios ativos, como pedir uma ação do usuário (sorrir ou piscar, por exemplo).

# Níveis de proteção e possíveis fraudes




Ao aumentar o nível de proteção, se **dificulta mais e mais o trabalho dos fraudadores**, aumentando a necessidade de tempo, recursos e experiência para infiltrar um sistema. Por isso, cada nível de proteção representa um ganho considerável em fraudes barradas.

**Fazenda de robô:** uma pessoa cadastra e controla várias contas, dando a impressão que cada uma delas é uma pessoa legítima.

**Algoritmo de "força bruta":** tática para invasão de sistemas protegidos por senha onde o hacker usa um algoritmo que tenta todas as combinações possíveis até que ache a senha correta.

**Câmera furtiva:** é a utilização de fotos que foram tiradas sem a permissão da pessoa em documentos forjados.

Fontes: Juniper Research 2021, OpinionBox e Mobile Time 2020, Visa/AYTM Market Research 2017.

# Biometria comportamental

A biometria comportamental utiliza **padrões de comportamento do usuário para realizar a autenticação**. Ela usa a interação do usuário com dispositivos, assim como padrões de localização, para que seja feita a autenticação contínua dos usuários confiáveis — o que os diferencia de possíveis fraudadores, que teriam um comportamento diferente identificado.

Existem diversos tipos de atividades comportamentais que podem ser utilizadas para diferenciar usuários confiáveis de fraudadores, como a força da pressão de toque dos dedos na tela do celular, a velocidade de rolagem de aplicativos e navegadores, o manuseio físico do próprio aparelho e o padrão de comportamento de localização do usuário.

## Prós

- A identificação do usuário acontece em tempo real e de forma contínua com a análise de inúmeros data points, o que oferece uma combinação única.
- Os dados são dinâmicos, ou seja, mudam de acordo com a mudança de comportamento do usuário — por isso, são virtualmente impossíveis de serem reproduzidos por terceiros.
- A fricção para o usuário é eliminada por completo, dado que ele não precisa fazer nenhuma ação ativa para se autenticar.

## Contras

- Dependendo da forma de tratamento de dados, a privacidade do usuário pode ser comprometida.

Existem poucas limitações de dispositivos para que a tecnologia seja implementada. Basicamente, qualquer smartphone pode gerar informações para que um usuário utilize biometria comportamental.

Um estudo recente aponta que o mercado de biometria comportamental deve ter um crescimento anual de mais de **20% ao ano, chegando ao valor de 5.2 bilhões de dólares em 2027**.

Isso coloca essa tecnologia como uma das de maior crescimento em adoção ao longo dos próximos cinco anos.

# Biometria comportamental por localização

A biometria comportamental por localização é o sinal mais forte para a autenticação mobile, pois utiliza o padrão do comportamento de localização para autenticar o usuário confiável em tempo real.

As informações de localização não dependem apenas do GPS, podendo utilizar também o Wifi e outros sensores do dispositivo. A combinação de sensores de movimento capta o comportamento dos usuários, que não precisam fazer nenhuma ação ativa para se autenticar. Isso elimina a fricção de qualquer transação autenticada por localização.

## Prós

- Eliminação de fricção para o usuário confiável, que não precisa realizar nenhuma ação para ser autenticado.
- A autenticação é contínua e em tempo real, o que previne com maior eficácia golpes de roubo de conta.
- Redução de custos das instituições com verificações de fraudes, já que os usuários legítimos são aprovados, e uma taxa consideravelmente menor de usuários não aprovados podem passar por outra forma de autenticação.

## Contras

- O usuário precisa compartilhar a localização com o aplicativo mobile para que o padrão de comportamento seja captado. Outras informações podem ser utilizadas, mas o padrão de comportamento tem menos pontos de dados.

## Insights de milhões de celulares da rede de dados de Incognia mostram que:


dos **logins legítimos** acontecem de locais confiáveis, como a **casa do usuário**


das **transações sensíveis** que não são fraudulentas acontecem a partir de locais confiáveis


das **compras em e-commerce** que não são fraudulentas acontecem em locais confiáveis


dos endereços de faturamento usados em transações legítimas de **comércio eletrônico estão correlacionados com a localização confiável de sua casa**

# Outros tipos de biometria

## Íris

A íris é a parte colorida dos olhos entre a pupila (parte preta) e a esclerótica (parte branca). Apresenta uma organização aleatória que é formada no período da gestação e não segue o código genético. Dessa forma, até irmãos gêmeos possuem íris diferentes.

A tecnologia de reconhecimento de íris nos smartphones funciona através da leitura dessa parte dos olhos por meio de luzes visíveis e/ou infravermelhas. Ainda não é uma tecnologia amplamente usada e, somente alguns fabricantes incluem essa feature no celular — enquanto outros descontinuaram sua adoção, seja pela falta de conveniência[1], seja pelo nível de segurança oferecido.[2]

## Voz

A tecnologia de reconhecimento de voz funciona através da transformação dos padrões da voz em texto, posteriormente armazenados em nuvem. No momento da autenticação, a fala do indivíduo é comparada com os padrões disponíveis — se há um match, o acesso é concedido.

Nos últimos anos. houve uma popularização desse tipo de tecnologia graças às assistentes digitais e aos preços mais acessíveis dos smart speakers.  Ainda assim, é possível usar gravações e outros artifícios de reprodução da voz alheia para burlar os sistemas, além de existir a possibilidade da mudança da voz de um indivíduo em momentos diversos ao longo do dia ou da vida.

Fontes: Banco Mundial, Techtudo, UOL.
1 Computerworld
2 Ars Technica

# As muitas oportunidades da biometria

As oportunidades de uso das tecnologias de biometria são muitas e ultrapassam seu uso habitual em procedimentos de onboarding.

A biometria pode ser utilizada **sempre que o usuário precisar ser identificado e/ou autenticado**, ou seja, nos dois momentos essenciais da jornada do cliente — incluindo login, troca de senha e recuperação de conta.

A praticidade da autenticação por biometria oferece uma experiência prática e sem fricção. A seguir, a listamos algumas possibilidades de uso; algumas já são empregadas hoje e outras são tendências para o futuro próximo.

## Possíveis usos da biometria facial

- Antes de transações financeiras de alto valor
- Check-ins e check-outs de estabelecimentos (hotéis, prédios comerciais ou residenciais, Airbnbs)
- Autenticação no processo de recuperação de contas
- Concessão de acesso a uma conta em novo dispositivo

## Possíveis usos da biometria comportamental

- Revogação automática do acesso à conta em caso de comportamentos suspeitos
- Verificação contínua da conta sem a necessidade de fazer o usuário deslogar e logar constantemente
- Verificação de transações em tempo real
- Detecção de fraudes de pagamento com QR Code pela identificação de localização

Além disso, há três perguntas-chave que podem ser feitas para identificar se é possível implementar essas tecnologias em determinado processo:

- **A ação envolve operação financeira?**
- **A ação envolve acesso a informações/ lugares restritos/ pessoais?**
- **A ação envolve a segurança de uma ou mais pessoas?**

# Mercado Financeiro

A fim de prevenir riscos relacionados ao acesso da conta de vítimas por fraudadores, através de furto de celular ou senha, o **Banco Original** e outras fintechs usam a biometria facial para a **validação de grandes transações**, mantendo a segurança do cliente mesmo depois de um ataque bem sucedido

Adicionalmente, aplicativos que disponibilizam informações sigilosas em suas telas principais como o **BTG Pactual Digital**, e por isso pedem senha toda vez que o usuário abre o app, estão dando a opção para o cliente usar a **biometria no lugar da senha**, melhorando sua experiência.

Além disso, também seria possível a implementação da biometria comportamental por localização para que, caso um comportamento de interação suspeito seja identificado, o aplicativo automaticamente possa pedir por nova autenticação, impondo fricção no momento do comportamento com suspeita de risco.

Segundo report global de 2021 da Mastercard, **93% dos consumidores consideram biometria e novas tecnologias para pagamentos e 60% se sentem mais seguros usando biometria para verificar compras do que o uso de PIN**.

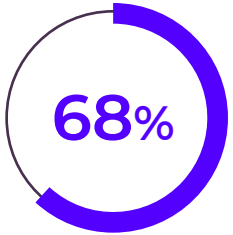
Pesquisa FEBRABAN de Tecnologia Bancária 2020, **35% dos investimentos de bancos em tecnologia está direcionado a Biometria Facial**.

Segundo pesquisa da TransUnion de maio de **2021, fraudes com serviços financeiros aumentou 457% desde o início da pandemia**

Fontes: Money Times, Contacorrente.com, Mastercard New Payments Index, FEBRABAN, TransUnion.

# Marketplaces

O **Banco Neon passou a confirmar compras no e-commerce por biometria facial e digital** em parceria com a Visa. **Em agosto** de 2020, o banco autenticou **98% das transações realizadas por seus clientes no e-commerce**, considerando-se todos os tipos de autenticações disponíveis – selfie, biometria por digital e senhas. A média de autenticação do mercado brasileiro é de apenas 4 em cada 10 pedidos de confirmação de compra.




**Preferiu o reconhecimento digital ou facial como forma de autenticação.**

**Um dos desafios do setor de marketplace é estabelecer confiança entre as 3 partes relacionadas: o comprador, o vendedor e o entregador**. Algumas das fraudes nesse ecossistema estão relacionadas a contas falsas de entregadores, que roubam mercadorias e, também, a perfis falsos de vendedores, que recebem pedidos que nunca serão enviados. Para inibir isso, **algumas empresas já usam a biometria facial tanto para o cadastro de vendedores quanto para entregadores**.

Outra possibilidade seria a validação de transações suspeitas ou de valores altos com biometria, o que adicionaria uma **camada extra de segurança**.

Fontes: Money Times, Contacorrente.com, Mastercard New Payments Index, FEBRABAN, TransUnion.

**MÉTODOS DE AUTENTICAÇÃO E RECUPERAÇÃO DE SENHAS NA JORNADA DO USUÁRIO**

## Delivery

Aplicativos de delivery também sofrem com indivíduos maliciosos que usam seus sistemas para fraudar tanto clientes quanto fornecedores. **Diferentes tipos de biometria podem ser usadas para autenticar periodicamente entregadores, por exemplo — isso já é feito por aplicativos como Rappi e Uber Eats.**

## Saúde

Alguns planos de saúde já estão usando o **Face Match no lugar da carteirinha**, evitando o empréstimo ou cobranças fraudulentas pelo prestador. **É o caso do Bradesco Saúde, que iniciou testes em 2020 para troca da carteirinha pelo reconhecimento facial.**

Fonte: Folha de São Paulo.



## Varejo

O reconhecimento facial também pode ser usado para efetuar pagamentos. No caso, o software faz a autenticação baseando-se na imagem do rosto da pessoa, permitindo que o pagamento ocorra a distância, sem a necessidade de tocar objetos para digitar senhas.

**Case GPA:** Um case de sucesso de uso da biometria facial no varejo é o Grupo Pão de Açúcar (GPA), que conseguiu reduzir o tempo de redefinição de senha de **48 horas para apenas poucos segundos usando a solução de Face Match da idwall.**

Com isso, o GPA atingiu uma maior assertividade e segurança no processo de validação de identidade de seus usuários. A empresa também conseguiu desafogar a central de atendimento e backoffice, além de contar com um processo mais seguro — somente o dono da conta recebe o acesso necessário.

Na China, já é comum o uso de reconhecimento facial para pagamentos em pontos de venda. **Em 2019, cerca de 1000 lojas de conveniência tinham instalado o método e mais de 100 milhões de chineses já haviam se registrado na tecnologia.**

Fonte: Tech Wire Asia

# Principais tendências

## Biometria single sign-on

O single sign-on dá a possibilidade de o usuário fazer a inscrição em um serviço somente uma vez e, depois, usar o mesmo cadastro para outras aplicações sem a necessidade de passar pelo processo de onboarding novamente.

Esse esquema de autenticação automática combinada a tecnologias de biometria traz mais uma camada de proteção à conta: além de o usuário poder usar somente um login para acessar outras contas, **é possível utilizar a biometria para autenticá-lo de forma rápida antes de acessar aplicações selecionadas**, como por exemplo a contas de chat, bancos e pagamentos online, marketplaces, apps de carros de carona, etc.

## Pagamentos

De acordo com um estudo da Unidade de Inteligência do The Economist e TransUnion, **85% dos executivos globais entrevistados acreditam que tecnologias de biometria serão usadas para autenticar a maioria dos pagamentos nos próximos 10 anos. Esse número sobe para 90% no Brasil**.

**Até 2024, a autenticação biométrica será utilizada para transacionar mais de US$ 2,5 trilhões em pagamentos móveis**, segundo relatório publicado pela Juniper Research. O valor representa um aumento de quase 1.000% em relação às transações efetuadas até o final de 2021.

## Deepfakes

A popularização das deepfakes é um dos maiores desafios futuros para as tecnologias de autenticação por biometria facial.

**Recentemente, pesquisadores da Coreia do Sul conduziram experimentos e chegaram à conclusão de que todas as APIs de reconhecimento facial testadas estão suscetíveis a serem enganadas por deepfakes.**

Da mesma forma que as deepfakes evoluem, formas de detectação também se desenvolvem; é esperado que as empresas invistam cada vez mais em ações para prevenir e diminuir ataques no mercado.

## Privacidade e segurança

Com a LGPD (Lei Geral de Proteção de Dados) em vigor, a necessidade que já existia de as empresas tratarem os dados pessoais dos usuários com responsabilidade se tornou ainda mais forte.

Dados biométricos são considerados dados sensíveis pela LGPD, uma vez que têm um potencial de discriminação.

O tratamento desses dados é autorizado para fins de prevenção à fraude e segurança do titular, sempre resguardados os direitos dos titulares e atendidos os princípios de proteção de dados. O descumprimento de tais regras pode gerar sanções legais e financeiras para as empresas.

Fontes: FEBRABAN, The Economist/ TransUnion, Juniper Research, VentureBeat/ Sungkyunkwan University, Cryptoid.

**MÉTODOS DE AUTENTICAÇÃO E RECUPERAÇÃO DE SENHAS NA JORNADA DO USUÁRIO**

# Conclusões



## As senhas...

... não são mais um método seguro de autenticação de identidade. As tecnologias disponíveis para enganar, hackear e adivinhar tais sistemas são bastante avançados. Não à toa, normalmente as senhas são combinadas com outros métodos de autenticação.

**Ainda assim, serviços de tokens e OTPs - a combinação mais comum - possuem vulnerabilidades consideráveis e dependem muito das tecnologias empregadas. Isso vale principalmente para o one-time-password via SMS e e-mail que, assim como as senhas, podem ser acessados de maneira relativamente fácil.**

## O futuro da autenticação...

... está nas tecnologias de biometria, que oferecem ao usuário uma experiência rápida, fácil, universal e sem fricção..

**Nesse sentido, as possibilidades de uso são inúmeras e podem estar presentes em qualquer momento da jornada do cliente em que a autenticação seja necessária.**

Métodos biométricos combinados (como reconhecimento facial unido à identificação digital ou biometria comportamental por localização) trazem ainda mais segurança e praticidade aos processos.

## Segurança e privacidade...

...são fundamentais, e as preocupações das empresas e usuários estão no centro da discussão de novas tecnologias.

Em pesquisa da Unisys de 2020, **85% dos entrevistados afirmaram que deixariam de fazer negócios com uma instituição financeira caso ela tratasse mal suas informações pessoais.**

Além disso, o estudo de mercado sobre bancos digitais realizado no primeiro semestre de 2021 pela idwall mostrou que **o descumprimento de normas KYC levaram à aplicação de R$ 900 milhões em multas nos últimos 10 anos no Brasil.**

Fonte: Unisys 2020.

**MÉTODOS DE AUTENTICAÇÃO E RECUPERAÇÃO DE SENHAS NA JORNADA DO USUÁRIO**

# Processos de recuperação de contas

# Background de mercado

É de grande importância o gerenciamento seguro da jornada do cliente em cada momento que há um ponto de contato com a empresa ou serviço. É comum que seja dada grande atenção ao onboarding, uma vez que é nessa fase em que a maior parte das fraudes são barradas antes mesmo de causar qualquer problema para todas as partes envolvidas.

Entretanto, também é necessário estar atento aos outros momentos em que infrações possam ocorrer. **Dentre as situações possíveis está o processo de recuperação de contas por procedimentos de recuperação de senhas, que na maioria dos casos depende de fatores de autenticação de conhecimento, que, como discutido anteriormente, são mais fáceis de burlar**.

Alguns setores em específico apresentaram crescimento de mercado grande ao longo de 2020 e preocupações relacionadas a fraudes de identidade é um problema que está no radar da maioria das empresas: segundo report global de 2021 do Serasa Experian, **62% das companhias brasileiras querem aumentar os investimentos nessa área**.

> Segundo a Ebit[1] o e-commerce apresentou um crescimento de 41% em relação à 2019. Foram 13,2 milhões de novos consumidores por esse canal e as vendas em marketplaces corresponderam a 78% do total faturado. Além disso, 57% dessas vendas aconteceram pelos celulares.

> De acordo com estudo recente da Visa, o roubo de identidade foi o segundo tipo de fraude mais relatado pelas empresas de e-commerce.

> Segundo a FEBRABAN, instituições financeiras registraram um aumento de 80% no número de tentativas de ataques online em 2020;

> Nossas análises mostram que o setor privado perde cerca de US$ 6 bilhões por ano só por fraudes de identidade

Com esses aspectos e desafios em mente, a seguir fizemos a **análise do processo de recuperação de senhas dos principais aplicativos de instituições financeiras, marketplaces, delivery e transportes**.

Fontes: Ebit/Nielsen, Visa, FEBRABAN, Serasa Experian, Cryptoid.
[1] A metodologia de pesquisa da Ebit/Nielsen não inclui nesta fase Mercado Livre, Elo7 e Enjoei.



# Metodologia

O processo de recuperação de conta foi avaliado em aplicativos tanto nas plataformas Android quanto iOS. Este relatório se baseia em dados coletados entre os dias **1º a 4 de junho de 2021**.

Foram coletadas as seguintes informações, levando-se em consideração a experiência do usuário final:

- Possibilidade de recuperação de conta de senha pelo processo "esqueci minha senha"
- Quais informações foram solicitadas
- Existência de autenticação de múltiplos fatores
- Tempo do processo

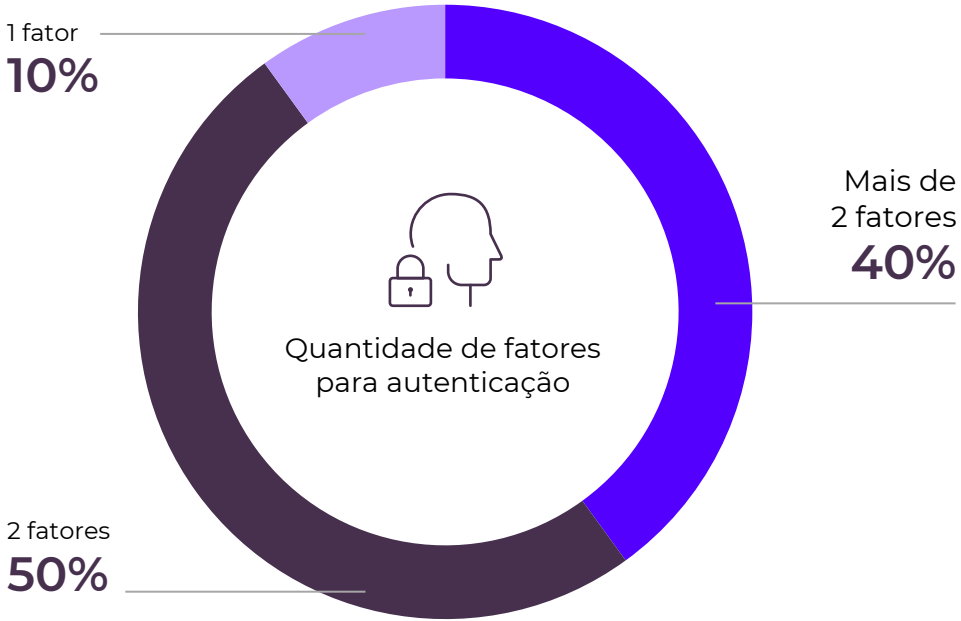
**Disclaimer: Estamos fazendo testes em um ambiente muito dinâmico, em que apps são atualizados com frequência e não temos controle de datas destas atualizações, que segue o cronograma das instituições donas dos apps. Portanto é possível que no dia seguinte à publicação deste report, alguma informação já esteja desatualizada, após alguma publicação de nova versão de alguns aplicativos.*

# Bancos

Foram feitos testes do processo de recuperação de senhas dos aplicativos de 10 bancos.

Foram pedidos em média **3 fatores de autenticação** por banco e a média de tempo foi de 2 minutos e 24 segundos para a finalização do processo.

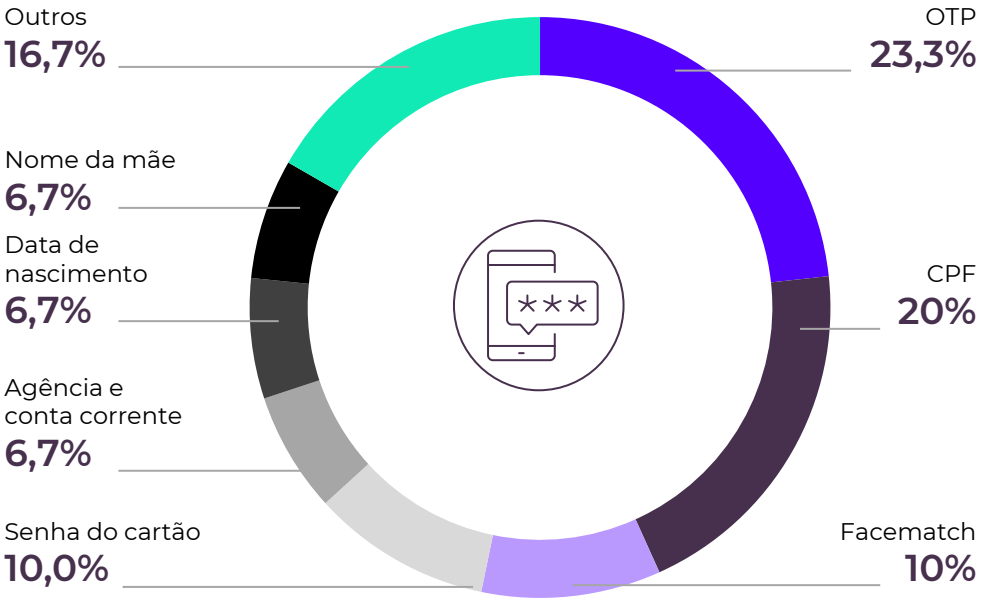
50% das instituições analisadas utilizam **2 fatores de autenticação e 40% utiliza 3 fatores ou mais**.



**De forma geral, não existe uma uniformidade nas formas de autenticação do usuário e há grande variação nas combinações usadas.**

A maioria das instituições utilizou o método OTP (one-time-password), seja por e-mail ou SMS e, nos casos em que não foi utilizado, foram pedidas outras informações, como o CPF e senha do cartão.

**Somente 3 instituições (todas bancos digitais) utilizaram Face Match.** Por outro lado, **todos os bancos digitalizados pediram a senha do cartão** como forma de autenticação



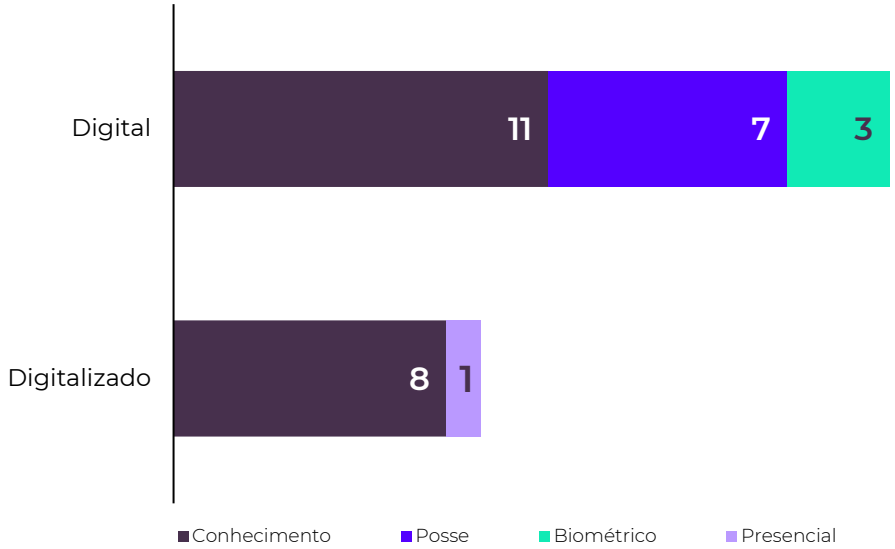

Observação: as informações apresentadas na tabela não necessariamente estão na ordem solicitada por cada banco.

# Métodos utilizados

Dentre os bancos digitalizados analisados, **pode-se observar que não utilizam a autenticação do usuário pelo que o indivíduo tem (como one-time-password) e sim por métodos de conhecimento, como senha do cartão, CPF e data de nascimento.**

Além disso, todos eles já apresentavam o aparelho autenticado anteriormente. Durante os testes, somente o Itaú pediu a confirmação presencial, enquanto o Santander solicitou apenas uma informação, sendo a senha do cartão.[1]

## Métodos usados por tipo de banco




[1] Testes para Itaú e Santander realizados no dia 1º de junho de 2021.

## Marketplaces

Foram analisados 9 aplicativos dos maiores marketplaces do mercado. **Todos pediram o e-mail como uma das opções para solicitar a recuperação de senha, sendo que na segunda etapa, todos enviaram link ou código de recuperação por esse canal.**

Somente 1 empresa pediu mais de 2 informações e solicitou a resolução de um quebra-cabeça. Além disso, somente 1 outra empresa não encaminhou o usuário a uma página de troca de senha, deixando-o logar após a inserção do código recebido por e-mail.

A média de tempo foi de 1 minuto e 7 segundos para a finalização do processo.

## Delivery

**Foram analisados 4 aplicativos de delivery, sendo que a possibilidade de se recuperar a conta só estava disponível para 1 app.** Nesse caso, foi necessário iniciar o processo no browser, o que só foi encontrado com pesquisa ativa na internet.

# Conclusões

Os processos de recuperação de conta são variados e há uma predominância dos fatores de autenticação de conhecimento (aquilo que o usuário sabe), como senhas e CPF. Também há um uso grande de autenticação em múltiplos fatores, principalmente com a utilização de OTP via SMS ou e-mail, sendo que a exceção foi o uso de somente um fator de autenticação.

**As instituições financeiras foram as que usaram os mais variados tipos de autenticação e os únicos que usaram biometria**, o que é esperado, dada a maior sensibilidade da natureza da conta.

Para o caso dos marketplaces, os processos se mostraram rápidos, porém dependentes do acesso a outra conta – nos casos analisados, o e-mail. Já para os aplicativos de delivery, ao mesmo tempo que oferecem maior segurança no momento do login ao possibilitarem o acesso à conta sem senhas, podem oferecer desconforto ao usuário em momentos específicos, seja na necessidade de atualizar informações cadastrais no aplicativo antes da troca de dispositivo e/ou na troca do número de telefone, seja na necessidade de buscar ativamente no browser o processo de recuperação de conta, sem a opção no aplicativo.

Dessa maneira, existem oportunidades de melhorias em todos os casos — nesse sentido, o **uso de métodos biométricos de autenticação junto com outros fatores possibilitam que o usuário não precise esperar mais**, sair do aplicativo ou até mesmo lembrar de muitas informações para acessar sua conta. É uma camada mais prática e rápida e é o futuro que já existe em diversos lugares do mundo.

## Sobre a Incognia

Incognia é uma empresa de identidade por localização fundada em 2014 e sediada em Palo Alto, Califórnia, com equipes em Nova Iorque e no Brasil. Incognia permite a prevenção avançada de fraudes mobile para bancos, empresas fintech e mcommerce. Utilizando a biometria comportamental por localização, a Incognia oferece verificação e autenticação de identidade sem fricção. A tecnologia de localização da Incognia utiliza sinais de rede e sensores no dispositivo para fornecer informações de localização altamente precisas. Ao construir um padrão de comportamento de localização anônimo, único para cada usuário, Incognia cria uma identidade digital privada para segurança de contas.

## Sobre a idwall

A idwall oferece soluções integradas e inteligentes de onboarding digital, agilizando o processo de validação de identidade e ajudando as empresas a cumprirem as normas de compliance. Fundada em 2016 por Lincoln Ando e Raphael Melo, a regtech visa criar relações de confiança para a era digital por meio de ferramentas como Background Check, OCR de documentos, Face Match e o app de identidade digital MeuID, automatizando os processos de cadastro e evitando fraudes em empresas. Em apenas cinco anos, já recebeu mais de R$ 260 milhões em investimentos. Para mais informações sobre a empresa, acesse o site: idwall.co