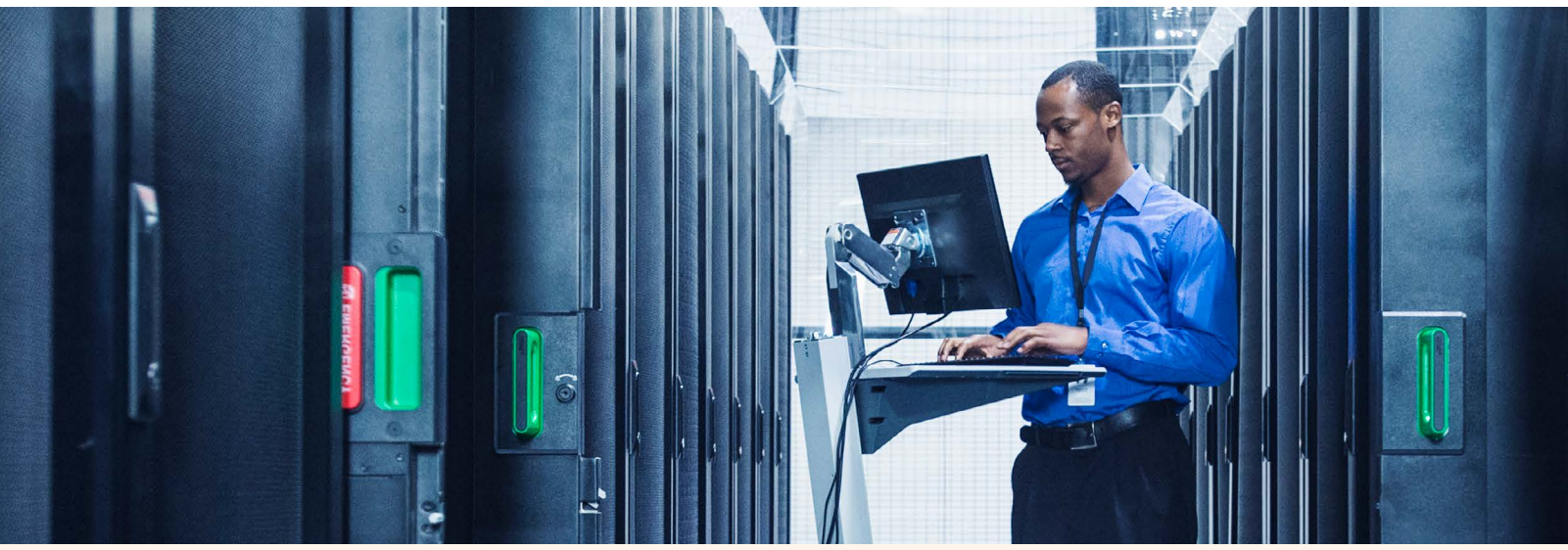
Novo mundo, novas regras: cibersegurança em tempos de incertezas

Pesquisa Global Digital Trust Insights 2026

Conteúdo

Apresentação

A segurança cibernética enfrenta um cenário totalmente novo. As mudanças aceleradas na ordem global e no ambiente de ameaças, alimentadas por avanços tecnológicos exponenciais, estão testando os limites das estratégias cibernéticas.



As organizações encaram hoje a realidade de uma era pós-globalização, marcada por alianças fragmentadas, instituições globais enfraquecidas, choques tarifários e cadeias de suprimentos desestruturadas. Vemos também avanços tecnológicos sem precedentes que ampliam os pontos de exposição das empresas e abrem espaço para ameaças cibernéticas inéditas – muitas delas patrocinadas por governos.

Toda essa incerteza força os executivos a reavaliar suas competências técnicas, talentos e tecnologias. Mais do que isso, leva à revisão de suas estratégias de cibersegurança, inclusive onde operam e com quem fazem negócios.

A **Pesquisa Global Digital Trust Insights 2026 da PwC**, que contou com a participação de mais de 3.800 executivos de negócios e tecnologia em 72 países, entre eles o Brasil, mostra como as empresas estão lidando com essa era de transformações, onde estão falhando e o que podem fazer para enfrentar os novos desafios.

Algumas das principais conclusões do estudo:

O risco geopolítico está redefinindo as estratégias: quase 70% dos líderes de negócios e de tecnologia brasileiros classificam o investimento para se proteger de riscos cibernéticos como uma de suas três prioridades estratégicas, devido às incertezas geopolíticas. Globalmente, o percentual é de 60%.

A resiliência ainda está em construção: no cenário geopolítico atual, cerca de metade das lideranças no Brasil diz que sua empresa é, no máximo, "razoavelmente capaz" de resistir a ataques que explorem vulnerabilidades específicas. Somente 6% dos respondentes globais se dizem confiantes em relação a todas as vulnerabilidades.

À espera de ameaças iminentes: menos de 30% das empresas brasileiras e globais investem mais em medidas proativas (monitoramento, avaliações, testes e controles) do que em medidas reativas (respostas a incidentes, multas e recuperação), o que seria o cenário ideal. A maioria (62% no Brasil e 67% no mundo), no entanto, ainda divide o investimento de forma equilibrada, o que pode ser mais caro e arriscado.

Agentes de inteligência artificial (IA) para segurança cibernética: a IA agêntica figura entre os principais recursos de segurança em IA que as organizações estão priorizando para os próximos 12 meses tanto no Brasil quanto no mundo. Seu plano é usar esses agentes inteligentes para reforçar a segurança em nuvem e a proteção de dados, além de apoiar as operações e a defesa cibernética.

A era quântica se aproxima: a computação quântica está entre as maiores ameaças para as quais as empresas se sentem menos preparadas no Brasil e no mundo. Menos de 10% priorizam essa área em seu orçamento e apenas 3% implementaram todas as medidas de segurança pós-quântica necessárias.

Repensando a crise de talentos na cibersegurança: a escassez de competências técnicas permanece como uma das maiores barreiras ao progresso da segurança cibernética. Quase 70% dos líderes brasileiros (53% no mundo) estão priorizando IA e ferramentas de aprendizado de máquina para suprir deficiências de capacidade. Já os serviços gerenciados especializados se consolidam como um vetor estratégico de expansão e expertise.

Encarar esse momento exige urgência, criatividade e novas abordagens. Neste relatório, traduzimos as descobertas da pesquisa deste ano em passos práticos para ajudar os *stakeholders* a fortalecer suas bases de segurança e implementar medidas eficientes, prontas para o tempo em que vivemos.

“Cada vez mais, a cibersegurança passa a orientar escolhas estratégicas sobre onde operar, com quem se conectar e como se proteger. Empresas maduras já entenderam que o desafio não está só na escassez de talentos, mas na velocidade com que conseguem decidir e agir em um ambiente cada vez menos previsível.”

Eduardo Batista,
Sócio e líder da prática
de Risk Services

01

Cenário de riscos: a geopolítica e as vulnerabilidades cibernéticas

66%

das empresas brasileiras (60% no mundo) estão aumentando o investimento em segurança cibernética em resposta à volatilidade geopolítica

Apenas 6%

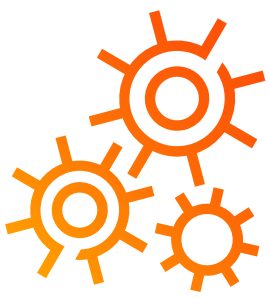
dos respondentes no mundo se dizem muito capazes de resistir a ataques cibernéticos em relação a todas as vulnerabilidades analisadas

2 ameaças

cibernéticas que mais expõem as empresas brasileiras: ataques à nuvem e o comprometimento das cadeias de suprimento de software

Os riscos cibernéticos são definidos hoje pela geopolítica e por tecnologias disruptivas. Alianças desfeitas, disputas comerciais, instituições internacionais enfraquecidas e outras forças desestabilizadoras estão reconfigurando o ambiente de ameaças. Mudam também os modelos tradicionais de negócios.

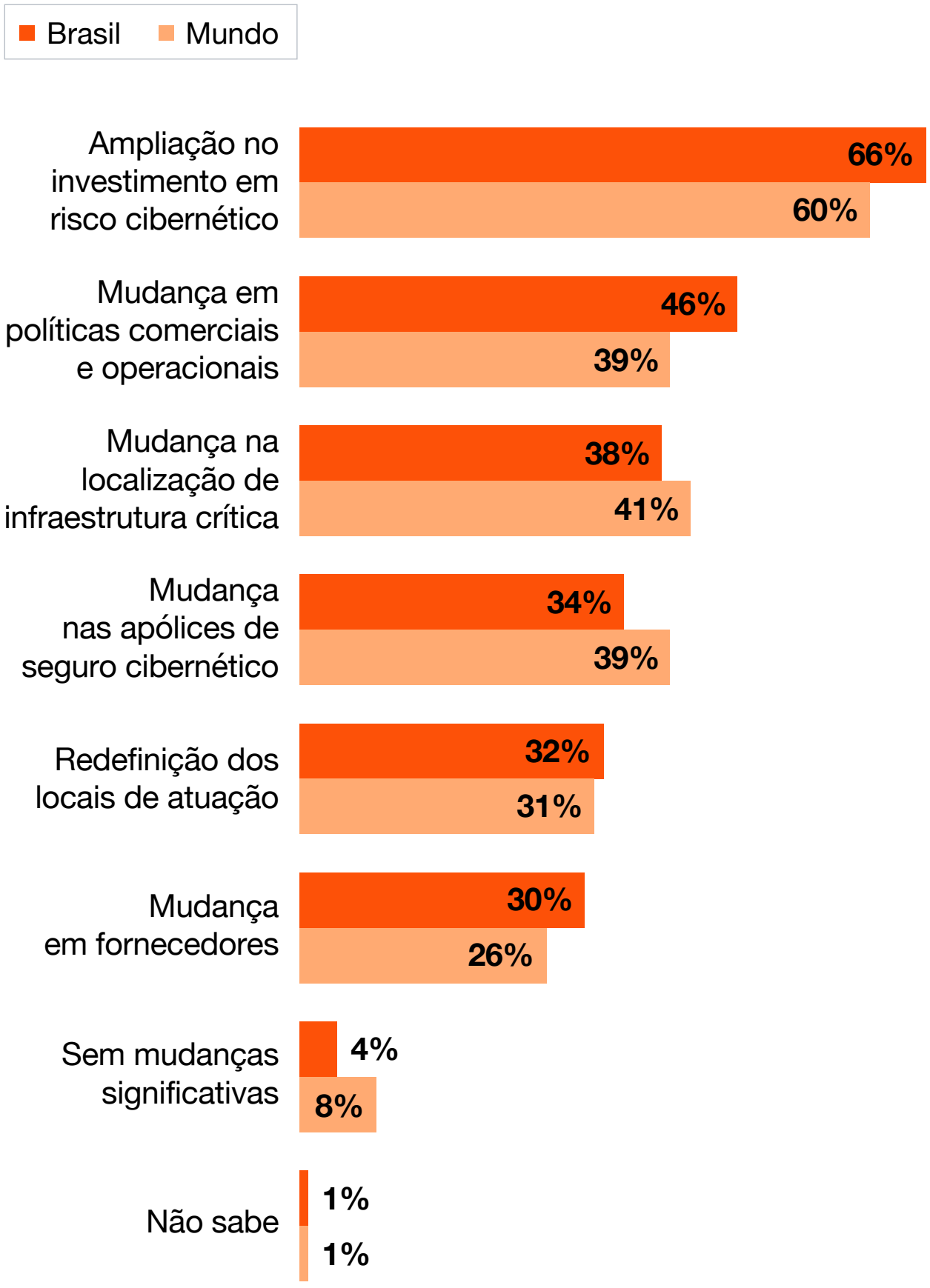
Nesse contexto, 66% dos líderes de negócios e tecnologia brasileiros apontam o investimento para se proteger de riscos cibernéticos como uma de suas três prioridades estratégicas para este ano. No mundo, são 60%.



Os brasileiros também pretendem priorizar investimentos em mudanças nas políticas operacionais e comerciais (46%), na localização da infraestrutura crítica (38%) e em apólices de seguro cibernético (34%). Globalmente, esses percentuais foram, respectivamente, 39%, 41% e 39%. Como a disrupção virou regra, a segurança cibernética é o principal fator para fortalecer a resiliência.

Mudanças na estratégia cibernética em resposta ao atual cenário geopolítico

Pergunta: Nos próximos 12 meses, quais das seguintes áreas da estratégia cibernética da sua empresa devem mudar em resposta ao cenário geopolítico atual?
(% dos que citaram a opção entre as três mais relevantes)



Base: todos os respondentes. Global = 3.887 | Brasil = 125.
Fonte: Pesquisa Global Digital Trust Insights 2026.

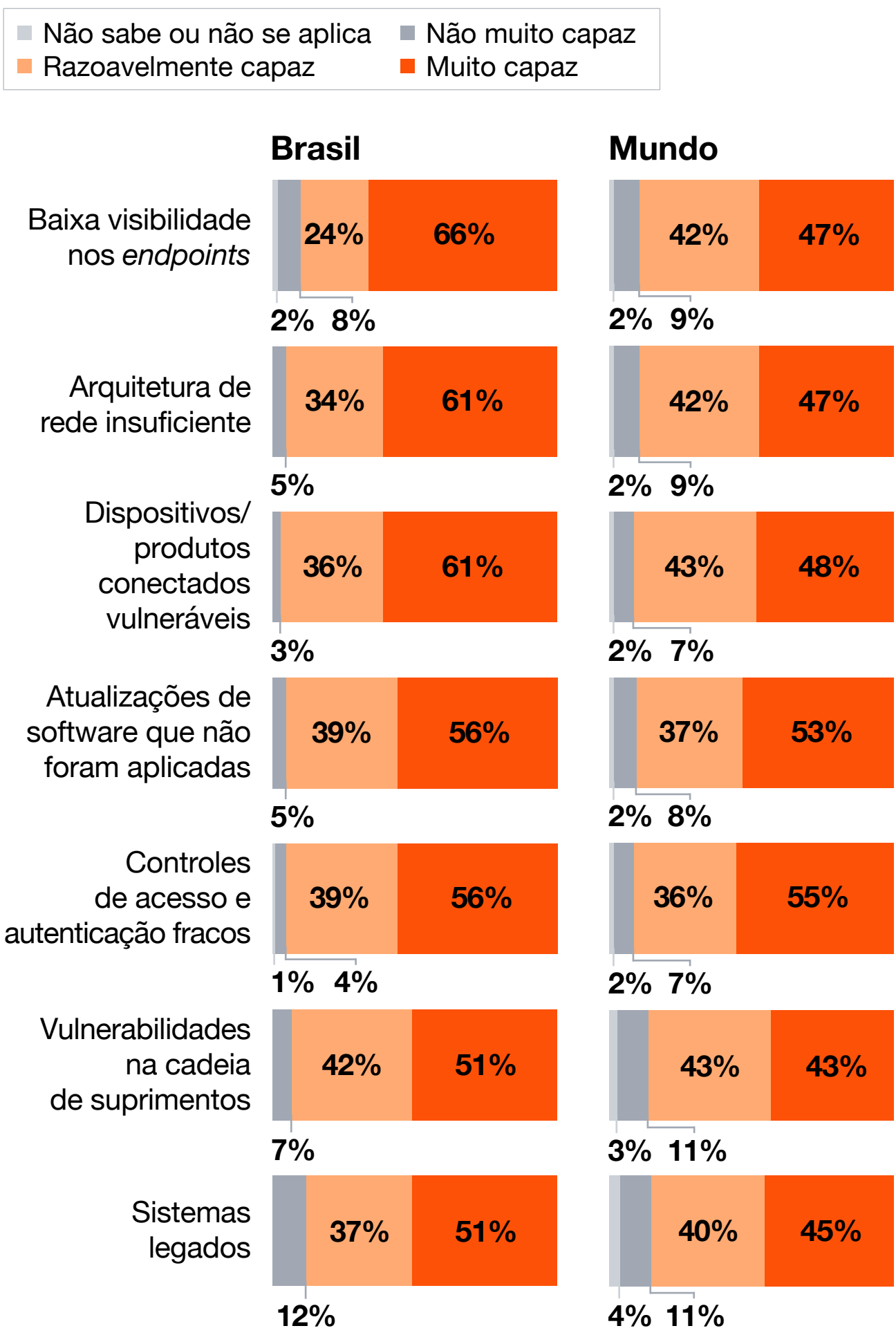
A diferença entre parecer seguro e estar seguro

O cenário geopolítico atual expõe uma divisão clara na confiança na prontidão cibernética. Pouco mais da metade dos respondentes brasileiros diz que sua empresa é “muito capaz” de resistir a ataques cibernéticos que explorem as vulnerabilidades específicas avaliadas na pesquisa. A outra metade afirma não estar suficientemente preparada.

Esses líderes apontam como principais vulnerabilidades os sistemas legados e as exposições nas cadeias de suprimentos – áreas em que se sentem menos preparados. Ambas são alvos frequentes de atores estatais que buscam desestabilizar infraestruturas críticas. Globalmente, apenas 6% dos entrevistados afirmam que suas organizações são “muito capazes” de resistir a um grande ataque cibernético.

Capacidade de resistir a um grande ataque cibernético

Pergunta: Diante do cenário geopolítico atual, qual é a capacidade da sua empresa de resistir a um grande ataque cibernético que explore as vulnerabilidades a seguir?



Base: líderes de segurança, COOs e diretores de operações. Global = 1.971| Brasil = 59.
Fonte: Pesquisa Global Digital Trust Insights 2026.

Quando as falhas persistem, o risco aumenta

Além dessas vulnerabilidades, os líderes se preocupam com sua prontidão em relação a certos tipos de ameaças. No Brasil, os ataques à nuvem e o comprometimento das cadeias de suprimentos de software estão no topo das preocupações das lideranças de cibersegurança (com 39% e 33%, respectivamente). Destaca-se ainda a atenção com as ameaças à infraestrutura em nuvem (31%).

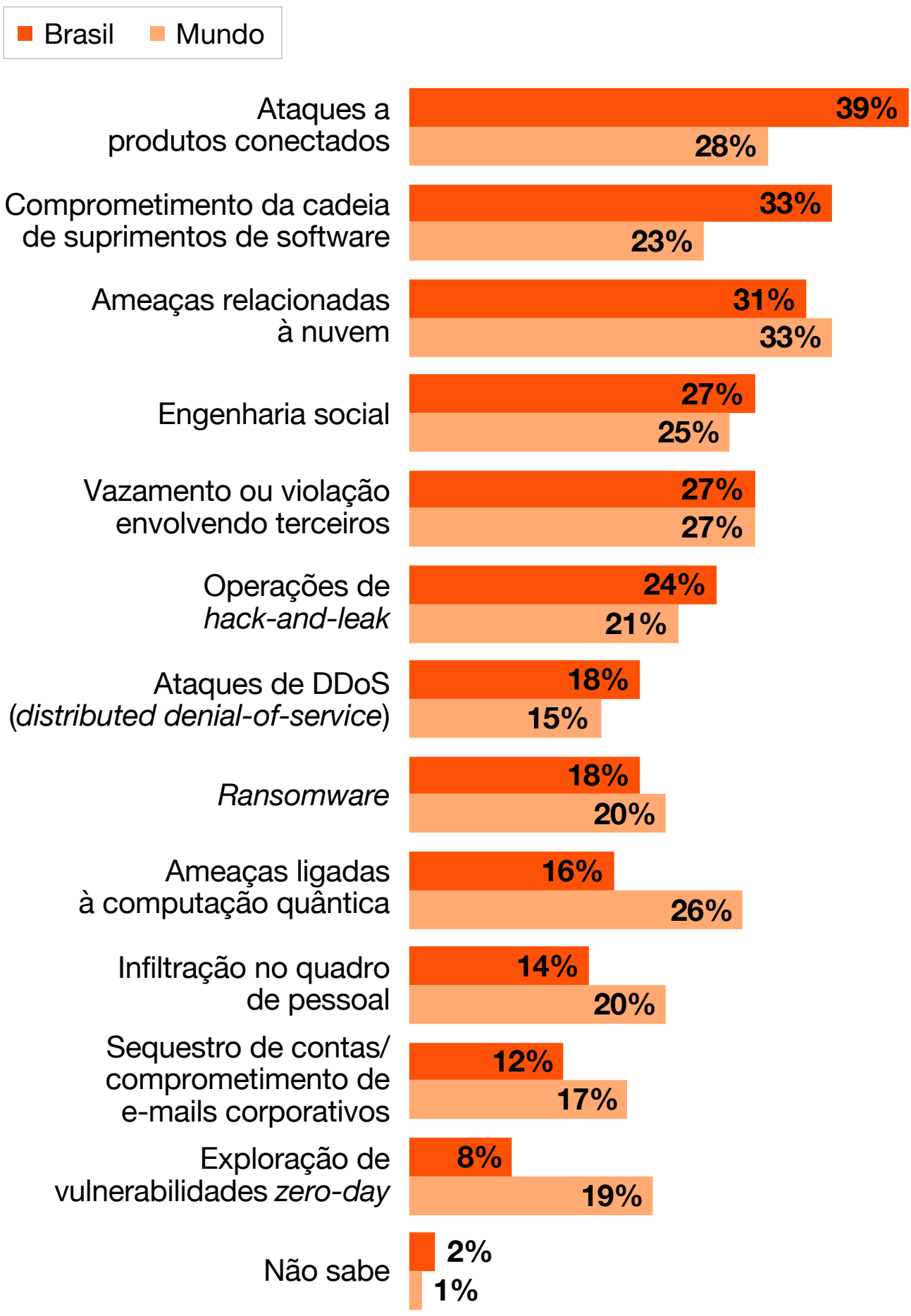
Mundialmente, os ataques à nuvem (33%) e a produtos conectados (28%) são as maiores preocupações, em níveis semelhantes aos do estudo do ano passado. Para cerca de um terço dos respondentes, essas duas ameaças cibernéticas estão entre as três principais para as quais as empresas estão menos preparadas.

Esses riscos não são novos. No entanto, com adversários que usam a IA para expandir seus limites de ataque, as lideranças têm refletido sobre os desafios persistentes de preencher lacunas críticas nas funções de governança, controle e visibilidade.

Com o avanço da tecnologia e o aumento da complexidade dos ecossistemas, muitas organizações enfrentam desafios para acompanhar esse ritmo, sobretudo em relação a terceiros e à cadeia de suprimentos.

Ameaças cibernéticas para as quais as empresas se sentem menos preparadas

Pergunta: Nos próximos 12 meses, quais destas ameaças cibernéticas sua empresa está menos preparada para enfrentar?
(% dos que citaram a opção entre as três mais relevantes)

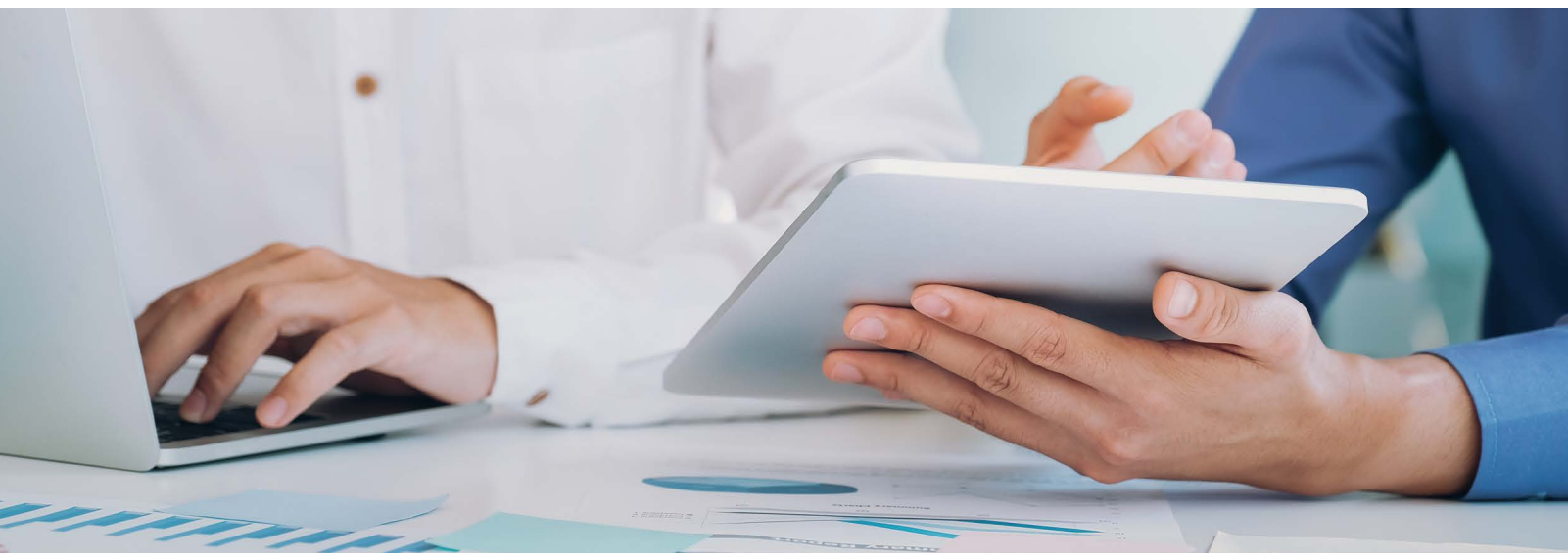


Base: líderes da segurança no mundo. Global = 1.740 | Brasil = 49.
Fonte: Pesquisa Global Digital Trust Insights 2026.

Aprendendo do jeito mais difícil

Há alguns anos, mais de um quarto dos executivos relata que a violação de dados mais grave sofrida por suas organizações nos últimos três anos custou, no mínimo, US$ 1 milhão tanto no Brasil quanto no mundo. Empresas com receita anual de US$ 5 bilhões ou mais (41%), as sediadas nos Estados Unidos (37%) e as de tecnologia, mídia e telecomunicações (33%) são as mais expostas. Para esses grupos, a escala e a complexidade das operações aumentam significativamente a probabilidade de incidentes de alto custo.

Para se recuperar, as empresas que passaram por grandes ataques estão transformando o aprendizado em ação. Elas se empenham mais para elevar seu orçamento cibernético (88% contra 78% no total) e adotar serviços gerenciados para suprir deficiências críticas de competências (48% contra 39% no total).



Também estão mais inclinadas a mudar suas apólices de seguro cibernético (49% contra 39% no total), muito possivelmente em decorrência da alta dos prêmios e das novas exigências das seguradoras. Além disso, muitas começam a adotar novas práticas para reduzir os volumes de dados sensíveis em suas organizações.

02

Operações e estratégia cibernética: investimento com propósito

Menos de 30%

dos líderes brasileiros (24% no mundo) estão investindo mais em medidas proativas de cibersegurança do que em ações reativas

90%

dessas lideranças (78% no mundo) projetam aumento dos gastos com segurança cibernética em 2026

Menos de 20%

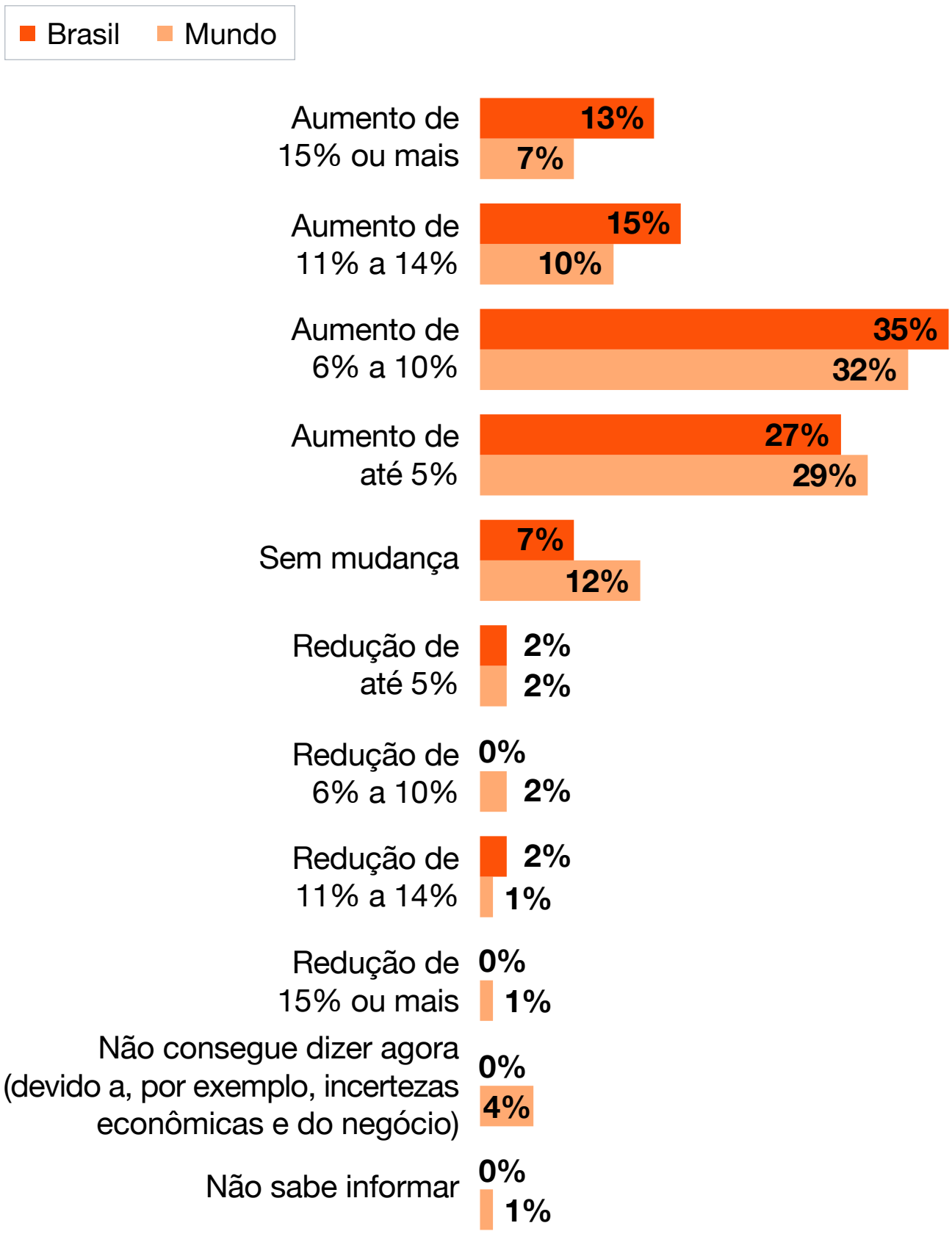
estão medindo os impactos financeiros dos riscos cibernéticos de forma consistente (no mundo, são 16%)

Os orçamentos em segurança cibernética parecem não estar à altura dos desafios do cenário atual. Embora 90% dos líderes brasileiros de segurança, CFOs e diretores financeiros afirmem que pretendem aumentar os investimentos na área em 2026, apenas cerca de um terço planeja elevar os gastos em mais de 10%.

Globalmente, quase oito em cada dez respondentes (78%) dizem que seu orçamento na área vai aumentar no próximo ano. Esse número, no entanto, praticamente repete o do ano passado (77%). Os entrevistados dizem que estão elevando os investimentos em risco cibernético em resposta ao contexto geopolítico atual, mas isso pode estar ocorrendo às custas de outras prioridades de gasto.

Mudança no orçamento da segurança cibernética em 2026

Pergunta: Como o orçamento de segurança cibernética da sua empresa vai mudar em 2026?



Total dos que preveem aumento – Brasil → 90%

Total dos que preveem aumento – Mundo → 78%

Base: líderes de segurança, CFOs e diretores financeiros no mundo. Global = 2.027 | Brasil = 60.
Fonte: Pesquisa Global Digital Trust Insights 2026.

Prevenir ou remediar: a diferença de custo

Cibersegurança é, acima de tudo, estar preparado. Isso significa se planejar e investir em medidas proativas – como monitoramento, avaliações, testes, controles e capacitação – antes que uma crise aconteça. A alternativa, baseada principalmente em ações reativas (como resposta a incidentes, atendimento a clientes, remediação, recuperação, litígios e multas), é mais cara, mais arriscada e insustentável no longo prazo.

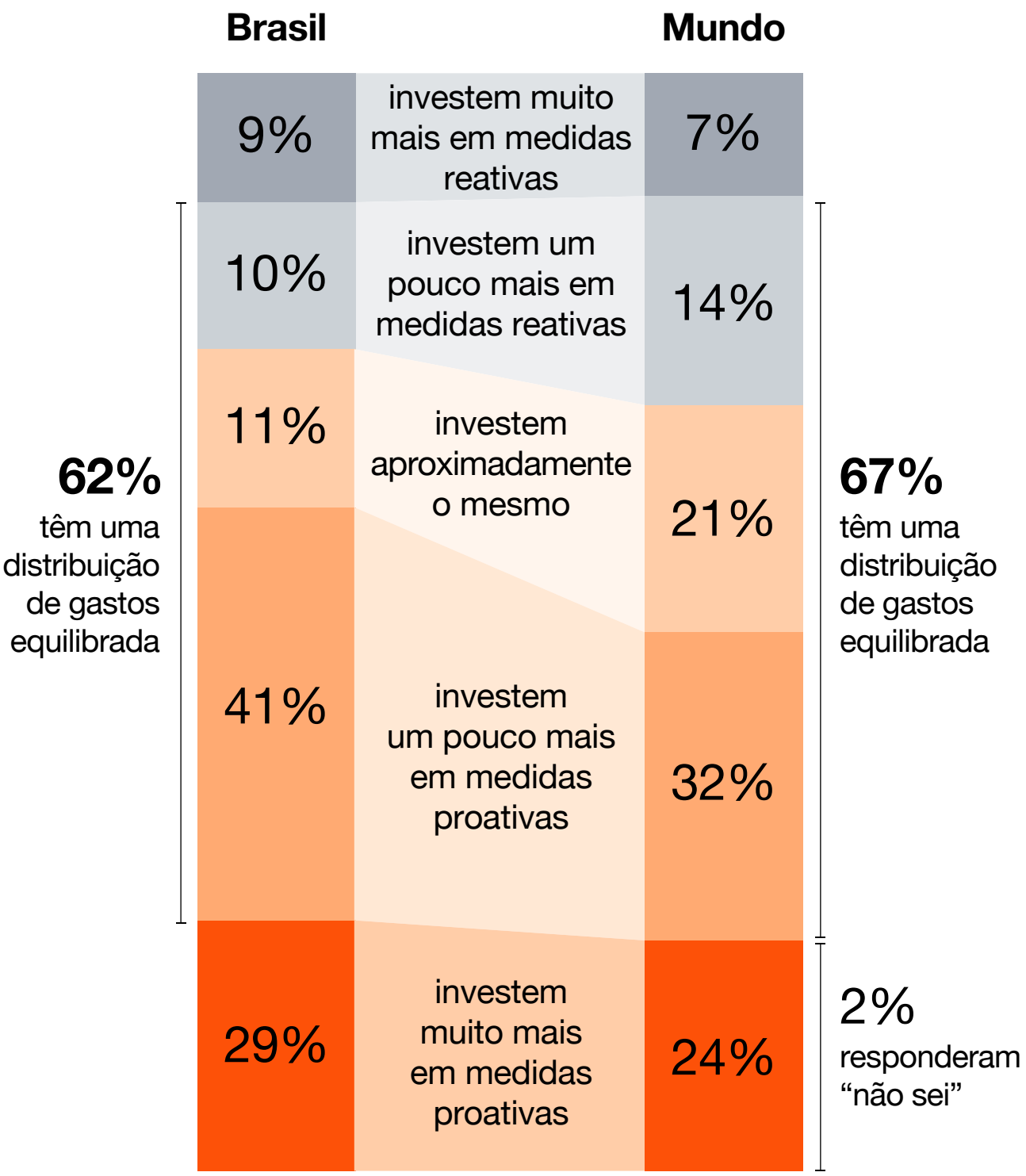
Cerca de dois terços das empresas dizem gastar praticamente o mesmo com ações proativas e reativas, ou apenas um pouco mais em uma delas. No Brasil, esse percentual é de 62%, enquanto, globalmente, chega a 67%. O cenário ideal, no entanto, é que elas invistam significativamente mais em ações de caráter proativo. Nesse ponto, o Brasil apresenta um desempenho ligeiramente melhor: 29% das empresas adotam essa abordagem, contra 24% no cenário global.

Esses dados provavelmente não refletem o custo real de reagir a incidentes. Enquanto os gastos proativos são centralizados na área de segurança e fáceis de rastrear, os reativos se diluem por toda a empresa – nos departamentos jurídico, de comunicação, operacional, TI, de produto, marketing e relações governamentais. E incluem perdas intangíveis, como danos à reputação.

Além disso, investir em medidas proativas não adianta se o foco estiver nos riscos errados ou se a estratégia não for ágil o suficiente para se adaptar a novos cenários. A verdadeira prontidão exige um entendimento profundo do panorama de riscos e ameaças, capaz de orientar a estratégia cibernética, as pessoas contratadas e os processos, sistemas e ferramentas adotados pela empresa.

Onde se gasta: reação ou prevenção

Pergunta: Sua empresa está investindo mais em medidas reativas ou proativas de segurança cibernética?



Reativas:
ações de resposta, atendimento ao cliente, correção, recuperação, disputas jurídicas, multas, etc.

Proativas:
monitoramento, avaliações, testes, controles, treinamento, governança, etc.

Base: todos os respondentes. Global = 3.887 | Brasil = 125.
Fonte: Pesquisa Global Digital Trust Insights 2026.

Alinhando prioridades de investimento e nível de preparo

Inteligência artificial e segurança na nuvem são as duas prioridades do orçamento de segurança cibernética para 2026, o que não é surpresa. No Brasil, 41% dos líderes de segurança apontam a IA como prioridade, e 35%, a nuvem. Os números globais são muito parecidos: 36% e 34%, respectivamente.

As ameaças à nuvem se destacam entre aquelas que as lideranças se sentem menos preparadas para enfrentar. Cerca de um terço faz essa afirmação: 31% no Brasil e 33% no mundo. A boa notícia é que a distância entre a percepção de risco e a prontidão para enfrentá-lo vem sendo reconhecida pelas empresas, e o investimento tem acompanhado esse movimento.

Já os ataques a produtos conectados aparecem como a primeira área em que as empresas brasileiras se sentem menos preparadas (39%). É a segunda no recorte global (28%). O problema, nesse caso, é que muito menos recursos estão sendo direcionados a esse tema. Esse descompasso indica que algumas ameaças ainda passam despercebidas.

Os serviços gerenciados de segurança cibernética aparecem com algum destaque entre as prioridades de investimento: 18% no Brasil e 21% no mundo. Empresas de alto crescimento vão além: 30% colocam esses serviços entre suas três prioridades. Isso mostra um movimento estratégico de recorrer à expertise externa para fechar lacunas críticas e fortalecer sua prontidão no *front* cibernético.

Investimentos que as empresas estão priorizando ao alocar orçamentos de cibersegurança

Pergunta: Quais desses investimentos você está priorizando ao alocar o orçamento de cibersegurança da sua empresa nos próximos 12 meses? (% dos que citaram a opção entre as três mais relevantes)

Base: líderes de segurança. Global = 1.740 | Brasil = 49.
Fonte: Pesquisa Global Digital Trust Insights 2026.

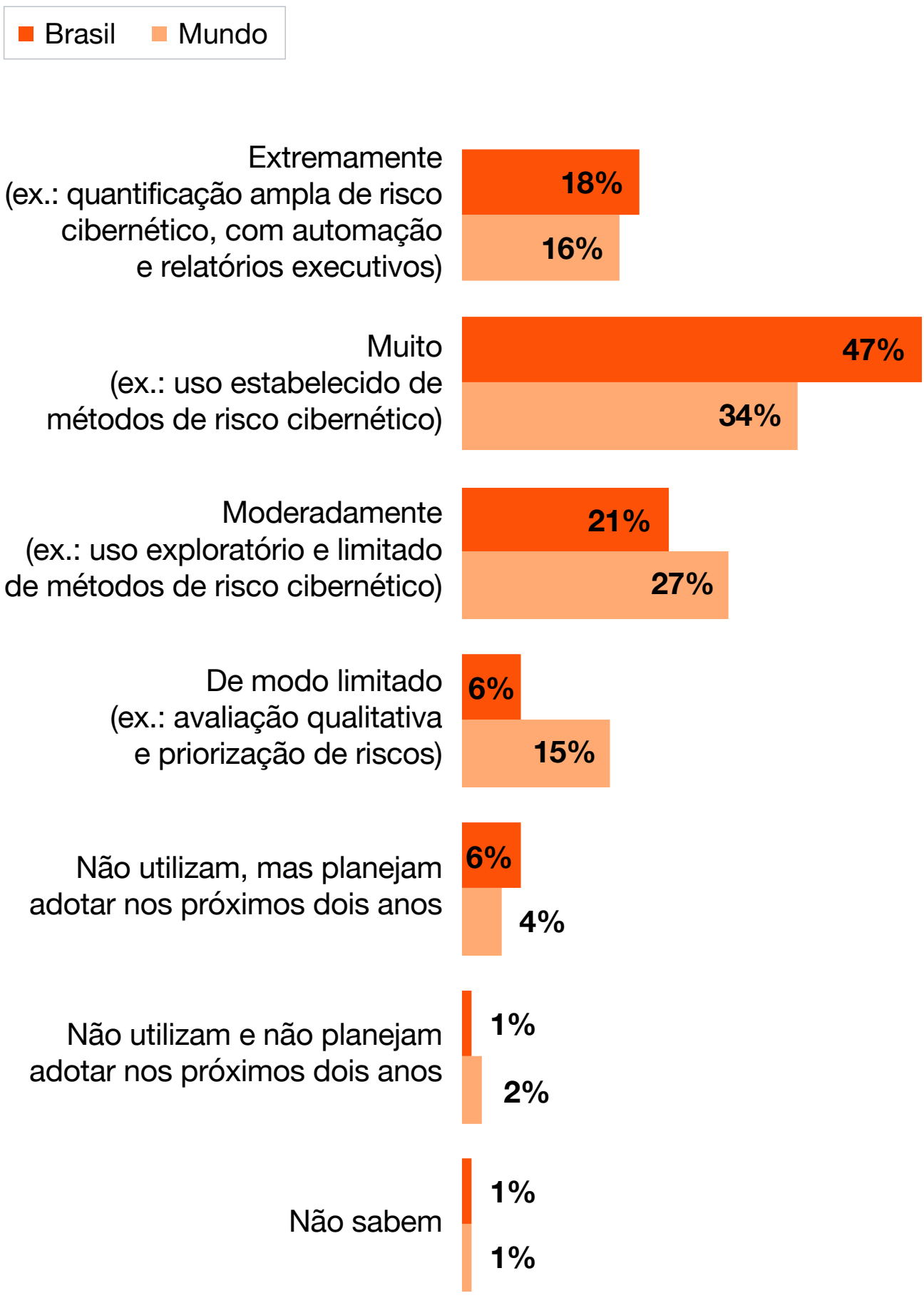
Colocando preço no risco cibernético

Um número cada vez maior de empresas está colocando preço em seus riscos. 65% das empresas brasileiras (50% no mundo) já dizem que usam muito ou extremamente a quantificação do risco cibernético para medir o impacto financeiro – acima dos 44% registrados no ano passado.

Porém, é importante olhar com cuidado. Só 18% das organizações brasileiras (16% no mundo) declaram que fazem isso em grau extremo, o que seria o mais recomendável. Para tomar decisões eficazes, as lideranças precisam de relatórios de risco cibernético confiáveis e úteis para a tomada de decisão, que permitam avaliar as ameaças enfrentadas pela organização e definir a melhor forma de resposta.

Mensuração do impacto financeiro dos riscos cibernéticos

Pergunta: Em que medida sua empresa está medindo o potencial impacto financeiro dos riscos cibernéticos (isto é, quantificando-os)?



Base 2026: líderes da segurança, CFOs, CEOs, CROs e membros do conselho. Global = 2.673 | Brasil = 87.
Fonte: Pesquisa Global Digital Trust Insights 2026.

03

IA em cibersegurança: da promessa à prioridade

#1

A prioridade de investimento em cibersegurança é a IA

#1

Entre as aplicações de IA em segurança, a caça a ameaças (*threat hunting*) lidera as prioridades dos líderes da área no Brasil e no mundo

3 apostas

da IA agêntica: segurança em nuvem, proteção de dados e defesa cibernética

O potencial da IA para transformar o que a empresa consegue fazer na área cibernética é claro e abrangente. O uso dessa tecnologia em funções críticas de cibersegurança tornou-se prioridade na alocação de orçamento, contratação de serviços gerenciados e mitigação das lacunas de competências técnicas na área.

Para fortalecer suas capacidades de segurança baseadas em IA nos próximos 12 meses, líderes de segurança apontam o *threat hunting* como prioridade número um. Eles também estão investindo em outras competências, como soluções agênticas, detecção de eventos e análises comportamentais, gestão de identidade e acesso, além de varredura e avaliação de vulnerabilidades.

IA agêntica entre as funções priorizadas de segurança em IA

Pergunta: Quais dessas funções de segurança em IA a sua empresa vai priorizar nos próximos 12 meses?
(ordem baseada nas respostas que apontaram a função como prioridade máxima)

Base: líderes de segurança. Global = 1.740 | Brasil = 49.
Fonte: Pesquisa Global Digital Trust Insights 2026.

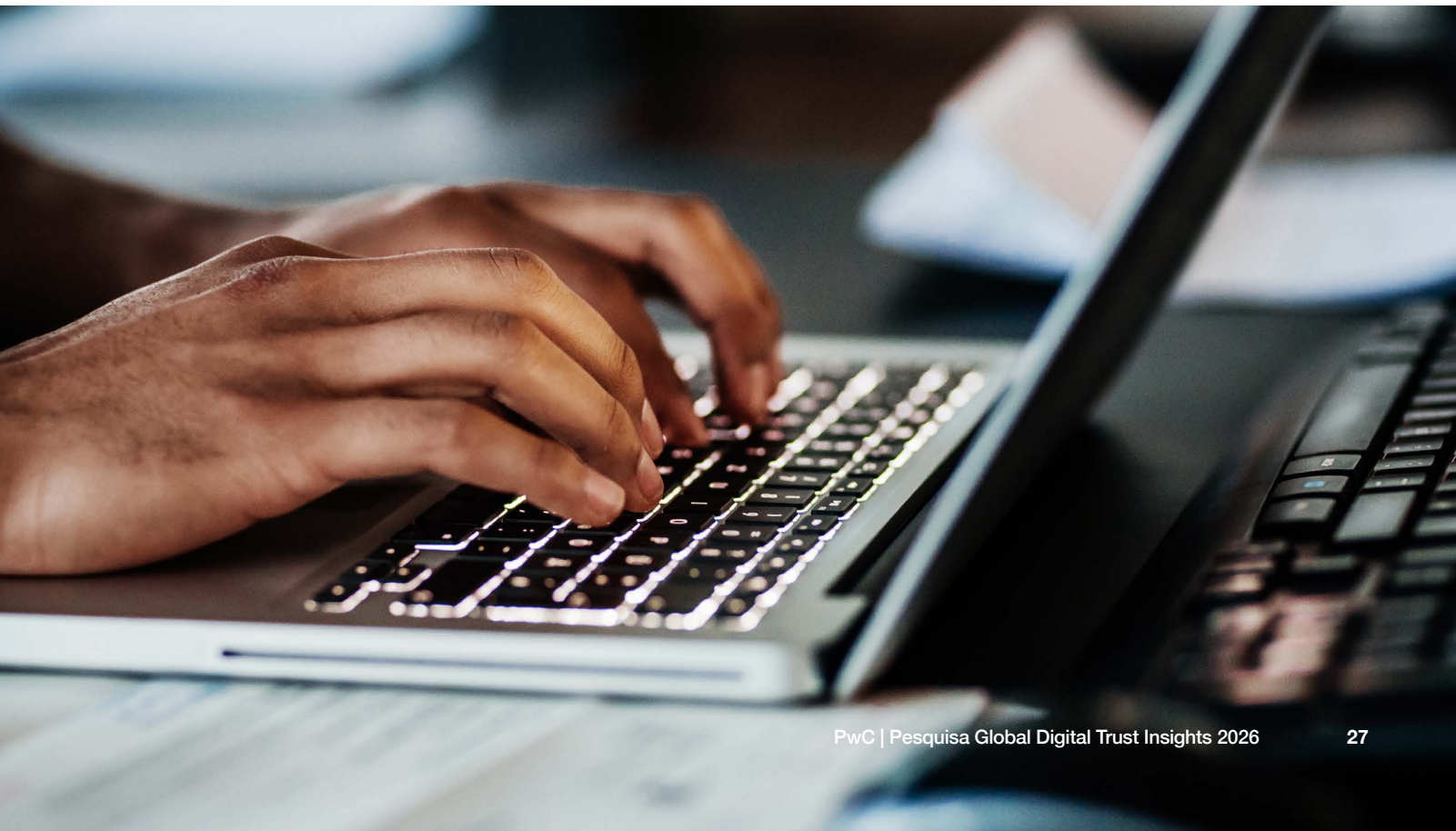
Agentes de mudança na defesa cibernética

As empresas começam a reconhecer que os agentes de IA – sistemas autônomos, orientados por resultados e capazes de executar tarefas com pouca intervenção humana – têm enorme potencial para transformar os programas de cibersegurança.

Após deixarem de ser apenas ferramentas de análise, os sistemas de IA estão se tornando assistentes digitais que conseguem agir sozinhos, colaborar com equipes humanas e até iniciar respostas de segurança, impulsionando, assim, a eficiência e a produtividade.

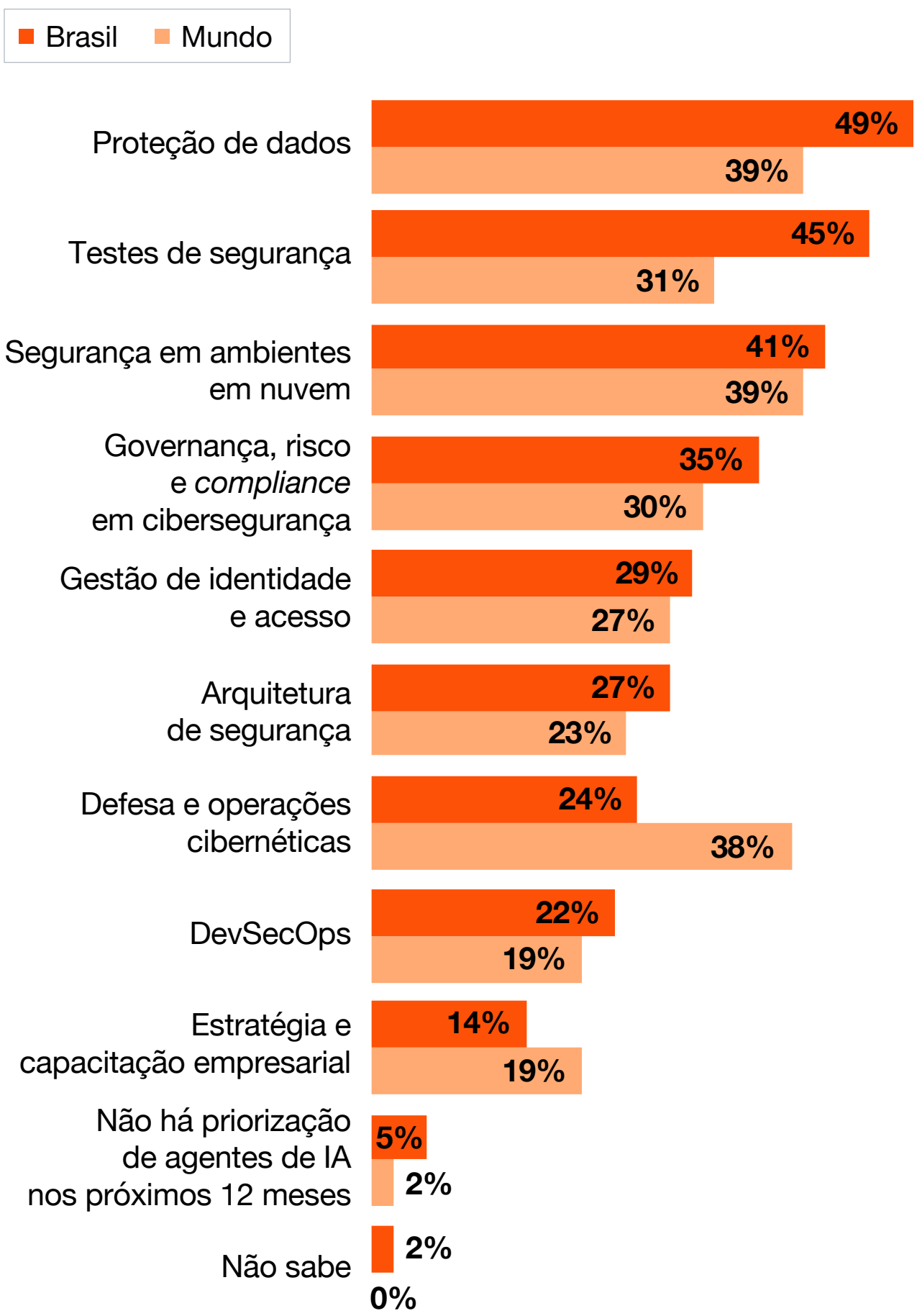
É por essa razão que os líderes de segurança brasileiros apontam esses agentes entre suas funções prioritárias de segurança de IA para este ano: proteção de dados, testes de segurança e segurança em ambientes em nuvem. Outras áreas são governança, risco e *compliance* (GRC) em cibersegurança e gestão de identidade e acesso.

Globalmente, as prioridades mudam um pouco. Segurança em nuvem, proteção de dados e defesa e operações cibernéticas estão no topo da lista para o uso de agentes de IA neste ano. Em seguida, estão testes de segurança, GRC e gestão de identidade e acesso.



Prioridades de IA agêntica para aumentar a eficiência e a produtividade

Pergunta: Em quais destas áreas sua empresa vai priorizar a adoção de IA agêntica para elevar a eficiência e a produtividade nos próximos 12 meses? (% dos que citaram a opção entre as três mais relevantes)



Base: líderes de segurança. Global = 1.740 | Brasil = 49.
Fonte: Pesquisa Global Digital Trust Insights 2026.

Gestão de risco de dados em IA

A adoção e o uso bem-sucedidos da IA dependem de práticas sólidas de gestão de riscos de dados. Isso ocorre porque soluções eficazes de IA exigem acesso a conjuntos de dados adequadamente tratados e de alta qualidade, além de governança e segurança fortes em toda a organização para garantir que esses dados sejam usados no contexto correto.

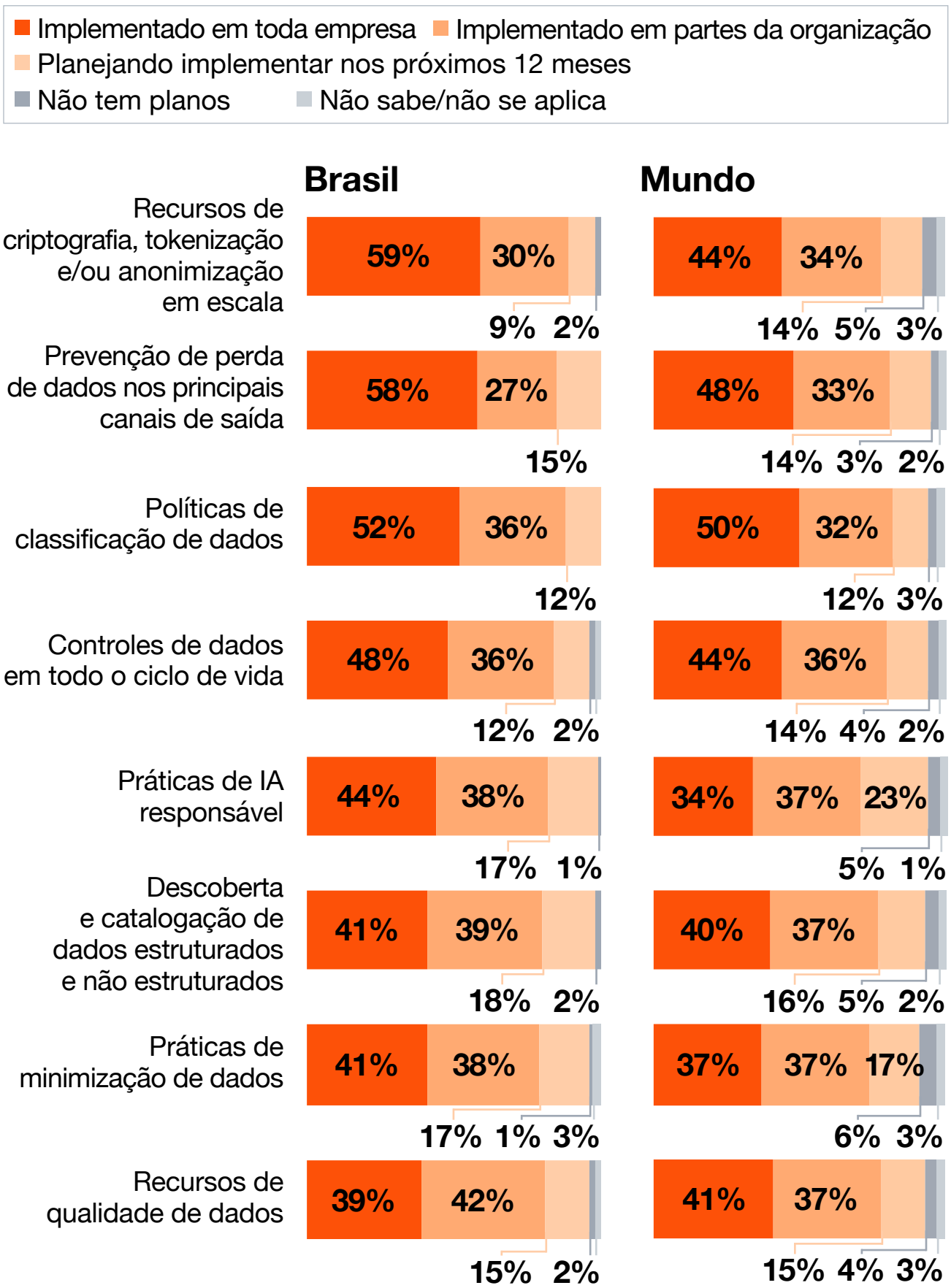
Quando perguntadas sobre os avanços na adoção de medidas de gestão de riscos de dados, quase 60% das empresas no Brasil responderam que adotam plenamente políticas de criptografia, tokenização e/ou anonimização em escala (59%) e de prevenção de perda de dados nos principais canais de saída (58%). Mais da metade (52%) afirmou que adota políticas de classificação de dados.

Globalmente, metade respondeu que implementa inteiramente políticas de classificação de dados e 48% de prevenção de perda de dados nos principais canais de saída. Outras medidas têm índices ainda menores, e apenas 6% aplicam todas as medidas avaliadas.

Essa deficiência mostra o tamanho do trabalho que as empresas ainda têm pela frente para extrair todo o potencial de seus dados em soluções de IA. Construir confiança digital com práticas transparentes, responsáveis e seguras será essencial para impulsionar a inovação e o crescimento com base nessa tecnologia.

Implementação de medidas para reduzir o risco de dados

Pergunta: Em que medida a sua empresa já adotou ou planeja adotar as medidas a seguir para reduzir os riscos de dados em toda a empresa?



Só 6% implementaram todas as medidas em toda a organização.

Base: líderes de segurança, CFOs, diretores financeiros, CDOs, Chief Counsel/GC/CLO, CROs, diretores de risco, CAEs e diretores de auditoria interna. Global = 2.395 | Brasil = 66.
Fonte: Pesquisa Global Digital Trust Insights 2026.

04

Preparação para a computação quântica: como encarar novas ameaças

Top 10

ameaças para as quais as empresas brasileiras estão menos preparadas para enfrentar agora incluem a computação quântica – no mundo, ela já está em 4º lugar

38%

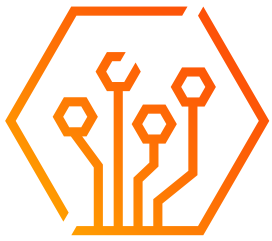
das empresas brasileiras ainda não adotaram nem sequer avaliaram medidas de segurança para resistir a ataques quânticos (49% no mundo)

Apenas 4%

dos líderes de segurança do Brasil (8% no mundo) incluem a preparação para a era quântica entre suas três prioridades de investimento

A contagem regressiva da computação quântica já começou. Deixou de ser apenas teórica e está saindo dos laboratórios, criando formas de resolver problemas complexos, como modelagem financeira e otimização logística. Ao mesmo tempo, ela está mudando os pressupostos que guiaram a cibersegurança por décadas.

Ainda que a computação quântica não seja uma ameaça imediata, quem adiar a transição para a criptografia pós-quântica corre o risco de deixar expostos dados sensíveis, serviços de autenticação e sistemas criptográficos. Por mais que essa transformação possa levar anos, criar bases sólidas para resistir a ataques quânticos exige ação imediata. É o que poderá evitar disrupções causadas por adversários no futuro.



Algumas empresas já estão avançando: 32% dos respondentes no Brasil afirmam que estão em fase de piloto e testes. Entretanto, só 30% passaram dessa etapa e 38% não consideraram nem começaram nenhuma medida de segurança para resistir a ataques quânticos.

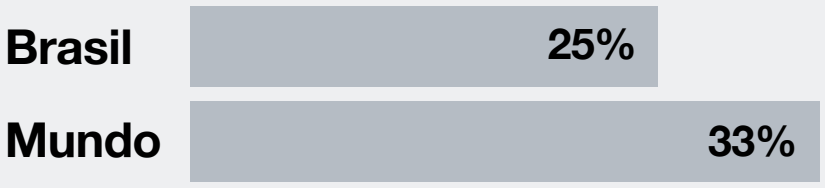
Mas os números no Brasil ainda são um pouco melhores do que no mundo. Globalmente, menos de 30% das empresas estão em fase de piloto e testes, e apenas 22% entraram na fase de implementação. Quase metade não está implementando nada nem há nada planejado nesse sentido. O que atrasa esse movimento é o fato de que, para muitas lideranças, há falta de entendimento sobre os riscos pós-quânticos, além das limitações de recursos e demandas concorrentes.

Avanço das medidas de segurança para resistir a ataques quânticos

Pergunta: Em que estágio está a sua empresa quando falamos de medidas de segurança para resistir a ataques quânticos?

Não começaram a pensar nessa questão nem têm planos: a empresa não iniciou a análise de medidas para resistir a ataques quânticos nem planeja fazer isso

Em fase de exploração: a empresa começou a olhar para o tema, mas ainda não deu nenhum passo para implementar medidas para resistir a ataques quânticos



Não consegue confirmar no momento

Brasil

38%

Não está implementando nem tem iniciativas planejadas

Mundo

49%

Não está implementando nem tem iniciativas planejadas

Em fase de implementação: a empresa está adotando medidas para resistir a ataques quânticos

Piloto e testes: a empresa já começou a adotar medidas e está em fase de testes e piloto

Base: todos os respondentes. Global: 3.887 | Brasil: 125.
Fonte: Pesquisa Global Digital Trust Insights 2026.

Ameaça quântica avança, prontidão atrasa

A preocupação com os riscos quânticos está crescendo. E a computação quântica já aparece globalmente entre as quatro principais ameaças que as empresas se sentem menos preparadas para enfrentar, subindo várias posições em relação à pesquisa do ano anterior.

Mas isso está sendo traduzido em ação? Sim e não. Mundialmente, cerca de um terço das empresas implementou uma ou mais medidas para resistir a ataques quânticos. Entretanto, só 3% adotaram todas as sete medidas avaliadas.

Embora não esgotem o tema, essas medidas são essenciais em uma jornada que pode durar vários anos e que exige atenção hoje. No entanto, apenas 8% dos líderes de segurança colocam a prontidão para a computação quântica entre as três principais prioridades de orçamento para o próximo ano.

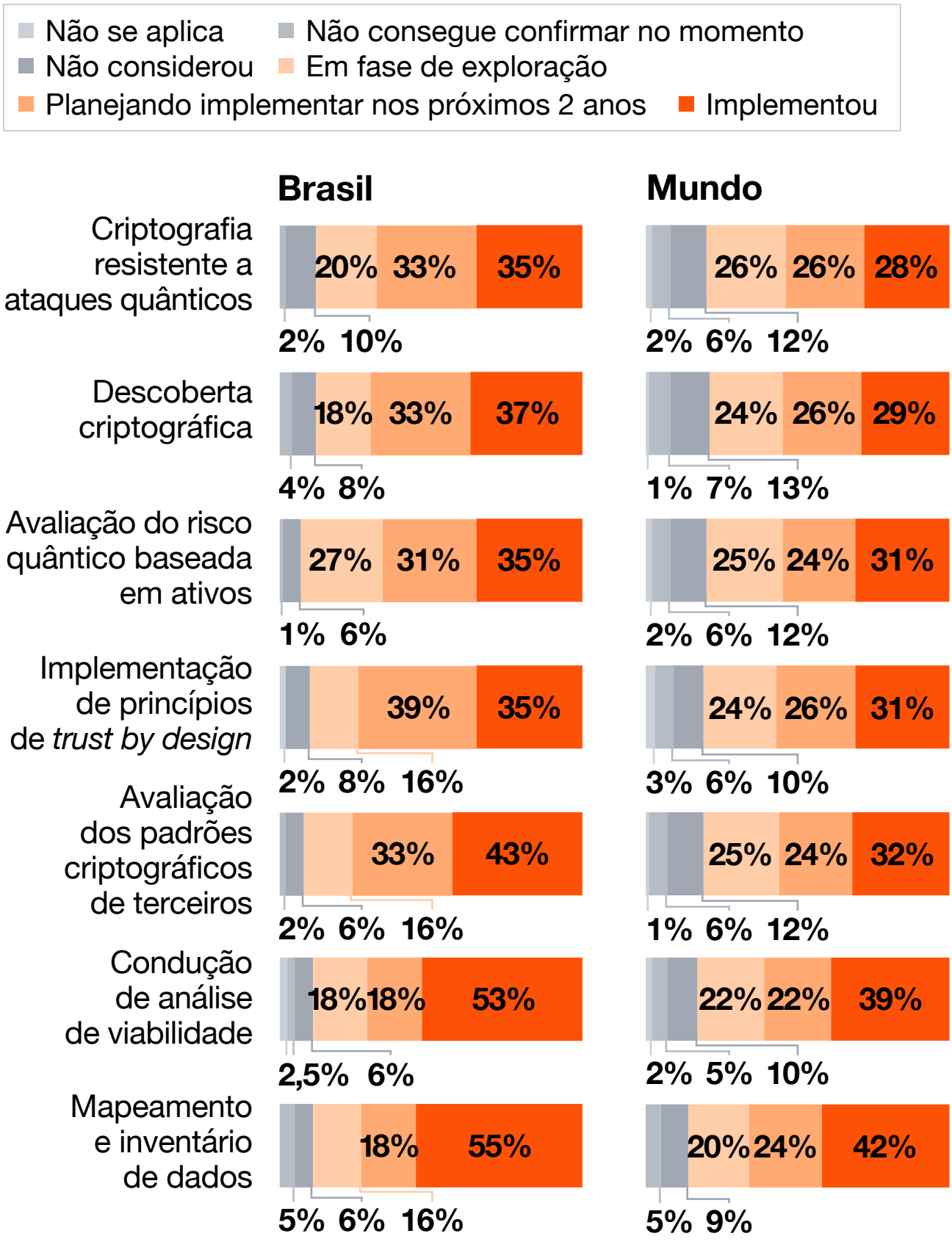
Olhando para o futuro, apenas 8% dos líderes de segurança incluem a prontidão para a computação quântica entre as três prioridades de seu orçamento para 2026.

Empresas com faturamento acima de US$ 5 bilhões estão mais avançadas. Elas já criam inventários de dados para mitigar o risco de “coletar agora, descriptografar depois”, fazem descoberta criptográfica para identificar ativos vulneráveis, testam e implementam criptografia resistente à computação quântica e conduzem análises de viabilidade e avaliações de risco quântico.

Empresas de maior crescimento também reconhecem o desafio e estão se posicionando para enfrentá-lo. No entanto, elas são a exceção por enquanto. À medida que a tecnologia avança, a capacidade de adotar rapidamente uma criptografia que resista a ataques quânticos tende a se tornar um diferencial estratégico para qualquer companhia.

Implementação de medidas de segurança para resistir a ataques quânticos

Pergunta: Em que estágio está a sua empresa quando falamos das seguintes medidas de segurança para resistir a ataques quânticos?



Só 3% adotaram todas as medidas de segurança para resistir a ataques quânticos.

Base: líderes de segurança. Global = 1.740 | Brasil = 49.
Fonte: Pesquisa Global Digital Trust Insights 2026.

Por que a criptografia pós-quântica é tão difícil?

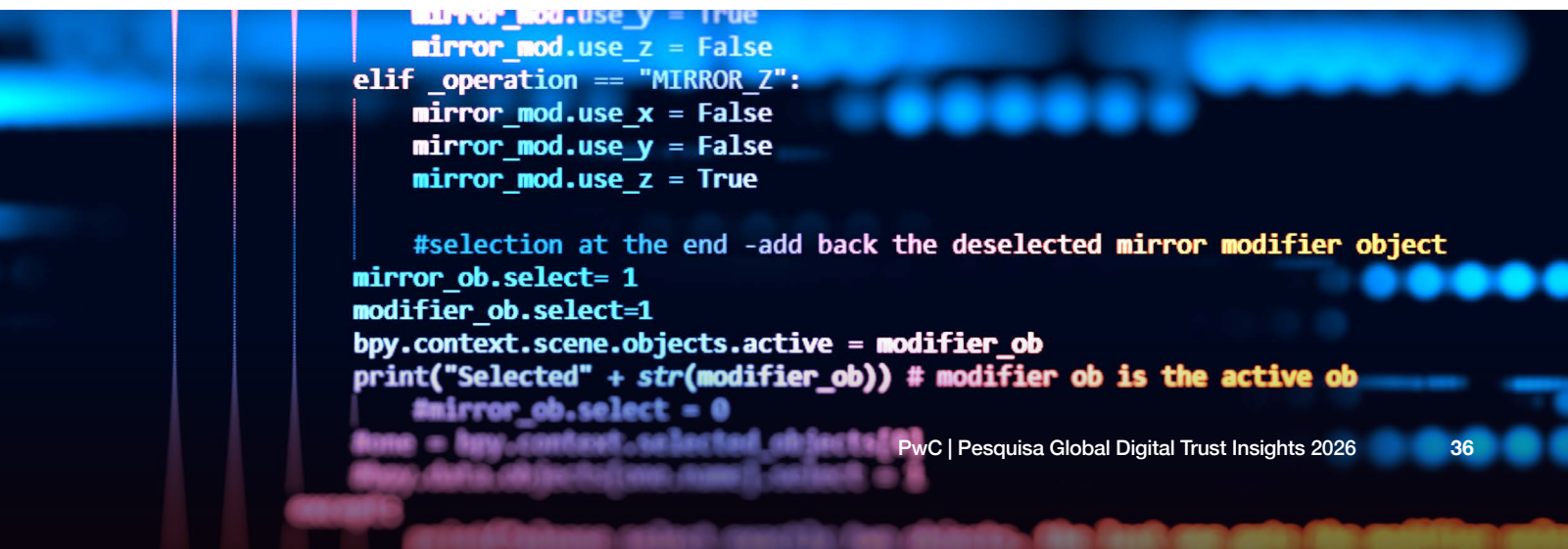
Estar preparado para a era quântica não é apenas uma questão de atualização técnica. É uma mudança de estratégia rumo a práticas de segurança pensadas para o futuro. Algumas barreiras internas podem gerar desafios, como falta de expertise técnica, conhecimento institucional limitado e sistemas legados engessados.

À medida que criam inventários criptográficos para avançar na adoção de uma criptografia que resista a ataques quânticos, as empresas precisam identificar algoritmos vulneráveis em toda sua arquitetura tecnológica.

Embora a vulnerabilidade da criptografia de chave pública ao modelo “coletar agora, descriptografar depois” já seja bem conhecida, os líderes de segurança também devem avaliar os sistemas de autenticação e assinaturas digitais, que podem estar baseados em algoritmos igualmente frágeis.

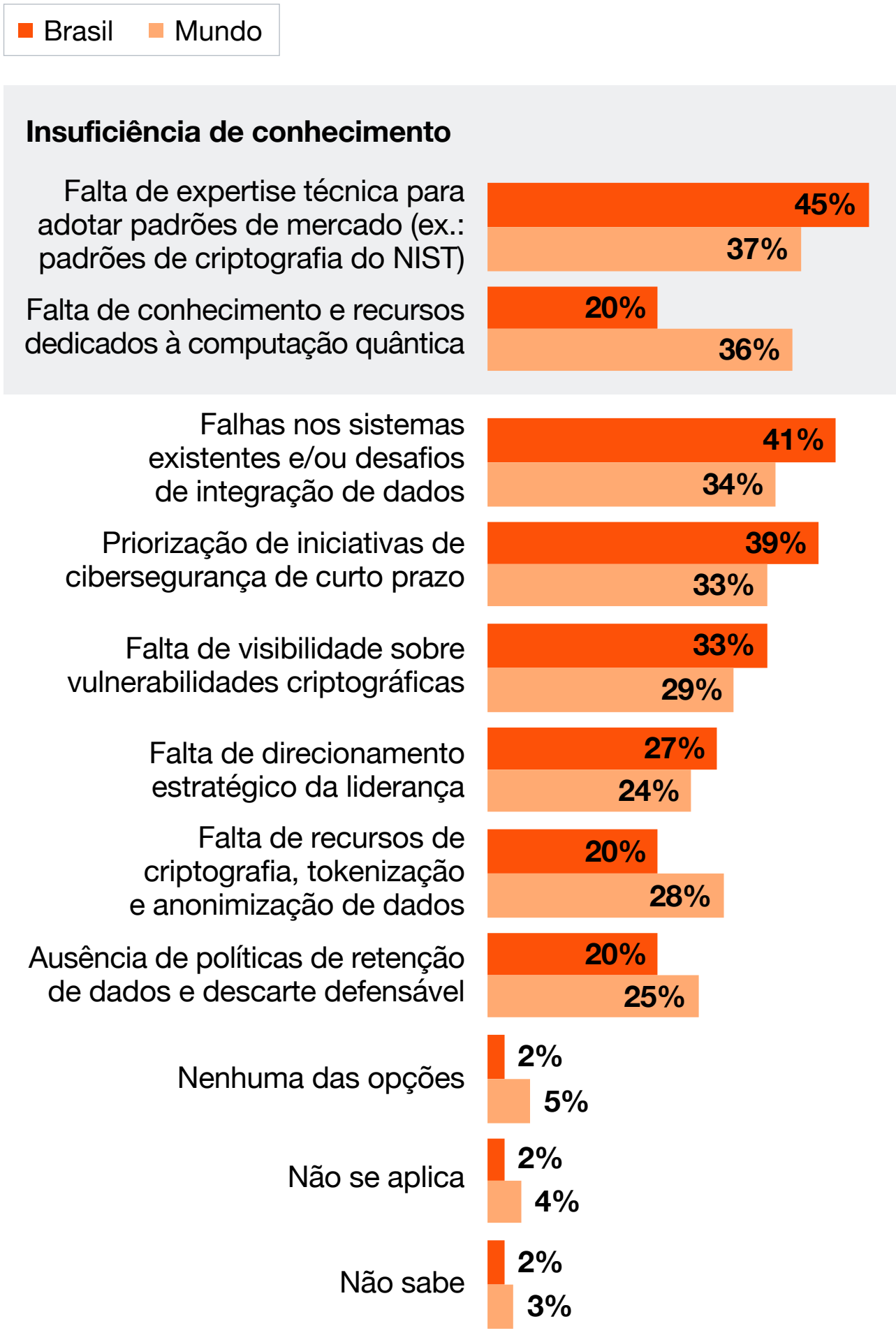
Essas barreiras deixam claro que a transição para a criptografia resistente à computação quântica, mesmo quando priorizada, é um processo que demanda tempo – algo cada vez mais escasso.

Os principais padrões de criptografia do mercado – como os do *National Institute of Standards and Technology* (NIST), dos EUA – recomendam abandonar os algoritmos vulneráveis antes que agentes mal-intencionados consigam desenvolver capacidade quântica. Por isso, é essencial agir para suprir deficiências de conhecimento, avaliar as dependências criptográficas e elaborar planos de preparação.



Desafios para alcançar a criptografia pós-quântica

Pergunta: Quais são os maiores desafios internos da sua empresa para alcançar a criptografia pós-quântica nos próximos 12 meses? (% dos que citaram a opção entre as três mais relevantes)



Base: líderes de segurança. Global = 1.740 | Brasil = 49.
Fonte: Pesquisa Global Digital Trust Insights 2026.

05

Talentos e competências em cibersegurança: serviços gerenciados na linha de frente

2 principais

desafios para usar a IA na defesa cibernética: deficiências de conhecimento e de competências

65% das empresas no Brasil

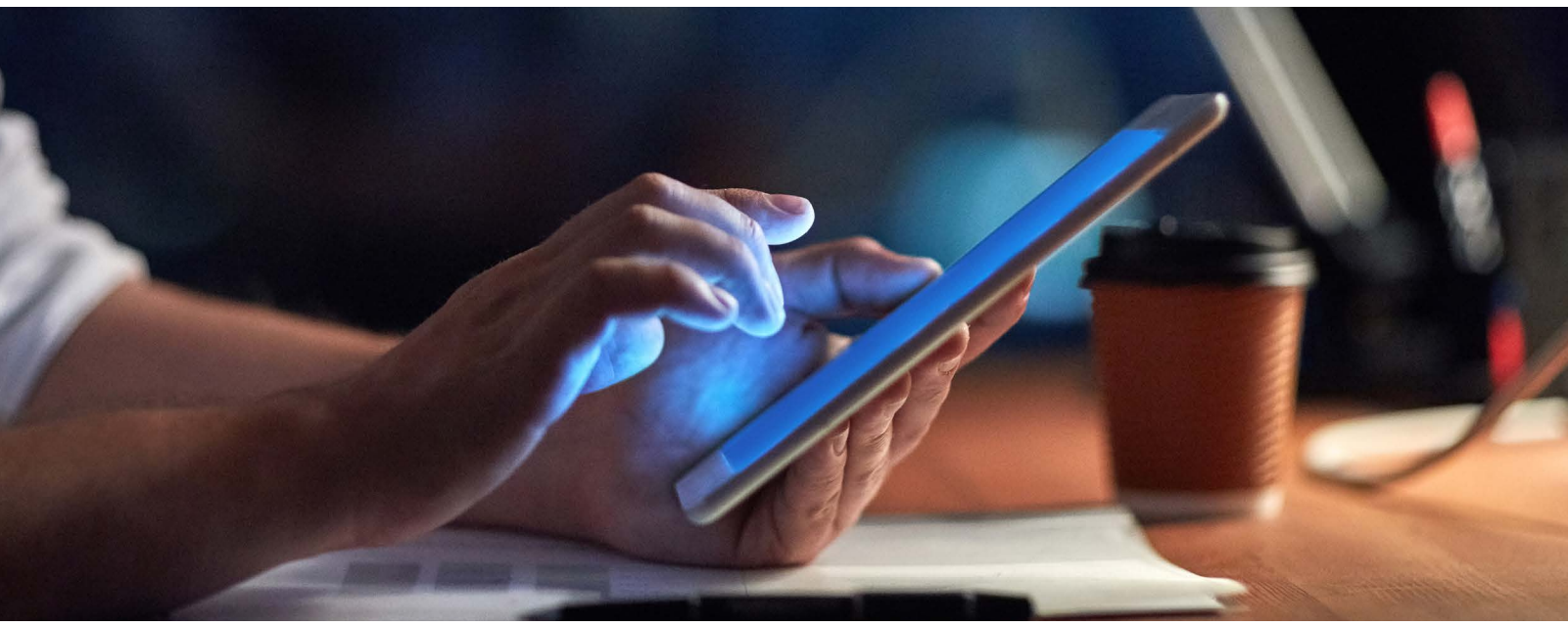
(53% no mundo) incluem a IA e o aprendizado de máquina entre as três prioridades para reduzir deficiências de talentos em cibersegurança nos próximos 12 meses

Quase 50% das organizações

que sofreram algum ataque grave estão priorizando serviços gerenciados para reduzir deficiências de talentos em cibersegurança

A insuficiência de profissionais na área de cibersegurança continua dificultando o avanço das empresas, especialmente das que tentam operacionalizar a IA, proteger ambientes complexos e se preparar para as ameaças. Deficiências de conhecimento e de competências técnicas foram as duas maiores barreiras à implementação da IA na defesa cibernética no último ano. Esse cenário forçou as empresas a repensar como evoluir no nível de proteção.

Para adotar a IA na defesa cibernética, por exemplo, 56% das empresas brasileiras apontam como desafio o fato de não haver conhecimento suficiente, e 47% dizem que não há competências técnicas relevantes para realizar o trabalho. Globalmente, 50% apontam a expertise insuficiente e 41% a falta de competências técnicas relevantes.



Diante disso, muitas organizações estão procurando novas formas de adquirir conhecimento técnico. Ferramentas de IA (53%), ferramentas de automação de segurança (48%), a consolidação de ferramentas de cibersegurança (47%) e a adoção de programas de *upskilling* e *reskilling* (47%) são as saídas mais apontadas. As empresas estão priorizando também os serviços gerenciados especializados – principalmente as que já sofreram algum tipo de ataque grave (48%).

Desafios para implementar IA na defesa cibernética

Pergunta: Quais foram os maiores desafios internos da sua empresa para implementar a IA na defesa cibernética nos últimos 12 meses? (% dos que citaram a opção entre as três mais relevantes)

Base: líderes de segurança, CEOs, CFOs, diretores financeiros, COOs e diretores de operações. Global = 2.764 | Brasil = 95.
Fonte: Pesquisa Global Digital Trust Insights 2026.

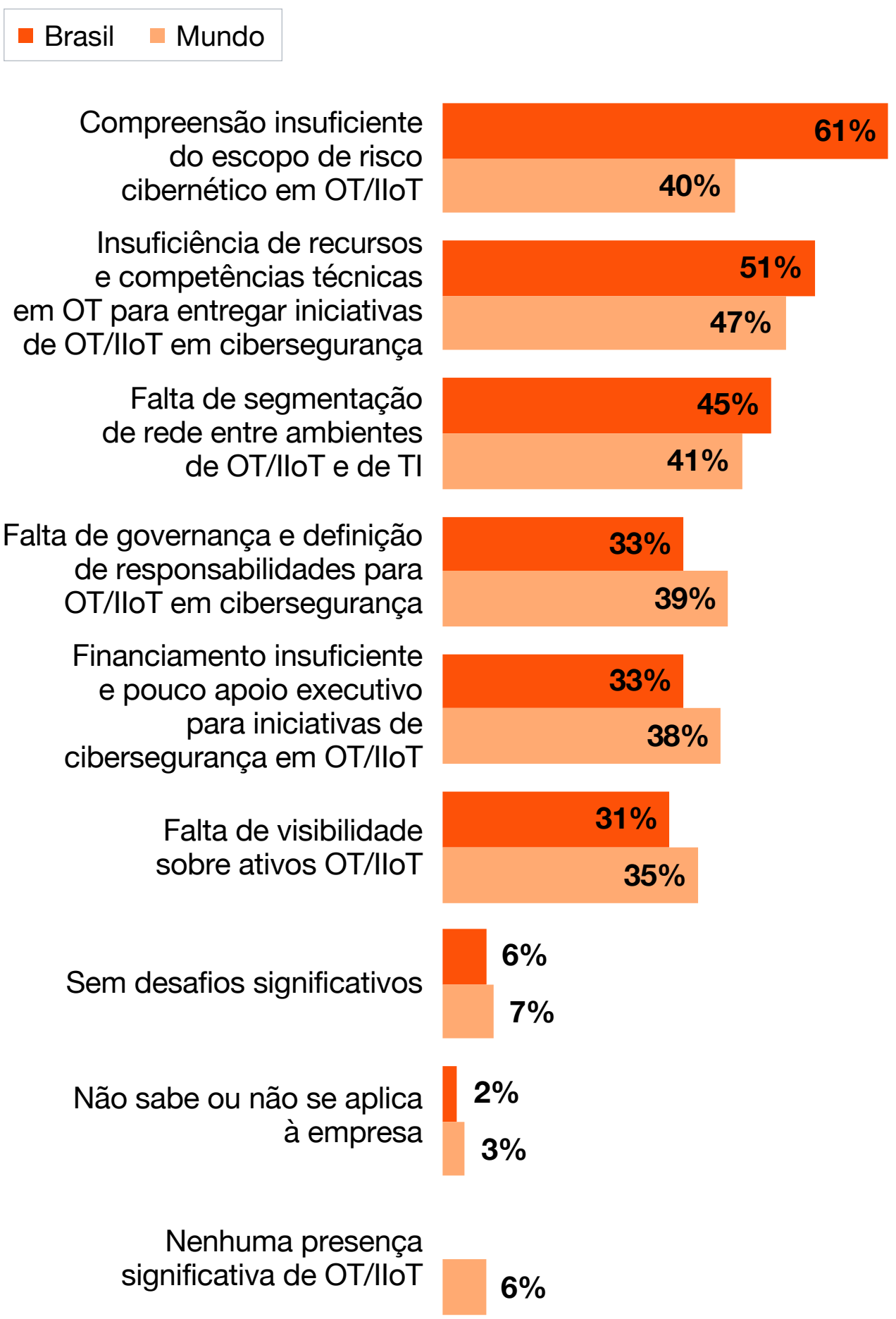
Competências em tecnologia operacional

A tecnologia operacional (OT) e a Internet das Coisas Industrial (IIoT) se tornaram pontos de pressão no cenário da segurança. Mais da metade dos líderes brasileiros (51%) e quase a metade dos globais (47%) citam a falta de profissionais qualificados entre os três maiores desafios para proteger a OT e a IIoT.

Cerca de um terço – 33% no Brasil e 39% no mundo – aponta como obstáculo a falta de governança e de uma definição clara de responsabilidades na alta liderança. Juntos, esses números mostram que muitas empresas ainda não dispõem de estrutura e conhecimento suficientes para gerenciar com confiança sistemas operacionais cada vez mais conectados.

Obstáculos para proteger sistemas OT e IIoT

Pergunta: Quais são os três maiores desafios da sua empresa para proteger sistemas de OT e/ou IIoT?
(% dos que citaram a opção entre os três maiores obstáculos)



Base: líderes de segurança. Global = 1.740 | Brasil = 49.
Fonte: Pesquisa Global Digital Trust Insights 2026.

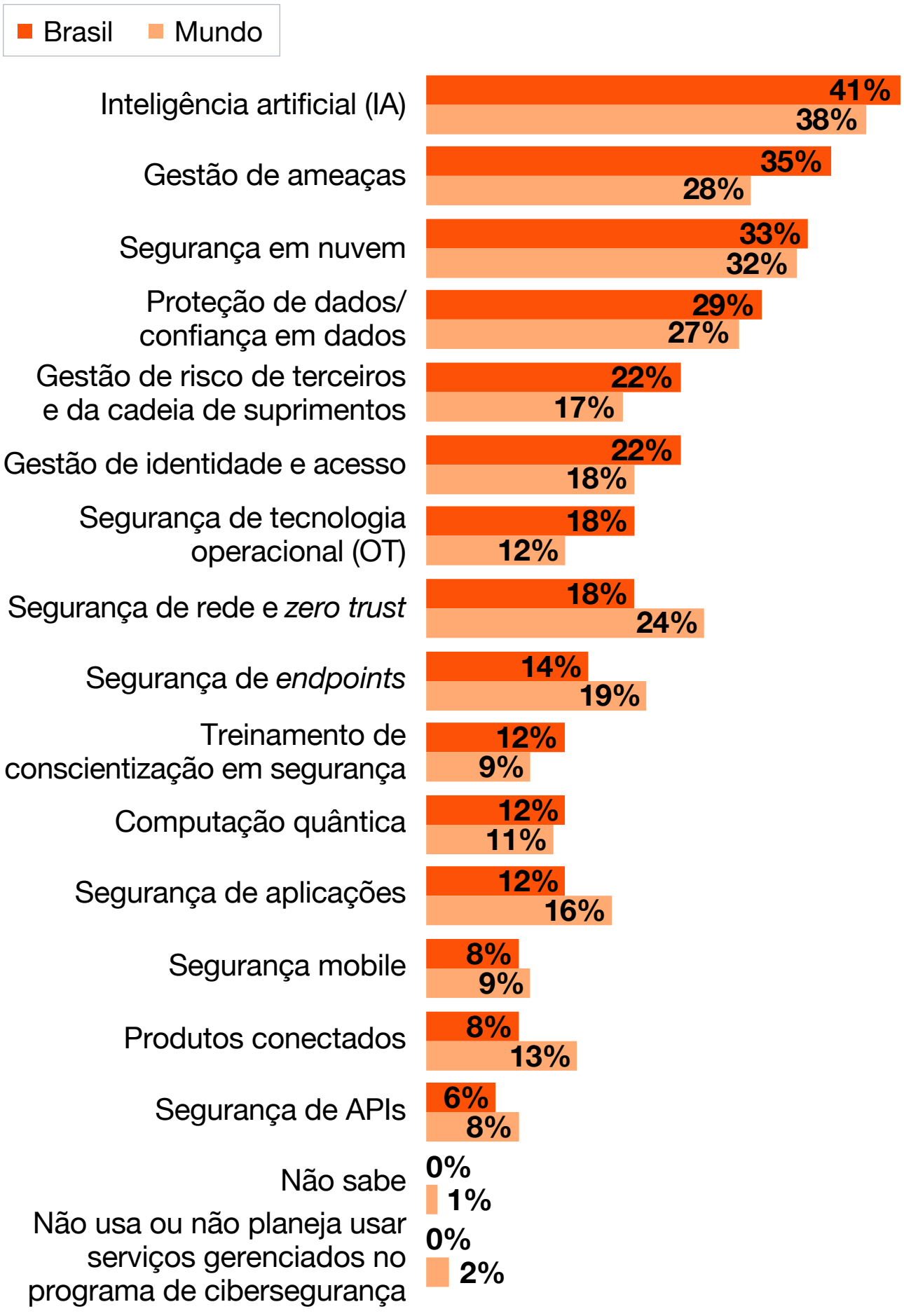
Serviços gerenciados como aceleradores estratégicos

A IA, a gestão de riscos e os ambientes em nuvem são mais do que áreas de investimento prioritárias em segurança cibernética. São também os principais casos de uso de serviços gerenciados especializados em segurança. As empresas estão usando esses serviços não apenas para terceirizar atividades. Elas estão criando parcerias com outras empresas especializadas para modernizar a entrega de sistemas críticos.

Diante disso, os serviços gerenciados estão se tornando aceleradores estratégicos, que chegam para compensar deficiências de competências técnicas e entregar velocidade, escala e conhecimento especializado. Em um cenário de ameaças crescentes e cada vez mais complexas, esses serviços oferecem um caminho para modernizar os sistemas de defesa sem tirar o foco da inovação e do crescimento.

Prioridades de cibersegurança para o uso de serviços gerenciados

Pergunta: Quais das seguintes áreas do seu programa de cibersegurança sua empresa pretende priorizar no uso de serviços gerenciados nos próximos 12 meses?
(% dos que citaram a opção entre as três mais relevantes)



Base: líderes de segurança. Global = 1.740 | Brasil = 49.
Fonte: Pesquisa Global Digital Trust Insights 2026.

06

Da incerteza à ação: o que líderes podem fazer agora

A Pesquisa Global Digital Trust Insights 2026 revela que as empresas mais visionárias estão alinhando a segurança cibernética à estratégia de negócio e, principalmente, priorizando sua prontidão para resistir a ataques.

Muitas organizações já adotaram abordagens mais estruturadas de gestão de riscos cibernéticos, fortalecendo a governança para alinhá-la aos principais *frameworks* do mercado, integrando controles de risco em toda a empresa e priorizando avaliações e relatórios.

No entanto, para as empresas estarem realmente preparadas para o futuro, elas precisam ir além do que fazem hoje. Isso significa encarar incertezas, tomar decisões firmes e bem fundamentadas e adotar uma estratégia mais ágil.

CISO/CSO

Sua capacidade de traduzir riscos cibernéticos complexos em riscos de negócio e de comunicar que a cibersegurança é uma responsabilidade compartilhada é essencial para garantir a adesão e a colaboração dos executivos *C-level*. Esse entendimento ajuda a fortalecer a governança, a resiliência, a conformidade regulatória e as ações de resposta.

É essencial tratar novos riscos de forma proativa, fortalecer a segurança *by design* – que pensa a segurança como requisito de projeto, e não como um remendo ou algo que se deve ser trabalhado somente depois. Além disso, use dados para medir e mostrar onde os investimentos em cibersegurança são mais necessários.

Medidas fundamentais

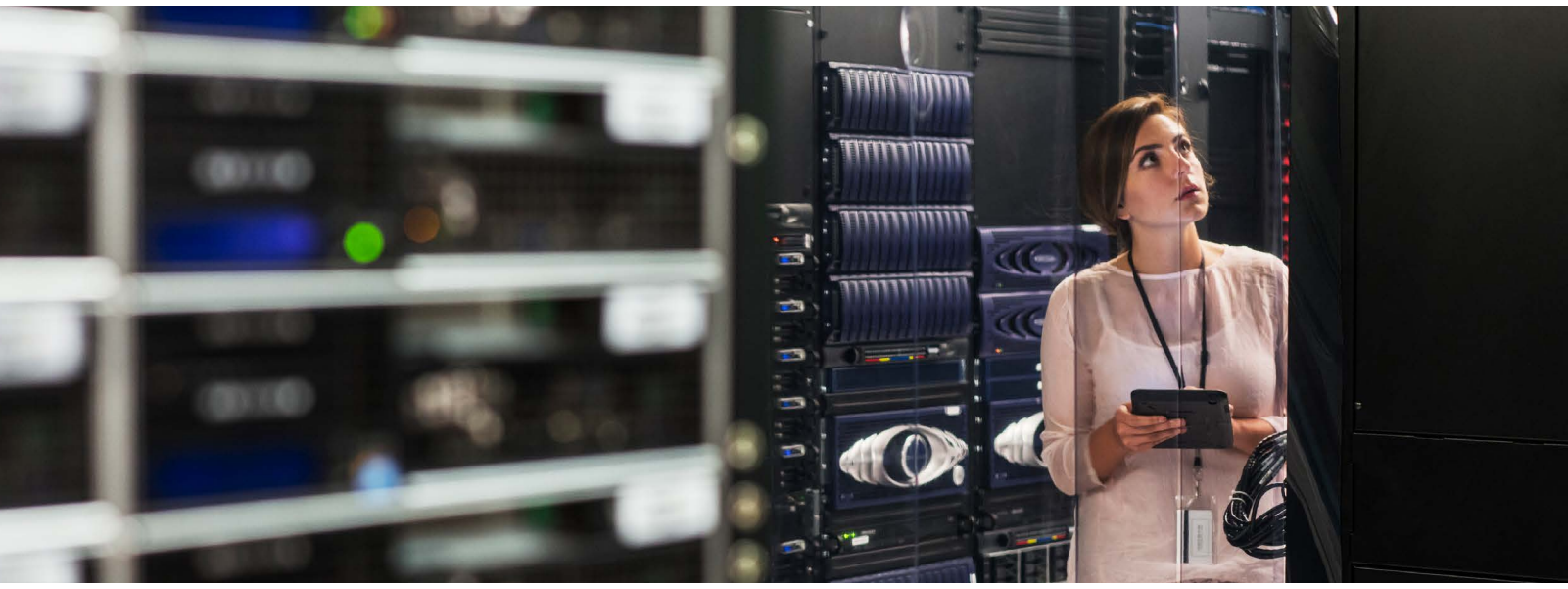
- Quantifique a exposição a riscos geopolíticos usando métricas relacionadas à infraestrutura crítica, às operações globais e às disrupções específicas do seu setor. Compartilhe esses resultados com a alta liderança.
- Adote uma modelagem dinâmica de ameaças alinhada à sua inteligência atual sobre regiões de alto risco, campanhas de riscos cibernéticos e tendências de extorsão de dados.
- Incorpore princípios de IA responsável em todas as iniciativas de tecnologia da sua empresa. Classifique os sistemas de IA (modelos, agentes e suas identidades, aplicações e dados de treinamento), conforme sua sensibilidade, criticidade e exposição.
- Aplique controles de segurança aos sistemas de IA, ampliando os controles existentes e identificando lacunas que exijam novas soluções e competências (como *guardrails* de IA ou *gateways* para LLMs).

- Reavalie e atualize regularmente os modelos de governança de riscos cibernéticos para incorporar os riscos associados a tecnologias em constante evolução, como a IA e a computação quântica.
- Fortaleça a governança com KPIs com foco em execução que acompanhem o desempenho na gestão de riscos relacionados a terceiros, à cadeia de suprimentos, a sistemas legados e a ambientes em nuvem.
- Realize exercícios de resposta a incidentes (*tabletop exercises*) e outras simulações para testar a tomada de decisão, definir caminhos de escalonamento e validar as etapas de recuperação.

Preparando-se para o futuro

- Defina a cibersegurança como uma responsabilidade compartilhada com os executivos *C-level* e o conselho, ao incluir, nas discussões de governança, análises de inteligência de riscos e resumos executivos sobre ameaças emergentes e capacidades dos adversários.
- Organize a supervisão e a governança dos agentes de IA por meio de processos de descoberta, classificação, mapeamento de exposição e monitoramento contínuo, incluindo simulações de ataque.
- Evolua de avaliações pontuais de fornecedores para um monitoramento contínuo de riscos de terceiros.
- Avalie quais sistemas dependem de criptografia e adote padrões de criptografia pós-quântica (PQC), quando necessário.

- Decida se sua empresa deve contratar serviços gerenciados por meio de um plano baseado em ROI que mapeie tecnologia, competências técnicas e necessidades de recursos.
- Avalie seus dados e identifique o que já deve estar pronto para a era quântica. Em seguida, trabalhe com as equipes de governança de dados para viabilizar a adoção quântica.



CTO/CIO

O foco em escalar tecnologia com segurança e em tratar de forma proativa as lacunas de formação e de competências técnicas é essencial para fortalecer a postura de cibersegurança da organização. Continue trabalhando em parceria com a liderança de segurança para integrar controles de risco e governança a todas as iniciativas de adoção tecnológica.

Daqui em diante, você estará à frente de iniciativas para testar e integrar tecnologias emergentes, como IA e computação quântica, já com segurança incorporada, impulsionando a inovação e antecipando riscos cibernéticos.

Medidas fundamentais

- Escale a IA e outras tecnologias emergentes de forma segura. Reserve orçamento e incorpore medidas proativas e críticas desde o início.
- Trabalhe lado a lado com o CISO e o CRO para alinhar a adoção de tecnologia à gestão de riscos e aos requisitos de conformidade legal.
- Proteja os sistemas de IA ao incorporar a governança e os controles de risco cibernético ao planejamento da implementação dessa tecnologia – tudo isso alinhado a uma abordagem *secure-by-design*.
- Adote controles consistentes de identidade, acesso e políticas em plataformas de terceiros, APIs e integrações.
- Adote uma governança robusta de IIoT e OT em sua estratégia de arquitetura para ganhar visibilidade e controle de ponta a ponta em ambientes distribuídos.

Preparando-se para o futuro

- Trabalhe com CISOs e líderes de dados para proteger informações sensíveis usadas em treinamentos e reforçar a governança de entrada e saída dos modelos de IA.
- Alinhe a adoção e os pilotos em computação quântica às estratégias corporativas de segurança resistente a ataques quânticos, em parceria com a liderança de segurança.
- Avance na adoção da automação e de ferramentas de detecção e resposta direcionadas pela IA para aumentar a eficiência operacional e a resiliência.
- Adote uma abordagem *secure-by-design* para produtos conectados em todas as fases do ciclo de vida operacional.

CRO

Seu foco em identificar riscos corporativos e emergentes – e suas interdependências com a cibersegurança – é essencial para proteger a organização. Você deve continuar ajustando os controles às novas vulnerabilidades, garantindo que os *frameworks* de risco permaneçam atualizados.

De agora em diante, seu papel exigirá integrar exposições a IA, computação quântica e fatores geopolíticos a uma estratégia de gestão de riscos adaptável e preparada para o futuro, que fortaleça a agilidade e a resiliência da organização.

Medidas fundamentais

- Incorpore cenários orientados por ameaças aos registros de risco e aos ciclos de testes de estresse, considerando vetores geopolíticos já conhecidos.
- Avalie os controles existentes para lidar com essas exposições e ajuste as estratégias de mitigação, quando necessário.
- Quantifique os riscos da IA e da computação quântica com base em análises customizadas de impacto no negócio, priorizando áreas com automação digital da força de trabalho.
- Apoie os esforços da área de *compliance* conectando a gestão de ameaças cibernéticas aos requisitos regulatórios.

Preparando-se para o futuro

- Amplie os modelos de riscos de terceiros para considerar a capacidade quântica nos ambientes de fornecedores e a resiliência ao uso indevido da IA por adversários.
- Use a IA para avaliar continuamente o risco cibernético em escala, desde a sua quantificação até as avaliações e os relatórios.
- Desenvolva um *framework* de risco integrado à inteligência (IIRF), que incorpore diferentes perspectivas de inteligência estratégica de ameaças nas pontuações de riscos corporativos.
- Teste ferramentas de modelagem preditiva de riscos para simular ameaças emergentes e quantificar impactos prováveis no negócio nos próximos 12 a 36 meses.

CFO

Definir orçamentos adequados para viabilizar medidas proativas de cibersegurança em iniciativas estratégicas e na implementação de tecnologia é essencial. É o que sustenta a resiliência da empresa. Você deve continuar identificando ineficiências e alinhando os investimentos a iniciativas de cibersegurança de alto impacto.

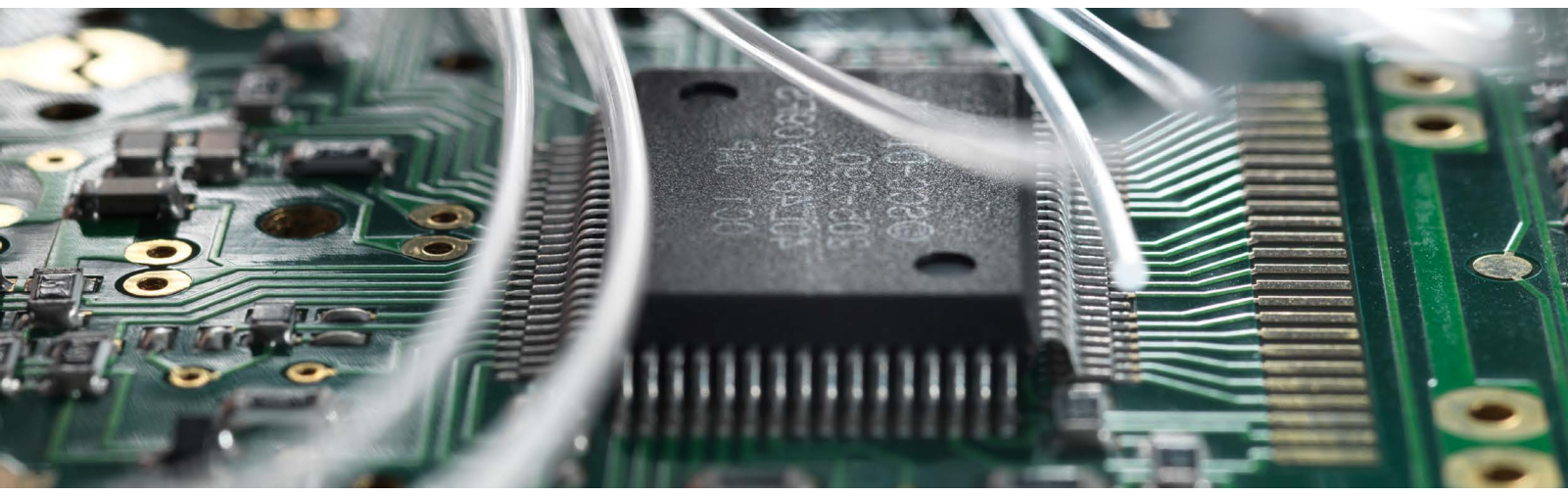
Olhando adiante, preparar a organização para riscos emergentes significa mapear de forma proativa as necessidades futuras de recursos financeiros e fomentar modelos de financiamento orientados por ROI. Assim, sua empresa poderá investir com sabedoria em tecnologias de segurança e desenvolvimento de competências técnicas.

Medidas fundamentais

- Apoie investimentos estratégicos que fortaleçam a resiliência no longo prazo, aumentem a vantagem competitiva e deixem a empresa preparada para cumprir os requisitos regulatórios.
- Avalie os custos de longo prazo de reagir a incidentes de segurança em relação aos investimentos em defesa cibernética, serviços gerenciados, seguros, *compliance* etc.
- Recalibre as métricas de ROI em cibersegurança para incluir economias geradas pela prevenção de incidentes, evitar multas regulatórias e reduzir o tempo de resposta.
- Trabalhe com CISOs, CTOs e CIOs para planejar orçamentos que desenvolvam efetivamente as competências técnicas em cibersegurança e ampliem o treinamento em tecnologia.
- Apoie modelos de financiamento sustentáveis que equilibrem os custos operacionais com investimentos estratégicos em segurança cibernética.

Preparando-se para o futuro

- Defenda a cibersegurança como uma função essencial do negócio, conectando os níveis de investimento aos objetivos de desempenho corporativo definidos pelo conselho.
- Crie uma reserva estratégica dedicada a iniciativas de resiliência, incluindo resposta a vulnerabilidades *zero-day* e segurança pós-quântica.
- Desenvolva *cases* orientados por ROI para serviços gerenciados de segurança.
- Identifique e reduza as ineficiências, como redundância de ferramentas, e consolide-as quando possível.



CEO

Seu compromisso de garantir que a cibersegurança seja uma prioridade do negócio continua sendo vital. Você deve seguir alinhando as iniciativas da empresa à estratégia de gestão de riscos cibernéticos, ao mesmo tempo em que fortalece a colaboração com o conselho e o *C-level*.

Em termos futuros, seu papel envolve construir parcerias de impacto e liderar investimentos que permitam à organização enfrentar os desafios cibernéticos que estão surgindo.

Medidas fundamentais

- Exija a participação da liderança executiva em exercícios de cenários cibernéticos que simulem disrupções específicas do setor e ameaças híbridas.
- Conecte a resiliência cibernética à geração de receita, com a proteção de plataformas digitais, o fortalecimento da confiança nos dados dos clientes e a expansão internacional.
- Apoie a inovação responsável, garantindo que os projetos de IA e de computação quântica incorporem, desde o início, salvaguardas éticas e de segurança.
- Tenha clareza sobre os *trade-offs* do orçamento de cibersegurança e assegure que estejam coerentes com o apetite a risco da empresa.
- Transforme a cibersegurança em uma responsabilidade compartilhada em todos os níveis – do conselho ao *back office*.
- Mantenha o conselho informado sobre as prioridades estratégicas de cibersegurança. Envolva os conselheiros nas discussões sobre as necessidades do programa.

Preparando-se para o futuro

- Lidere alianças multissetoriais para a padronização pós-quântica, posturas conjuntas de defesa e a troca de inteligência sobre ameaças.
- Defenda investimentos em tecnologias emergentes (IA e computação quântica) com segurança incorporada desde o início.
- Institucionalize análises prospectivas sobre riscos quânticos e geopolíticos nos ciclos de planejamento estratégico e nos comitês de risco do conselho.
- Participe ativamente de testes de estresse para se preparar para disrupções geopolíticas e tecnológicas.

Sobre a pesquisa

A pesquisa **Global Digital Trust Insights 2026** da PwC é um levantamento realizado com mais de 3.800 executivos de negócios e de tecnologia, entre maio e julho de 2025.

Um terço dos executivos (33%) atua em empresas de grande porte, com faturamento acima de US$ 5 bilhões. A amostra reúne organizações de diversos setores, como serviços financeiros (21%); produção industrial e automotiva (21%); tecnologia, mídia e telecomunicações (19%); varejo e consumo (16%); saúde (10%); energia e serviços de utilidade pública (9%); e governo (4%).

Os participantes representam 72 países, com a seguinte distribuição regional: Europa Ocidental (32%), América do Norte (27%), Ásia-Pacífico (18%), América Latina (11%), Europa Central e Oriental (6%), África (4%) e Oriente Médio (3%).

A *Pesquisa Global Digital Trust Insights* (DTI) era antes conhecida como *Global State of Information Security Survey* (GSISS). Em seu 28º ano, é a pesquisa anual mais antiga sobre tendências em cibersegurança. Também é a maior do setor e a única que conta com a participação de altos executivos de negócios, não apenas de executivos de segurança e tecnologia.

A pesquisa foi conduzida pelo PwC Research, nosso Centro de Excelência Global para pesquisa de mercado e insights.

Contatos

Eduardo Batista
Sócio e líder da prática de Risk Services
eduardo.batista@pwc.com

Fernando Mitre
Sócio
fernando.mitre@pwc.com

Larissa Escobar
Sócia
larissa.escobar@pwc.com

Magnus Santos
Sócio
magnus.santos@pwc.com

Rafael Cortes
Sócio
cortes.rafael@pwc.com

Ezequiel Souza
Sócio
ezequiel.souza@pwc.com

Siga a PwC nas redes sociais