RSA

RSA.com

Relatório RSA ID IQ de 2026

A medição de segurança em identidades da RSA

Índice.

Sumário executivo.

O Relatório RSA ID IQ de 2026 solicitou a mais de 2.000 especialistas globais que detalhassem com que frequência a segurança de identidade falhou com eles, quanto perderam quando isso aconteceu e quais vulnerabilidades eles mais temem.

O que nos contaram foi alarmante: a identidade falhou em mais organizações do que no ano passado, causando ainda mais prejuízos financeiros. A menos que os líderes ajam, os riscos que suas organizações enfrentam se tornarão mais graves — e as consequências desses riscos lhes custarão ainda mais.

Os dados revelam uma crescente lacuna na segurança de identidade, com a maioria das organizações ainda utilizando soluções antigas que não conseguem lidar adequadamente com os novos desafios. A maioria dos usuários ainda depende de senhas para autenticação; suas organizações relatam violações mais frequentes e maiores prejuízos.

Ao mesmo tempo, enfrentam dificuldades para avançar rumo a sistemas sem senha devido a ambientes operacionais complexos e casos de uso desafiadores.

As organizações não possuem as capacidades necessárias para se defenderem contra engenharia social e contornarem ataques às suas centrais de atendimento de TI, mesmo que essa tática esteja se tornando um risco cada vez mais alarmante. E embora as organizações monitorem identidades humanas, de máquinas e de serviços, fica claro, pela frequência de violações de dados, que elas não estão usando essas informações para reduzir os riscos de forma proativa ou eficaz.
Talvez devido a esses riscos crescentes, especialistas relatam que estão apostando todas as fichas na IA para a segurança cibernética.

Em todos os setores, mais usuários acreditam que a IA contribuirá mais para a segurança cibernética do que para o cibercrime, com um número recorde de organizações relatando planos para integrar alguma forma de IA em sua infraestrutura de segurança cibernética. As organizações também relatam, por ampla maioria, que a IA ativa para segurança cibernética será a principal funcionalidade que priorizarão.
Deixarei que as conclusões falem por si. E embora esta informação por si só seja útil, é essencial que os líderes ajam com base nela, priorizando a autenticação sem senha, implementando métodos modernos para se defenderem contra fraudes em serviços de suporte, identificando e resolvendo proativamente os riscos de identidade antes que se transformem em violações e utilizando a IA como um multiplicador de forças para automatizar e agilizar a tomada de decisões.

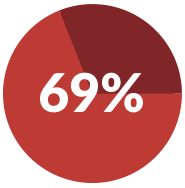
O primeiro passo para resolver qualquer problema é admitir que ele existe. O Relatório RSA ID IQ de 2026 deixa claro que existem grandes preocupações com a segurança de identidade da maioria das organizações.

A segurança da identidade simplesmente falha com muita frequência em diversas organizações. A probabilidade de uma violação de segurança — e o custo da inação — são simplesmente altos demais para manter o status quo.

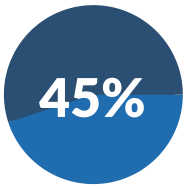
Greg Nelson, CEO, RSA

Principais conclusões do Relatório RSA ID IQ de 2026

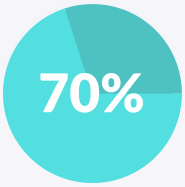
O Relatório RSA ID IQ de 2026 compartilha informações de 2.120 especialistas que atuam em cibersegurança, gerenciamento de identidade e acesso (IAM), TI ou outras áreas. As principais conclusões incluem:



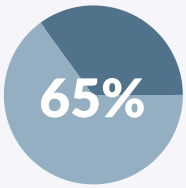
das organizações relataram uma violação de identidade nos últimos três anos, um aumento de 27 pontos percentuais em relação a 2025.



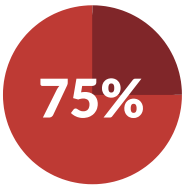
das organizações afirmaram que as violações de dados relacionadas à identidade lhes custaram mais do que a violação de dados média.



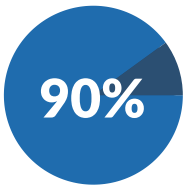
das organizações afirmaram que as violações de identidade lhes causaram danos significativos.



das organizações disseram estar seriamente preocupadas com a possibilidade de seus serviços de suporte ou help desk de TI não conseguirem impedir um ataque de engenharia social.

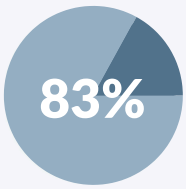


das organizações estão operando em ambientes híbridos, um aumento de 5 pontos percentuais em relação a 2025.

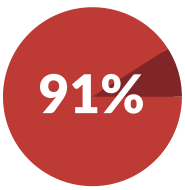


das organizações relataram desafios na transição para a autenticação sem senha.

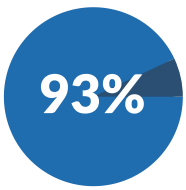
As organizações continuam a usar senhas como seu principal método de autenticação.



99% das organizações acreditam que a IA contribuirá mais para a segurança cibernética do que para o combate ao cibercrime, um aumento de 3% desde 2025.



das organizações planejam implementar alguma forma de IA em sua infraestrutura tecnológica no próximo ano, um aumento de 12 pontos percentuais desde 2025.



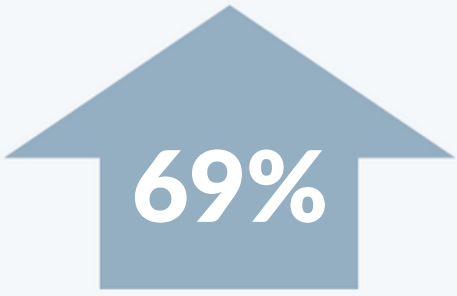
da maioria das organizações não atingiu o nível ideal de maturidade Zero Trust.

Mais violações de identidade causaram ainda mais danos este ano.

A análise das respostas da pesquisa revelou que as organizações sofreram mais violações resultantes de falhas na segurança de identidade este ano: 69% das organizações relataram uma violação nos últimos três anos, um aumento de 27 pontos percentuais desde o Relatório RSA ID IQ de 2025.

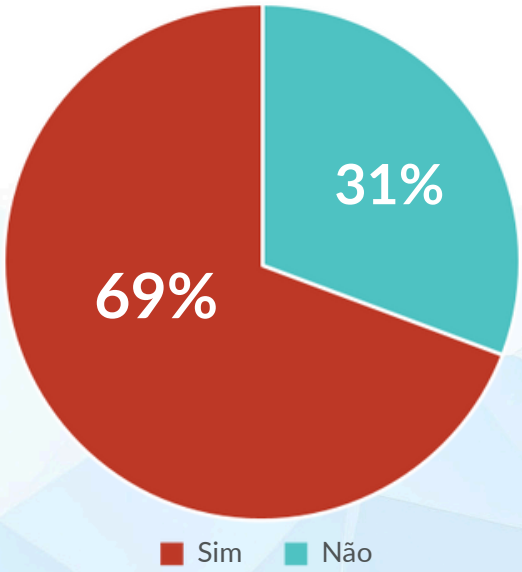
Além de ocorrerem com mais frequência, essas violações causaram maiores danos e tiveram maior impacto. custos. Mais de um quinto (21%) de todos os entrevistados relataram que uma violação de identidade lhes custou entre US$ 5 e 10 milhões, enquanto quase um quarto (24%) relatou que o custo de uma violação de identidade ultrapassou US$ 10 milhões. As violações que custaram mais de US$ 10 milhões aumentaram três pontos percentuais em comparação com o relatório do ano passado.

Esses números são alarmantes em qualquer perspectiva. São particularmente preocupantes quando comparados ao custo médio global de uma violação de dados resultante de qualquer vetor de ataque: o custo da **IBM um relatório da Data Breach Report 2025** revelou que uma violação de dados custa, em média, US$ 4,44 milhões. Quando a identidade é comprometida, as organizações sofrem perdas consideráveis. Não é de se admirar que 70% dos entrevistados tenham classificado a gravidade de uma violação como quatro ou cinco em uma escala de cinco pontos.



das organizações relataram ter experimentado
Uma violação de identidade nos últimos 3 anos
representa um aumento **de 27 pontos percentuais.**

Sua organização sofreu alguma violação de identidade nos últimos tempos **três anos?**



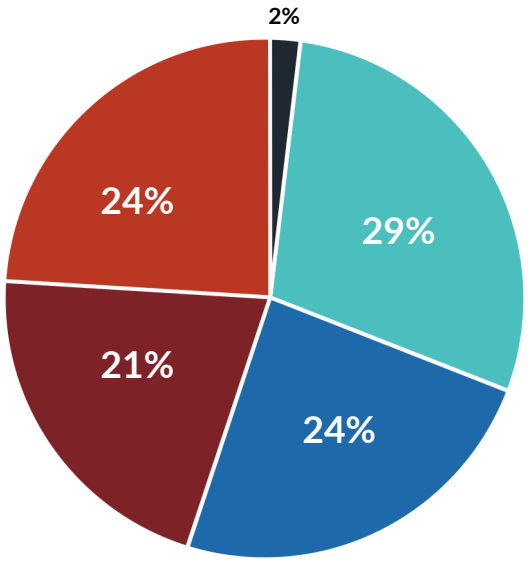
24%

Das organizações que sofreram violações de identidade, as que relataram custos com a violação foram as que, de acordo com relatos, representaram um custo significativo para a segurança.

Mais de 10 milhões de dólares, um aumento de 3 pontos percentuais em relação a 2025.

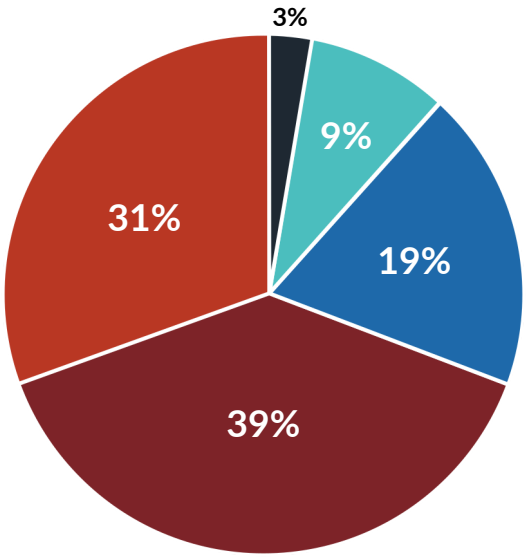
Quanto dinheiro você acredita que sua organização perdeu devido a violações de dados relacionadas à identidade ao longo dos anos?

nos últimos três anos?



Não sei | Menos de 1 milhão de dólares | Entre 1 milhão e 5 milhões de dólares | Entre 5 milhões e 10 milhões de dólares | Mais de 10 milhões de dólares

Se você sofreu uma violação de identidade nos últimos três anos, avalie a gravidade do impacto disso em sua vida pessoal organização de 1 a 5.



1 | 2 | 3 | 4 | 5

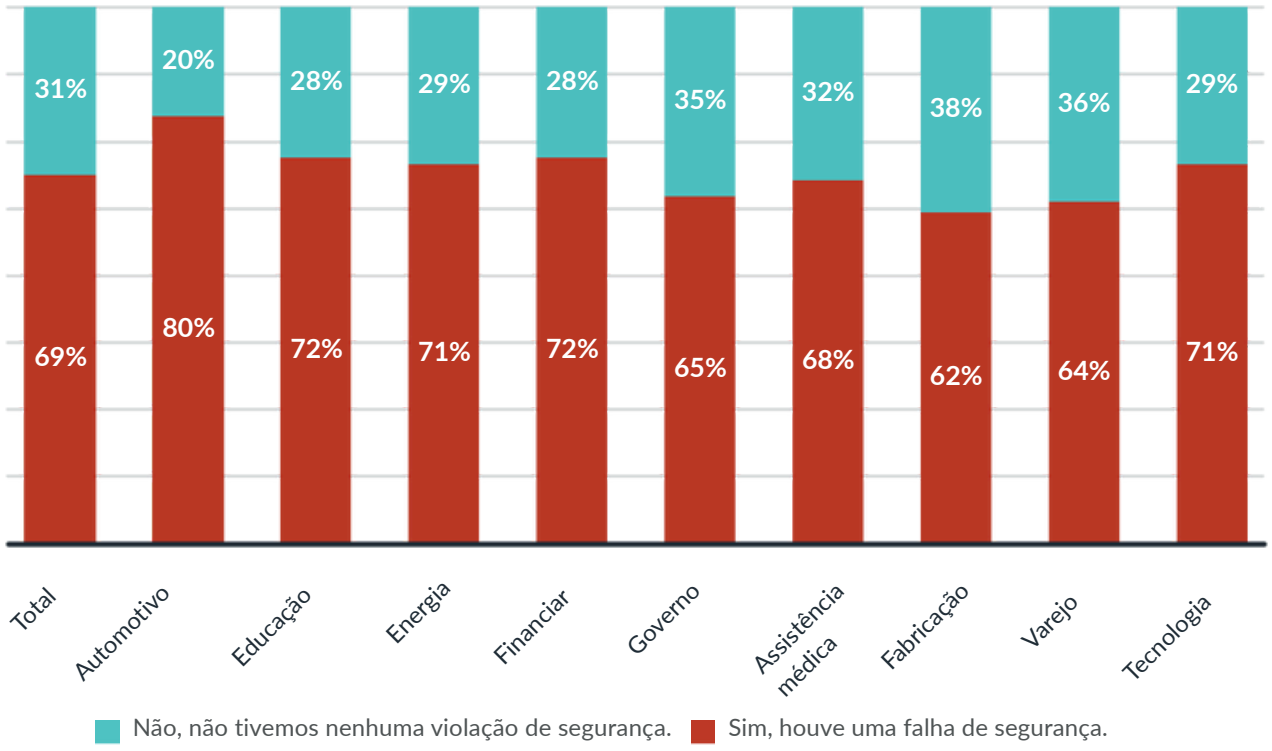
$ 4,44 Milhão

Custo médio global de todas as violações de dados, segundo o relatório **"IBM Cost of a Data Breach Report 2025"** (Relatório de Custo de Violação de Dados da IBM de 2025).

Violações de segurança por setor

Ao analisar as taxas de violação de dados por setor, a indústria automotiva (80%), o setor financeiro (72%), o setor de energia e serviços públicos (71%) e o setor de tecnologia (71%) apresentaram a maior frequência de violações de dados. O varejo (64%) e o setor manufatureiro (62%) representam os setores menos afetados por violação de dados.

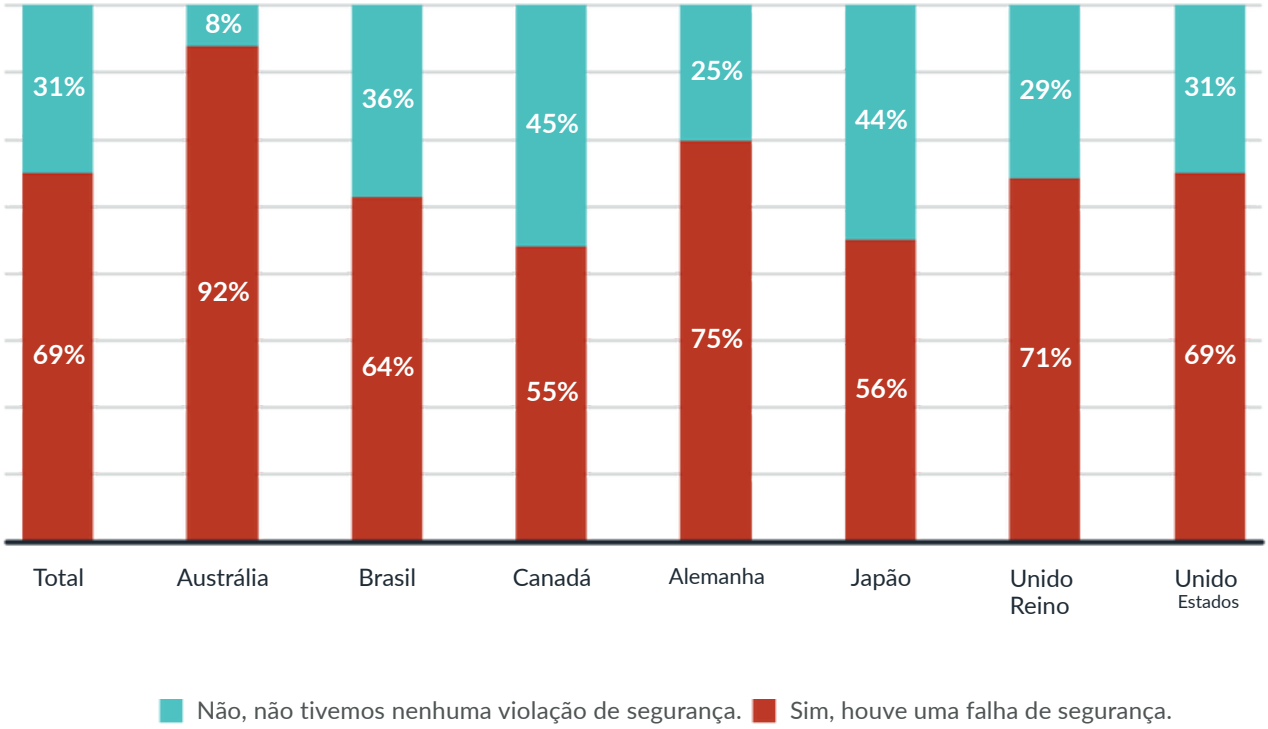
Por setor: Sua organização sofreu alguma violação de identidade nos últimos três anos?



Violações de segurança por país

Por país, a Austrália (92%), a Alemanha (75%), o Reino Unido (71%) e os Estados Unidos (69%) relataram as violações de identidade mais frequentes nos últimos três anos, enquanto o Japão (56%) e o Canadá (55%) relataram o menor número de casos. Explicamos mais adiante neste relatório como certas práticas se correlacionam com a frequência e o impacto dessas violações.

Por país: Sua organização sofreu alguma violação de identidade nos últimos três anos?



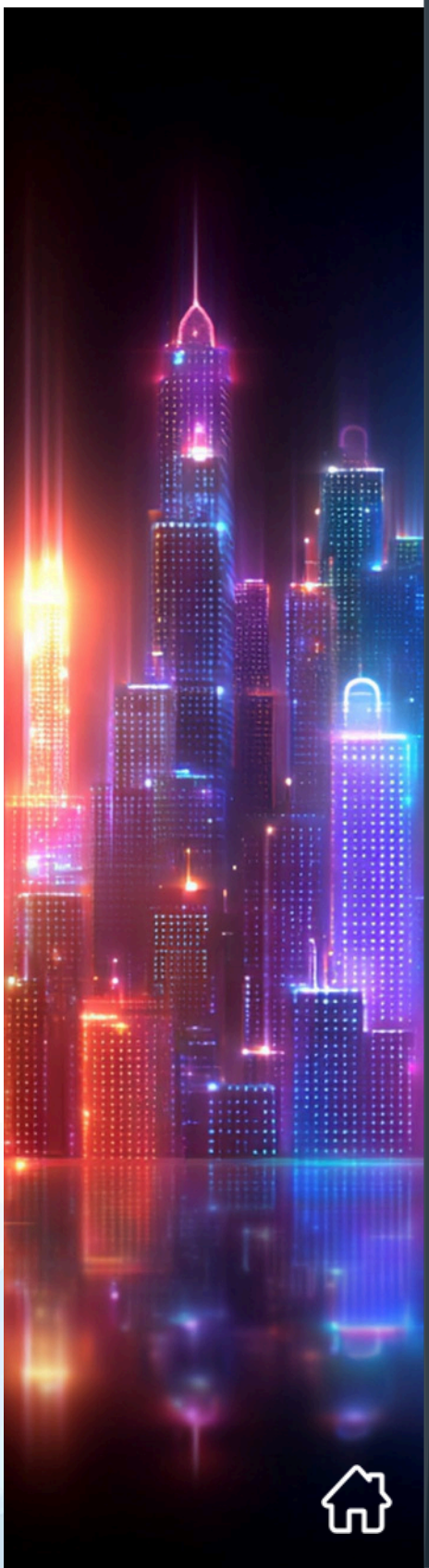
Zero Trust “progresso”

Embora apenas 7% das organizações relatem ter atingido o nível ideal de maturidade Zero Trust para identidade, conforme definido pela CISA, a maioria — 57% — acredita ter alcançado o estágio “Avançado” de Zero Trust, que inclui:

- MFA resistente a phishing
- Consolidação e integração segura de repositórios de identidades
- Avaliações automatizadas de risco de identidade
- Acesso baseado em necessidades/sessões

Essa confiança é contradita pelo fato de que 69% dos **Foram registradas violações de segurança em diversas organizações, e 70% delas relataram que essas violações foram graves.**

Isso não significa desencorajar as organizações de aprimorarem sua postura de Confiança Zero — muito pelo contrário. Em vez disso, a discrepância entre o estágio em que as organizações acreditam estar em sua jornada de Confiança Zero e a frequência com que sofrem violações de segurança deve servir de alerta para que os líderes de segurança intensifiquem seus esforços de proteção.



Os riscos de cibersegurança que tiram o sono dos especialistas

Os entrevistados selecionaram o phishing como o vetor de ameaça que representa o risco de cibersegurança mais significativo para suas organizações. E há um bom motivo para priorizar o phishing: ano após ano, o phishing (que leva ao roubo de credenciais) e o uso de credenciais roubadas permanecem entre os ataques mais frequentes e de maior impacto. Uma das melhores maneiras de evitar o phishing é remover as credenciais que os phishers tentam roubar: em vez de usar segredos compartilhados, as organizações devem se esforçar para implementar autenticação sem senha e resistente a phishing.

192 dias

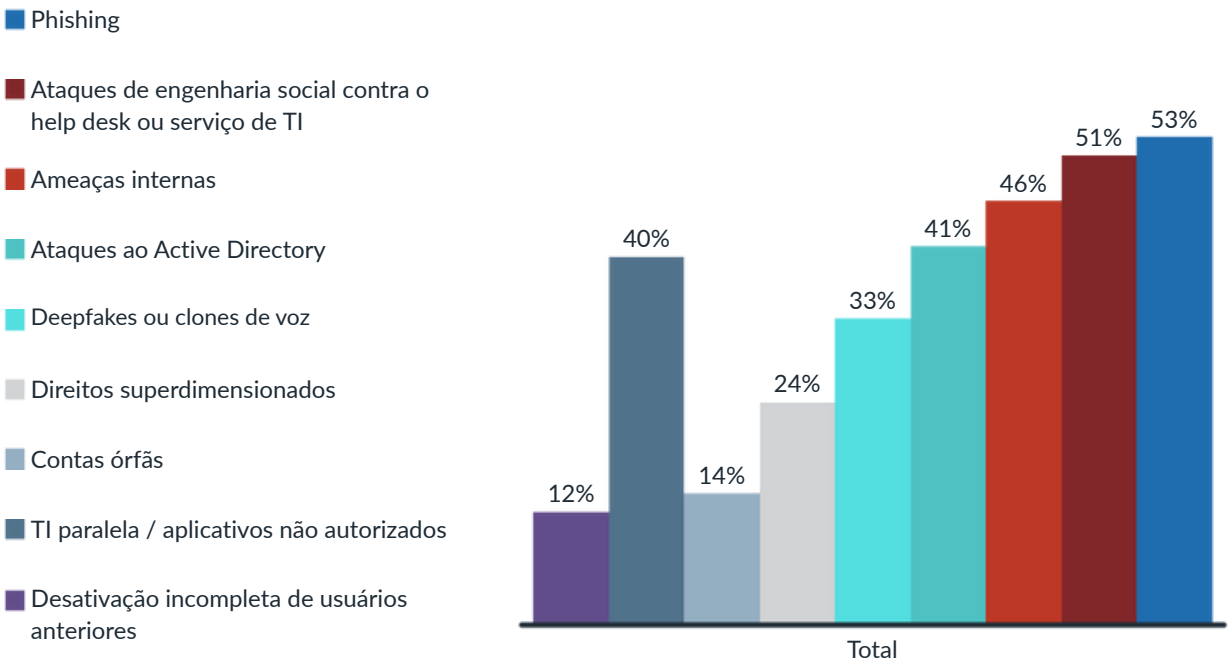
Tempo médio que as organizações levam Identificar e conter uma violação originada por phishing.

$ 4,8 Milhão

Custo médio das violações de dados originário de phishing

Relatório da IBM sobre o custo de uma violação de dados em 2025

Embora o phishing seja um risco de segurança cibernética perene, os riscos emergentes estão rapidamente ganhando terreno como ameaças significativas. 51% dos entrevistados afirmaram que os ataques de engenharia social contra o help desk ou service desk de TI representam o risco mais significativo para suas organizações.



Seu Help Desk precisa de ajuda.

Considerando os ataques de grande repercussão contra o suporte técnico de empresas como MGM Resorts, Caesars Entertainment Group, Marks & Spencer, Co-op e House of Dior, há bons motivos para priorizar esse risco. Como demonstrado pelo grupo Scattered Spider e outros cibercriminosos, existe um risco significativo quando criminosos cibernéticos tentam burlar a autenticação multifator (MFA) ligando para um suporte técnico ou central de atendimento se passando por um usuário legítimo e solicitando a criação de novas contas, a suspensão da MFA ou o cadastro de novos usuários ou dispositivos. De fato, especialistas em segurança cibernética classificaram os ataques de engenharia social contra o suporte técnico como o principal risco enfrentado por suas organizações.

Para agravar esse risco, as organizações simplesmente não estão utilizando métodos mais recentes e resistentes a phishing para garantir a identidade dos usuários.
A maioria das organizações utiliza métodos antigos para autenticar usuários: 58% usam senhas, 50% usam OTP (senha de uso único) e 46% usam segredos compartilhados. Em comparação, apenas 36% relataram usar autenticação bidirecional, que permite que ambas as partes verifiquem uma à outra, e apenas um quarto (25%) relatou usar soluções baseadas em risco para ajudá-los a priorizar usuários e casos de uso.

Quem está ligando?

Desde 2023, BlackCat, ALPHV,
O grupo Scattered Spider e outros cibercriminosos têm usado engenharia social para manipular funcionários do suporte de TI de diversas organizações, levando-os a lançar ataques de bypass de MFA (autenticação multifator), causando danos e prejuízos significativos:

Resorts MGM:

US$ 145 milhões

Caesars Entertainment:

US$ 15 milhões

Marks & Spencer:

£300 milhões

Métodos antigos para garantir a identidade dos usuários

58%
organizações usam senhas

50%
usar OTP

Novos métodos para garantir a identidade dos usuários

36%
usar garantia de identidade bidirecional

25%
usar soluções baseadas em risco

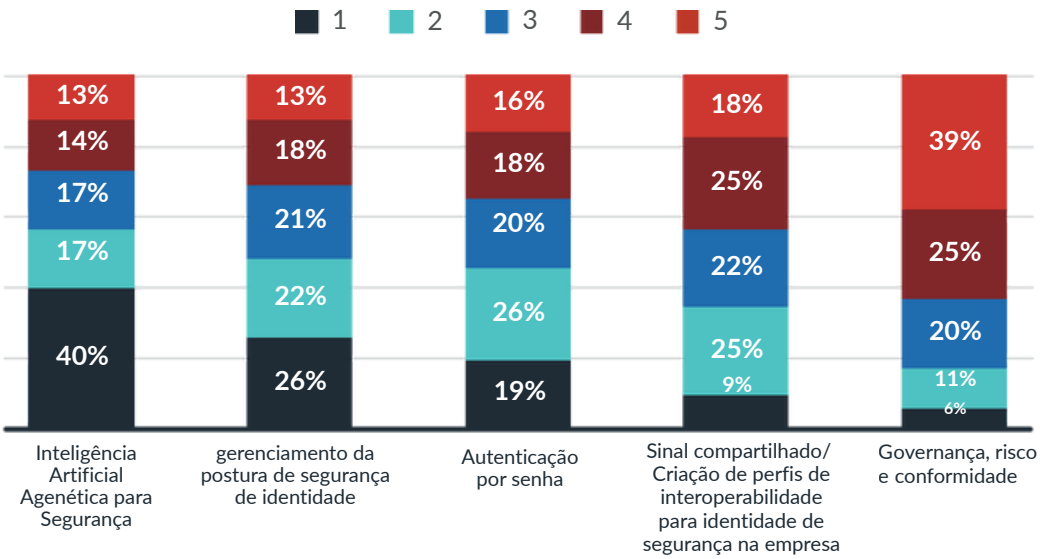
Um terço (33%) dos usuários afirmou que novas técnicas como deepfakes ou clones de voz representam o maior risco para suas organizações. Essas táticas podem se mostrar mais eficazes sem os métodos modernos de prevenção de ataques de bypass de MFA.

Alguns dos outros riscos que os especialistas mais temem se concentram nos estágios do ciclo de vida da identidade e na expansão descontrolada de privilégios. Ameaças internas (46%), TI paralela e aplicativos não provisionados (40%) e permissões excessivamente provisionadas (24%) destacam-se como riscos prioritários entre os usuários. Esses problemas podem ser agravados pela visibilidade inadequada do risco de identidade, processos manuais do ciclo de vida da identidade e mitigação retroativa de riscos.

As capacidades de cibersegurança que os utilizadores priorizam

A IA ativa para segurança foi a principal escolha entre os usuários por uma ampla margem, com 40% dos entrevistados a classificando como sua prioridade número um. O gerenciamento da postura de segurança de identidade (ISPM) — uma nova estrutura de cibersegurança que permite às organizações gerenciar riscos, aplicar políticas e fortalecer a conformidade em ambientes cada vez mais complexos — foi listada como a segunda capacidade mais crítica, sendo a principal escolha entre 26% dos entrevistados.

Classifique as seguintes capacidades de cibersegurança de 1 a 5.



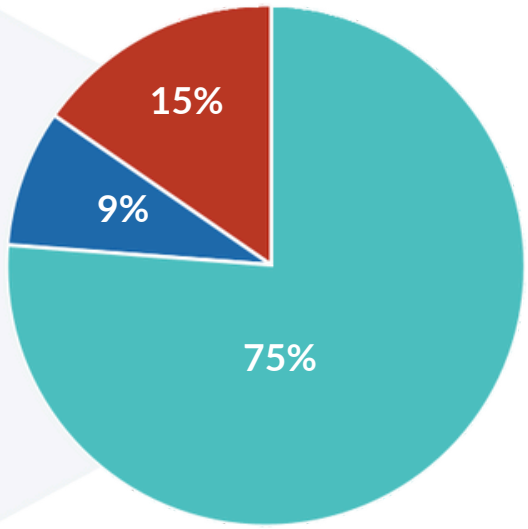
Ambientes operacionais

A maioria das organizações opera em ambientes híbridos, utilizando uma combinação de recursos em nuvem e locais. As empresas devem garantir que todos os usuários, dispositivos, permissões e ambientes estejam adequadamente protegidos.

75%

organizações operam em um modelo híbrido ambientes, um aumento **de 5 pontos percentuais**

Em qual dos seguintes ambientes você oferece suporte a aplicativos e usuários?

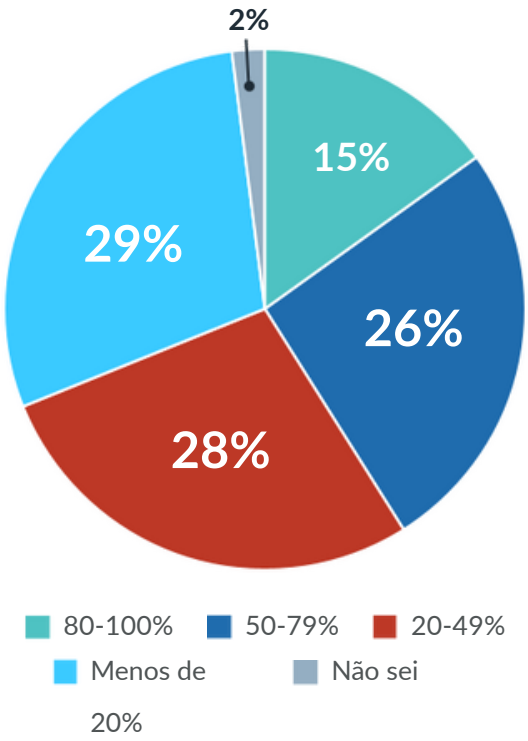


Híbrido (nuvem e local) Somente na nuvem Somente para instalação no local

Senhas — e os riscos associados a elas — persistem.

A maioria das organizações não utiliza autenticação sem senha como método principal. Isso é uma ótima notícia para os cibercriminosos: ano após ano, o uso de credenciais roubadas é a principal causa de violações de dados.
Ambientes complexos, casos de uso mistos e grupos de usuários diversos representam um desafio para as organizações na implementação de soluções abrangentes sem senha.
A persistência da autenticação baseada em senhas está correlacionada com violações de dados mais frequentes e mais custosas. As organizações australianas relataram uma das menores taxas de adoção de autenticação sem senha entre os países, com 50% ainda no estágio inicial de adoção.
As organizações australianas também sofrem com a maior taxa de violações de dados relacionadas à identidade entre os países (92% das organizações r elataram uma violação). violação nos últimos três anos), a mais grave consequências (47% disseram que a violação causou grandes prejuízos) e as maiores perdas financeiras (44% relataram que uma violação lhes custou mais de 10 milhões de dólares).

Qual a porcentagem de seus usuários que utilizam principalmente formulários sem senha para concluir a autenticação?



Compare esses resultados com os do Japão, que apresentou a maior incidência de uso de autenticação sem senha como método principal (37% das organizações afirmaram utilizá-la em pelo menos 80% dos casos). O Japão também apresenta uma das menores taxas de violações de dados relacionadas à identidade (56% das organizações) e consequências menos graves.

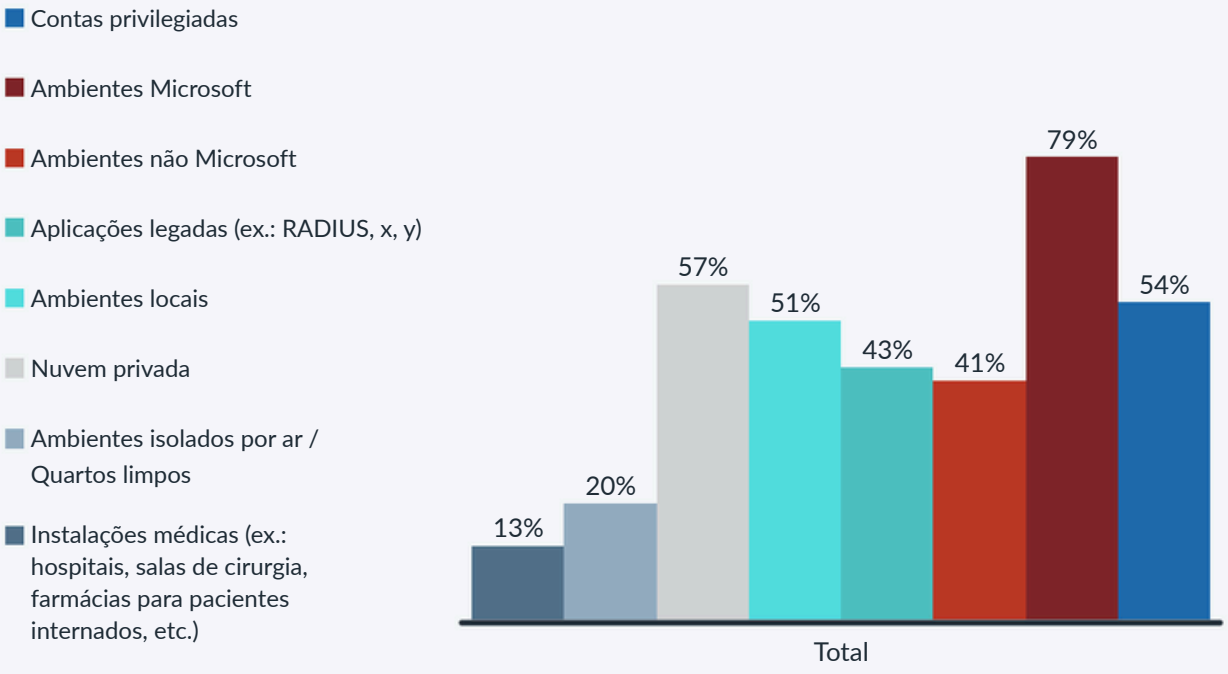
	organizações australianas	organizações japonesas
Classificação geral do uso de autenticação sem senha, por país.	#5	#1
Percentual de usuários que usam autenticação sem senha como principal forma de autenticação.	10%	37%
Usuários que relataram uma violação de segurança.	92%	56%
Percentual de usuários que relataram que a violação causou danos graves (5 de 5).	47%	44%
Percentual de violações que custaram mais de US$ 10 milhões.	24%	28%

> “Ambientes complexos, casos de uso mistos e grupos de usuários diversos representam um desafio para as organizações na implementação de soluções abrangentes sem senha.”

O que está causando a lentidão do Passwordless?

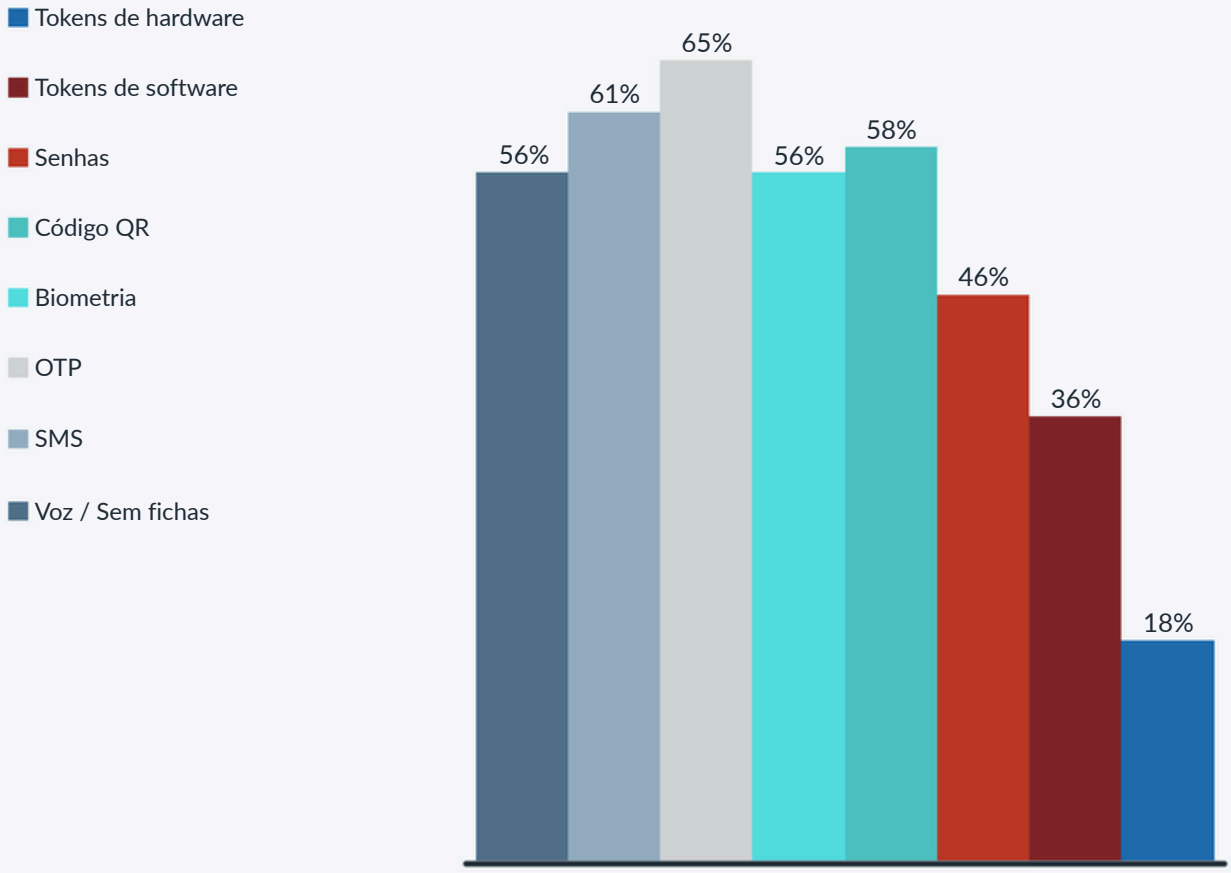
Ao implementar sistemas sem senha, a maioria das organizações precisa levar em conta uma ampla gama de usuários e casos de uso. Acreditamos que isso representa um desafio significativo para as organizações, visto que a tecnologia sem senha ainda está em desenvolvimento.

Quais dos seguintes ambientes, grupos de usuários ou casos de uso sua organização oferece suporte?



Como a maioria das organizações opera em ambientes híbridos e precisa dar suporte a diversos usuários e casos de uso, os especialistas em identidade estão se preparando para usar uma ampla gama de formatos para fornecer a todos os usuários autenticação sem senha.

Qual dos seguintes formatos você pretende usar para implementar soluções sem senha?



Especialista em IAM

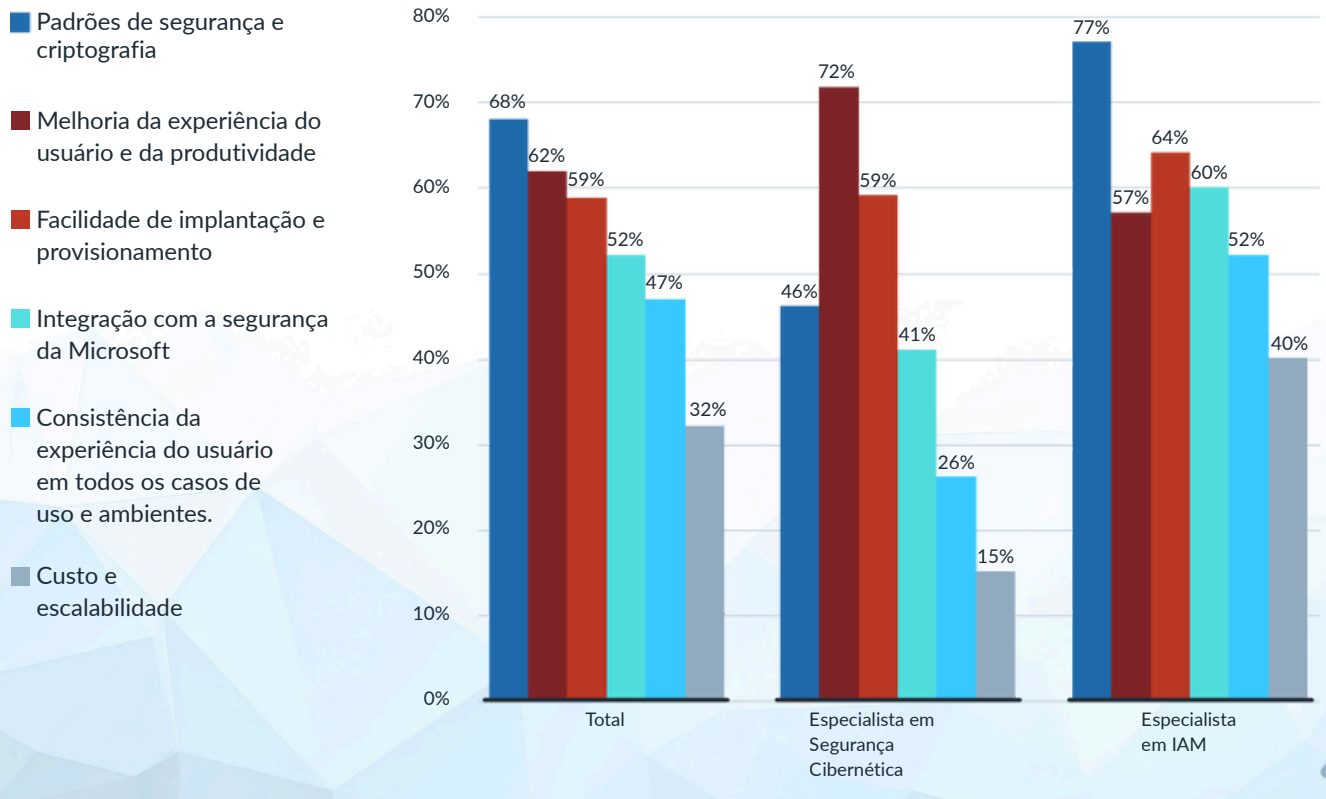
A luta pela ausência de passwords

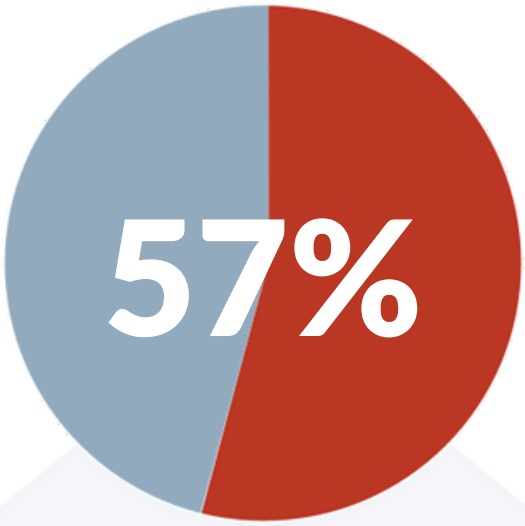
Quase todos (90%) os entrevistados disseram que havia algum desafio que os impedia de implementar soluções sem senha. Mas, para esses usuários, não há um único desafio específico a ser enfrentado. Em vez disso, existem três: 57% dos entrevistados disseram que as preocupações com a segurança estavam atrasando a implementação de soluções sem senha, 56% citaram preocupações com a experiência do usuário e 52% disseram que a falta de suporte completo da plataforma (incluindo aplicativos legados e sistemas de terceiros) era o principal desafio que os impedia de implementar soluções sem senha.

Essas são preocupações vitais que as organizações devem superar para implementar o acesso sem senha de forma eficaz. Curiosamente, as restrições mais práticas representam um problema muito menor: apenas 47% dos usuários disseram não ter recursos financeiros para implementar o acesso sem senha.

Não existe um único desafio claro que as organizações devam abordar. Para atender às diferentes prioridades dos especialistas em relação a sistemas sem senha (e para superar os desafios que os impedem de implementá-los), as empresas precisam equilibrar padrões de segurança e criptografia, melhoria da experiência do usuário e facilidade de uso.

Quais são os fatores mais importantes para você na escolha de uma solução sem senha?





As organizações não usam sistemas sem senha como seus principal meio de autenticação

Ano novo, mesmo problema

Ano após ano, as senhas são uma das principais causas de violações de dados:

Relatório de Investigações de Violação de Dados da Verizon de 2025: Abuso de credenciais “ainda é o vetor mais comum.”

Relatório de Investigações de Violações de Dados da Verizon de 2024: “Nos últimos 10 anos, credenciais roubadas apareceram em quase um terço (31%) das violações.”

Relatório de Investigações de Violações de Dados da Verizon de 2023: "As credenciais ganharam muita importância nos últimos cinco anos, já que o uso de credenciais roubadas se tornou o ponto de entrada mais comum para violações de segurança."

O Relatório de Investigações de Violações de Dados da Verizon de 2022 observou que práticas inadequadas de senhas foram "uma das principais causas de violações de dados" todos os anos nos últimos quinze anos.

Monitoramento e gerenciamento de riscos de identidade

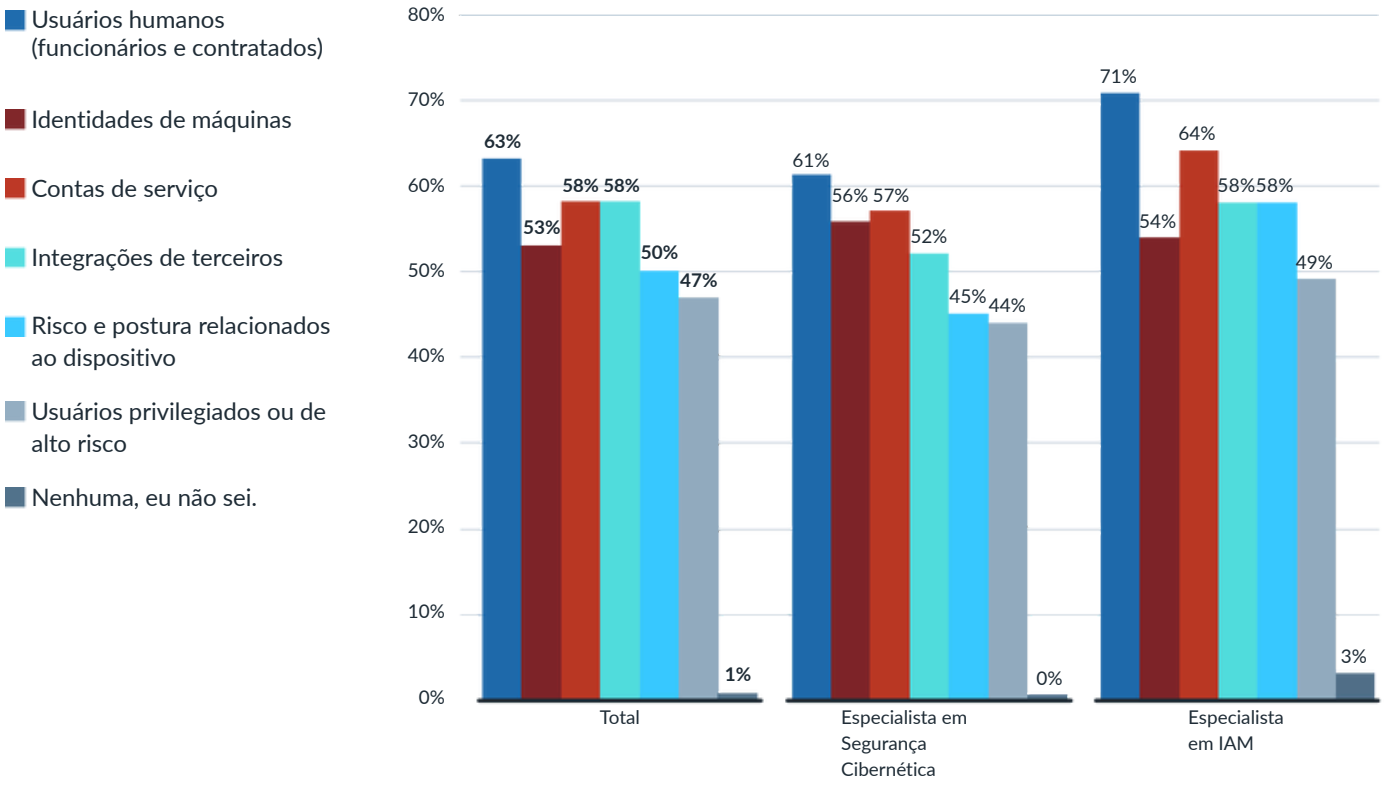
As organizações demonstram uma alta taxa de monitoramento de riscos de identidade em todos os tipos de usuários, com a maioria dos respondentes afirmando que monitoram usuários humanos, contas de máquinas, contas de serviço e integrações de terceiros, e metade deles dizendo que também monitoram o risco e a postura de segurança dos dispositivos. Os especialistas em IAM (Gestão de Identidades e Acessos) são mais propensos a monitorar essas contas em busca de riscos de identidade do que seus pares em cibersegurança.

É encorajador ver que as organizações estão abordando a amplitude de sua superfície de ataque de identidade.
Mas integrar todas essas informações — e usá-las de forma eficaz — será um desafio. Com milhares de permissões por conta, há uma quantidade considerável de ruído que as equipes de segurança precisarão analisar para encontrar riscos e priorizar ações.

Esse enorme conjunto de dados pode estar influenciando as prioridades de investimento em cibersegurança dos entrevistados: mais de um quarto (26%) deles afirmou que o ISPM era sua principal prioridade. O ISPM pode ajudar.
As organizações avaliam sua exposição de acesso e priorizam ações para limitar os riscos.

Um exemplo de por que as organizações precisam de ISPM (Gerenciamento de Prevenção de Incidentes de Segurança da Informação) para identificar o sinal em meio ao ruído e reduzir riscos é a questão das identidades de máquinas. Organizações que monitoram identidades de máquinas relataram as violações mais frequentes, com maior impacto e maiores perdas. Quase três quartos (72%) das organizações que monitoram identidades de máquinas relataram uma violação relacionada à identidade no último ano. Essas organizações também relataram os maiores prejuízos decorrentes dessas violações, com 34% afirmando que as violações causaram danos significativos, e as perdas mais catastróficas, com 27% relatando perdas superiores a US$ 10 milhões.

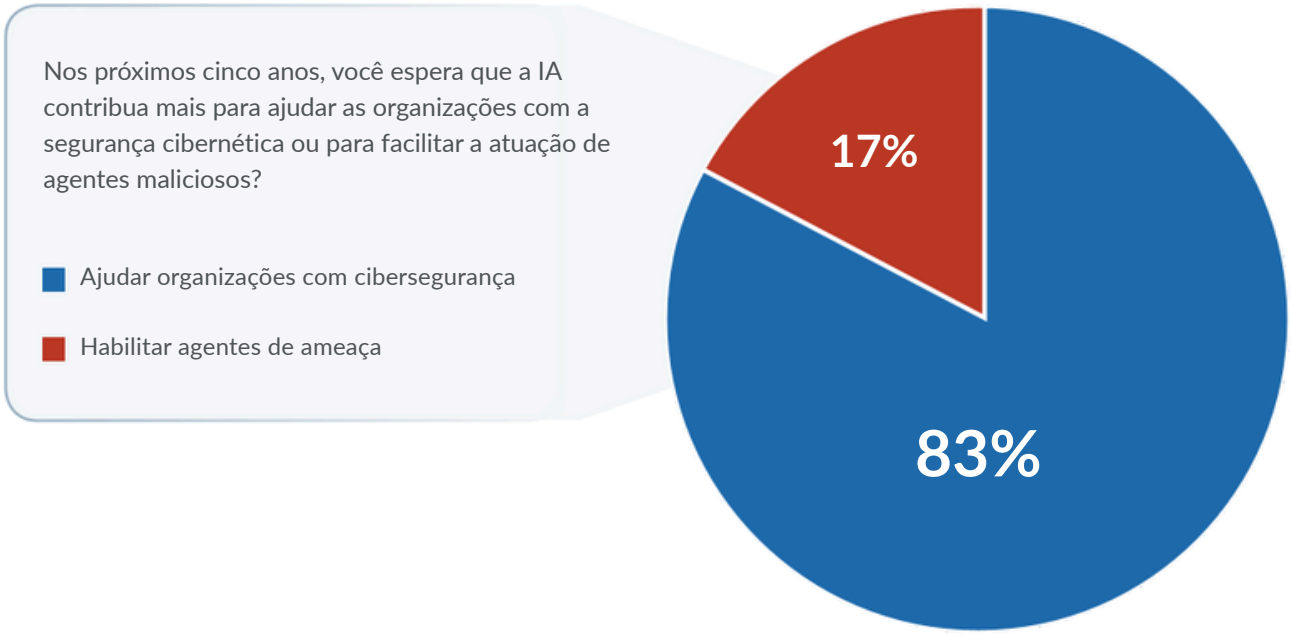
Quais áreas você está monitorando ou avaliando ativamente em relação ao risco de identidade?

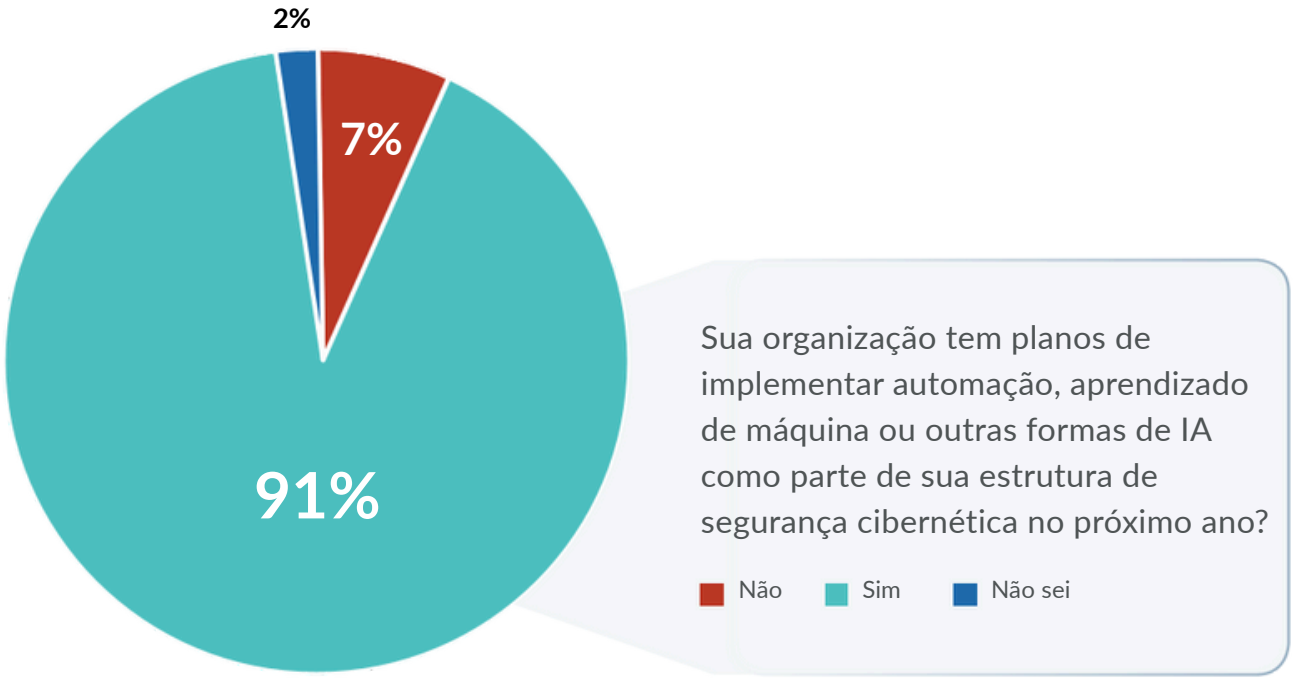


Inteligência artificial para cibersegurança

Há um consenso crescente de que a IA contribuirá mais para a segurança do que para o cibercrime, com 83% dos usuários afirmando que a tecnologia representa um trunfo maior para a defesa organizacional do que para os adversários. Da mesma forma, 91% dos entrevistados disseram que planejam implementar IA em sua infraestrutura tecnológica no próximo ano, um aumento de 12 pontos percentuais em relação à pesquisa do ano passado.

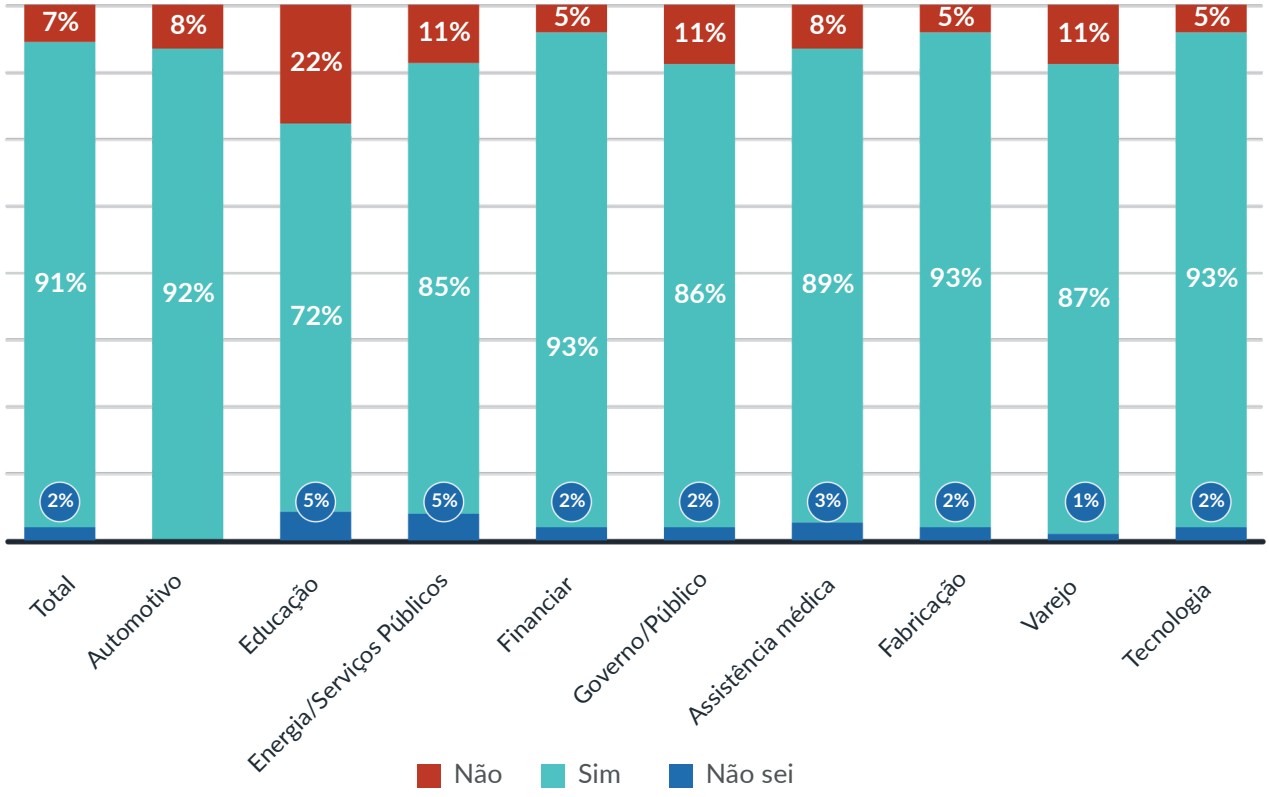
Essas respostas estão alinhadas com o que os usuários disseram ser sua prioridade entre os recursos de segurança cibernética: 40% dos entrevistados colocaram a IA ativa para segurança como sua principal escolha, a maior porcentagem entre todos os recursos.





Por setor, quase todos os setores relatam uma alta probabilidade de implementar alguma forma de IA em sua infraestrutura tecnológica no próximo ano. Os setores financeiro (93%), manufatureiro (93%), tecnológico (93%) e automotivo (92%) relataram altos níveis de integração de IA em sua infraestrutura tecnológica. O setor educacional (72%) apresenta os níveis mais baixos de implementação de IA.

Por setor: Sua organização tem planos de implementar automação, aprendizado de máquina ou outras formas de IA como parte de seus processos da sua infraestrutura de cibersegurança no próximo ano?



Metodologia e fontes do relatório

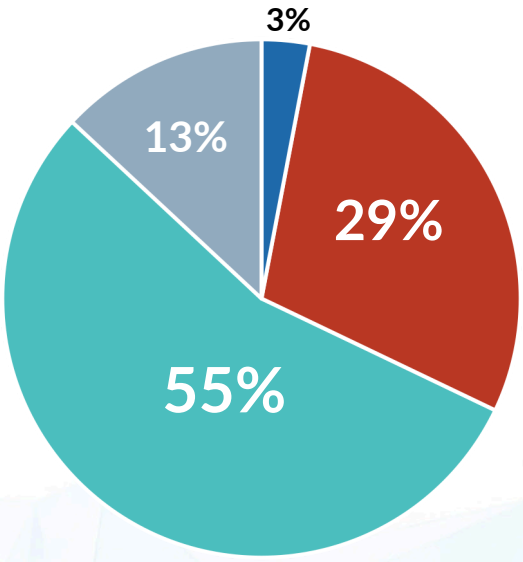
A RSA divulgou a Pesquisa RSA ID IQ de 2026, realizada entre 20 de julho de 2025 e 15 de agosto de 2025, na qual os usuários responderam a 26 perguntas sobre suas prioridades em cibersegurança, os riscos que suas organizações enfrentam, a frequência e o impacto de violações de dados relacionadas à identidade e outros fatores no âmbito da identidade. Nesse período, recebemos 2.120 respostas da Austrália, Brasil, Canadá, Alemanha, Japão, Reino Unido e Estados Unidos.

Os participantes foram solicitados a identificar sua função na organização e o setor em que atuam. trabalhavam e o tamanho da sua organização.

A RSA analisou todas as respostas, correlacionando algumas com outras para verificar se havia alguma relação entre elas.

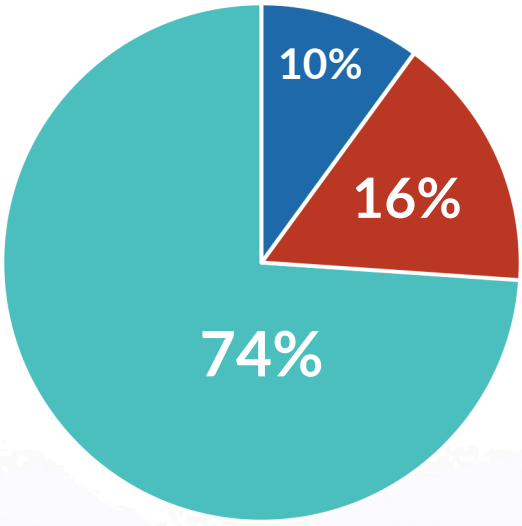
Dados demográficos do RSA ID IQ de 2026

Papel na organização

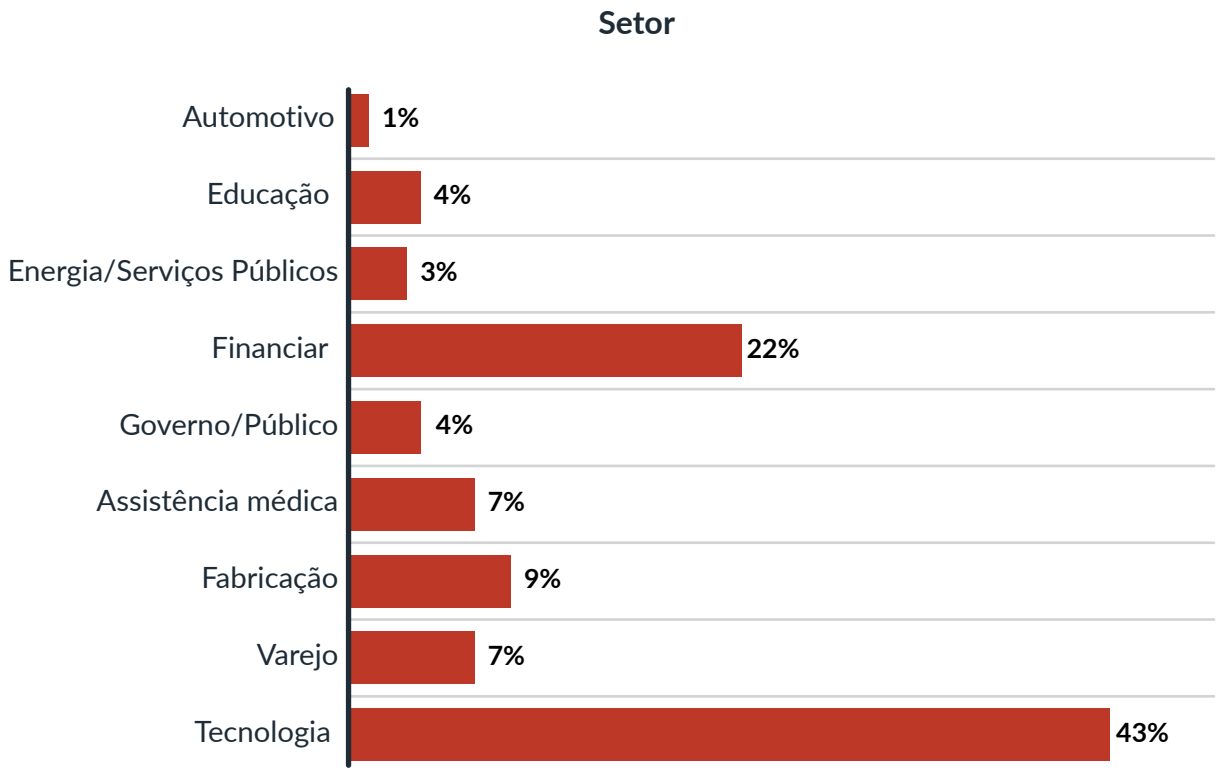


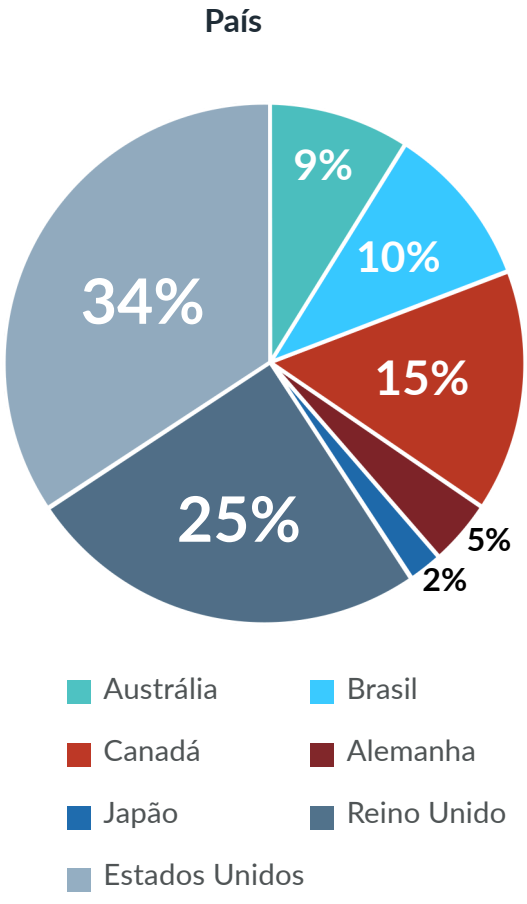
- Responsável pela conformidade ou gestão de riscos
- Especialista em cibersegurança
- Tomador de decisões ou arquiteto de TI
- Especialista em IAM ou identidade

Tamanho da organização



- 2.500 - 4.999
- 5.000 - 9.999
- 10.000+


Setor
Automotivo
1%
Educação
4%
Energia/Serviços Públicos
3%
Financiar
22%
Governo/Público
4%
Assistência médica
7%
Fabricação
9%
Varejo
7%
Tecnologia
43%


País
9%
10%
15%
5%
2%
25%
34%
Austrália
Brasil
Canadá
Alemanha
Japão
Reino Unido
Estados Unidos

Relatório RSA ID IQ 2026:

Insights do Brasil

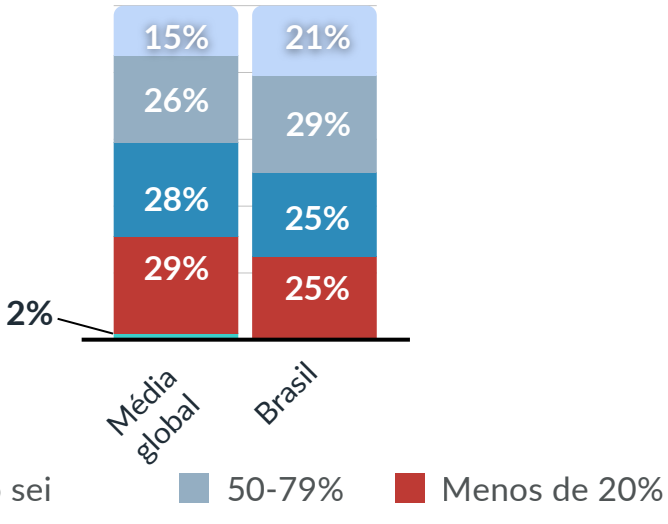
Em comparação com o resto do mundo, o Brasil se destaca pelo progresso na autenticação sem senha e pelos planos de adoção da IA. No entanto, o país também demonstra profundo ceticismo quanto ao poder que a IA poderá exercer sobre os cibercriminosos.

A seguir, apresentamos as diferenças entre o Brasil e o resto do mundo no Relatório RSA ID IQ de 2026. Esses destaques são baseados em 218 respondentes brasileiros:

Liderança sem senha

Mais usuários brasileiros utilizam a autenticação sem senha como principal forma de autenticação em comparação com o resto do mundo. Metade dos usuários no Brasil utiliza a autenticação sem senha pelo menos metade do tempo, nove pontos percentuais a mais do que a média global.

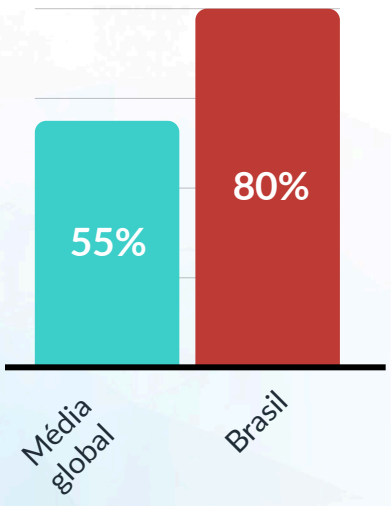
Qual a porcentagem de seus usuários que utilizam principalmente formulários sem senha para concluir a autenticação?



Apostando alto na biometria

O Brasil lidera o mundo em seus planos de implantação da biometria como um meio de autenticar sem senha, com 80% das organizações brasileiras afirmando que pretendem utilizá-la.

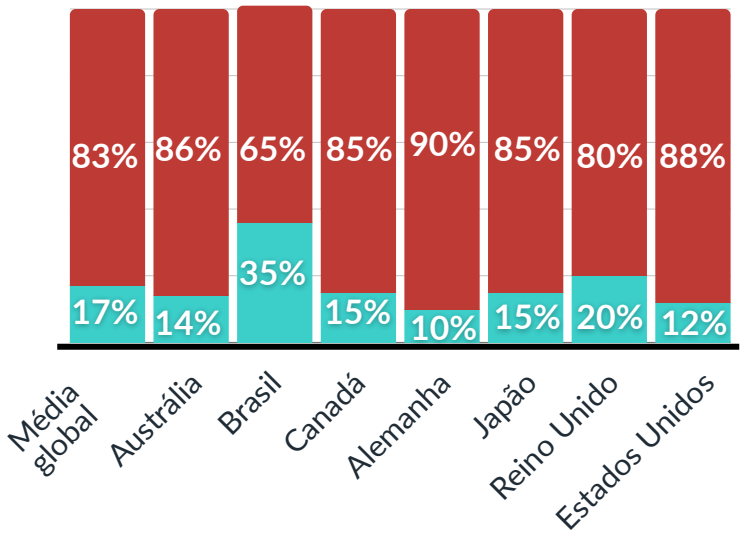
Quais formatos você pretende usar para implementar soluções sem senha?



Grandes expectativas e profundo ceticismo em relação à IA.

O Brasil encontra-se em extremos opostos do espectro da IA. 35% das organizações brasileiras relatam que a IA contribuirá mais para o combate ao cibercrime do que para a cibersegurança nos próximos cinco anos, em comparação com 17% das organizações em todo o mundo. Apesar desse ceticismo, o país demonstra a maior probabilidade de integrar alguma forma de IA em sua infraestrutura tecnológica no próximo ano.

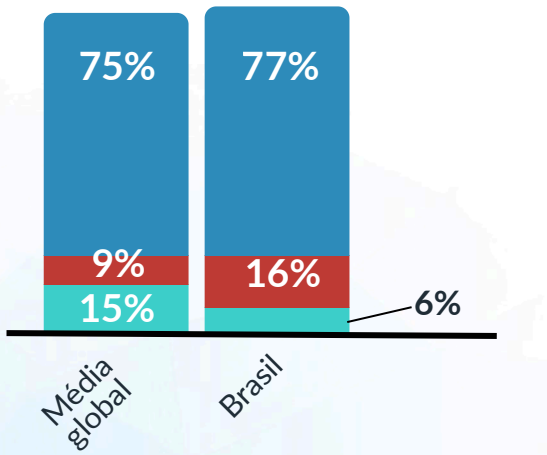
Nos próximos cinco anos, você espera que a IA contribua mais para ajudar as organizações com a segurança cibernética ou para facilitar a atuação de agentes maliciosos?



O Brasil é líder em computação exclusivamente em nuvem.

As organizações brasileiras relatam a maior dependência de arquitetura exclusivamente em nuvem.

Em qual dos seguintes ambientes você oferece suporte a aplicativos e usuários?



Da informação à ação

O primeiro passo para solucionar qualquer problema é admitir que ele existe. O Relatório RSA ID IQ de 2026 demonstra que a identidade é um problema significativo para muitas organizações, resultando em violações de dados de alto custo e grande impacto.

As organizações devem priorizar as capacidades que podem mantê-las seguras, incluindo:

- Autenticação sem senha que funciona para todos os usuários, em todos os ambientes, sempre.
- O ISPM deve identificar riscos e recomendar ações.
- Suporte a ambientes cruzados, capaz de proteger usuários em nuvem, híbridos e locais.
- Verificação de identidade bidirecional para proteger a equipe de suporte de TI e os usuários contra ataques de bypass de MFA e engenharia social.
- Inteligência de identidade automatizada para avaliar riscos dinamicamente e automatizar respostas.

Entre em contato com a RSA para uma demonstração dessas funcionalidades. Ou descubra por que as organizações mais seguras do mundo utilizam a segurança da RSA: inicie agora mesmo seu teste gratuito de **45 dias do RSA ID Plus.**

Sobre a RSA

A RSA fornece soluções de cibersegurança de missão crítica que protegem as organizações mais sensíveis à segurança em todo o mundo. A Plataforma de Identidade Unificada da RSA oferece verdadeira segurança de identidade sem senha, acesso baseado em risco, inteligência de identidade automatizada e governança de identidade abrangente em ambientes de nuvem, híbridos e locais. Mais de 9.000 organizações de alta segurança confiam na RSA para gerenciar mais de 60 milhões de identidades, detectar ameaças, proteger o acesso e garantir a conformidade.

Para obter informações adicionais, **visite nosso site** para entrar em **contato com a equipe de vendas**, **encontrar um parceiro** ou saber mais sobre a RSA.