Novo mundo, novas regras: cibersegurança em tempos de incertezas

Pesquisa Global Digital Trust Insights 2026

Recorte da indústria de Serviços Financeiros

Conteúdo

Apresentação

O setor de serviços financeiros opera na interseção de dois mundos igualmente desafiadores: da regulação rigorosa e da inovação acelerada. Essa dinâmica molda a exposição da indústria a riscos cibernéticos, em um ambiente no qual as instituições financeiras são alvos prioritários; os impactos potenciais são sistêmicos; e o custo de uma falha pode se materializar rapidamente.

Esta análise setorial da nossa **Pesquisa Global Digital Trust Insights 2026**, que contou com a participação de mais de 3.800 executivos de negócios e tecnologia em 72 países, examina como as instituições financeiras estão respondendo a um cenário de ameaças redefinido pela geopolítica, inteligência artificial e proximidade da era quântica — que representa uma nova fase tecnológica a partir de computadores milhões de vezes mais rápidos, sensores precisos e segurança de dados avançada.

Os dados da pesquisa mostram uma indústria global que, em muitas frentes, já avançou além da média, mas que ainda enfrenta lacunas relevantes entre o diagnóstico e a execução.

Destaques desta edição

Investimento em alta, prontidão evoluindo

62% dos líderes do setor pretendem ampliar os orçamentos de cibersegurança, mas vulnerabilidades em sistemas legados, cadeia de suprimentos e visibilidade de *endpoints* continuam preocupando.

IA como ameaça e como resposta

Deepfakes e envenenamento de dados preocupam mais o setor do que a média global. Para enfrentá-los, a caça a ameaças com IA e a detecção de comportamento anômalo lideram as prioridades de investimento.

Governança em evolução

Embora o CISO mantenha níveis de colaboração com a liderança executiva acima da média global, o engajamento direto com o CEO permanece relativamente limitado – um sinal de que a integração estratégica da cibersegurança ainda pode avançar.

A corrida quântica em ritmo de mercado

O setor mapeia riscos e avalia caminhos de transição, mas ainda avança pouco na implementação de criptografia resistente a ataques quânticos.

Traduzir urgência em ação estruturada é o desafio central que este relatório busca evidenciar. As páginas a seguir oferecem dados, comparações e perspectivas para ajudar líderes do setor financeiro no Brasil a tomar decisões mais estratégicas – e a agir antes que o próximo incidente force essa agenda.

“No setor financeiro, cibersegurança deixou de ser uma agenda sobre tecnologia para se tornar um tema que influencia decisões estruturais de negócio. O desafio já não está em reconhecer os riscos, mas em transformar diagnóstico em execução consistente, com governança, priorização clara e integração real entre segurança, estratégia e regulamentação.”

Lindomar Schmoller,
sócio e líder da indústria de Serviços Financeiros
da PwC Brasil

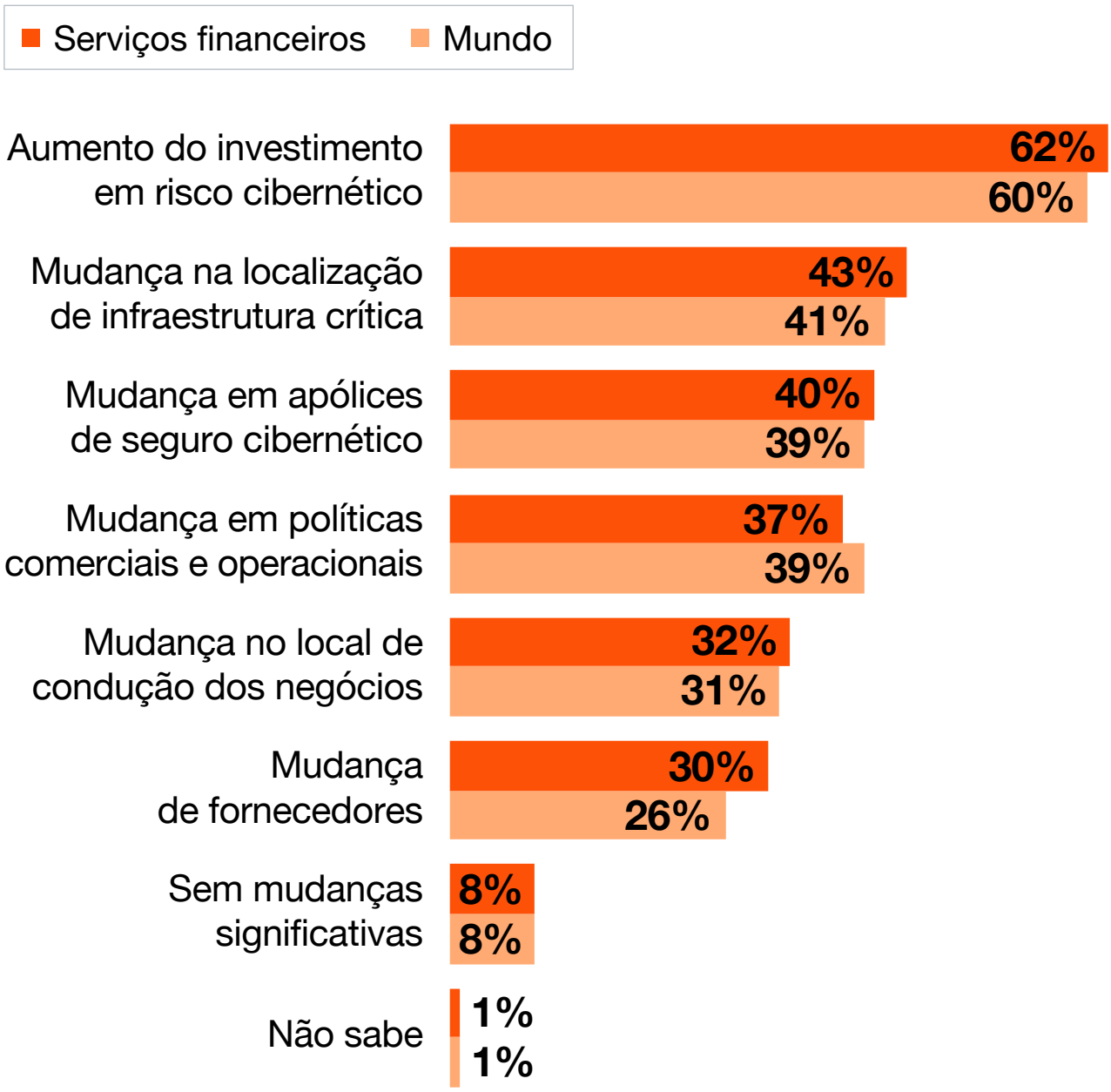
01

Cenário de riscos: a geopolítica e as vulnerabilidades cibernéticas

A geopolítica e as tecnologias disruptivas redefinem o cenário dos riscos cibernéticos. O setor de serviços financeiros acompanha a tendência global: 62% dos respondentes afirmam que vão ampliar os investimentos em cibersegurança nos próximos 12 meses – acima dos 60% registrados no resultado global.

O setor se diferencia ao priorizar a troca de fornecedores como resposta ao cenário geopolítico: 30% dos respondentes citam essa mudança, contra 26% no resultado global. Também registra maior adesão a mudanças nas apólices de seguro cibernético e na localização de infraestrutura crítica. Em contrapartida, a revisão de políticas comerciais e operacionais é citada por apenas 37% dos respondentes do setor, abaixo da média global – sinal de que a resposta estratégica ainda não é uniforme em todas as frentes.

Mudanças na estratégia cibernética nos próximos 12 meses

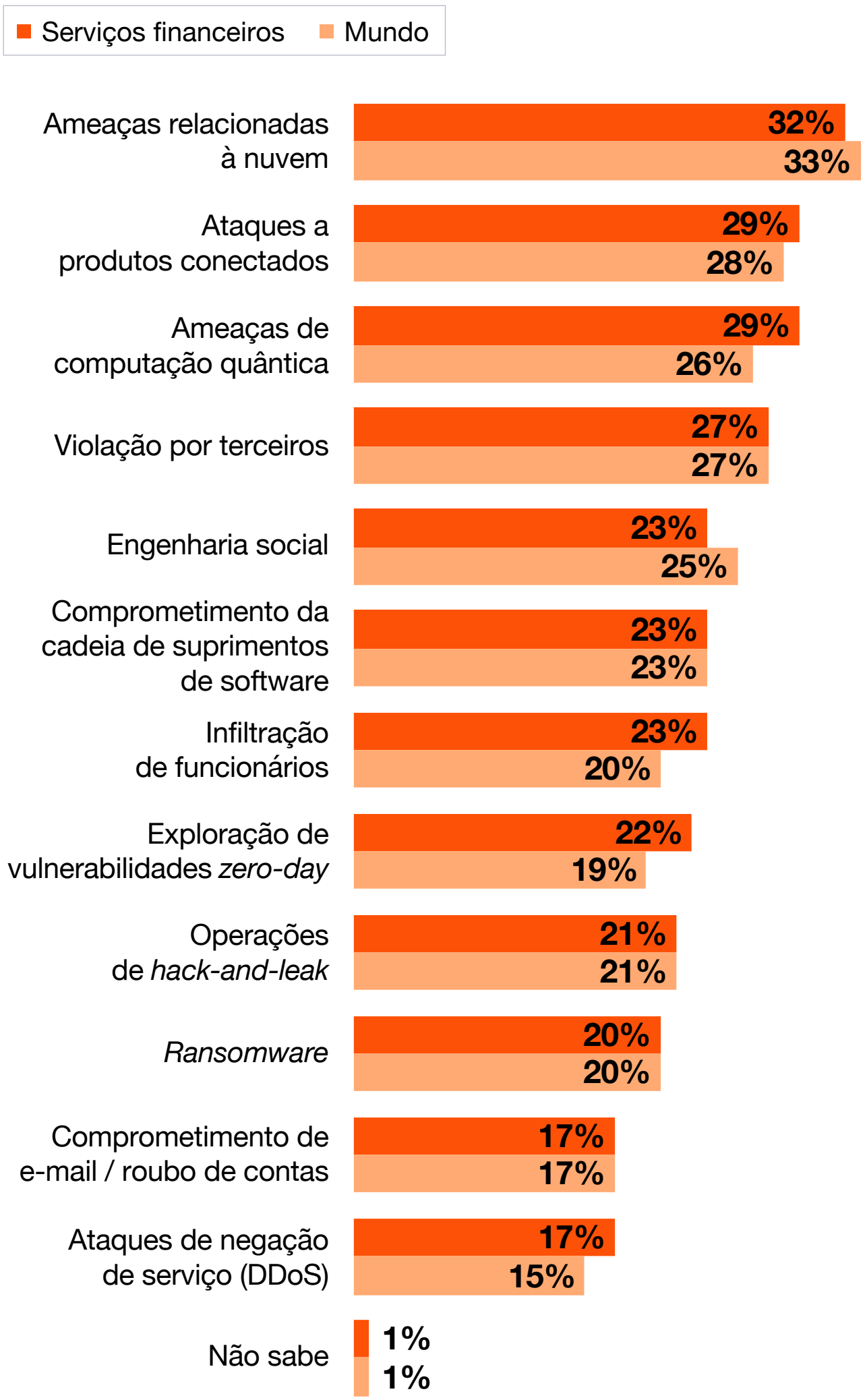


Ameaças iminentes, respostas insuficientes

As ameaças relacionadas à nuvem lideram as preocupações (32%), em linha com o resultado global (33%). O destaque do setor está na maior preocupação com ameaças de computação quântica: 29% dos respondentes de serviços financeiros citam essa categoria entre as três em que estão menos preparados, em comparação com 26% globalmente. Em compensação, o setor apresenta menor exposição percebida à engenharia social (23% vs. 25% no geral).

Nota: os percentuais refletem as três respostas principais selecionadas pelos respondentes.

Ameaças cibernéticas para as quais as empresas se sentem menos preparadas

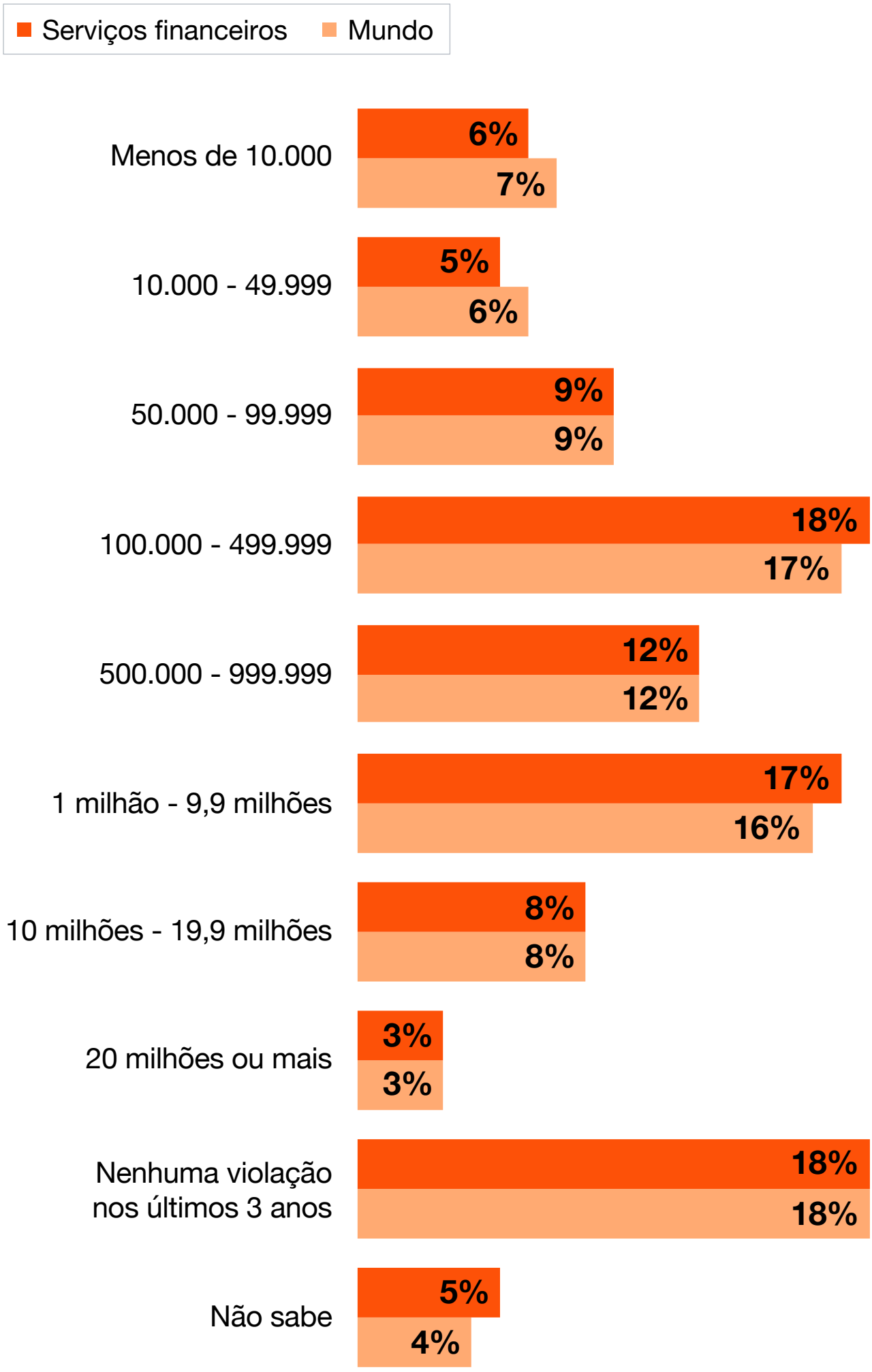


Custo da violação de dados mais grave nos últimos três anos

Quando ocorre uma violação no setor financeiro, o custo tende a ser elevado. Os dados mostram que 17% dos respondentes do setor relatam incidentes com custo entre US$ 1 milhão e US$ 9,9 milhões – pouco acima dos 16% registrados globalmente. Nas faixas abaixo de US$ 50 mil, o setor aparece menos representado do que a média (11%, em comparação com 13%), o que reforça um padrão claro: os incidentes são menos frequentes, mas mais caros.

Esse perfil reflete a densidade de dados sensíveis e a complexidade dos ecossistemas do setor como alvos prioritários. A proporção de empresas sem violações nos últimos três anos é idêntica à média global (18%) – e o índice ligeiramente maior de respondentes que não sabem estimar o custo (5% vs. 4%) sugere que a visibilidade sobre incidentes ainda é um ponto a desenvolver.

Custo estimado da violação de dados mais prejudicial (US$)

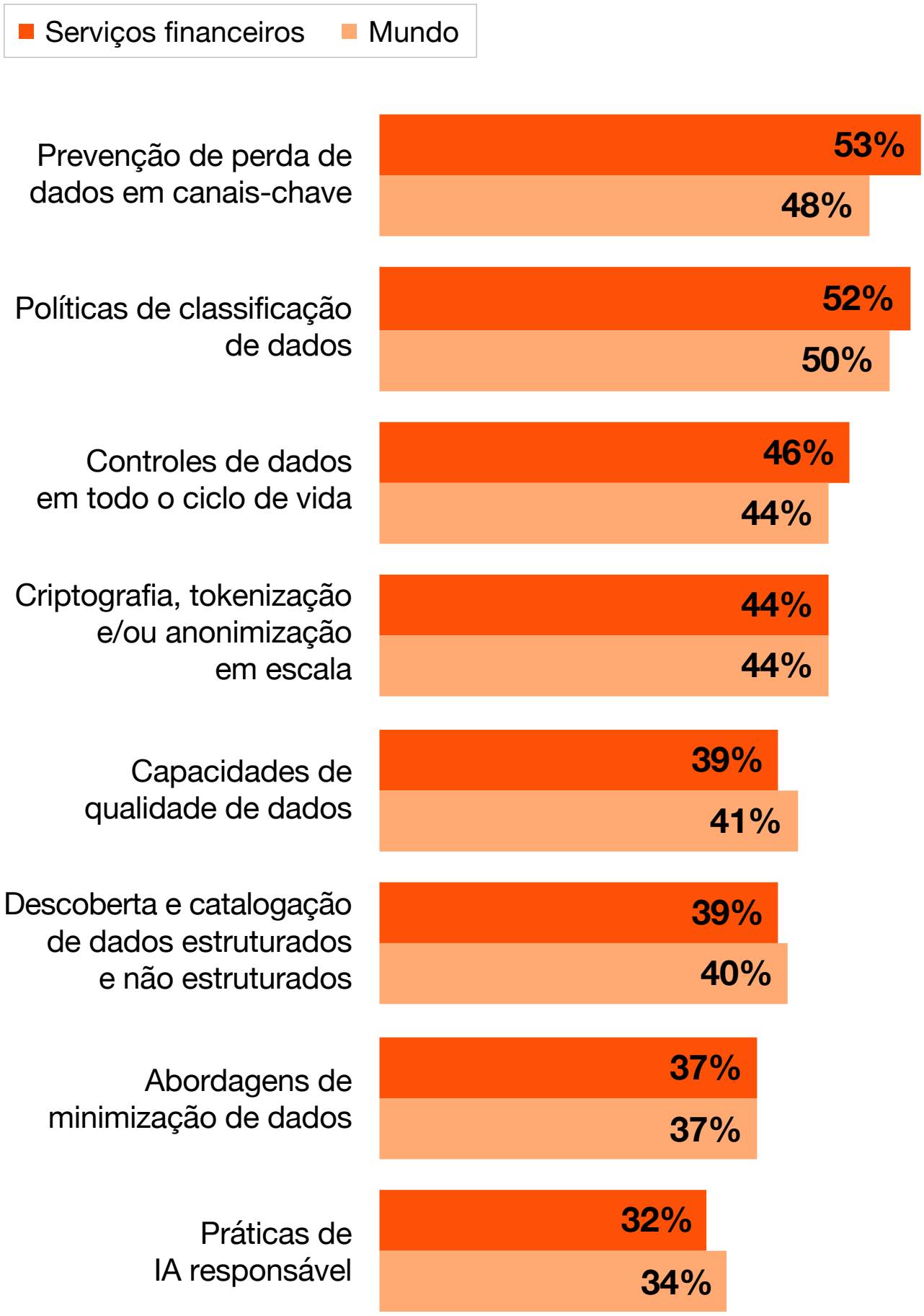


Proteger os dados que importam

O setor financeiro adota medidas de redução de risco de dados com maior intensidade do que a média global nas frentes mais operacionais. O destaque vai para a prevenção de perda de dados em canais-chave, citada por 53% dos respondentes do setor contra 48% globalmente – a maior diferença positiva do gráfico. Políticas de classificação de dados (52% vs. 50%) e controles ao longo do ciclo de vida (46% vs. 44%) também ficam acima da média.

Em contrapartida, o setor investe menos em práticas de IA responsável (32% vs. 34%) e capacidades de qualidade de dados (39% vs. 41%) – dimensões mais associadas à governança de longo prazo do que à proteção imediata. O padrão é consistente: o setor prioriza o que protege ativos críticos no curto prazo, mas ainda tem espaço para avançar nas práticas que sustentam uma gestão de dados mais madura e estruturada.

Medidas para reduzir o risco de dados



02

Operações e estratégia cibernética: investimento com propósito

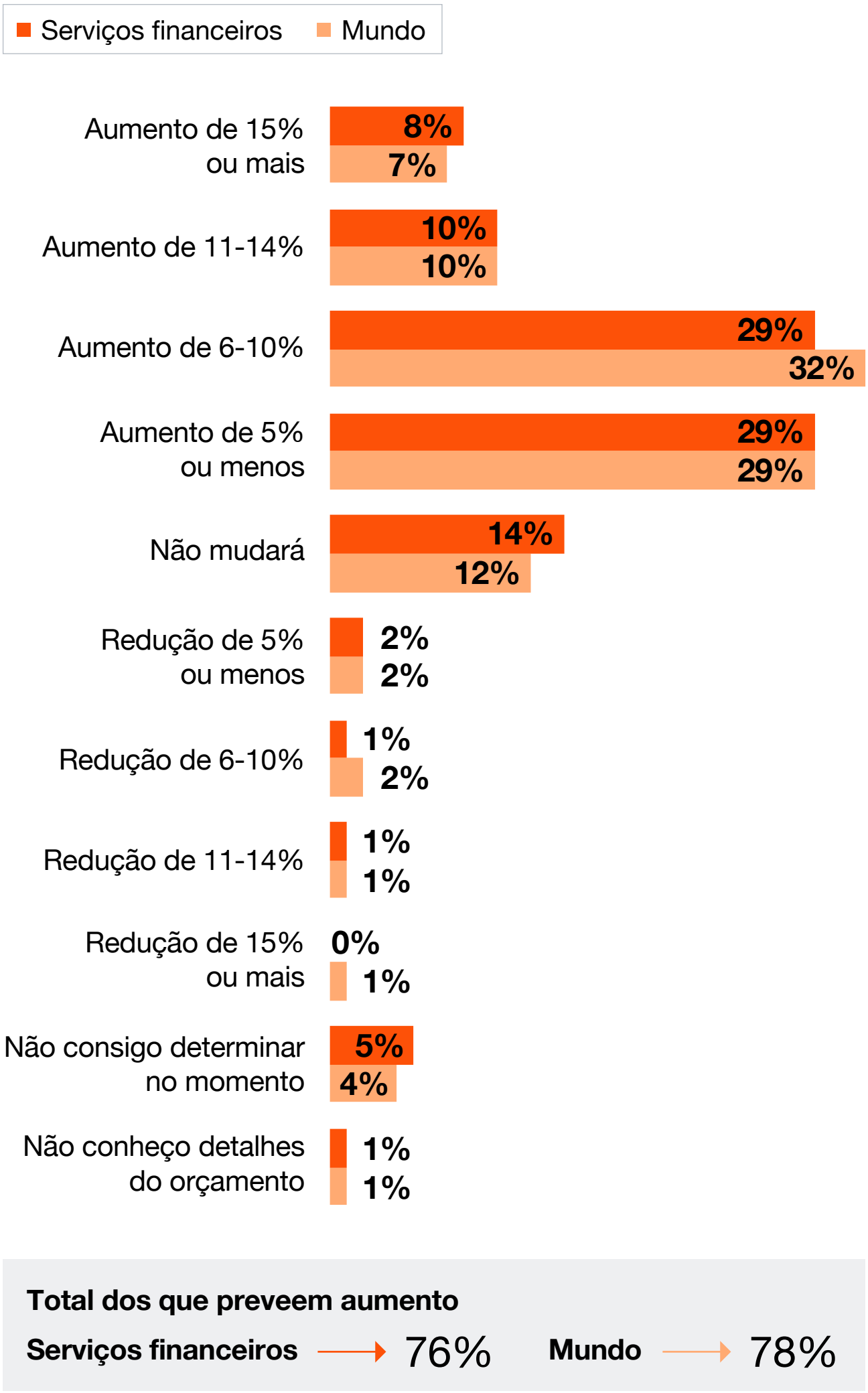
As instituições de serviços financeiros planejam aumentar os investimentos em cibersegurança em 2026, mas o ritmo de crescimento é ligeiramente mais conservador do que a média global. O *compliance* regulatório é o grande diferencial do setor como fator indutor de investimento.

Investimento em alta, mas com cautela

O setor financeiro prevê aumento nos orçamentos de cibersegurança em 2026 – 76% dos respondentes indicam algum crescimento, contra 78% no resultado global. A diferença está na intensidade: o setor concentra menos respostas na faixa de aumento de 6% a 10% (29% vs. 32% global) e registra maior proporção de orçamentos sem mudança (14% vs. 12%).

No extremo oposto, lidera discretamente nos aumentos mais expressivos, acima de 15% (8% vs. 7%). O perfil resultante é de um setor comprometido com o crescimento do investimento, mas que avança de forma mais gradual e seletiva do que a média – o que pode refletir tanto maturidade na alocação de recursos quanto a pressão por eficiência em um ambiente regulatório exigente.

Mudança no orçamento de cibersegurança em 2026



Total dos que preveem aumento

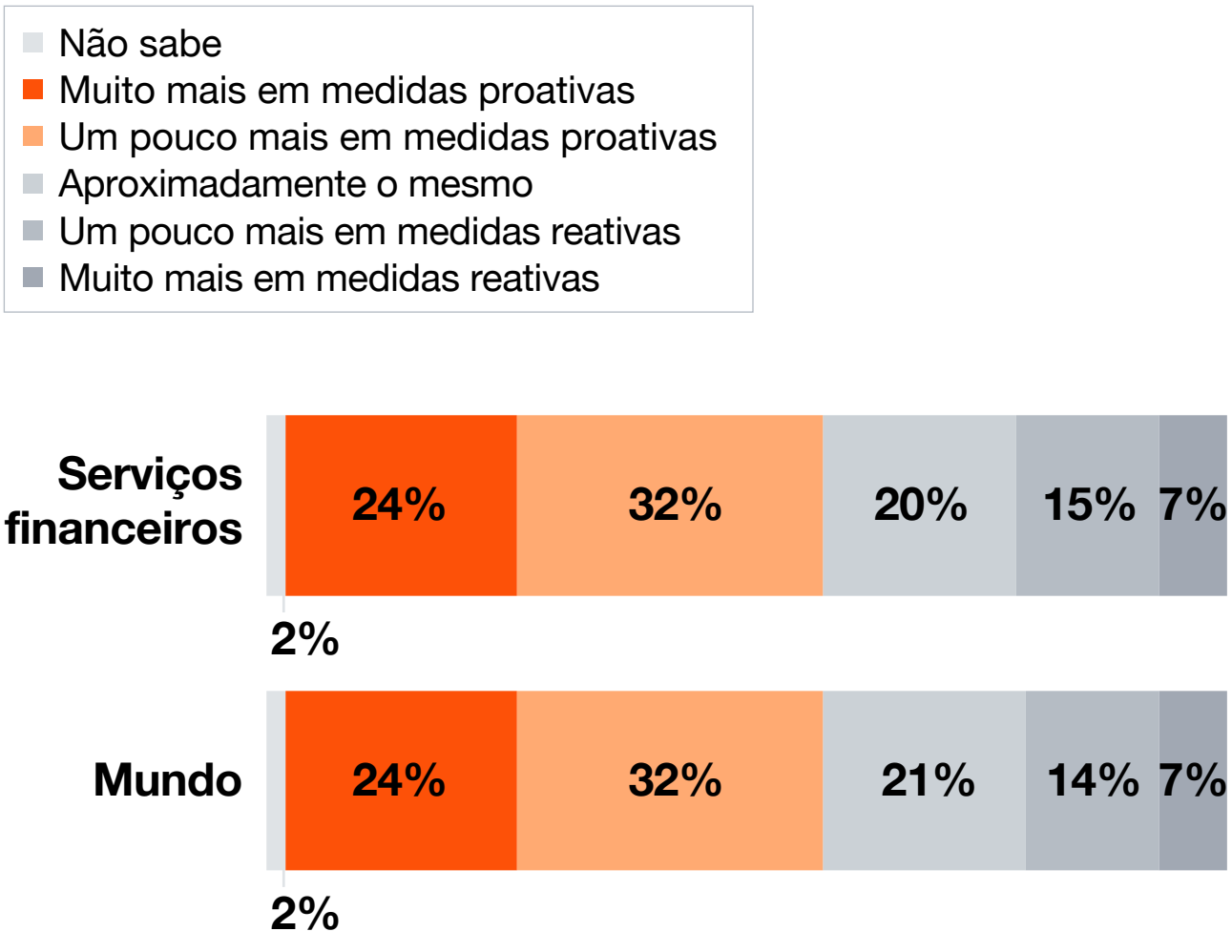
Serviços financeiros → 76% **Mundo** → 78%

A lógica do investimento

A distribuição dos investimentos em cibersegurança no setor financeiro praticamente espelha a média global. Em ambos os casos, 56% dos respondentes destinam mais recursos a medidas proativas do que a reativas, o que reflete uma orientação estratégica que prioriza a prevenção.

Com perfis tão próximos, o diferencial competitivo não estará na distribuição do orçamento, mas na qualidade e na precisão da execução – tanto nas iniciativas proativas quanto na velocidade de resposta aos incidentes.

Reação ou prevenção: distribuição de investimentos em cibersegurança



Prioridades que revelam estratégia

A inteligência artificial lidera as prioridades de investimento no setor financeiro com 36% – em linha com a média global e sinal de que a corrida por IA aplicada à cibersegurança é transversal a todos os setores. O diferencial mais expressivo está na segurança de rede e *zero trust*: 32% dos respondentes do setor apontam esse aspecto como prioridade, contra 28% globalmente – reflexo da necessidade de proteger ecossistemas altamente interconectados, com múltiplos parceiros, APIs e acessos remotos.

Já a segurança da tecnologia operacional (OT) recebe menos atenção do setor (7% vs. 10%), o que é esperado, dado o perfil menos industrial das operações financeiras. A segurança em nuvem aparece ligeiramente abaixo da média, mas permanece como segunda prioridade – o que é coerente com a rápida migração de infraestruturas críticas para ambientes em nuvem. O conjunto revela um setor que investe em áreas em que os riscos são mais concretos: dados, identidade, conectividade e inteligência sobre ameaças.

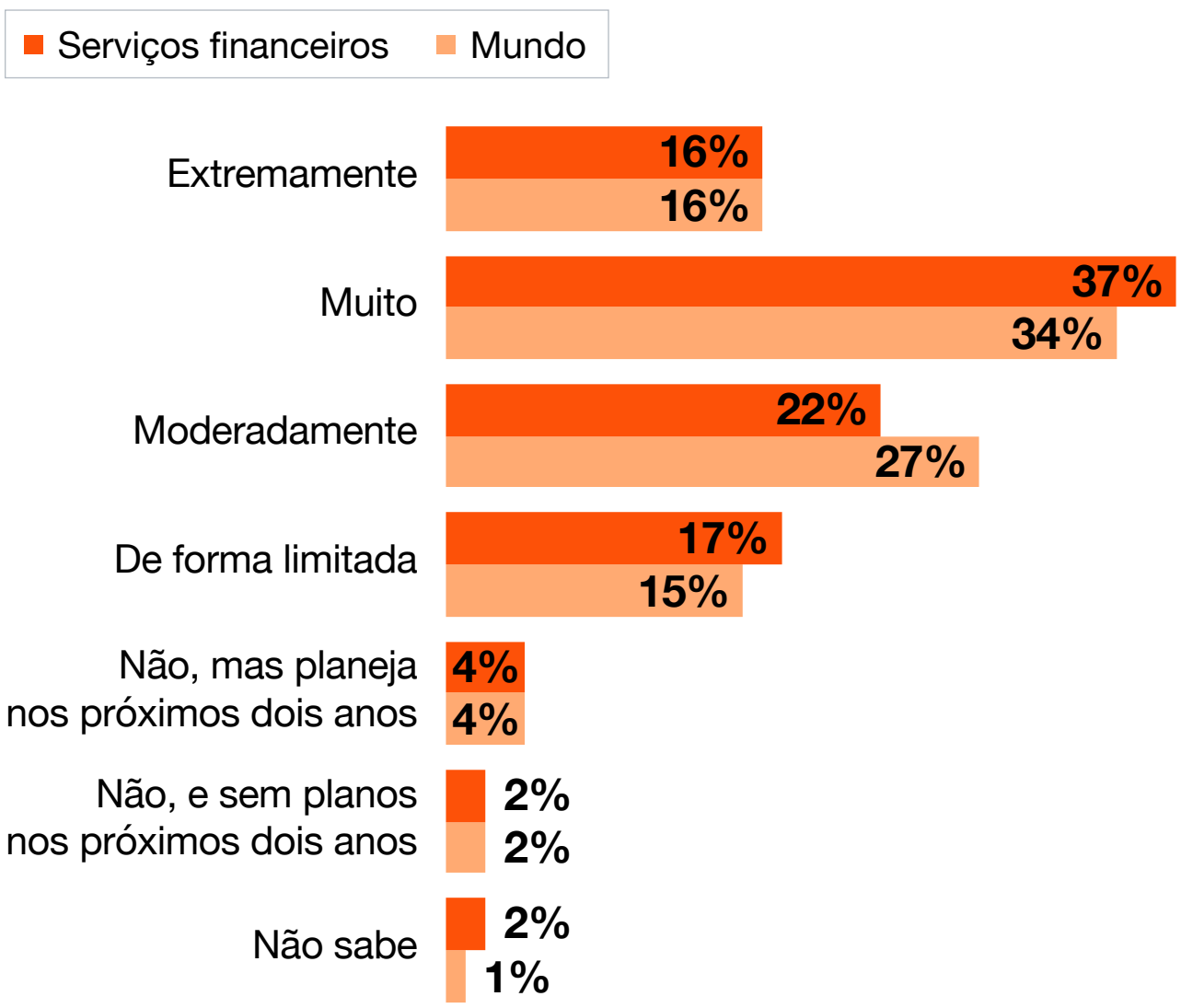
Investimentos priorizados no orçamento de cibersegurança

Medir para decidir

O setor mede o impacto financeiro dos riscos cibernéticos com maior profundidade do que a média global. A soma das respostas “extremamente” e “muito” chega a 53%, contra 50% globalmente. Já a medição “de forma moderada” é menos frequente no setor (22% vs. 27%), o que sugere menor tolerância à imprecisão na quantificação de riscos.

Esse padrão é consistente com um setor submetido a exigências regulatórias rigorosas, que historicamente demandam maior transparência e rastreabilidade na gestão de riscos. Medir bem o impacto financeiro dos incidentes é o primeiro passo para justificar investimentos, calibrar apólices de seguro e demonstrar resiliência a reguladores e investidores.

Medição do impacto financeiro de riscos cibernéticos



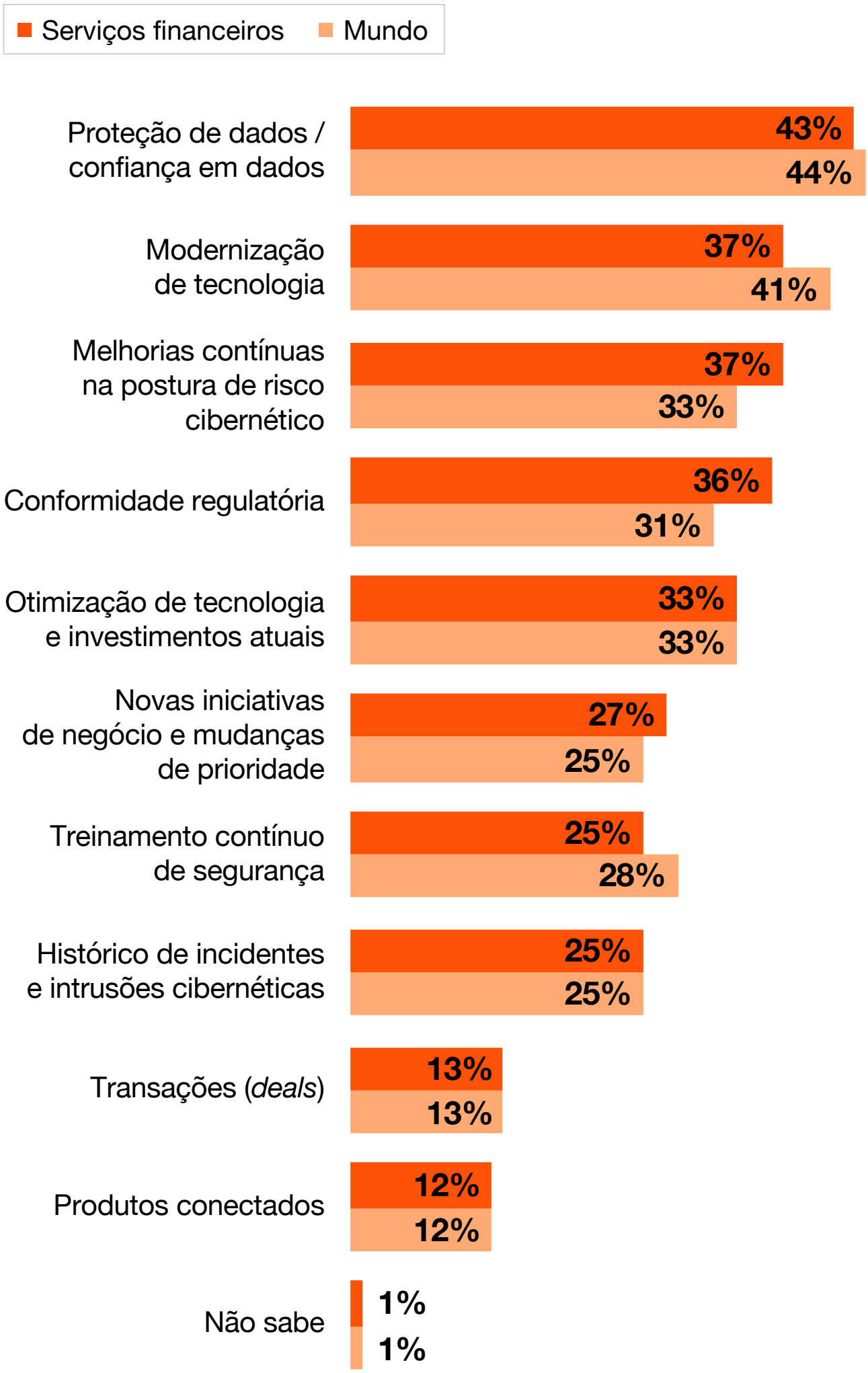
O que motiva os gastos com cibersegurança

A proteção de dados lidera os fatores que influenciam os gastos com cibersegurança no setor financeiro (43%), em linha com a média global (44%). O padrão mais relevante, porém, está nas diferenças abaixo da média: o setor registra menor peso da conformidade regulatória como motivação para gastos (31% vs. 36%).

O resultado é, aparentemente, paradoxal para um setor conhecido pela densidade regulatória. Uma leitura possível é que, para as instituições financeiras mais maduras, a conformidade já está incorporada à operação e deixa de ser percebida como um fator isolado de pressão orçamentária.

Isso vale para a modernização de tecnologia (37% vs. 41%) e melhorias contínuas na postura de risco (33% vs. 37%), em que o setor também fica abaixo da média global. Em conjunto, os dados sugerem um setor que gasta orientado pela proteção de dados e pela otimização do que já existe – mais do que por pressão externa ou reação a incidentes.

Fatores que influenciam os gastos com cibersegurança

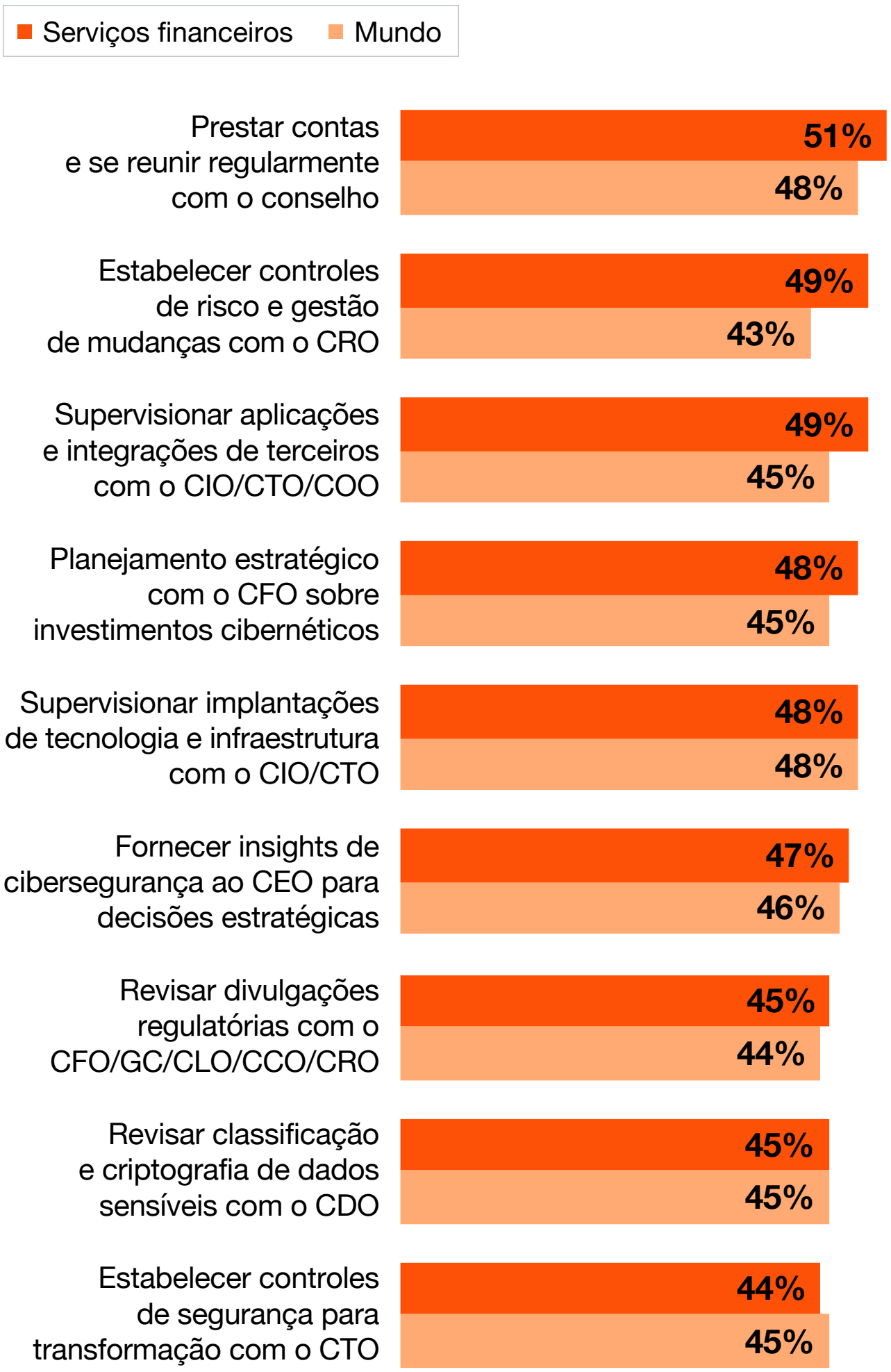


O CISO no centro das decisões

O CISO do setor financeiro colabora com a alta liderança de forma mais intensa do que a média global. Os diferenciais mais expressivos estão na atuação conjunta com o CRO para controles de risco e gestão de mudanças (49% vs. 43% global) e na supervisão de aplicações e integrações de terceiros com CIO, CTO e COO (49% vs. 45%), um reflexo direto da exposição do setor a riscos de cadeia de suprimentos e da densidade regulatória que exige alinhamento contínuo entre cibersegurança e gestão de risco.

A prestação de informações e as reuniões regulares com o conselho também ficam acima da média (51% vs. 48%), um sinal de que a pauta cibernética já ganhou espaço no mais alto nível de governança. O planejamento estratégico de investimentos com o CFO (48% vs. 45%) reforça a percepção de que a cibersegurança deixou de ser custo operacional e passou a ser decisão de alocação estratégica de capital.

Áreas em que o CISO trabalha com a liderança executiva



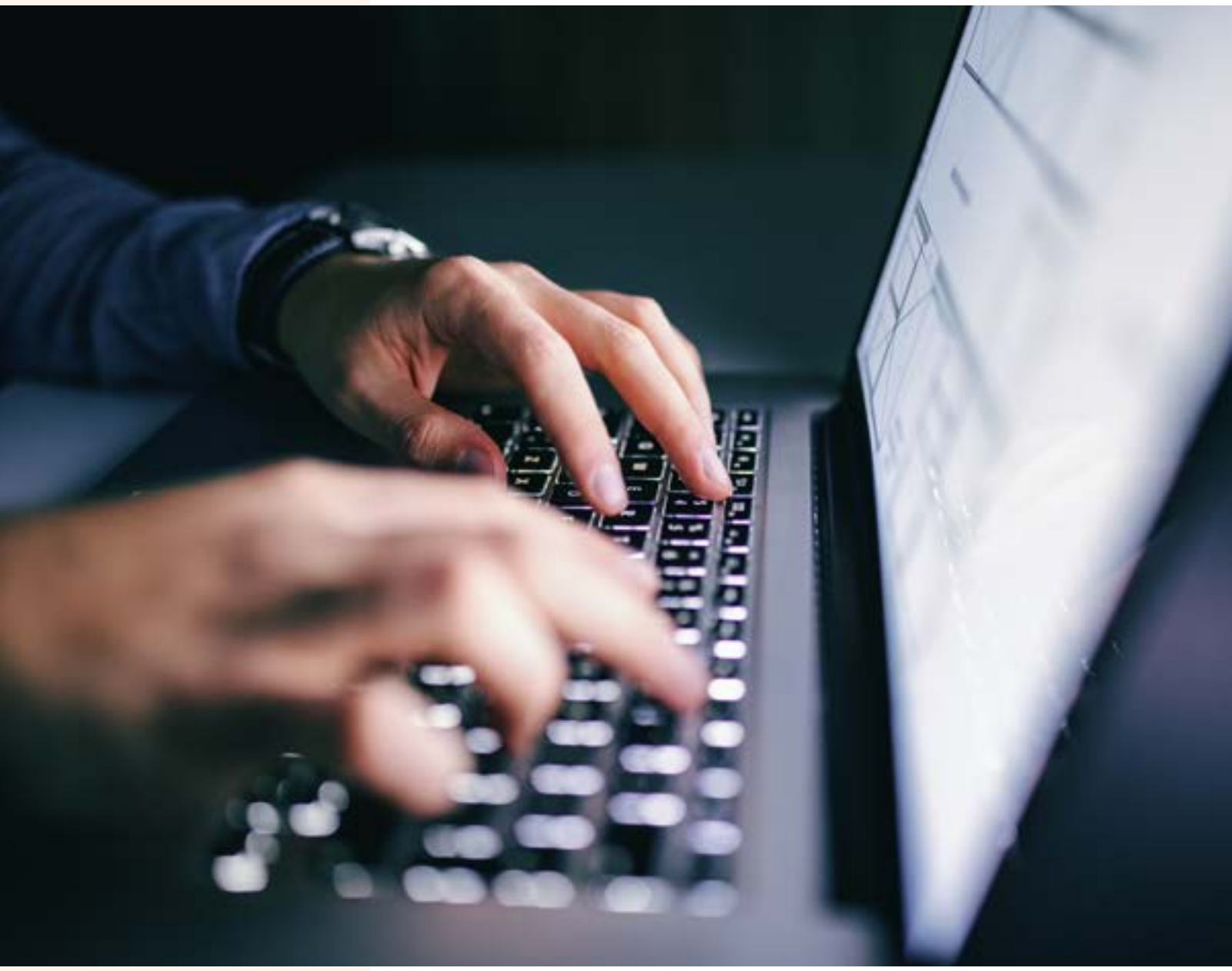
Nota: Todos os respondentes, excluindo CISOs. Apenas respostas “Extremamente”

Esse posicionamento é corroborado pelos dados de frequência: os CISOs do setor interagem semanalmente com o CIO/CTO em maior proporção do que a média global (51% vs. 48%), e o CRO é consultado semanal ou mensalmente por 68% dos CISOs do setor, ante 61% globalmente, o que reforça a integração entre segurança cibernética e gestão de riscos institucionais.

A liderança executiva como um todo mantém contato mensal com o CISO em 41% dos casos, um ponto percentual acima do global, com zero registros de “nunca” em ambos os recortes. O ponto de atenção está no engajamento com o CEO: apenas 42% dos CISOs do setor o consultam semanal ou mensalmente, contra 49% na média global. Apesar dos avanços, a agenda cibernética parece ainda não estar totalmente conectada à liderança máxima.

03

IA em cibersegurança: da promessa à prioridade



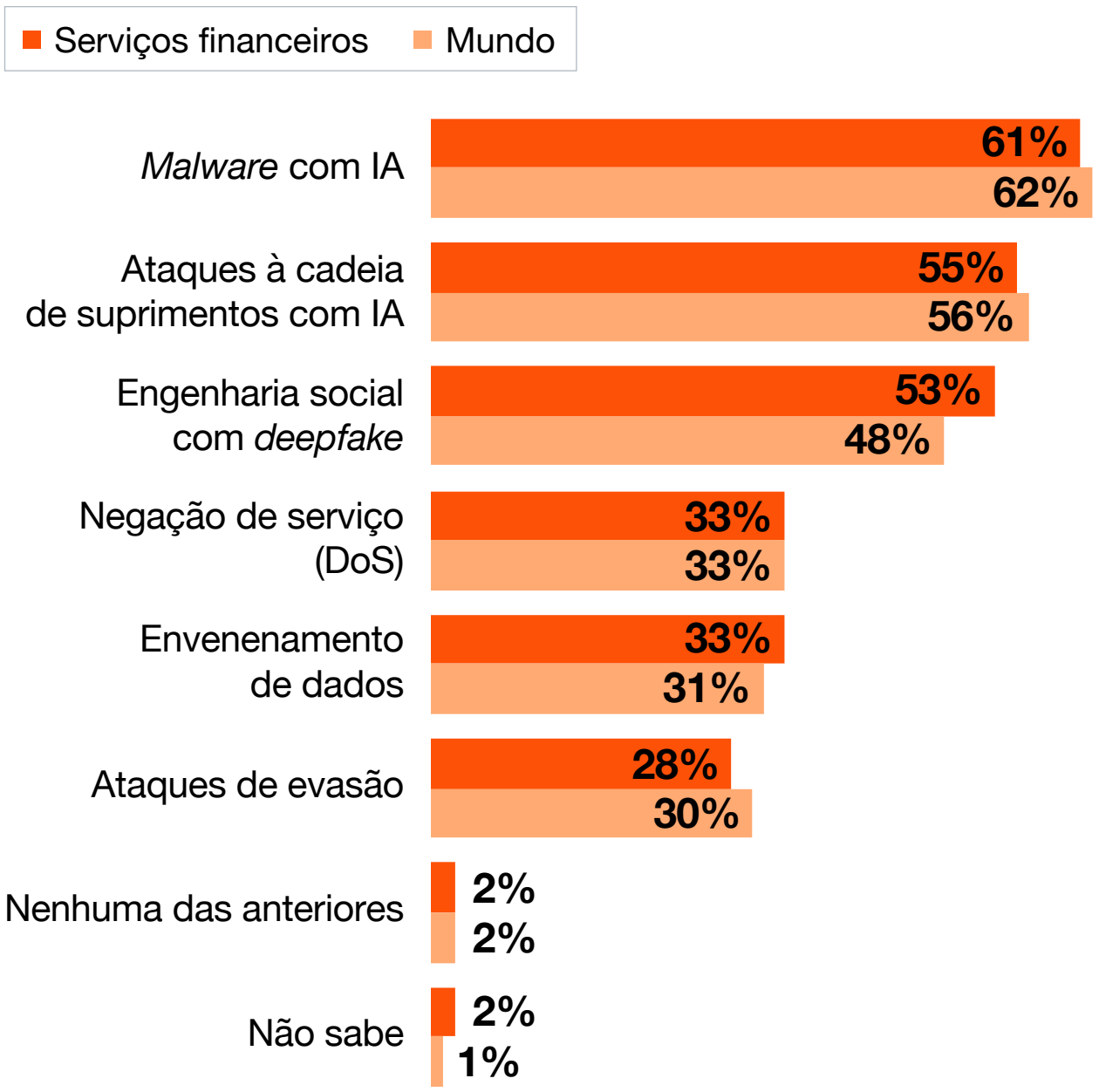
O setor de serviços financeiros acompanha de perto a tendência global de adotar IA como prioridade estratégica em cibersegurança. Há, no entanto, diferenças importantes no perfil de preocupações e nos casos de uso priorizados.

IA como vetor de ataque

O *malware* com IA lidera as preocupações do setor financeiro (61%), em linha com a média global (62%). O diferencial mais expressivo está na engenharia social com *deepfake*: 53% dos respondentes a apontam como cenário preocupante, contra 48% globalmente – uma diferença que reflete a vulnerabilidade específica de um setor em que transações de alto valor, autorizações e negociações dependem de confiança e identidade verificada.

O envenenamento de dados também preocupa mais o setor, o que faz sentido em um ambiente no qual modelos de crédito, detecção de fraudes e precificação de risco são alimentados por grandes volumes de dados. Em contrapartida, o setor se mostra ligeiramente menos preocupado com ataques à cadeia de suprimentos com IA e com ataques de evasão. O conjunto revela atenção aos vetores de IA que exploram diretamente os ativos mais sensíveis: identidade, confiança e integridade dos dados.

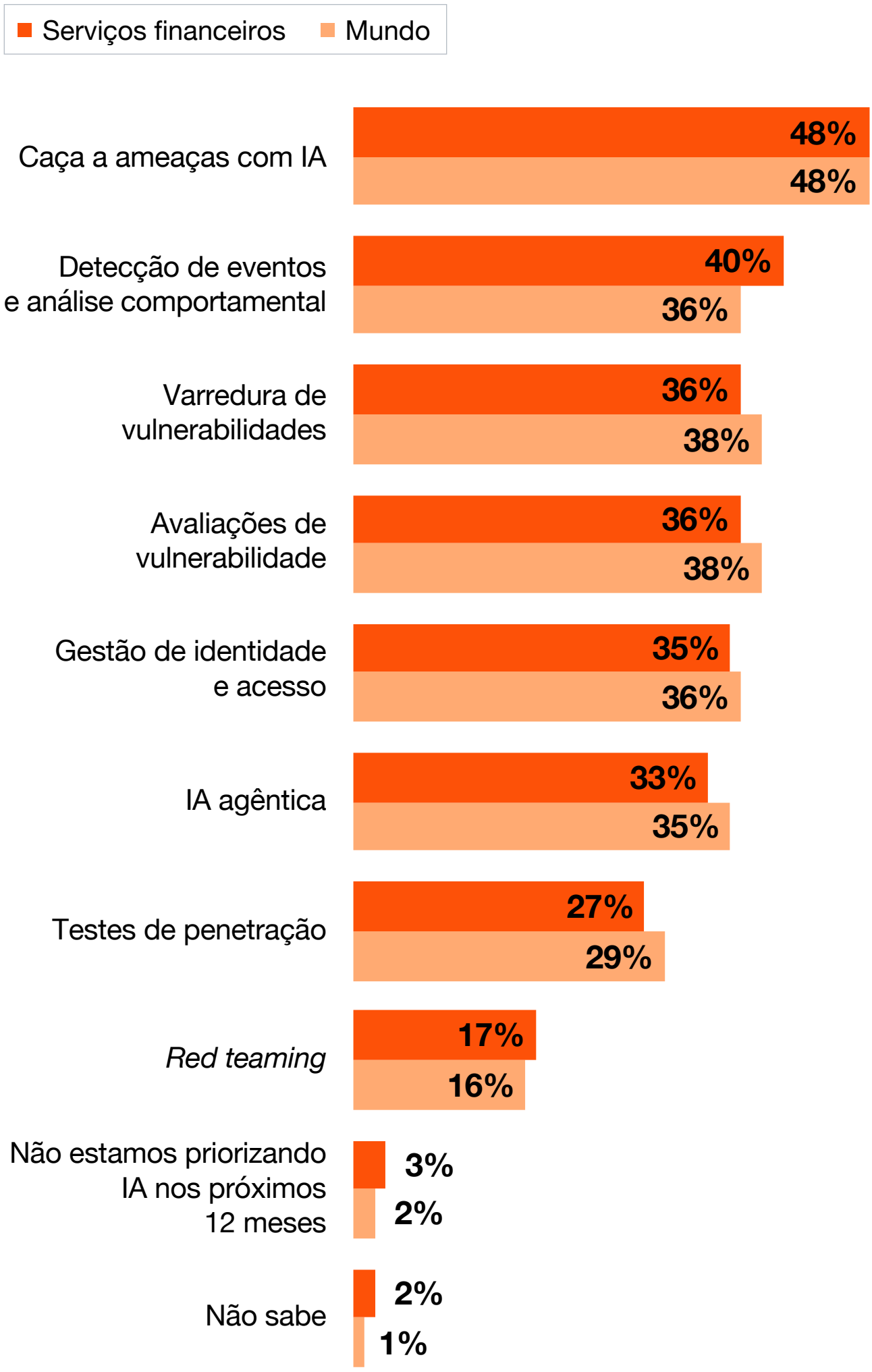
Cenários mais preocupantes de ataque com IA



IA também como escudo

A caça a ameaças com IA lidera as capacidades priorizadas no setor financeiro (48%), em linha exata com a média global – sinal de que a detecção proativa é uma aposta universal. Em quase todas as demais categorias, porém, o setor fica abaixo do global, como varredura e avaliações de vulnerabilidades (36% vs. 38% em ambas) e IA agêntica (33% vs. 35%). A principal exceção é a detecção de eventos e análise comportamental (40% vs. 35%), capacidade especialmente relevante para detectar fraudes, movimentações suspeitas e ameaças internas.

Capacidades de segurança com IA priorizadas



Autonomia com critério

Na aplicação de IA agêntica à cibersegurança, o setor financeiro se diferencia da média global em dois sentidos opostos. O destaque positivo está em defesa e operações cibernéticas: 40% dos respondentes do setor priorizam essa área, contra 38% globalmente – o maior diferencial favorável e coerente com um setor que opera sob ameaça constante e pressão regulatória por resposta rápida a incidentes.

Os *gaps* negativos mais expressivos estão exatamente nas áreas em que a IA agêntica teria maior potencial transformador: segurança em nuvem (34% vs. 39%) e proteção de dados (33% vs. 39%). Esse padrão sugere que o setor ainda está calibrando onde confiar na IA para agir com autonomia – priorizando o que é urgente e operacional, mas avançando com mais cautela nas áreas que tocam diretamente dados sensíveis e infraestrutura crítica.

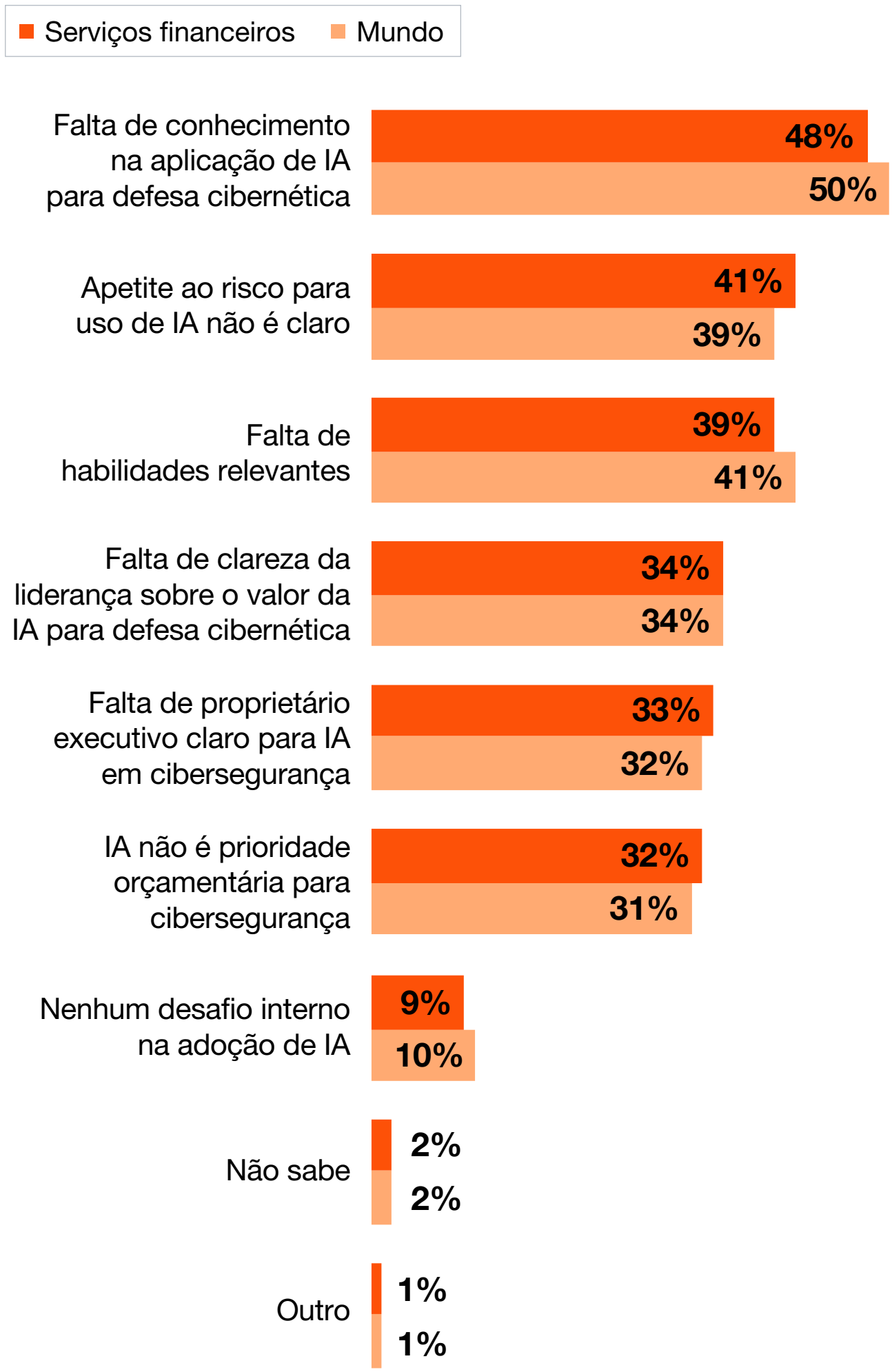
Áreas de priorização de IA agêntica

Obstáculo à adoção da IA não é só técnico

A falta de conhecimento na aplicação de IA para defesa cibernética lidera os desafios internos no setor financeiro (48%), mas fica dois pontos percentuais abaixo da média global, possivelmente porque o setor já investiu mais em capacitação. O diferencial mais relevante está no apetite ao risco: 41% dos respondentes do setor apontam que o nível de tolerância ao risco para uso de IA não está claro, contra 39% globalmente.

Em um ambiente no qual reguladores monitoram de perto o uso de algoritmos em decisões críticas, a ausência de uma política interna clara sobre o quanto se pode delegar à IA trava a adoção, mais do que a falta de habilidades técnicas. O setor também registra maior dificuldade em definir um proprietário executivo para IA em cibersegurança (33% vs. 32%) e em garantir que IA seja prioridade orçamentária (32% vs. 31%).

Desafios internos na adoção de IA para defesa cibernética



04

Preparação para a computação quântica: como encarar novas ameaças

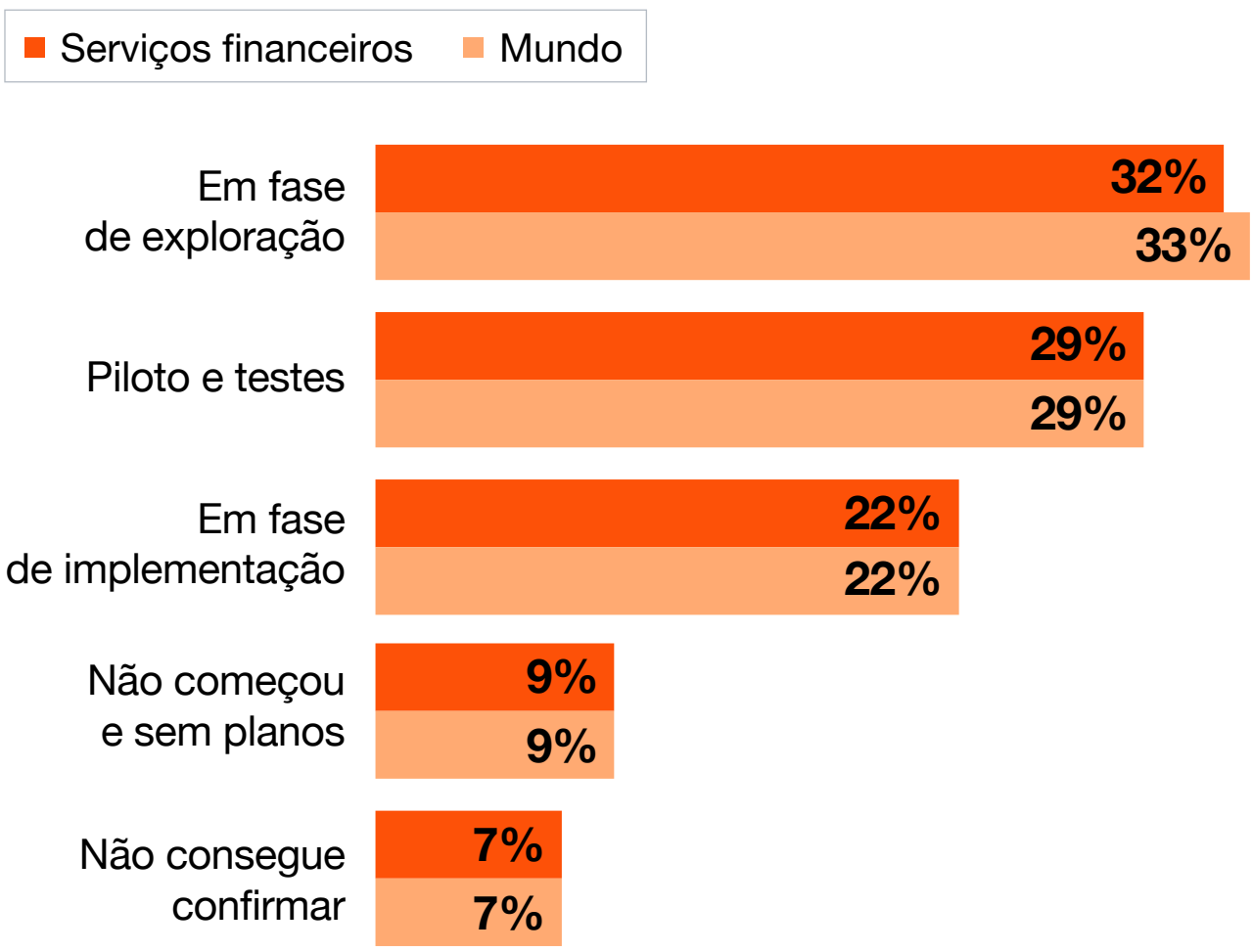
A computação quântica representa uma das ameaças emergentes mais relevantes para o setor financeiro, dado o uso intensivo de criptografia para proteger transações e dados. O setor apresenta um nível de preparação alinhado à média global, com progressos semelhantes na implementação de medidas resistentes a ataques quânticos.

A corrida quântica já começou

O setor financeiro caminha em ritmo praticamente idêntico ao da média global na jornada rumo à segurança quântica. As diferenças entre os dois grupos são nulas ou marginais em todas as categorias. A maioria das organizações ainda está nas fases iniciais: 61% em exploração e ou piloto e testes. Apenas 22% já estão em fase de implementação – percentual idêntico ao global.

O dado mais relevante é que apenas 9% afirmam não ter começado e não ter planos, o que indica que a ameaça quântica já entrou na agenda da maioria. Algoritmos de criptografia que protegem transações, dados de clientes e comunicações internas são exatamente os alvos mais vulneráveis à computação quântica no setor.

Maturidade em segurança quântica



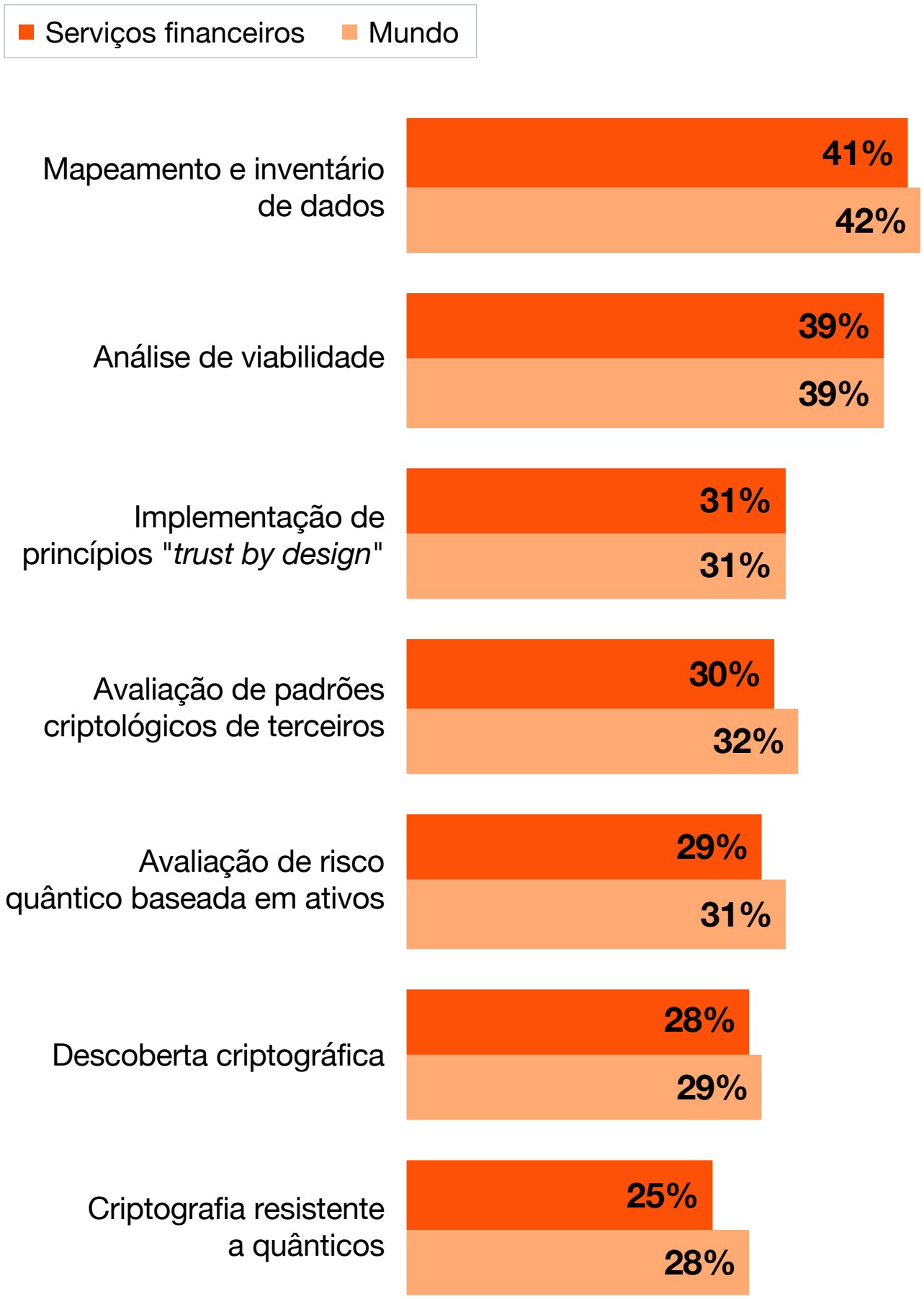
Preparar o terreno antes de blindar a casa

Entre as organizações que já implementaram medidas de segurança quântica, o setor financeiro segue de perto a média global, mas com um padrão revelador. As iniciativas mais avançadas ficam abaixo da média global: criptografia resistente a quânticos (25% vs. 28%), avaliação de risco quântico com base em ativos (29% vs. 31%) e avaliação de padrões criptológicos de terceiros (30% vs. 32%).

O setor lidera em análise de viabilidade (39%, em linha com o global) e está muito próximo do topo em mapeamento e inventário de dados (41% vs. 42%). O padrão indica investimento nas etapas preparatórias – mapear, catalogar e analisar – mas ainda sem converter esse diagnóstico em ação criptográfica concreta.

Para instituições que dependem de criptografia para proteger transações, contratos e dados de clientes, a lacuna entre o mapeamento do problema e a implementação de soluções resistentes a ataques quânticos é o próximo passo crítico a vencer.

Empresas com medidas de segurança quântica implementadas



O conhecimento é o gargalo

O setor financeiro enfrenta desafios semelhantes aos do mercado global na jornada para a criptografia pós-quântica, mas em menor intensidade – o que pode refletir maior maturidade ou maior investimento acumulado na área. Os dados mais favoráveis estão na priorização de iniciativas de curto prazo e nas lacunas de conhecimento e recursos de computação quântica, sugerindo que já começa a haver um equilíbrio melhor entre o olhar de longo prazo e as demandas imediatas.

A única categoria em que o setor enfrenta um desafio maior do que o global é a falta de direção estratégica da liderança. Embora a diferença seja pequena, ela pode indicar que a agenda quântica ainda não tem patrocínio executivo claro em parte das instituições. No conjunto, os dados reforçam a leitura do gráfico anterior: o setor sabe que precisa agir, tem diagnóstico razoável do problema, mas ainda enfrenta lacunas de expertise técnica (35%) e de conhecimento especializado (33%) que travam a transição do planejamento para a execução.

Desafios internos para a criptografia pós-quântica

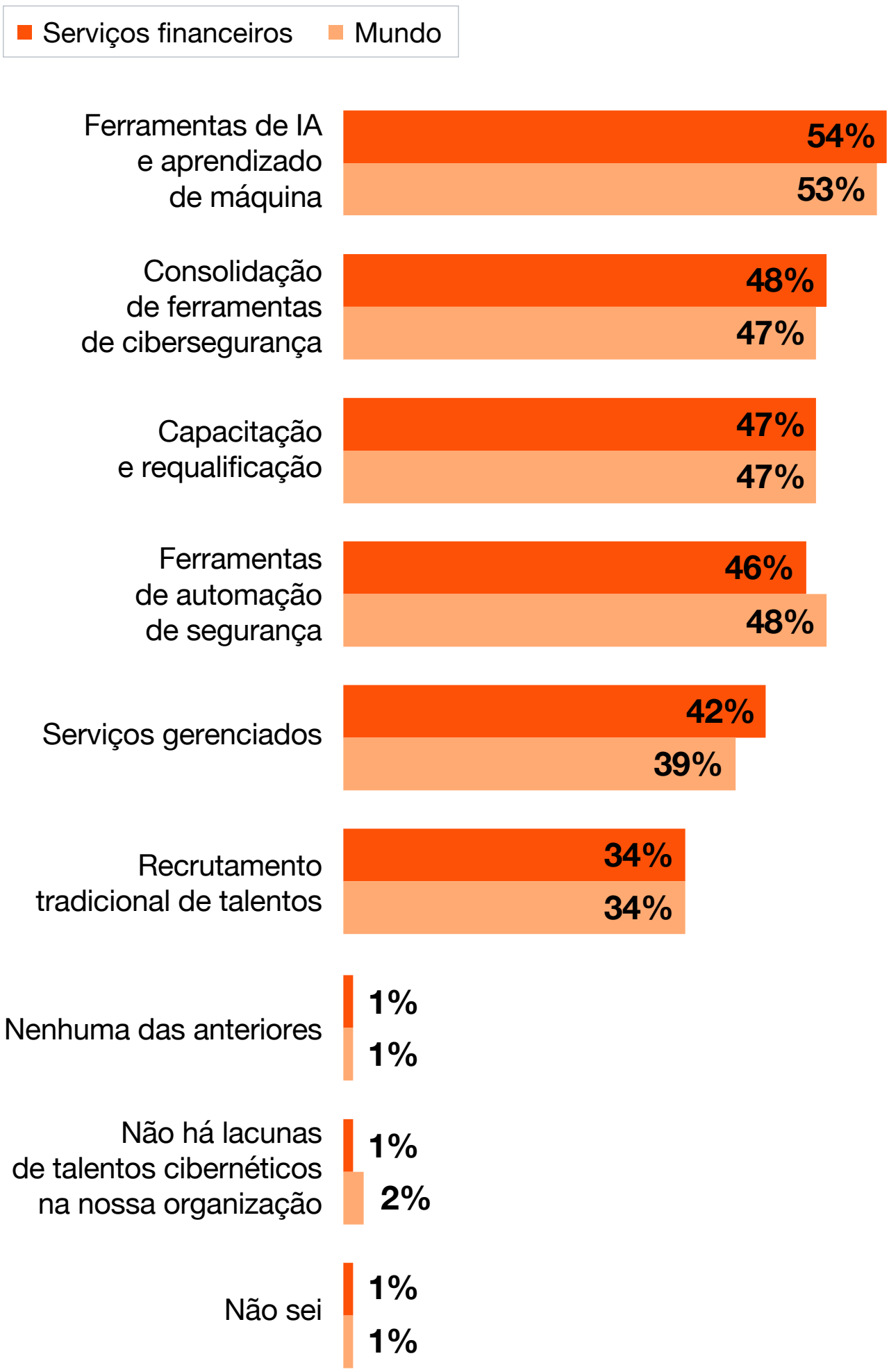
05

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

O setor financeiro aposta no uso de IA e aprendizado de máquina para suprir lacunas de talentos em cibersegurança e recorre mais a serviços gerenciados do que a média (42% vs. 39%) – sinal de que contratar especialistas no mercado é mais rápido do que formá-los internamente.

A consolidação de ferramentas (48%) e a capacitação interna (47%) completam uma estratégia que combina tecnologia, parceiros externos e desenvolvimento de quem já está na casa. A menor ênfase na automação de segurança (46% vs. 48%) sugere cautela quanto à substituição do julgamento humano em contextos de alto risco regulatório.

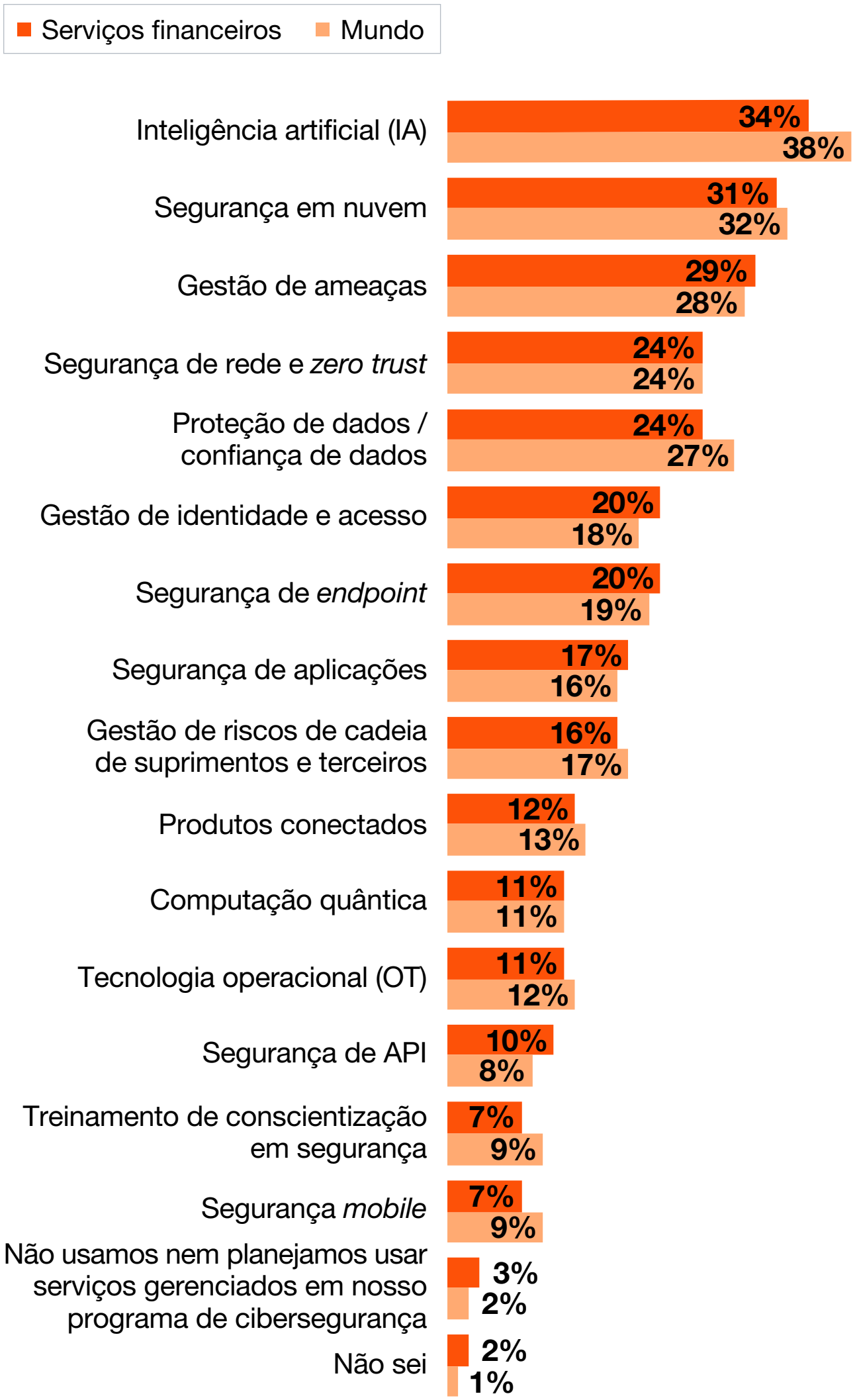
Prioridades para abordar lacunas de talentos em cibersegurança



Serviços gerenciados na gestão de ameaças

Na escolha das áreas para aplicação de serviços gerenciados, o setor financeiro prioriza menos a IA (34% vs. 38% global) e a proteção de dados (24% vs. 27%). Em compensação, a gestão de ameaças recebe atenção ligeiramente maior no setor (29% vs. 28%). O resultado aponta que o setor busca serviços gerenciados principalmente para funções de monitoramento e resposta, enquanto IA e proteção de dados tendem a ser internalizadas.

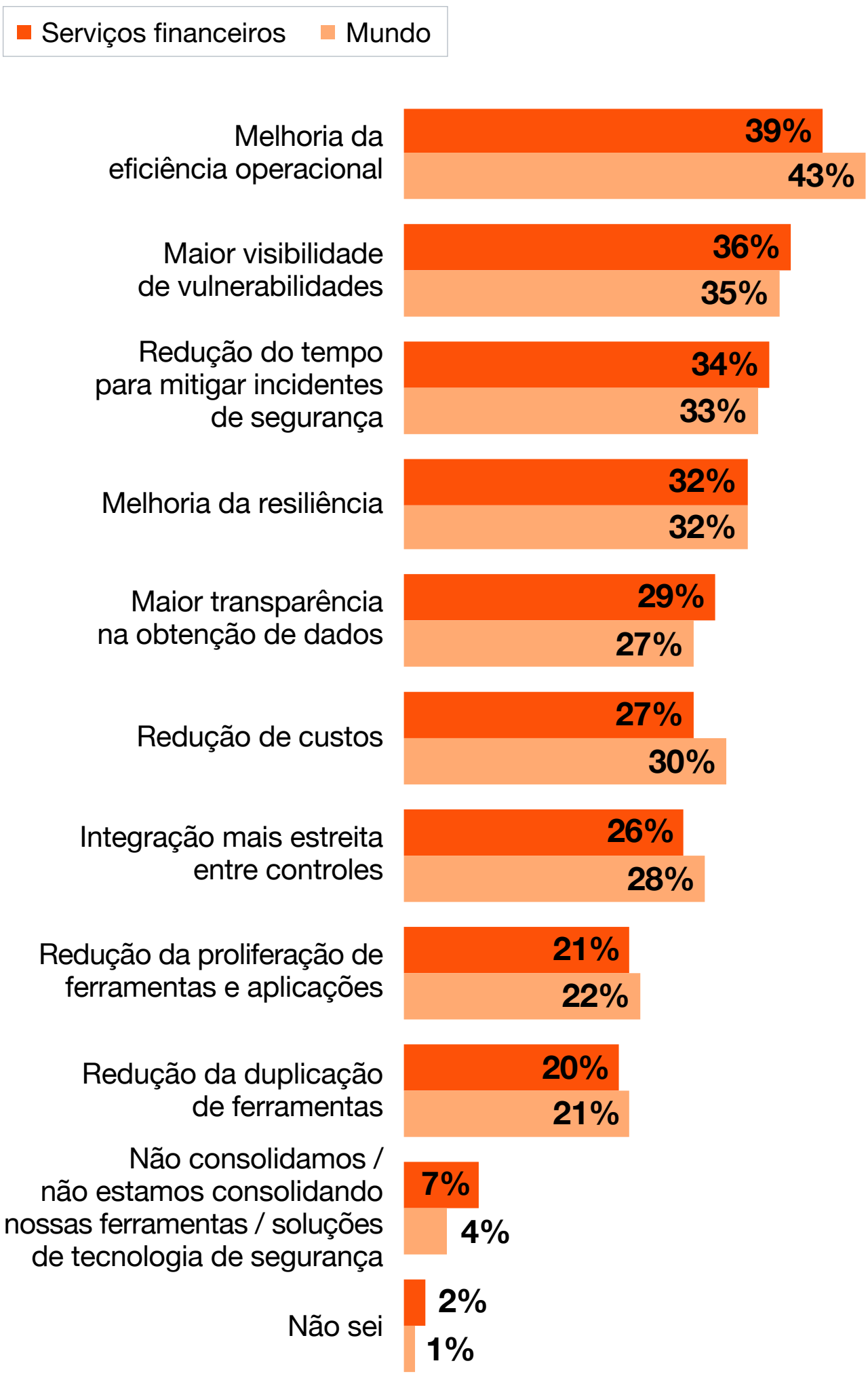
Áreas de cibersegurança priorizadas para usar serviços gerenciados



Consolidação de ferramentas beneficia governança

Quanto aos benefícios da consolidação de ferramentas, o setor financeiro apresenta resultado ligeiramente inferior ao global em eficiência operacional (39% vs. 43%), mas acima da média em visão das vulnerabilidades (36% vs. 35%), transparência nas fontes de dados (29% vs. 27%) e redução no tempo de resposta a incidentes (34% vs. 33%). Isso indica que a consolidação gera benefícios mais orientados à governança e ao controle no setor do que a ganhos de produtividade.

Principais benefícios da consolidação de ferramentas de segurança

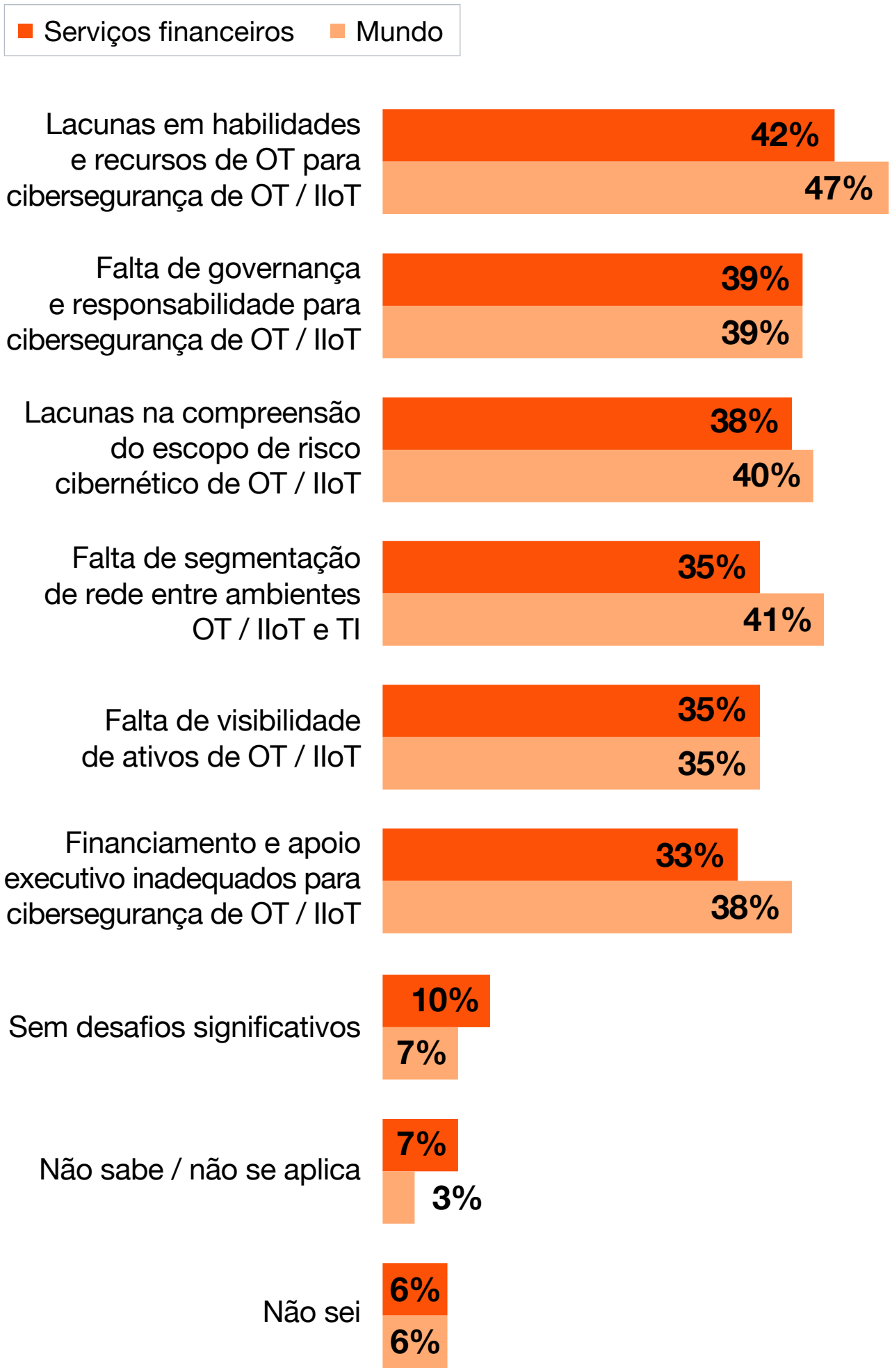


Um risco que ainda não é prioridade

Os desafios de segurança em OT/IIoT no setor financeiro têm intensidade inferior à média global – o que reflete, em parte, uma presença menos significativa dessas tecnologias em relação a setores industriais. O *gap* mais expressivo está nas lacunas de habilidades e recursos (42% vs. 47%), na falta de segmentação de rede entre os ambientes OT/IIoT e TI (35% vs. 41%) e no financiamento e no apoio executivo inadequados (33% vs. 38%).

A única categoria em que o setor supera o global é a ausência de desafios significativos (10% vs. 7%). O resultado indica que uma parcela relevante das instituições simplesmente não enxerga OT/IIoT como vetor de risco relevante para sua operação. Esse dado merece atenção: com a expansão de dispositivos conectados em agências, ATMs, centros de dados e infraestrutura de pagamentos, a superfície de ataque via OT/IIoT cresce silenciosamente – e a baixa percepção de risco pode ser o maior risco de todos.

Principais desafios em segurança de OT / IIoT



06

Da incerteza à ação: o que líderes podem fazer agora

A **Pesquisa Global Digital Trust Insights 2026** mostra que empresas mais avançadas estão alinhando a segurança cibernética à estratégia de negócios e priorizando a prontidão para responder a ataques. Muitas organizações já adotam abordagens mais estruturadas de gestão de riscos, fortalecendo a governança, alinhando-se a *frameworks* de mercado e integrando controles e avaliações de risco em toda a empresa.

No entanto, para se preparar para o futuro, é preciso ir além do que se faz hoje: enfrentar incertezas, tomar decisões bem fundamentadas e adotar estratégias mais ágeis.

DO

CISO/CSO

Os líderes de segurança devem traduzir riscos cibernéticos complexos em riscos de negócio e promover a colaboração entre executivos. Isso fortalece governança, resiliência e conformidade regulatória. Também é essencial incorporar a segurança desde o design dos projetos e usar dados para orientar investimentos em cibersegurança.

DO

CTO/CIO

Seu papel é fechar lacunas de competências em segurança e trabalhar com a liderança de cibersegurança para integrar controles de risco e governança nas iniciativas tecnológicas. A partir de agora, será essencial incorporar segurança desde o início na adoção de tecnologias emergentes, como IA e computação quântica.

DO

CRO

Você deve continuar identificando riscos corporativos e emergentes e garantindo que os *frameworks* de gestão de risco estejam atualizados. Também será necessário integrar riscos associados à IA, à computação quântica e a outros fatores geopolíticos em uma estratégia de gestão de riscos mais adaptável.

DO

CFO

Cabe a você definir orçamentos adequados para fortalecer a cibersegurança e apoiar iniciativas estratégicas de tecnologia. O foco deve ser alinhar investimentos às prioridades da empresa e preparar recursos financeiros para riscos emergentes, adotando modelos de financiamento orientados por ROI.

DO

CEO

Seu papel é garantir que a cibersegurança seja tratada como uma prioridade estratégica em toda a organização, integrando-a à gestão de riscos e fortalecendo a colaboração entre o conselho e a liderança executiva para enfrentar desafios futuros.

Contatos

Lindomar Schmoller
Sócio e líder da indústria
de Serviços Financeiros
lindomar.schmoller@pwc.com

Eduardo Batista
Sócio e líder de Cibersegurança
e Privacidade
eduardo.batista@pwc.com

Siga a PwC nas redes sociais