docusign | ENTRUST
SECURING A WORLD IN MOTION

Whitepaper

# O futuro da verificação de identidade global

Como as organizações líderes conciliam a segurança digital com a experiência do usuário

À medida que os casos de fraude de identidade se tornam mais frequentes, organizações ao redor do mundo buscam novas formas de verificar e autenticar as identidades de seus clientes. As soluções de verificação de identidade (IDV) e autenticação oferecem essa camada essencial de segurança. Ao entender melhor como as organizações de ponta implementam essas soluções, e ao conhecer os pontos mais vulneráveis da jornada do cliente, as empresas podem se proteger melhor de riscos cada vez maiores.

A Docusign e a Onfido, uma empresa Entrust, criaram este relatório juntas para entender melhor como as fraudes de identidade praticadas ao redor do mundo funcionam, e o papel que a verificação de identidade (IDV) desempenha no combate ao problema. A Docusign e a Onfido pesquisaram os desafios específicos enfrentados por organizações em nível regional e industrial, além de realizarem uma análise macro global sobre a ocorrência de fraudes de identidade na jornada do cliente e como as equipes estão lidando com a ameaça crescente.

# Principais descobertas

1 **Os incidentes de fraude de identidade estão crescendo e gerando um desperdício de tempo, dinheiro e recursos humanos nas organizações.**

Uma parte significativa das organizações pesquisadas perde mais de US$ 1 milhão todo ano devido a custos diretos e indiretos relacionados à fraude de identidade, e essas despesas deverão aumentar à medida que a tecnologia da inteligência artificial (IA) avança. Mesmo com as dificuldades, algumas organizações hesitam em implementar medidas de prevenção contra fraudes de identidade temendo prejudicar a experiência do cliente. 66% das organizações pesquisadas concordam que a experiência do cliente e a prevenção de fraudes de identidade são prioridades conflitantes. No entanto, na prática, muitas empresas estão descobrindo que não precisam fazer concessões: nossa pesquisa revela que empresas que adotam a IDV apresentam o dobro de satisfação em comparação com aquelas que não implementam a IDV.

2 **A fraude de identidade ocorre ao longo de toda a jornada do cliente, e geralmente quando os clientes fazem login e autorizam pagamentos.**

Além de fraudes de identidade em várias etapas da jornada do cliente, elas são variadas. As formas mais comuns em todos os setores são roubo de identidade, criação de contas, falsificação de documentos digitais e fraude de estorno. O método de autenticação mais associado à fraude de identidade é o uso de nome de usuário e senha. Uma análise mais aprofundada do comportamento organizacional revela que dois terços das organizações aplicam diferentes níveis de autenticação para cada interação com o cliente, com base nos perfis de risco dos clientes ou no tipo de interação.

3 **A IDV não apenas protege as organizações contra fraudes de identidade, como também as coloca em uma posição de vantagem competitiva.**

Usuários da IDV conseguem identificar fraudes de identidade com antecedência e com mais frequência na jornada do cliente em comparação com não usuários. Como resultado, organizações que adotam a IDV economizam, em média, mais de US$ 8 milhões no total ao prevenir fraudes de identidade. 63% das organizações que investiram significativamente mais em IDV do que a concorrência acreditam que as medidas que tomaram para prevenir a fraude de identidade tiveram um impacto positivo em sua marca.

4 **A maioria das organizações acredita que, para eliminar ou reduzir fraudes de clientes, é preciso adotar o uso da tecnologia.**

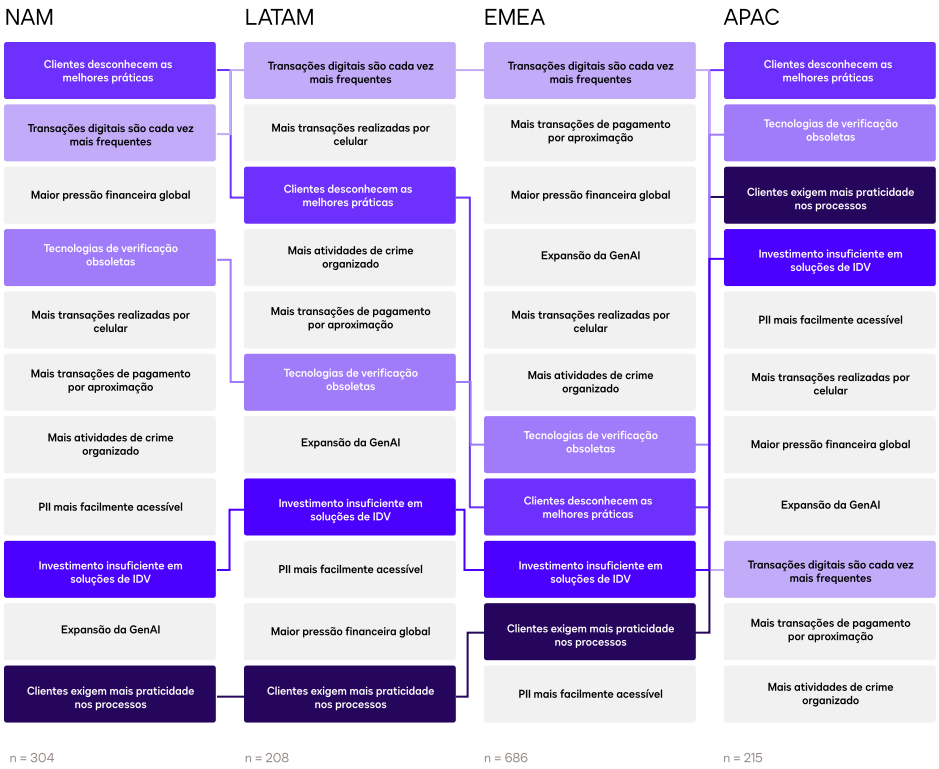
70% das organizações pesquisadas acreditam que investir pesadamente em soluções tecnológicas é a melhor maneira de mitigar o risco financeiro gerado por fraudes de identidade, e a IDV é uma de suas principais prioridades — 74% das empresas planejam reforçar seu investimento em IDV no futuro.

# A fraude de identidade é uma preocupação crescente, assim como a alta dos custos e o aumento das expectativas dos clientes

Sessenta e nove por cento das organizações pesquisadas concordam: as tentativas de fraude de identidade estão crescendo. Embora a maioria das empresas ao redor do mundo enfrente essa mesma dificuldade, suas crenças sobre a causa variam entre setores e regiões. No entanto, podemos destacar dois motivos em nossa pesquisa:

- Mais transações digitais são efetuadas hoje em dia
- Os clientes não conhecem as melhores práticas para proteger suas informações de login e outros dados confidenciais.

**A falta de conhecimento dos clientes sobre as melhores práticas e o aumento das transações digitais são os principais motivos para o aumento das tentativas de fraude**



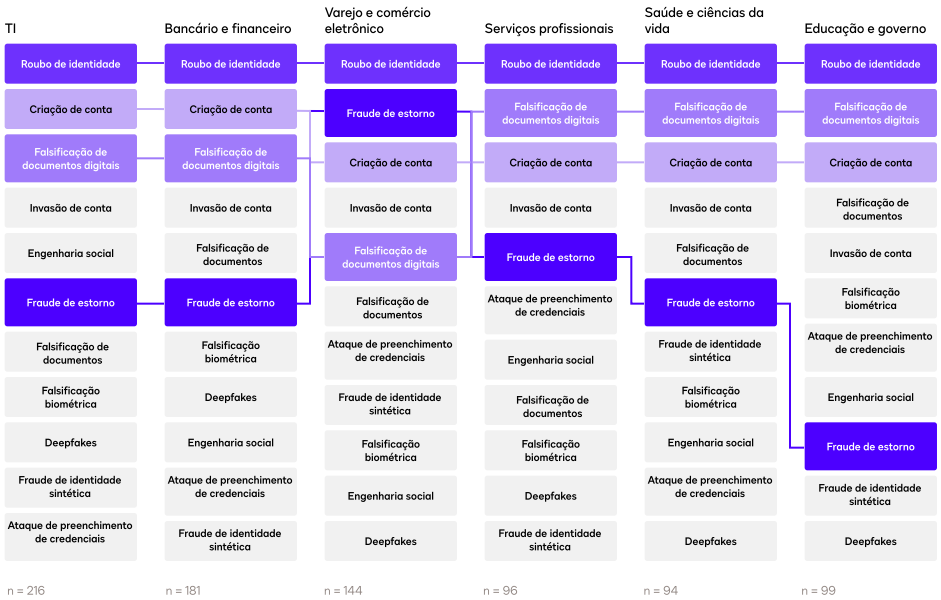

Em sua opinião, quais os principais motivos para o aumento de tentativas de fraude?

Embora poucas organizações nesta pesquisa tenham entendido a IA como um dos principais fatores de fraude, outros levantamentos indicam que ela pode contribuir significativamente para as mudanças ocorrendo na área de segurança. O 2025 Identity Fraud Report (Relatório de Fraudes de Identidade de 2025) da Entrust revelou que a falsificação de documentos digitais, frequentemente criada com IA generativa, aumentou 244% no último ano. Deepfakes como essas agora representam 40% de todas as fraudes biométricas. Descobrimos também que muitas empresas veem a IA como uma ferramenta fundamental para combater a fraude de identidade: 82% dos entrevistados acreditam que a IA generativa será mais eficaz do que os métodos utilizados atualmente para reduzir o risco de fraude dos clientes.

Existem também padrões nas diferentes variedades de organizações de fraude de identidade observadas. Em diversos setores, o roubo de identidade foi o tipo de fraude mais frequentemente relatado, seguido por falsificação de documentos digitais e fraude na criação de contas. O varejo e o comércio eletrônico são os únicos setores que contêm outro tipo de fraude entre os três principais: a fraude de estorno, quando os clientes contestam intencionalmente uma cobrança para receber um reembolso, não devolvendo o produto ou serviço, originado por compras de consumidores neste setor.

Essas descobertas indicam que a maioria das fraudes de identidade ocorre em momentos críticos, quando os clientes interagem ativamente com uma empresa, seja ao criar uma conta pela primeira vez, redefinir sua senha ou inserir informações de pagamento. Para proteger a jornada do cliente nestes momentos cruciais, as empresas precisam oferecer maneiras seguras de abrir contas e verificar continuamente as identidades dos usuários ao longo de todo o ciclo de vida do cliente.

### Roubo de identidade, criação de contas e falsificações de documentos digitais são os tipos mais comuns de fraude de identidade em diversos setores



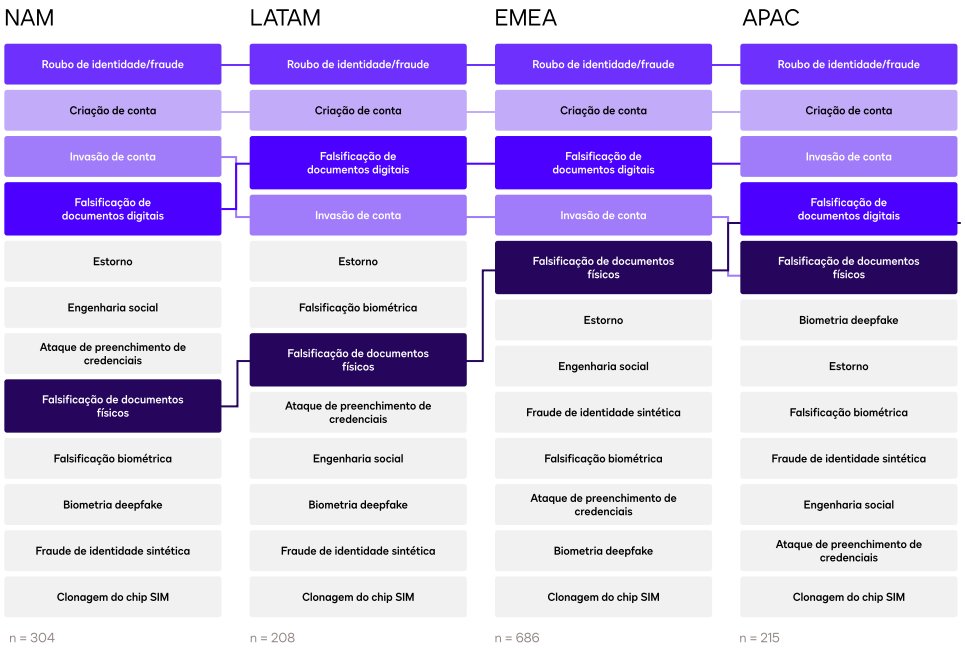

Quais tipos de fraude relacionados à verificação de identidade/autenticação de usuário são mais comuns na sua organização durante o processo de transação com o cliente?

Entre os países pesquisados, os respondentes no Brasil relataram o maior aumento nas tentativas de fraude de identidade, em que

79%

das organizações reportaram um aumento nas fraudes.

## Roubo de identidade, criação de contas e falsificações de documentos digitais são os tipos mais comuns de fraude de identidade em diversas regiões




Quais tipos de fraude relacionados à verificação de identidade/autenticação de usuário são mais comuns na sua organização durante o processo de transação com o cliente? Clique para escolher até três que ocorrem regularmente, começando pelo mais frequente.

**Descobertas do setor**

O setor bancário e financeiro relatou os maiores custos diretos de fraude de identidade (51% relataram custos diretos anuais superiores a US$ 1 milhão).

O setor de serviços profissionais relatou os maiores custos indiretos de fraude de identidade (20% relataram custos indiretos anuais superiores a US$ 1 milhão.)

**Porcentagem de organizações com custos diretos de fraude de identidade superiores a US$ 1 milhão**

Países com a maior porcentagem

55% **Alemanha**
65% **Austrália**

Países com a menor porcentagem

30% **Reino Unido**
29% **Brasil**

**Porcentagem de organizações com custos indiretos de fraude de identidade superiores a US$ 1 milhão**

Países com a maior porcentagem

24% **Brasil**
29% **Austrália**

Países com a menor porcentagem

6% **México**

# A fraude de identidade custa às organizações US$ 7 milhões por ano, em média

Muitas empresas acreditam que os custos associados à fraude de identidade são simplesmente o preço a ser pago por fazer negócios. Entretanto, esse preço está aumentando a cada dia. As organizações frequentemente enfrentam despesas superiores a sete dígitos devido aos custos diretos de estornos, reembolsos e outras perdas financeiras, além dos custos indiretos associados à alocação de recursos humanos valiosos para identificar e corrigir transações fraudulentas e administrar os danos à marca e à reputação. Nossa pesquisa revelou que:

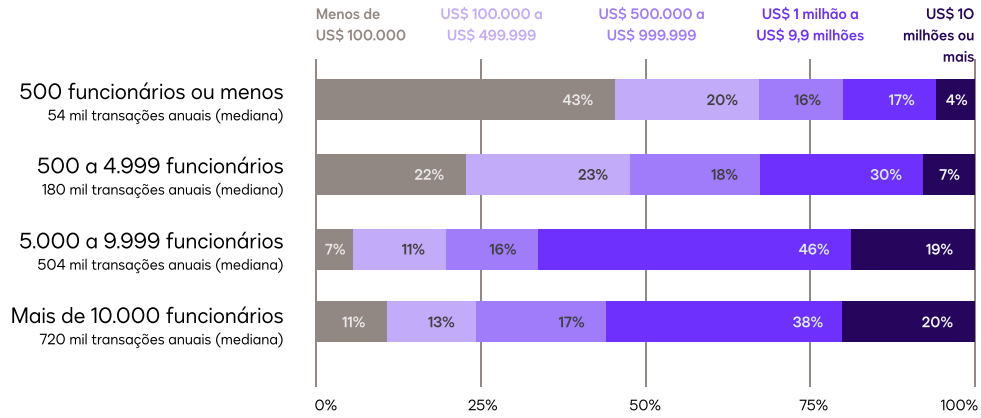
**41%**
das organizações têm um custo anual direto de fraude de identidade superior a US$ 1 milhão.

**15%**
das organizações têm um custo anual indireto de fraude de identidade superior a US$ 1 milhão.

**Organizações maiores, que envolvem mais clientes, dados e receitas, enfrentam custos ainda mais elevados. Entre as organizações com mais de 5 mil funcionários:**

- **Têm um custo anual direto de fraude de identidade de US$ 13 milhões, em média.** 28% têm um custo anual indireto de fraude de identidade superior a US$ 1 milhão.
- E os custos crescem exponencialmente à medida que o tamanho das empresas aumenta. **Entre as organizações com mais de 10 mil funcionários, 20% têm um custo anual de fraude de identidade direto e indireto superior a 50 milhões de dólares.**

## Grandes organizações enfrentam custos mais elevados com fraudes diretas de identidade




Se você tivesse que estimar, qual seria o custo financeiro direto anual aproximado da fraude de clientes para sua organização? Por custo financeiro direto, entendemos o valor monetário perdido devido à fraude, independentemente de ser compensado pelo seguro.

O setor bancário e financeiro enfrenta os maiores custos diretos de fraude de identidade. Isso ocorre porque, na fase de integração do cliente, os fraudadores criam contas falsas, o que lhes permite acessar serviços financeiros; ou obtêm acesso a contas legítimas em uma fase posterior do ciclo de vida do cliente e esvaziam seus fundos. Em ambos os casos, a empresa alvo perde dinheiro diretamente ou tem que reembolsar o cliente verdadeiro.

O setor de serviços profissionais apresenta os maiores custos indiretos de fraude de identidade. A fraude de identidade tende a impactar negativamente a reputação da marca dessas empresas e a confiança dos clientes, resultando em uma diminuição de receita futura e custos indiretos significativos.

66%
das organizações pesquisadas acreditam que a experiência do cliente e a prevenção de fraudes de identidade são prioridades conflitantes.

45%
das organizações pesquisadas priorizam a experiência do cliente em detrimento da prevenção de fraudes.

58%
das organizações pesquisadas estão preocupadas que deixarão os clientes insatisfeitos e aumentarão o índice de abandono se intensificarem a prevenção de fraude de identidade.

**Resultados regionais**

A região APAC (Ásia e Pacífico) está ainda mais preocupada com o atrito entre a experiência do cliente e a prevenção de fraudes de identidade, com

80%
das organizações concordando que são prioridades conflitantes.

# Os clientes esperam cada vez mais experiências rápidas e integradas

## 79% das organizações pesquisadas concordam que a experiência do cliente é muito importante para o seu sucesso.

As empresas sofrem pressão para oferecer experiências digitais práticas, convenientes e competitivas, enquanto protegem as informações dos clientes. Por exemplo, muitos clientes esperam experiências personalizadas, transações fáceis em seus dispositivos móveis e formulários pré-preenchidos com informações que já forneceram, mas também esperam que seus dados permanecerão seguros durante essas interações. Muitas organizações enfrentam dificuldades para equilibrar esses objetivos.

No entanto, as ações para equilibrar a prevenção de fraudes de identidade e a experiência do cliente variam entre regiões, setores e gerações. Os setores de TI, bancário e financeiro são mais propensos a submeter os clientes a medidas rigorosas de autenticação para proteger dados confidenciais e transações de alto valor, respectivamente, mesmo quando essas medidas acabam criando mais atrito.

Os tomadores de decisão das gerações Millennial e Gen Z, que estão mais habituados às verificações de identidade digital, esperam experiências de usuário excepcionais e sentirem segurança durante as transações digitais e, como resultado, estão impulsionando a inovação tecnológica.

## No geral, as empresas que utilizam IDV estão duas vezes mais satisfeitas do que as empresas que não utilizam IDV e tendem a considerar seus métodos de prevenção de fraudes significativamente mais eficazes.

## Conclusão principal

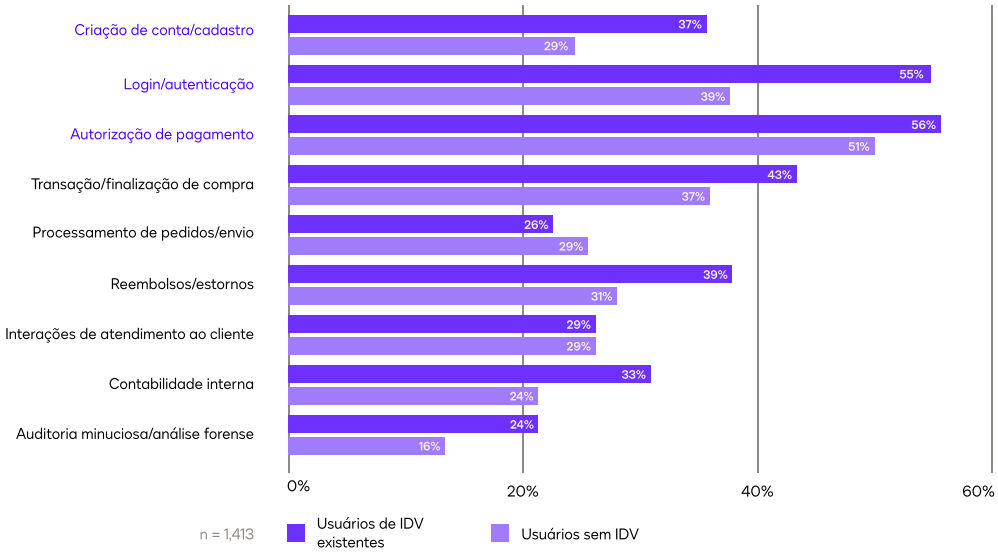
Gerenciar tentativas crescentes de fraude de identidade enquanto oferece uma experiência prática e integrada é um desafio crescente, mas a verificação de identidade (IDV) ajuda as organizações a reduzir a fraude de identidade enquanto proporciona maior satisfação organizacional. As empresas que utilizam tecnologias desatualizadas ou insuficientes para reduzir o risco de fraude de identidade terão dificuldades para combater técnicas complexas de fraude de identidade ou acompanhar as novas ameaças.

# A fraude de identidade ocorre durante toda a jornada do cliente

A fraude de identidade ocorre ao longo de toda a jornada do cliente, mas as organizações **normalmente conseguem detectá-la nos estágios iniciais de login e autorização de pagamento.**

**As organizações que adotam IDV têm ainda mais probabilidade de detectar tentativas de fraude de identidade no início das transações, melhorando suas chances de prevenir ou reduzir os danos.**

### Usuários de IDV têm mais chances do que não usuários de identificar fraudes nos estágios iniciais da jornada do cliente




Em que momento do processo de transação sua organização costuma descobrir que ocorreu uma transação fraudulenta? As opções listadas abaixo estão em ordem decrescente, desde as interações iniciais com o cliente até o processamento após o engajamento do cliente.

Quando questionadas sobre quais ferramentas de autenticação estão associadas ao maior número de fraudes de identidade, as empresas selecionaram **a autenticação por nome de usuário e senha como o método mais fraco a ser utilizado.** O motivo pode ser o fato de nomes de usuário e senhas serem facilmente comprometidos, suscetíveis a violações de dados e não possuírem autenticação multifatorial. Em 2024, credenciais roubadas, como nome de usuário e senha, foram os incidentes de violação de dados mais comuns.[1]

1 "2024 Data Breach Investigations Report," Verizon Business.

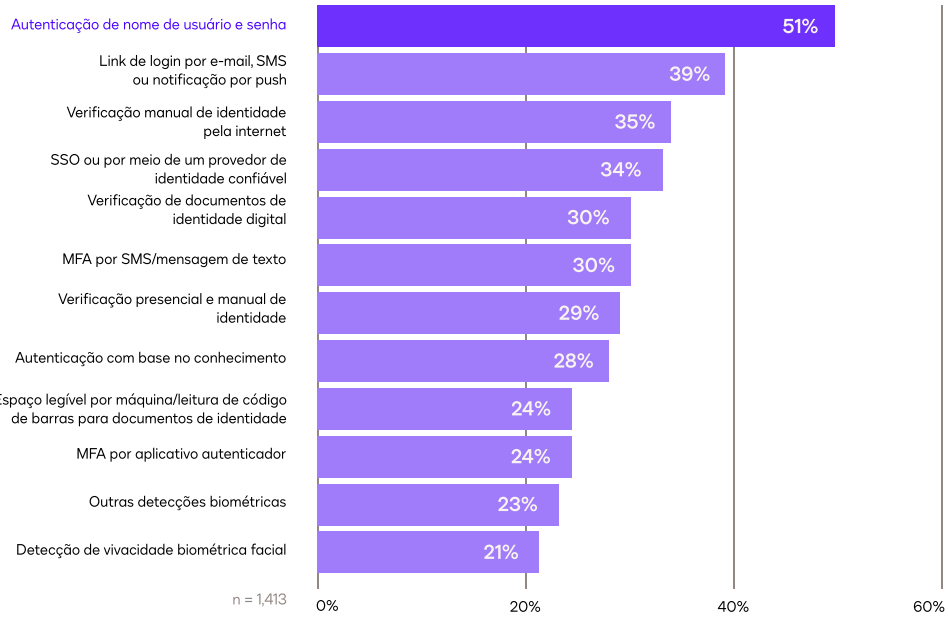
Organizações que adotam a IDV, em média, identificam tentativas de fraude de identidade em

**20%**

mais etapas da jornada do cliente do que aquelas que não adotam a IDV.

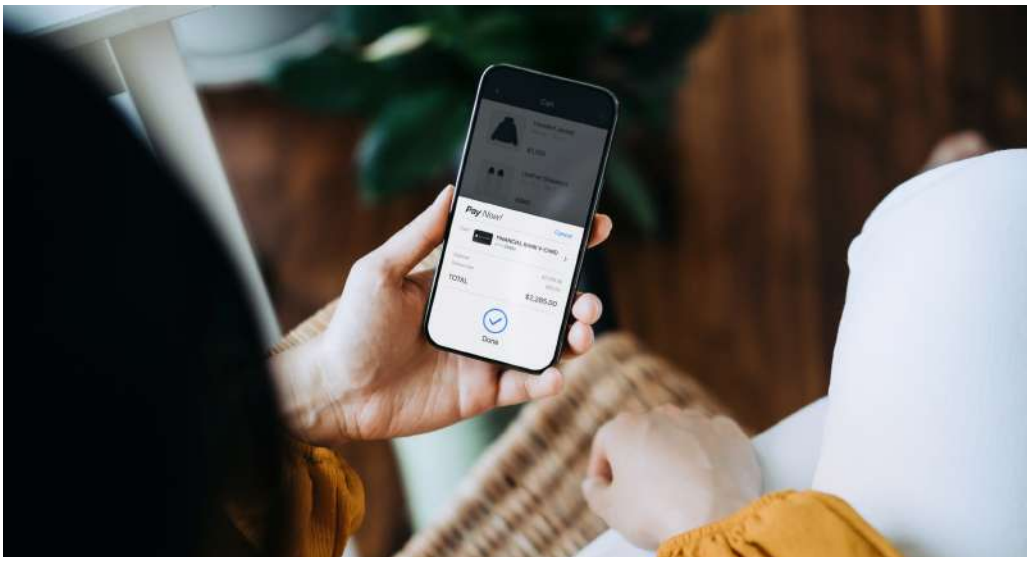
## A fraude de identidade ocorre com mais frequência quando apenas o nome de usuário e a senha são usados como método de autenticação

A fraude de identidade é mais comum com esta técnica

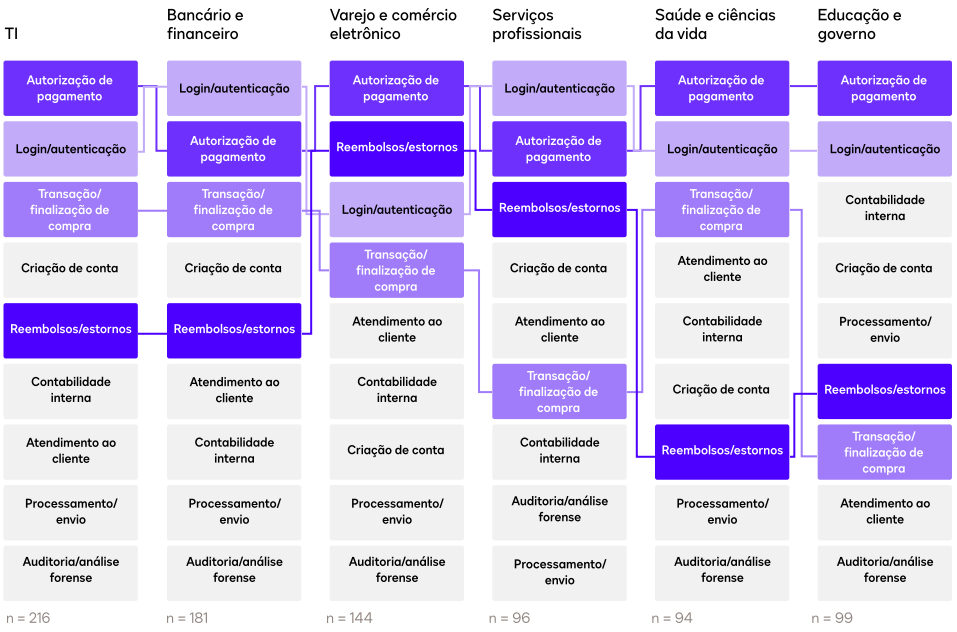



Para cada tipo de autenticação de usuário, indique com que frequência você observa fraudes em comparação com outros tipos de autenticação.

A pesquisa também revelou que, quanto mais transações digitais uma organização realiza, maior é a probabilidade dela encontrar fraudes em diversos métodos de autenticação.



## A autorização de pagamento e o login são as etapas mais comuns para detectar fraudes em todos os setores

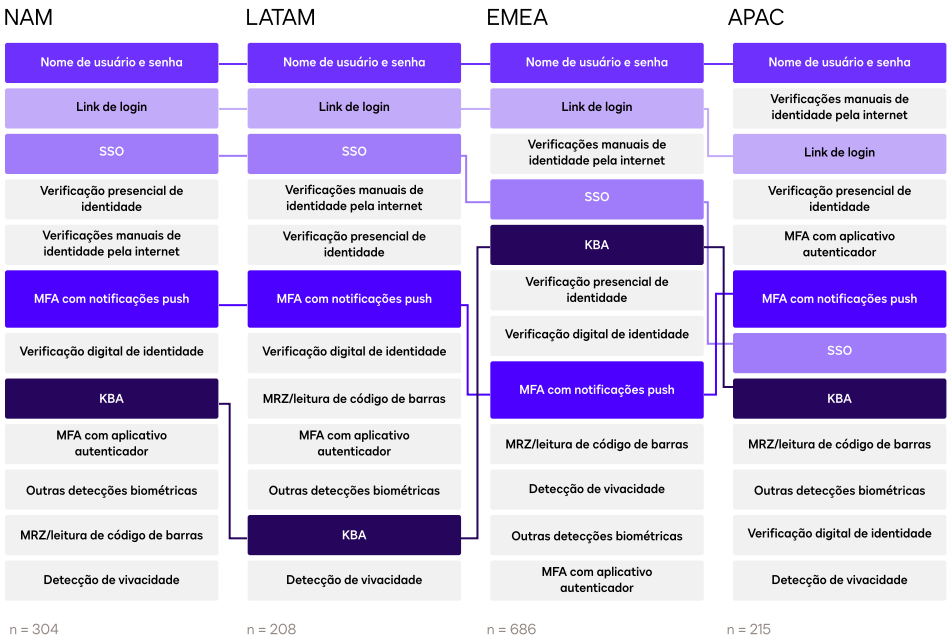



Em quais momentos do processo de transação sua organização descobre que ocorreu uma transação fraudulenta?

## Resultados regionais

Entre os tomadores de decisão de TI e de negócios, os líderes das gerações Millennial e Gen Z têm maior probabilidade de usar a IDV do que os "baby boomers" ou a Gen X. Eles também têm mais chances de avaliar sua organização como "muito boa" em suas ações de combate a fraudes.

### Nome de usuário e senha são o método de autenticação associado à maior parte das fraudes em todas as regiões




A fraude é muito mais comum do que se imagina com esta técnica.

## Conclusão principal

O nome de usuário e a senha é o método de autenticação mais vulnerável, mas mesmo a MFA não é suficiente para proteger contra tentativas cada vez mais complexas de fraude de identidade. Formas avançadas de IDV, como autenticação biométrica e verificação de documentos, são essenciais para combater os fraudadores.

# Investimentos significativos em IDV geram resultados concretos

Em média, uma organização economiza mais de

**US$ 8 milhões**

no total ao prevenir fraudes por meio da adoção de uma solução de verificação de identidade (IDV).

Entretanto, implementar uma solução de verificação de identidade é apenas o primeiro passo. As empresas que conquistam os melhores resultados focam intensamente em sua segurança, investindo significativamente mais do que seus concorrentes em IDV. Além disso, as empresas que investem mais tornam sua organização um alvo menos atraente para fraudadores, criando uma vantagem competitiva.

## Organizações que afirmam investir significativamente mais do que seus concorrentes em IDV:

### Economizam mais

**1.5x**

vez mais propensos a ter economizado mais de US$ 1 milhão no total do que aqueles que investiram um pouco mais.

**2.2x**

vezes mais propensos a ter economizado mais de US$ 1 milhão no total do que aqueles que investiram o mesmo ou menos.

### Reduzem a quantidade de fraudes de identidade

**1.7x**

vez mais propensos a ter reduzido uma quantidade significativa de fraudes de identidade.

### Continuam investindo em IDV

**2.8x**

vezes mais propensos a planejar investir mais em IDV.

### Aumentam a satisfação interna e dos seus clientes

**4x**

vezes mais propensos a estarem muito satisfeitos com as soluções de IDV que utilizam.

**1.6x**

vez mais probabilidade de ter tido um impacto positivo em sua marca

### São mais competitivas

**2.7x**

vezes mais propensos a acreditar que têm uma vantagem competitiva.

**Os dados sugerem que os clientes têm mais confiança em empresas que não medem esforços para proteger seus dados pessoais.**

## 77%

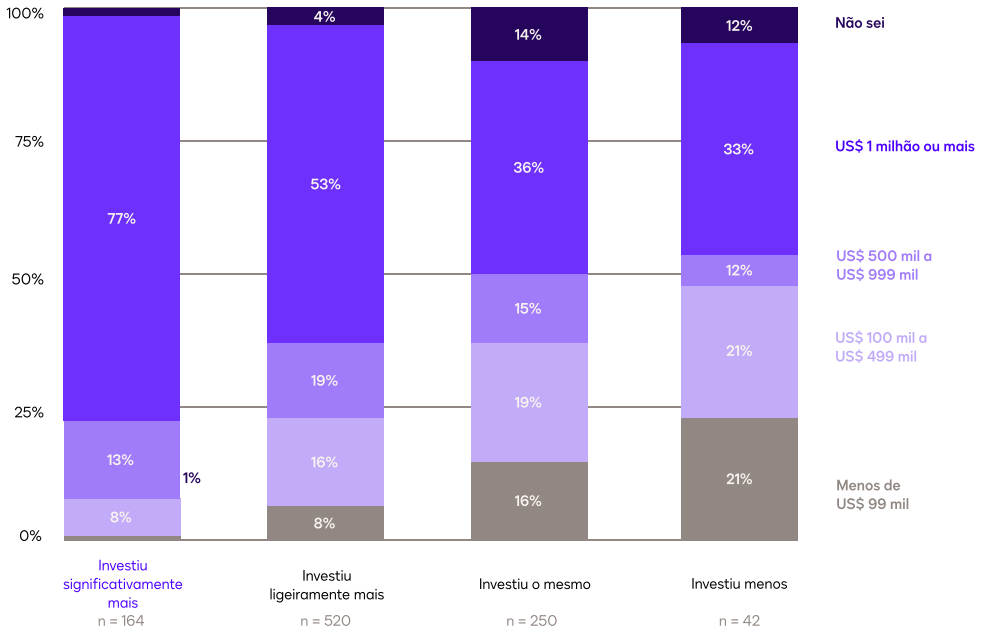
das organizações que investiram significativamente mais em tecnologias de verificação de identidade do que seus concorrentes

## economizaram mais de US$ 1 milhão

no total, em comparação com 36% que investiram a mesma quantidade que empresas do mesmo setor.

**As organizações que investiram em IDV significativamente mais do que seus concorrentes tinham maior probabilidade de economizar um total de US$ 1 milhão ou mais**

Verba economizada entre aqueles que utilizam a IDV




Se você tivesse que estimar, aproximadamente quanto dinheiro sua organização economizou ao prevenir fraudes de clientes usando suas soluções existentes de verificação de identidade/autenticação de usuário?

# Grandes organizações investem mais em IDV e obtêm um retorno sobre o investimento (ROI) desproporcionalmente maior

Para empresas que enfrentam uma quantidade considerável de fraudes de identidade, investir na verificação de identidade (IDV) gera um aumento no retorno sobre o investimento (ROI). Os dados indicam que grandes organizações, que costumam ter custos mais elevados de fraude de identidade, tendem a investir significativamente mais em soluções de verificação de identidade (IDV) do que seus concorrentes e, como resultado, obtêm um retorno sobre o investimento (ROI) desproporcionalmente maior.

**78%**

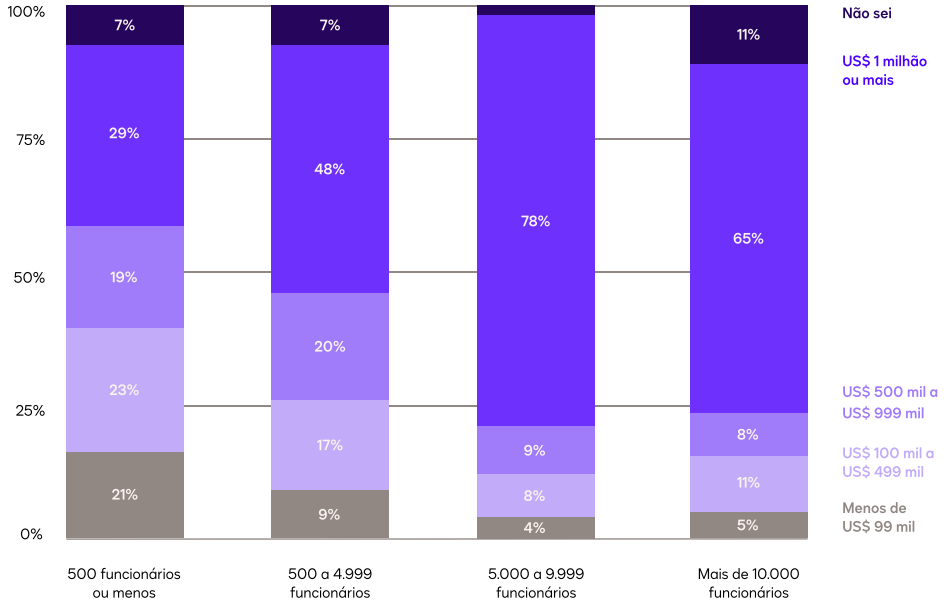
das organizações com 5.000 a 9.999 funcionários economizaram um total de US$ 1 milhão ou mais com a IDV.

**65%**

das organizações com mais de 10 mil funcionários economizaram um total de US$ 1 milhão ou mais com a IDV.

**Grandes organizações investem significativamente mais do que seus concorrentes em IDV**

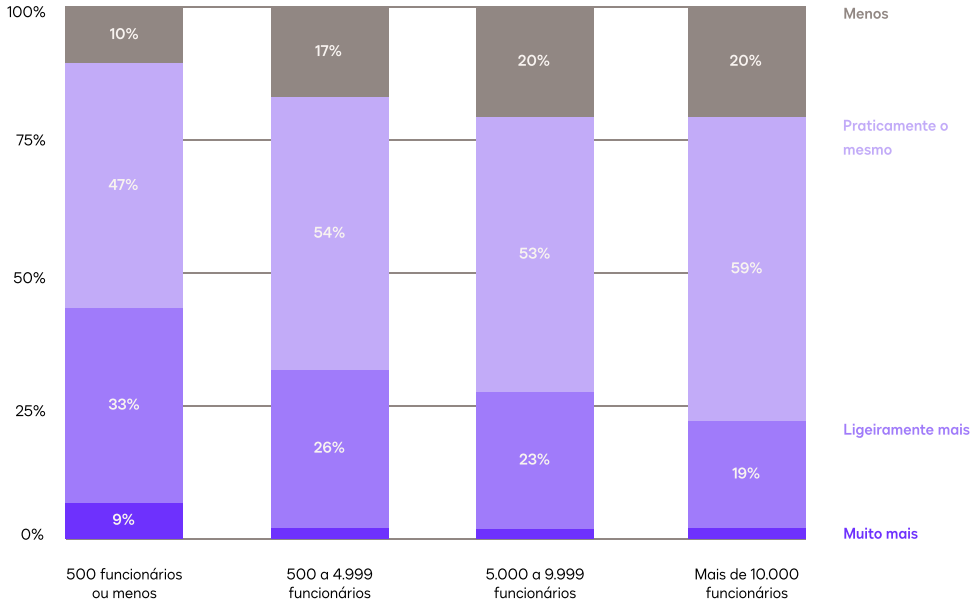
Verba economizada entre aqueles que utilizam a IDV




Qual das seguintes opções melhor descreve o investimento atual da sua organização em soluções/métodos de verificação de identidade/autenticação de usuários?

### Grandes organizações economizam mais com soluções de IDV

Investimento em IDV em comparação com concorrentes




Se você tivesse que estimar, aproximadamente quanto dinheiro sua organização economizou ao prevenir fraudes de clientes usando suas soluções existentes de verificação de identidade/ autenticação de usuário?

## Conclusão principal

As organizações que investem significativamente em IDV obtêm uma série de benefícios, incluindo maior economia, menos incidentes de fraude de identidade, melhor percepção da marca, experiências aprimoradas do cliente e uma vantagem competitiva sobre seus concorrentes.

# As principais organizações adotam a tecnologia para combater a fraude

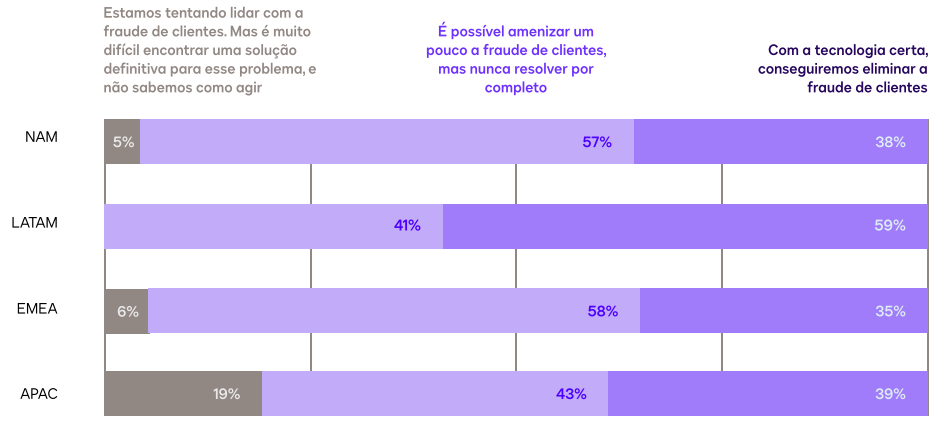
A confiança das empresas em gerenciar fraudes de identidade varia muito. 56% acreditam que podem reduzir fraudes, mas nunca eliminá-las por completo, enquanto 40% acreditam que podem solucioná-las completamente utilizando a tecnologia certa. Grandes organizações com mais de 10 mil funcionários tendem a acreditar na redução.

Apesar dos diferentes tipos de percepção, a maioria das organizações está alinhada em uma solução:

**70% concordam** que a melhor forma de reduzir o risco financeiro da fraude de identidade é investir fortemente em tecnologia.

Este investimento de 70% em tecnologia supera outras abordagens, como o investimento em funcionários e talentos (18%) e o investimento em seguro contra crimes empresariais para compensar os custos de fraude (11%), tidas como opções reativas que buscam reparar danos em vez de defender proativamente suas organizações contra ameaças.

### As organizações da América Latina são mais otimistas em solucionar por completo o problema da fraude




com qual das seguintes afirmações você concorda mais?

## Descobertas geracionais

Líderes organizacionais das gerações Millennial e Gen Z têm mais probabilidade do que "baby boomers" ou Gen X de acreditar que a fraude pode ser completamente resolvida com a tecnologia certa.

# A ferramenta de IDV mais comum é a autenticação multifator

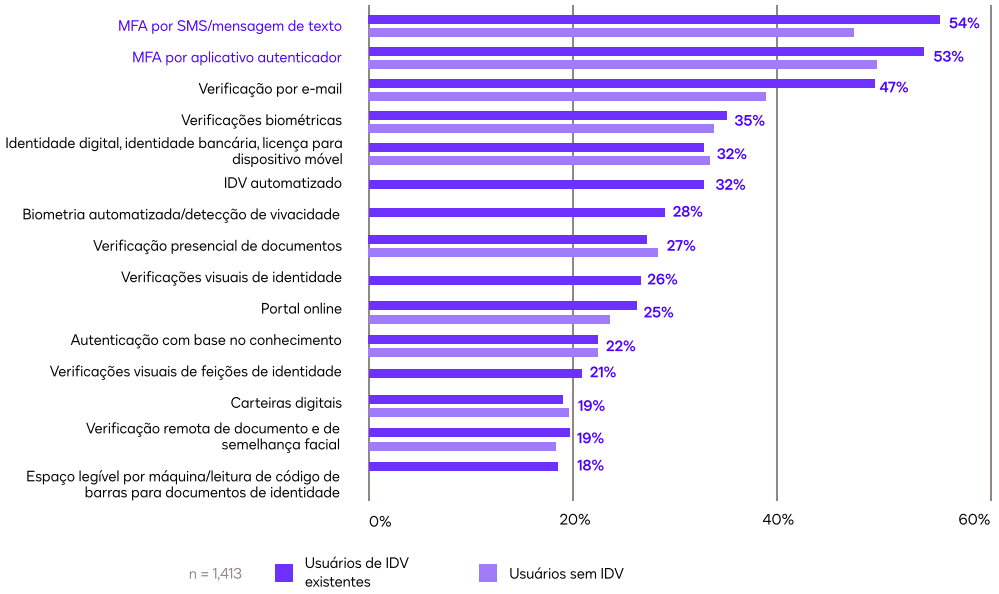
As organizações utilizam ferramentas de IDV em diversos pontos de contato na jornada do cliente, mas a etapa mais comum é na autenticação de nome de usuário e senha—onde as organizações relatam a maior quantidade de fraudes.

**A autenticação multifator (MFA) é a ferramenta mais comum utilizada por organizações para verificar e autenticar identidades, seja por meio de SMS e texto ou com um aplicativo de autenticação.**

A popularidade da MFA é justificada: é um dos métodos mais antigos de identificação digital, e os clientes estão habituados a ela, reduzindo o atrito para os usuários enquanto fornece uma camada fundamental de segurança.

## MFA é a ferramenta de verificação de identidade e autenticação mais comum

Tipos de verificação de identidade e autenticação de usuário atualmente em uso




Quais dos seguintes tipos de verificação de identidade/autenticação de usuário sua organização usa atualmente? Marque todas as opções válidas.

## Verificações biométricas são mais comumente usadas na APAC; verificação de e-mail é mais comumente usada na América Latina

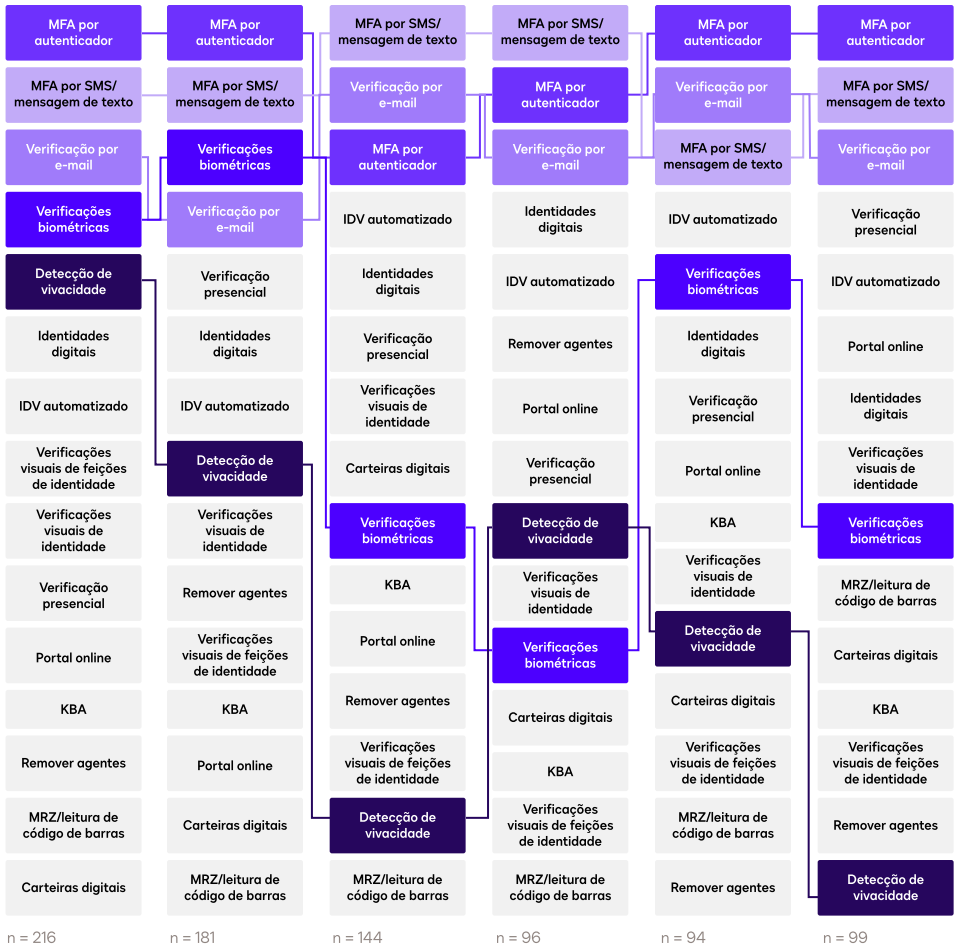

Quais dos seguintes tipos de verificação de identidade/autenticação de usuário sua organização utiliza atualmente?

Os tomadores de decisão na França e na Alemanha adotam ferramentas biométricas a uma taxa inferior à dos tomadores de decisão no Reino Unido e em outras regiões.

## Descobertas do setor

Líderes organizacionais que são Millennials ou da Gen Z acreditam que a biometria é importante para a autenticação online. Segundo pesquisas da IDEX Biometrics, 47% desse grupo demográfico usaram métodos de segurança biométrica no último mês. Dentre esse grupo, 52% preferem a autenticação biométrica a outros métodos.

### Os setores bancário/financeiro e de TI são os mais propensos a utilizar verificações biométricas

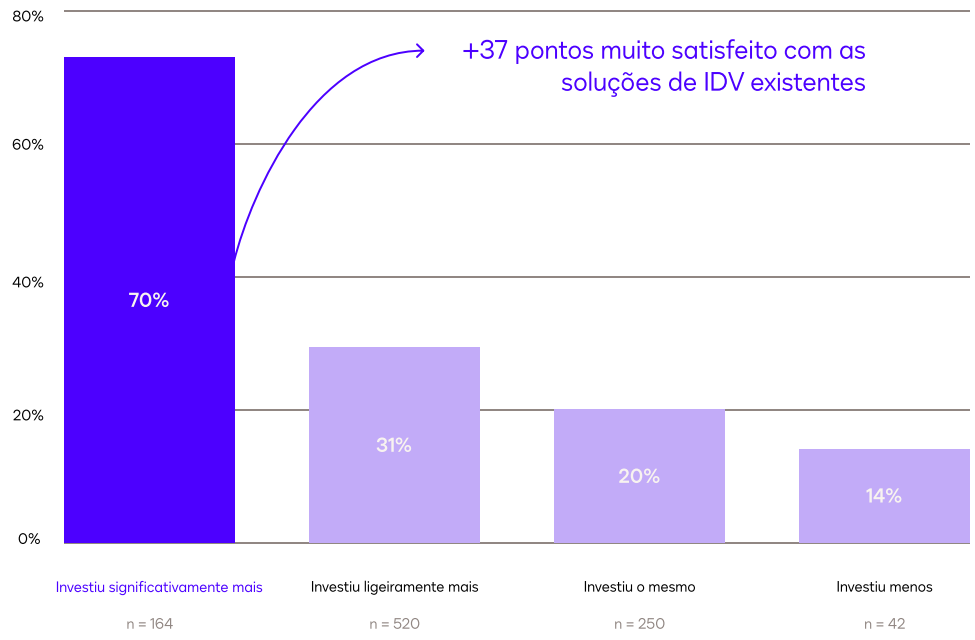



Quais dos seguintes tipos de verificação de identidade/autenticação de usuário sua organização utiliza atualmente?

# Empresas que investem mais em IDV relatam maior satisfação com ferramentas de IDV

Embora a MFA seja a ferramenta mais comum, as organizações que investem mais em segurança acabam adotando medidas adicionais. Por exemplo, investidores de alto nível têm maior probabilidade de utilizar ferramentas sofisticadas, como verificações biométricas e recursos de identificação visual no momento de login. Este esforço adicional está associado a uma maior satisfação dos clientes com as soluções de IDV.

**Um investimento maior em IDV em comparação com os concorrentes está relacionado a uma satisfação maior**




Qual é o nível de satisfação da sua organização com a verificação de identidade/autenticação de usuário utilizada atualmente?

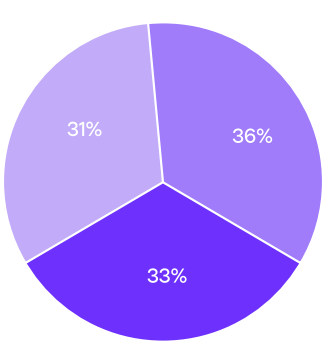
80%

das organizações estão dispostas a submeter os clientes a níveis intensos de autenticação, mesmo que isso gere algum tipo de incômodo.

# As organizações usam diversos métodos para determinar o nível adequado de autenticação para cada cliente.

Mais de duas em cada três organizações atualmente utilizam diferentes níveis de autenticação em seus processos de segurança. Ou seja, uma organização pode implementar meios adicionais de autenticação para clientes considerados de alto risco devido a fatores como o endereço IP, a distância do remetente ou o país. Ela também pode adotar outras medidas para tipos específicos de interações com clientes, como abrir uma nova conta ou acessar suas informações financeiras.

**A maioria das organizações altera os níveis de autenticação para cada transação com base no perfil de risco do cliente ou no tipo de solicitação do cliente**




Níveis de autenticação

- **36%** Usamos diferentes níveis de autenticação com base no perfil de risco calculado do cliente
- **31%** Usamos diferentes níveis de autenticação com base no tipo de interação/solicitação que os clientes estão realizando
- **33%** Gerenciamos todas as interações de verificações de identidade digital com os clientes usando o mesmo nível de autenticação

Qual afirmação descreve melhor como sua organização lida com a prevenção de fraudes?

As organizações usam uma variedade de critérios para determinar o nível adequado de autenticação para cada interação com o cliente, e 62% afirmam encontrar dificuldades em escolher. As empresas normalmente se apoiam em políticas internas e perfis de risco dos clientes, mas consideram o **valor da transação e a análise de custo-benefício como os critérios mais importantes** para avaliar o risco.

62%

dos entrevistados afirmam ter dificuldade em escolher o nível adequado de autenticação.

## Resultados regionais

O método de requisitos regulatórios é o mais comum usado para determinar os níveis de autenticação nos EUA. (17%). Ele também é mais comumente usado no Canadá (20%) e na França (16%) do que em outros países.

## Descobertas do setor

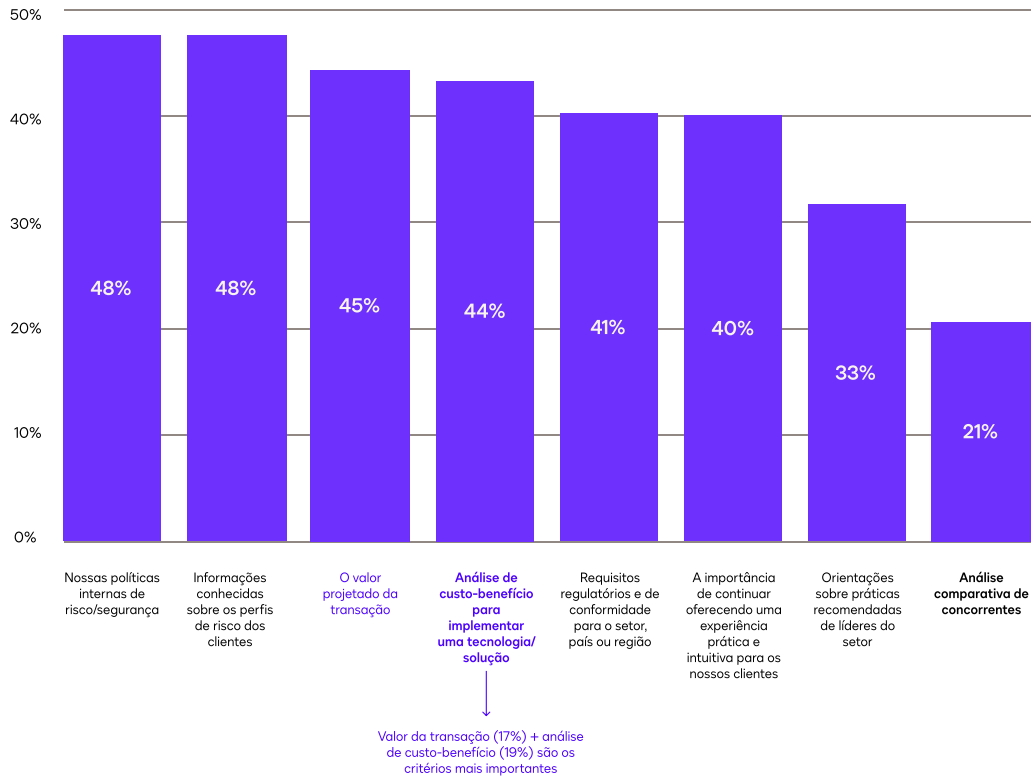
O método de requisitos regulatórios é o mais comum usado para determinar os níveis de autenticação no setor da saúde (29%). Ele também é mais comumente usado no segmento imobiliário (25%) e nos setores bancário e financeiro (20%) do que em outras indústrias.

### Políticas internas e perfis de risco do cliente são os métodos mais comuns para determinar o nível de autenticação adequado

**O valor da transação e a análise de custo-benefício são considerados mais importantes**

Como você decide qual nível usar?

Métodos mais usados para determinar o nível de autenticação

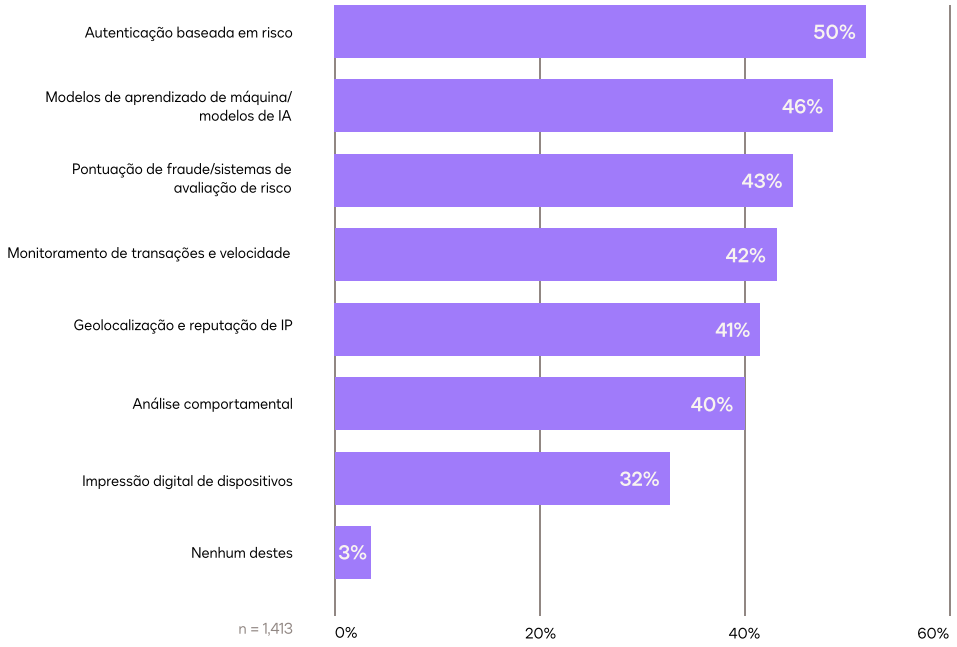



Quais fatores são considerados ao decidir qual nível de autenticação exigir de um usuário em uma interação específica?

Além de seguir uma variedade de métodos para avaliar o risco do cliente, as organizações utilizam uma ampla gama de ferramentas. As ferramentas de autenticação baseadas em risco mais comuns ajustam automaticamente o nível necessário de verificação de identidade para cada interação com base no risco avaliado do cliente. Um cliente de alto risco, por exemplo, pode acionar uma verificação biométrica, enquanto um cliente de baixo risco pode precisar apenas concluir a MFA.

## A autenticação baseada em risco é a ferramenta mais comum para avaliar o risco do cliente

Ferramentas para a avaliação do risco de autenticação




Qual das seguintes opções sua organização utiliza ao avaliar o risco associado a uma interação específica?

74%

das organizações planejam investir mais em soluções de IDV no futuro.

# As organizações planejam investir continuamente em IDV

Em face da evolução das fraudes de identidade, as organizações, independentemente do tamanho, região ou setor, continuam monitorando estratégias e ferramentas para reduzir riscos, mas permanecem unânimes: a tecnologia é a chave para solucionar o problema.

Os tomadores de decisão estão particularmente interessados no papel que a biometria e a IA generativa terão no combate à fraude. Comparado aos seus métodos atuais de autenticação e verificação de usuários:

84%

dos entrevistados acreditam que a autenticação biométrica será mais eficaz na redução do risco de fraude de clientes.

82%

dos entrevistados acreditam que a IA generativa será mais eficaz na redução do risco de fraude de clientes.

78%

dos entrevistados acreditam que a avaliação baseada em riscos será mais eficaz na redução do risco de fraude de clientes.

Dentre essas três soluções, a IA generativa é considerada a mais interessante para os clientes, contudo, muitos respondentes ainda se mostram apreensivos em relação a possíveis reações negativas. Enquanto 46% das organizações acreditam que seus clientes se sentirão frustrados ou descontentes com a adoção de IA generativa em seu processo de IDV, 59% preveem um aumento considerável em fraudes caso não a adotem.

# Conclusão

Organizações ao redor do mundo estão enfrentando uma nova conjuntura de riscos. O aumento da IA generativa e a adoção generalizada de transações digitais, juntamente com a falta de conscientização dos clientes sobre as melhores práticas de segurança, criaram um cenário de risco ideal para a fraude de identidade. À medida que a ameaça de fraude cresce, as principais empresas do mundo investem em ferramentas de segurança de ponta, como a IDV.

## Nossa pesquisa revelou uma descoberta importantíssima: A tecnologia é fundamental para identificar fraudes de identidade ao longo de toda a jornada do cliente, enquanto também reduz gastos desnecessários.

Com a IDV, as empresas podem desenvolver defesas poderosas para proteger sua imagem e seus resultados financeiros. Mesmo em ambientes de negócios limitados, investir em IDV oferece benefícios de longo prazo, como a redução de riscos e um ótimo retorno sobre o investimento. A segurança das informações pessoais garante aos clientes maior tranquilidade, sem comprometer a fluidez da experiência digital.

À medida que a IA avança, os custos da fraude de identidade aumentarão. Para organizações que desejam proteger seus clientes, defender suas reputações e atrair as gerações mais novas, que estão mais acostumadas a interagir com ferramentas de verificação de identidade digital, adotar uma postura proativa e investir em tecnologia antifraude nunca foi tão crucial.

# Principais recomendações

### Reavaliar suas defesas antifraude.

Há um bom motivo pelo qual 74% das organizações analisam novas soluções pelo menos uma vez por ano: Os fraudadores estão constantemente aprendendo e adotando novas técnicas, e as empresas precisam atualizar suas defesas de maneira correspondente. A maneira mais fácil de fazer isso é trabalhar com fornecedores que aprimoram regularmente suas próprias ferramentas de defesa contra as táticas e obstáculos mais recentes.

### Investir em tecnologia impulsionada por IA.

Segundo a maioria dos tomadores de decisão entrevistados, a melhor forma de reduzir o risco financeiro da fraude de identidade é investir maciçamente em tecnologia. Em vez de gastar recursos valiosos em medidas reativas (como seguros) ou tempo contratando mais funcionários, investir em soluções de verificação de identidade baseadas em IA oferece às empresas uma ótima vantagem no combate à fraude de identidade, especialmente contra ameaças sofisticadas como a IA generativa.

### Identificar as etapas mais vulneráveis do ciclo de vida do cliente.

Conforme revelado pela nossa pesquisa, a criação de conta, o login e a autorização de pagamento são as etapas da jornada do cliente mais impactadas pela fraude de identidade. Considere essas áreas para concentrar seus esforços iniciais, entretanto, recomendamos trabalhar com uma equipe qualificada para mapear a jornada dos seus próprios clientes e identificar onde sua empresa enfrenta mais riscos.

### Proteger contra fraudes e oferecer uma ótima experiência de usuário não são excludentes.

Os respondentes mais perceptivos da nossa pesquisa observaram que adotar melhores medidas contra fraudes não significa comprometer a experiência do usuário. Pelo contrário, a IDV pode complementar a experiência do cliente e melhorar a imagem da marca. Para proporcionar a melhor experiência de IDV e garantir uma implementação integrada, incentive a colaboração entre suas equipes de risco, produto e crescimento e priorize soluções intuitivas e automatizadas.

### Calcular o ROI dos seus investimentos em medidas antifraude.

Organizações que investiram significativamente mais do que seus concorrentes em IDV passaram a economizar mais do que aquelas que continuaram investindo a mesma quantia de sempre. Para aumentar o ROI, considere alguns fatores importantes ao pesquisar novas tecnologias, incluindo a redução esperada no custo da fraude, economia em relação aos funcionários por meio da automação, redução dos custos de aquisição de clientes e ganhos de receita com novos clientes.

### Incorporar as expectativas dos jovens consumidores.

Os tomadores de decisão das gerações Millennial e Gen Z nas organizações têm maior probabilidade de entender o valor das ferramentas de IDV para melhorar a segurança e percepção da marca. Há um paralelo semelhante com seus clientes: os consumidores das gerações Millennial e Gen Z preferem tecnologias inovadoras, como autenticação biométrica, entre outros métodos. As empresas podem ter certeza de que a adoção de tecnologias avançadas renderá o respeito de jovens clientes e funcionários, preparando suas organizações para o sucesso agora e no futuro.

## Saiba mais sobre o Docusign Identify e a Entrust.

# Apêndice: metodologia

O relatório sobre O futuro da verificação de identidade global é baseado em dados coletados durante uma pesquisa online quantitativa e global realizada entre 6 de novembro de 2024 e 4 de dezembro de 2024. Durante o processo de coleta de dados, nossa equipe de pesquisa entrevistou tomadores de decisão de negócios e TI de diversos setores e regiões. Os tomadores de decisão entrevistados neste relatório trabalham em organizações com 150 a mais de 10 mil funcionários e enfrentam os mesmos desafios de verificar as identidades de seus clientes.

## Total N=1,413

| Público | |
|---|---|
| Usuários de IDV existentes | N=976 |
| Autenticação de usuário/usuários digitais... | N=309 |
| Autenticação manual/usuários sem IDV | N=128 |
| **Mercado*** | |
| Estados Unidos e Canadá NAM | N=304 |
| Reino Unido EMEA | N=227 |
| Alemanha EMEA | N=233 |
| França EMEA | N=226 |
| México LATAM | N=104 |
| Brasil LATAM | N=104 |
| Austrália APAC | N=102 |
| Japão APAC | N=113 |

*Cada mercado foi pesquisado usando em seu idioma preferencial

| Tamanho da organização | |
|---|---|
| 150-499 | N=254 |
| 500-999 | N=266 |
| 1,000-2,499 | N=274 |
| 2,500-4,999 | N=204 |
| 5,000-9,999 | N=213 |
| 10,000+ | N=202 |
| | N=395 |

## Setores pesquisados

- Serviços bancários
- Serviços profissionais
- Educação
- Serviços financeiros
- Serviços de saúde
- Seguros
- Serviços de TI
- Ciências da vida
- Farmacêuticas
- Varejo e comércio eletrônico
- Construção e engenharia
- Manufatura
- Segmento imobiliário
- Telecomunicações
- Energia e serviços públicos

## Funções pesquisadas

- Operações de TI/ departamento de TI
- Segurança de TI
- Gestão de compras e cadeia de suprimentos
- Operações
- Experiência do cliente
- Gestão de produtos
- Gestão de risco/ conformidade
- Análise de fraude
- Recursos humanos
- Atendimento ao cliente
- Jurídico
- Vendas

2 A Docusign e a Entrust contrataram a TL;DR Insights, uma empresa de pesquisa de mercado, para conduzir a pesquisa.

## Sobre a Docusign e a Entrust

A Docusign dá vida aos acordos. Mais de 1,6 milhão de clientes e mais de um bilhão de pessoas em mais de 180 países usam as soluções da Docusign para acelerar seus processos de negócios e simplificar suas vidas. Com o gerenciamento inteligente de acordos, a Docusign desbloqueia dados críticos de negócios que antes estavam presos nos documentos. Dados desconectados nos sistemas custam tempo, dinheiro e oportunidades às empresas. Ao utilizar Docusign IAM, as empresas agora podem criar, formalizar e gerenciar acordos com soluções criadas pela empresa número 1 em assinatura eletrônica e gerenciamento do ciclo de vida de contratos (CLM).

A Entrust é uma líder inovadora em soluções de segurança centradas em identidade, fornecendo uma plataforma integrada de ofertas de segurança escaláveis e habilitadas pot IA. Permitimos que as organizações protejam suas operações, evoluam sem comprometimento e protejam suas interações em um mundo interconectado – para que possam transformar seus negócios com confiança. A Entrust oferece suporte a clientes em mais de 150 países e trabalha com uma rede global de parceiros. Temos a confiança das organizações mais confiáveis do mundo.

Docusign, Inc.
Avenida Jornalista Roberto Marinho, 85
2° andar, Cj. 21 Cidade Monções
São Paulo, SP
docusign.com

Para mais informações
contato@docusign.com
Ligue para +5511 3330-1000