www.pwc.com.br

Pesquisa *Global Digital Trust Insights 2023*

Nova era da cibersegurança

A segurança digital se tornou um campo dinâmico, que deve se ajustar rapidamente para acompanhar a inovação e a disrupção nos negócios. É preciso unir forças para enfrentar com resiliência desafios cada vez mais complexos

PwC Brasil

pwc

Conteúdo

Um ambiente de negócios novo e arrojado

Impulsionados por eventos imprevistos, os líderes executivos e suas empresas saíram de suas zonas de conforto nos últimos anos. Passaram a trabalhar remotamente, na nuvem e com cadeias de abastecimento quase totalmente digitais. A cada nova empreitada, tiveram que lidar com novos riscos cibernéticos.

A boa notícia é que os executivos de Segurança da Informação (CISOs) e as equipes cibernéticas estão se mostrando à altura do desafio. Nesse esforço, eles recebem apoio dos demais executivos, os quais começaram a reconhecer que seus movimentos inovadores aumentaram a exposição de suas organizações ao risco cibernético.

Esse cenário e outros pontos relevantes são explorados na **Pesquisa Global Digital Trust Insights 2023**, que retrata as perspectivas de mais de 3.500 líderes de negócios e TI em todo o mundo.

Os dados mostram que a segurança cibernética se tornou um campo dinâmico, ajustando-se rapidamente para acompanhar a inovação e a disrupção nos negócios.

Também apresentamos um guia sobre cibersegurança e privacidade, avaliando os cenários esperados para 2023 e como os executivos podem trabalhar juntos para encarar o futuro.

“A pesquisa capturou de forma clara quais são as prioridades cibernéticas dos executivos, suas maiores preocupações e quem é responsável pelo tema nas áreas de negócios. O relatório destaca os pontos fortes e os desafios das organizações, além da visão de líderes renomados de cibersegurança no Brasil. Oferecemos orientações claras, que ajudarão as empresas a se preparar melhor para o futuro cibernético.”

Eduardo Batista
Sócio e líder de Cibersegurança e Privacidade da PwC Brasil

Boas notícias: houve progresso na segurança cibernética

Mais de 70% dos executivos de negócios e tecnologia entrevistados para a pesquisa **Global Digital Trust Insights 2023** no Brasil e no mundo apontam melhorias na segurança cibernética de suas empresas em 2022 – graças a investimentos cumulativos e à colaboração da alta administração.

A segurança cibernética evoluiu em muitas frentes

Ações realizadas pela equipe de cibersegurança nos últimos 12 meses

P: Indique se a equipe de segurança cibernética da sua organização realizou ou não o seguinte nos últimos 12 meses.

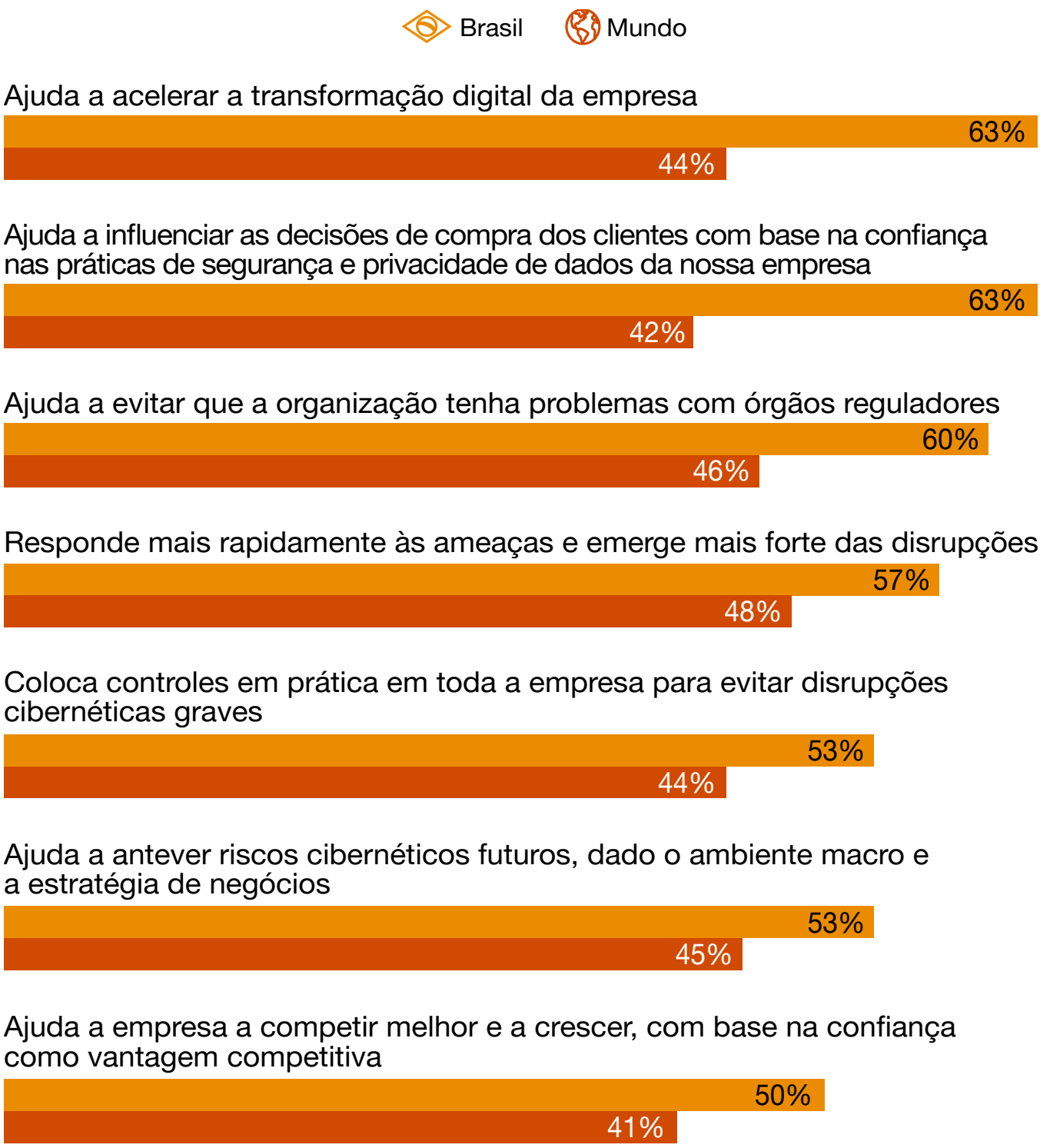
Base: 3.522 (Mundo) | 109 (Brasil)

Entre os participantes que apontam melhorias em todas as áreas:

- Os CEOs são três vezes mais propensos do que os outros a dizer que seus CISOs dão contribuições excelentes para melhorar os resultados, como responder mais rápido do que no passado a ameaças e antecipar riscos cibernéticos. Quase 8% disseram que o CISO está fazendo isso em todas as áreas.
- Os diretores de risco (CROs) e operações (COOs) são duas vezes mais propensos a classificar como excepcionais seus programas cibernéticos e de privacidade. Mais de 5% disseram que seus programas são excepcionais em relação a todos os quesitos perguntados.
- Os diretores de marketing (CMOs), dados (CDOs) e privacidade (CPOs) são 2,5 vezes mais propensos a concordar que seus programas cibernéticos e de privacidade são valiosos para a organização. Seu maior benefício é a capacidade de reforçar a confiança do consumidor.

CEO e conselheiros dão notas altas para CISOs e suas equipes

P: Como o CISO está se saindo em relação aos seguintes resultados e às expectativas quanto à segurança cibernética da sua organização em 2022-2023? (% dos que acreditam que o CISO supera muito as expectativas)



Os alvos continuam expostos

A digitização torna a segurança uma preocupação de todos. O futuro promete sistemas mais conectados e uma quantidade muito maior de dados, além de organizações criminosas mais sofisticadas. Diante de um cenário de riscos cibernéticos crescentes, os líderes terão muito trabalho pela frente – e num ambiente econômico instável.

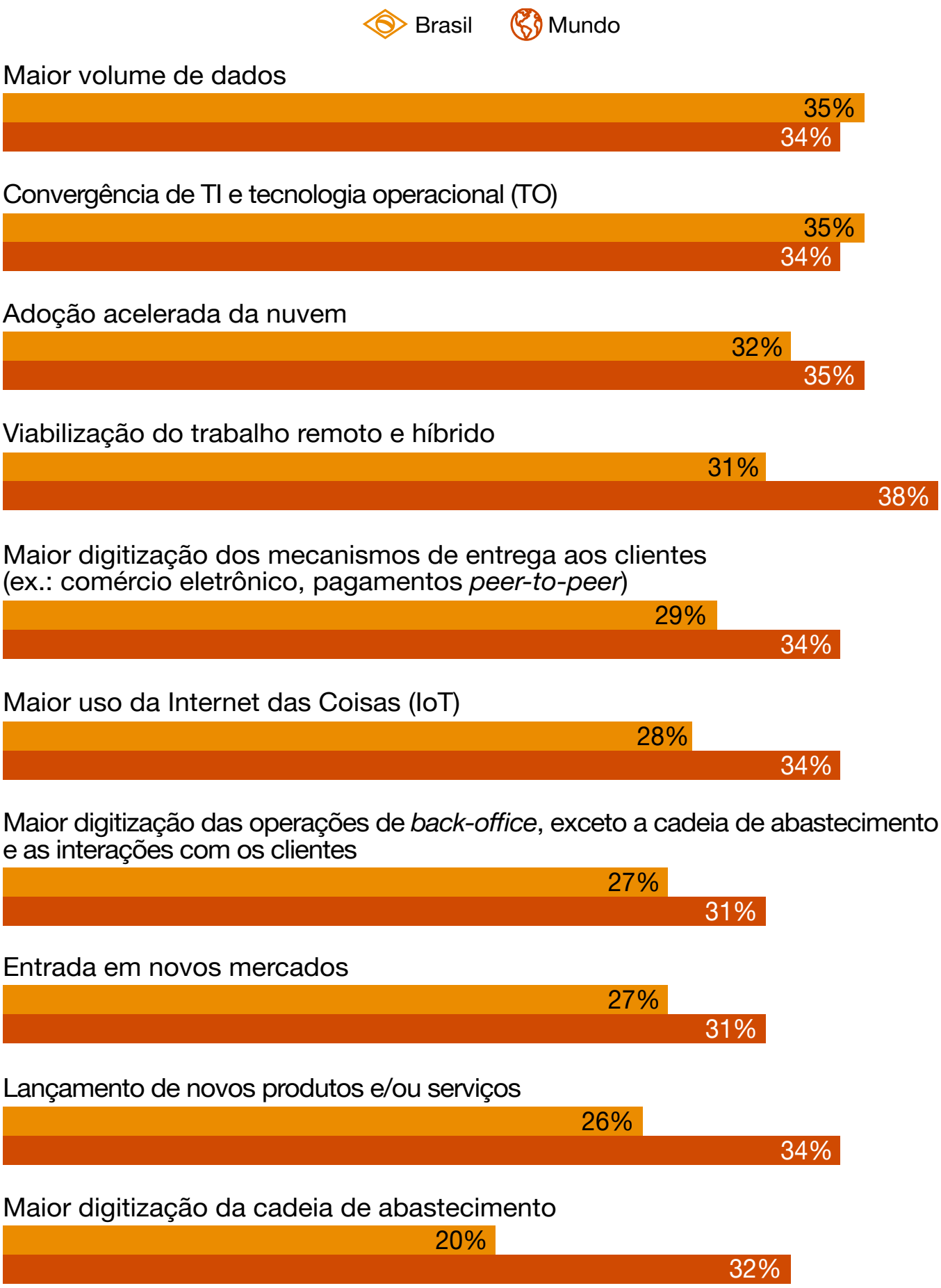
Menos de 40% dos entrevistados no Brasil e no mundo dizem ter mitigado totalmente os riscos a que ficaram expostos durante a pandemia de covid-19. De modo geral, no entanto, os participantes globais afirmam ter alcançado melhores resultados de mitigação.

No Brasil, o maior volume de dados e a convergência entre TI e tecnologia operacional receberam mais atenção (35% de citações cada). No mundo, são apontados o trabalho remoto (38%) e a migração para a nuvem (35%).

Em âmbito global, organizações maiores (mais de US$ 1 bilhão em receitas) e aquelas sediadas na América do Norte são muito mais propensas a dizer que mitigaram esses riscos. Menos de 3% dos entrevistados no mundo dizem que conseguiram mitigar totalmente todos os dez riscos.

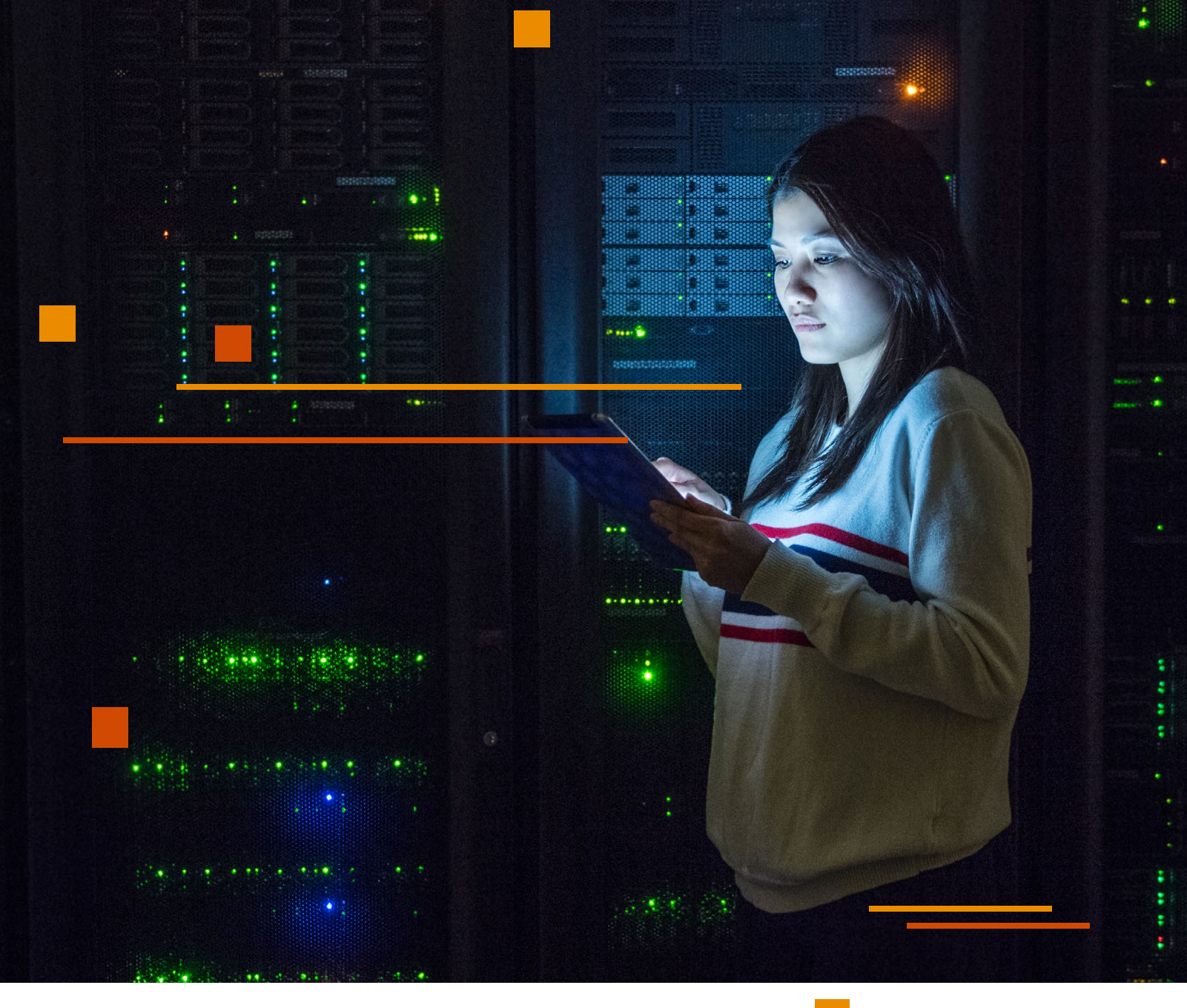
Menos de 40% mitigaram totalmente os riscos cibernéticos a que ficaram expostos

P: Em uma escala de 1 a 10, até que ponto sua organização mitigou os riscos de cibersegurança nos últimos 12 meses? (% dos que mitigaram o risco totalmente)



Globalmente, os CISOs veem a necessidade de avançar ainda mais em relação às cinco competências cibernéticas descritas no *framework* de Segurança Cibernética do National Institute of Security and Technology (NIST) – órgão do governo americano. Apenas 3% responderam que estavam "otimizando" todas as cinco.

Organizações maiores, com receitas superiores a US$ 1 bilhão, são mais propensas a dizer que estão otimizando a identidade (21%); aquelas que tiveram aumentos de receita e esperam que eles continuem são mais propensas a otimizar todas as cinco capacidades.



Visão da liderança

Alexandre Domingos
CISO da Dasa

Algo inesperado pode aparecer como uma nova demanda ou ameaça sem precedentes. É essencial ter uma liderança madura, preparada para disrupções, com possíveis grandes repercussões midiáticas. Evoluímos na detecção de possíveis problemas, nos planos de resiliência, na capacidade de antecipar um incidente e manter uma estrutura que, em meio a uma adversidade, conseguirá se recuperar o mais rápido possível, diminuindo a indisponibilidade.

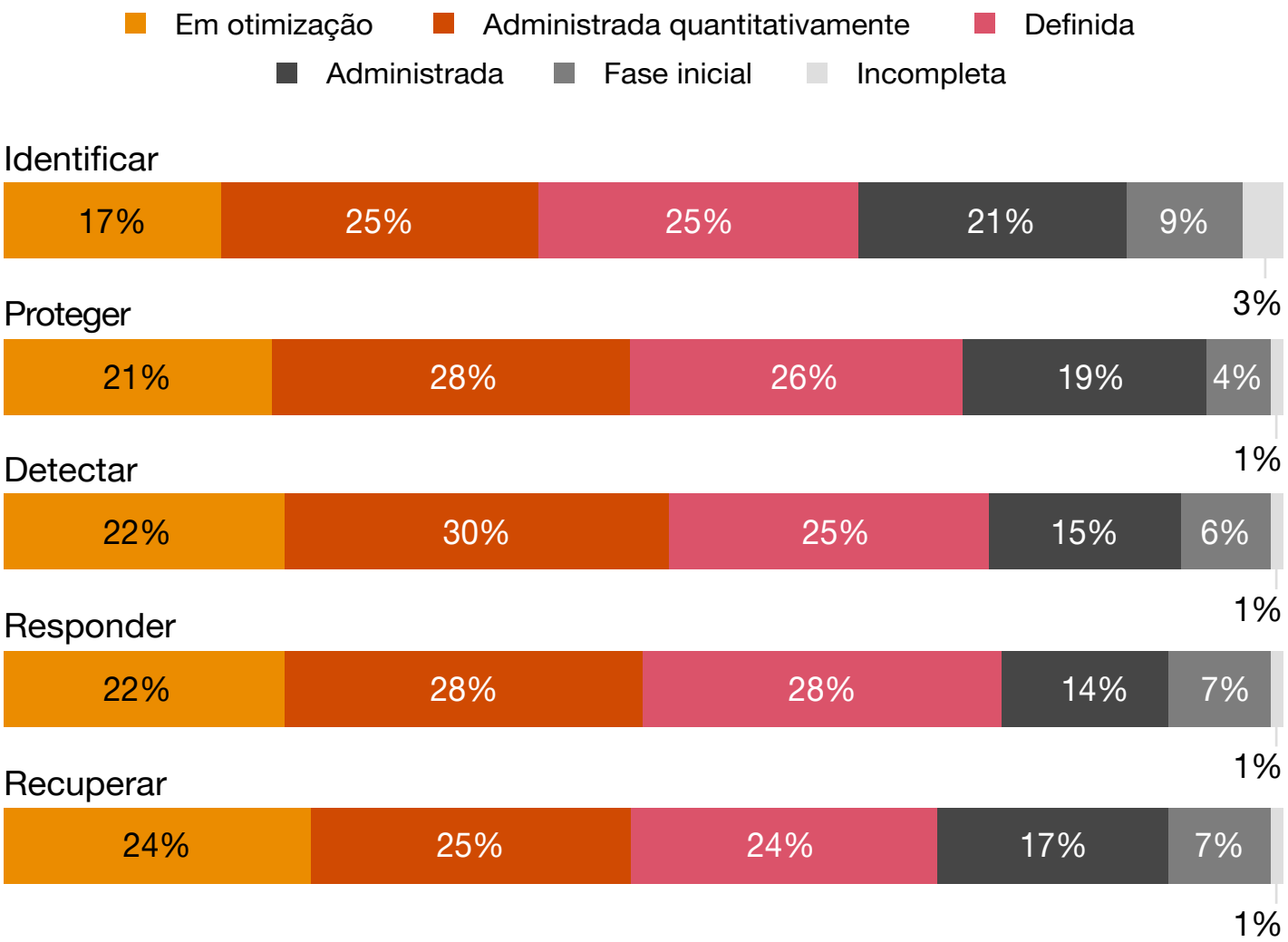
É urgente investir na capacidade de resiliência cibernética, pensando nos riscos de indisponibilidade do negócio e de processos básicos, como proteção do *backup*, em um modelo inicial de *disaster recovery*, avaliando as infraestruturas *on premises* e de *cloud*, na garantia de alta disponibilidade dos ativos críticos.

Esses processos são uma grande oportunidade, pois permeiam todas as principais áreas do negócio. Isso dá visibilidade aos processos de segurança, mostra a relevância deles e o papel de cada envolvido nesse modelo de resiliência. É dessa forma que saímos do mundo de TI e nos colocamos para o negócio. Por outro lado, dar oportunidade à alta direção para experimentar o que é um risco é altamente recomendável. Para isso, tangibilizamos a situação com simulações para que se vivencie tanto a detecção quanto a resposta às principais ameaças a que o negócio está exposto.

Em nível global, CISOs veem a necessidade de avançar ainda mais em cinco competências cibernéticas

P: Pensando em todos os seus recursos de segurança cibernética, indique o grau de maturidade de sua organização em cada uma das áreas a seguir.

Mundo



Os altos executivos se preocupam com o fato de suas empresas não estarem totalmente preparadas para lidar com as ameaças crescentes. De acordo com Alexandre Domingos, CISO da Dasa, “acompanhar essa transformação digital do negócio é desafiador, uma vez que as prioridades mudam rapidamente. Em um plano de três anos, pelo menos 20% das metas mudam, o que pode deixar o time desconfortável”. É essencial ter uma gestão madura, preparada para disrupções, quando ocorrer uma exposição.

Outra questão é garantir a proteção de dados com o uso da linguagem adequada. “A conscientização de segurança, no dia a dia dos profissionais, é importantíssima. Em vez de falar sobre assuntos complexos e segmentados do setor, torna-se mais interessante explicar ao profissional de enfermagem, por exemplo, que ele tem um papel fundamental na proteção dos dados e na garantia da privacidade dos pacientes”, afirma Domingos.

No topo da lista das preocupações para 2023 no Brasil, envolvendo agentes e vias de ataque, estão:

- Atividade cibercriminosa
- Hacktivistas/hackers, concorrentes
- Aplicativos web
- Dispositivos móveis

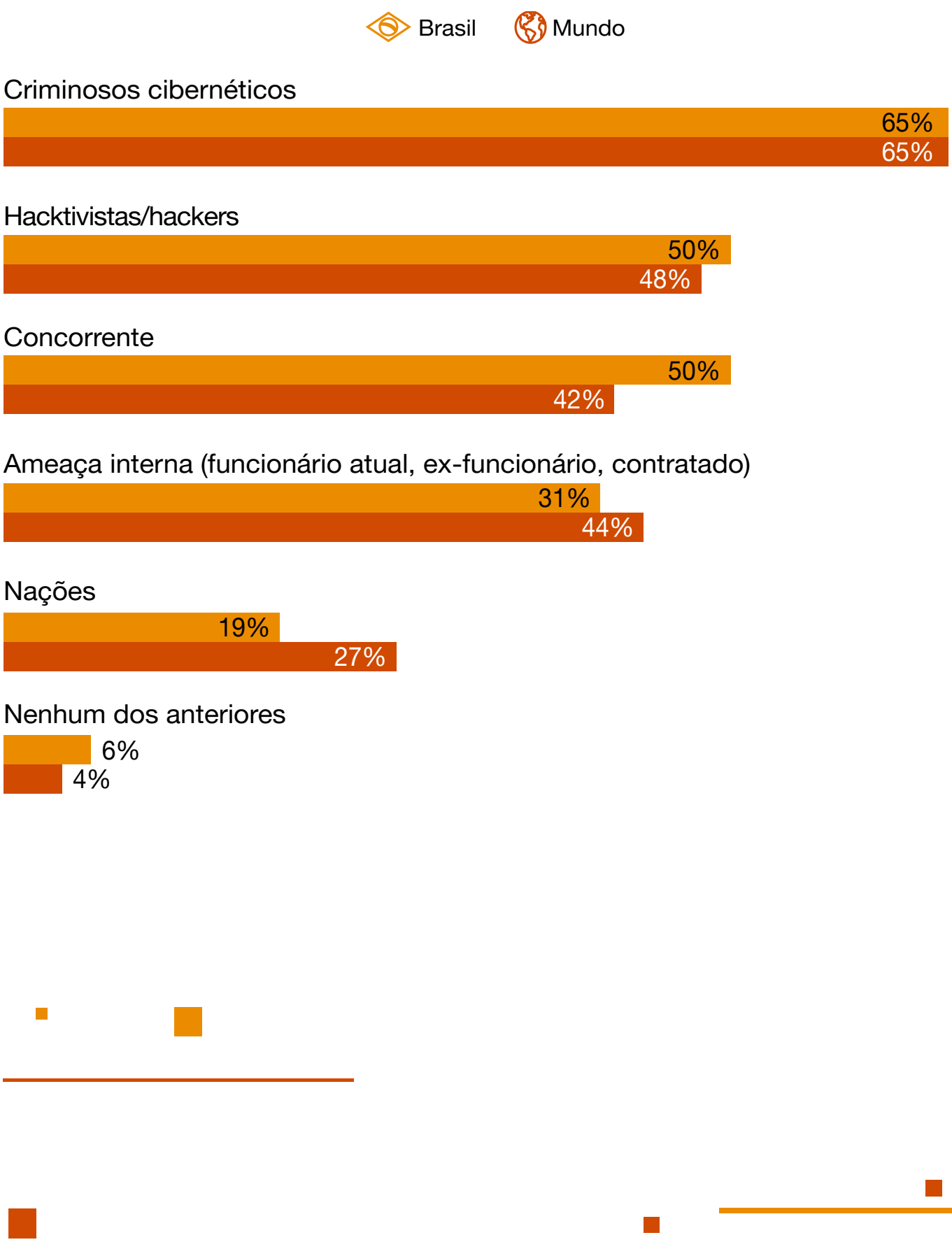
> “É essencial que as organizações avaliem sua resiliência cibernética como parte de uma estratégia de resiliência operacional mais ampla. Planos e processos bem desenhados são cruciais para apoiar os negócios em sua resposta a disrupções causadas não só por um ataque cibernético, mas pela própria evolução do negócio em resposta a novas demandas do mercado.”

Rafael Cortes
Sócio da PwC Brasil

Organizações se preocupam com a ocorrência de mais ameaças e eventos cibernéticos em 2023

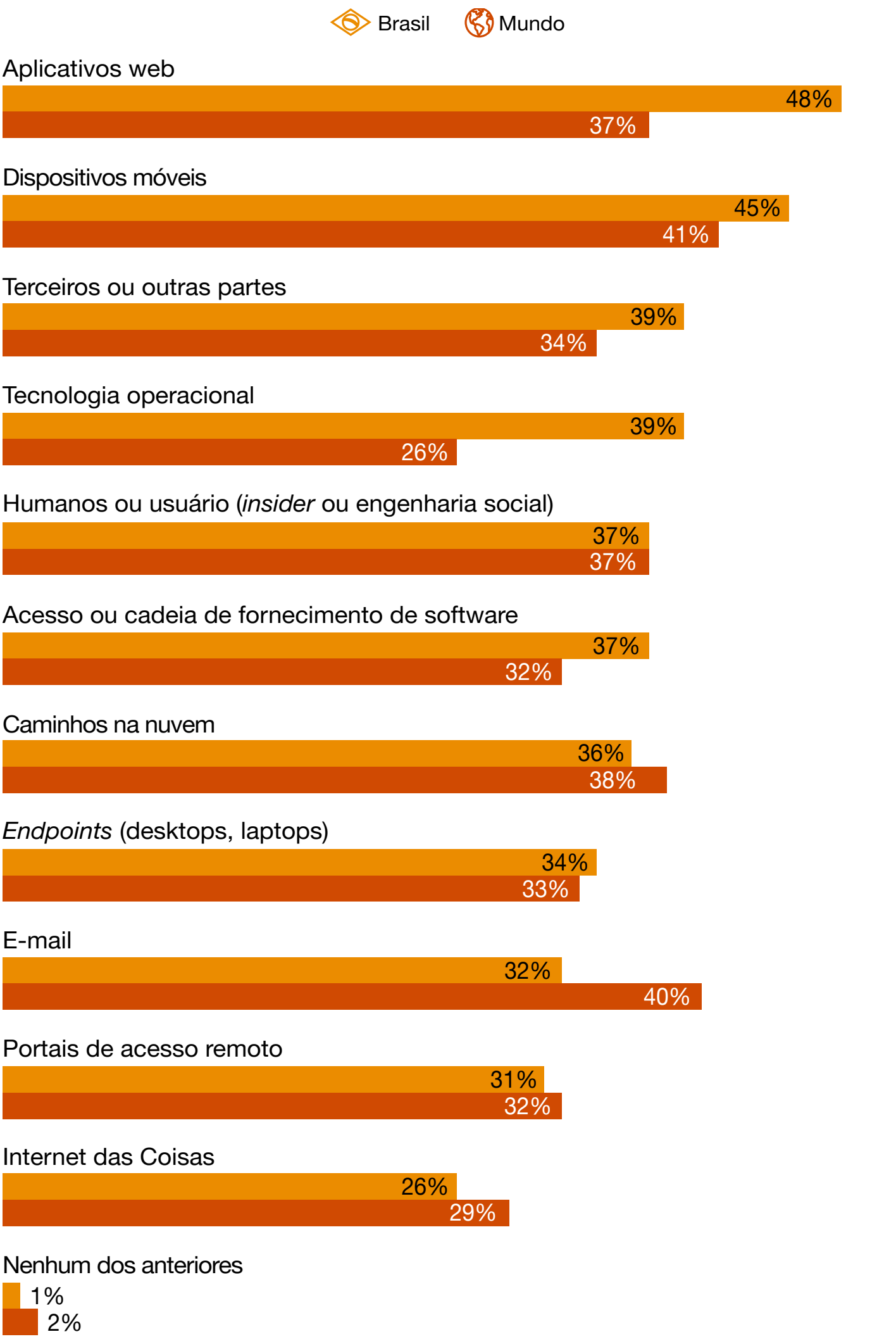
Agentes de ameaças

P: Para cada um dos agentes de ameaças abaixo, quais você espera que afetem muito sua organização em 2023 em comparação com 2022?



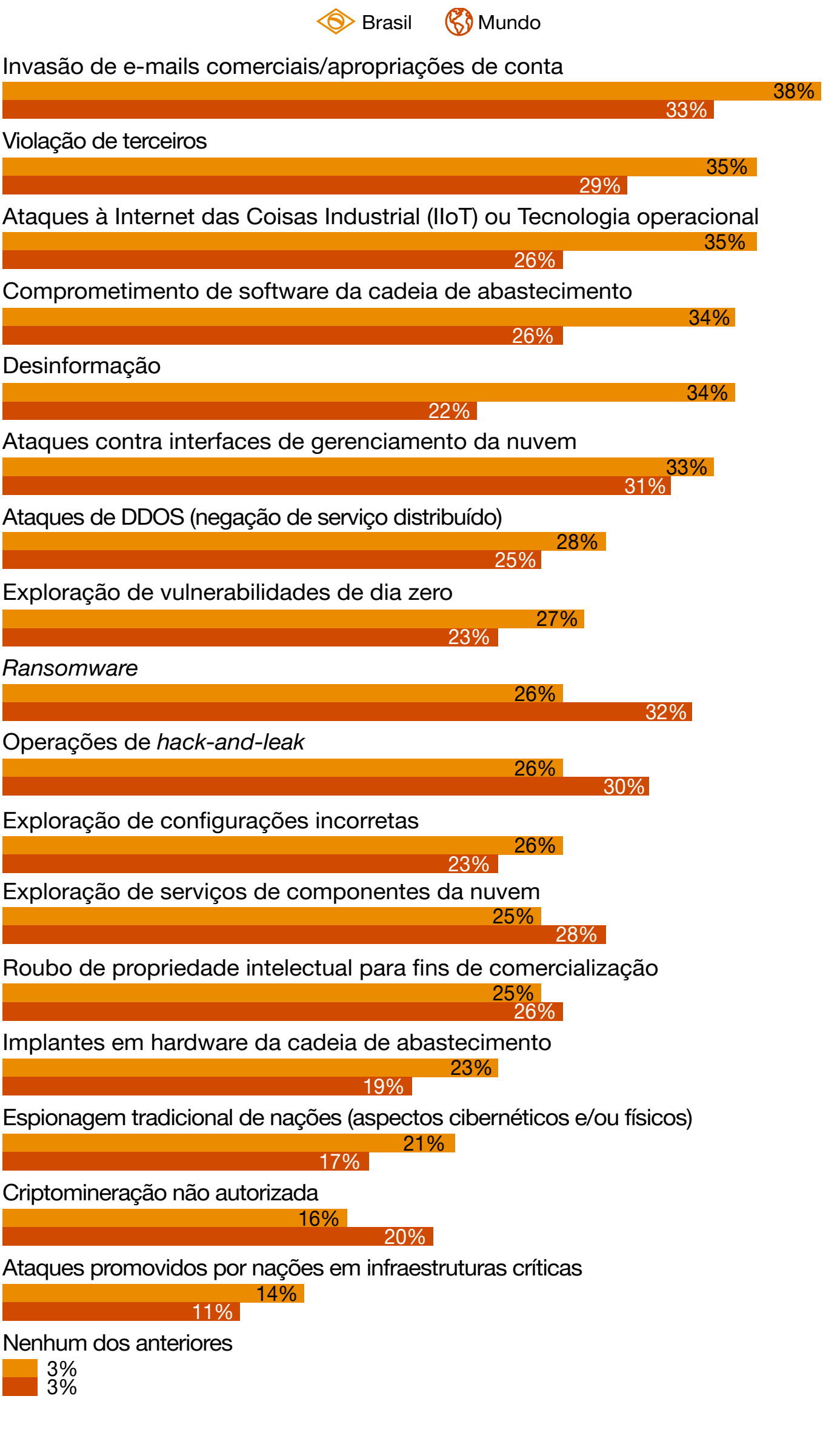
Vias de ataques

P: Para cada uma das vias pelas quais os adversários podem obter acesso a seus sistemas, selecione aquelas que você espera que afetem muito sua organização em 2023 em comparação com 2022.



Eventos cibernéticos

P: Quais dos seguintes ataques você espera que aumentem muito em 2023 em comparação com 2022?



Novos desafios para 2023

Globalmente, apenas 9% dos entrevistados se sentem altamente confiantes em sua capacidade de cumprir todos os requisitos de divulgação – mesmo com o aumento da pressão dos reguladores para relatar incidentes cibernéticos.

Os altos executivos estão se preparando não apenas para um ataque cibernético catastrófico, mas também para uma recessão global, uma nova crise sanitária, inflação persistente e gargalos na cadeia de suprimentos. No entanto, apenas 7% no mundo abordam a resiliência de forma integrada.

Consumidores, reguladores mais favoráveis ao consumidor, defensores da privacidade e ativistas ESG estão conquistando espaço. A segurança e a privacidade dos dados são o calcanhar de aquiles de muitas organizações: menos de 5% dos altos executivos dizem que sempre implementam as dez práticas comuns e mais recomendadas para proteger e controlar os dados dos clientes.

“A cibersegurança se tornou um campo dinâmico, que se ajusta e muda rapidamente para acompanhar a inovação nos negócios. A agilidade é necessária para lidar com os árduos desafios à frente. Destacamos na pesquisa o que os CISOs fizeram, o que estão fazendo agora e o que precisam fazer – em um trabalho conjunto com todos os outros executivos da organização – para enfrentar os desafios de 2023 e construir um futuro pronto para a realidade cibernética.”

Fernando Mitre
Sócio da PwC Brasil

Guia sobre cibersegurança para a liderança

O CISO está saindo de sua função de especialista cibernético independente para fazer parceria com toda a liderança. Essa colaboração entre os executivos nunca foi tão importante.

No mundo, 42% dos altos executivos dizem que as violações cibernéticas de seus sistemas aumentaram desde 2020. Executivos e conselhos se perguntam com frequência: “fomos afetados?” e, se não, “estamos vulneráveis?”

Mais de um quarto dos participantes no mundo registrou uma violação de dados nos últimos três anos que custou mais de US$ 1 milhão. Cerca de 10% tiveram despesas de US$ 10 milhões ou mais, segundo informaram CISOs e diretores financeiros (CFOs).

Cíntia Scovine Barcelos, diretora de Tecnologia do Bradesco, responsável por Infraestrutura de TI e Cibersegurança, entende que se houver um incidente de segurança, a organização e sua credibilidade são afetadas. “Em termos de estratégia, o foco deve ser a ciber-resiliência: a preparação é chave, se algo ocorrer, é preciso ter resiliência para se recuperar rapidamente”, afirma.

“O Bradesco tem trabalhado massivamente para trazer automação em todos os momentos, desde a detecção e análise das informações, até a forma como as disrupções serão resolvidas”, afirma Barcelos. Para os CFOs, de acordo com nossa pesquisa, as consequências mais devastadoras decorrentes de uma violação (que não tenha sido relacionada a dados) foram:

- Tempo de inatividade ou disrupções
- Danos ao serviço e qualidade do produto
- Perda de contratos e oportunidades de negócios

Para executivos de privacidade e dados que trabalham com o público, os efeitos mais prejudiciais de uma violação foram:

- Perda de clientes
- Custos para recuperar dados (sem contar pagamentos de resgate)
- Perda de dados do cliente (caso não tenham sido recuperados)

Ao aumentar a conscientização sobre os efeitos de uma única violação, desde o chão de fábrica até a diretoria, esses momentos angustiantes podem servir como um catalisador de colaboração e levar toda a liderança a se mobilizar para agir em conjunto.

Como resultado, a alta administração renova sua determinação de melhorar a atuação em relação à cibersegurança e à privacidade. Para chegar lá, os líderes estão começando a entender a necessidade de trabalhar de forma coesa – o foco da liderança.

No centro dessa atuação conjunta está o CISO, empoderado pelo CEO para defender, colaborar e orquestrar um futuro cibernético melhor. Globalmente, 46% dos CEOs querem dar ao CISO mais autoridade para conduzir a colaboração sobre segurança no próximo ano.

Visão da liderança

Cíntia Scovine Barcelos
Diretora de Tecnologia do Bradesco, responsável por Infraestrutura de TI e Cibersegurança

Avaliar continuamente a ciber-resiliência se tornou imperativo para o Bradesco. Identificamos as principais tendências e necessidades e criamos um *roadmap* para os próximos anos. A base precisa ser o risco, entender as vulnerabilidades e como ser resiliente a elas. As pessoas são fundamentais nesse processo, seja em termos de desenvolvimento de novos *skills* como de mudança de cultura e postura.

Na jornada para *cloud*, devemos considerar os desafios de cibersegurança nesse novo perímetro, com múltiplos *data centers* e com colaboradores trabalhando remotamente. É necessário ter uma mudança de *mindset* e treinar as pessoas para um volume de desafios cada vez maior. Temos uma grande organização com múltiplos negócios (banco, seguradora, fundação, hospital, entre outros) operando com foco no cliente e na busca constante por inovação e segurança.

A união entre as instituições financeiras no combate ao crime cibernético, capitaneada por instituições como a FEBRABAN e também outros órgãos da sociedade e governamentais, é um ponto essencial para garantir que as informações circulem na velocidade necessária de uma resposta à altura das disrupções emergentes. Não deve existir competição entre as organizações quando o assunto é segurança. Está claro que devemos estar juntos.

CEOs assumem uma postura mais ativa em relação à cibersegurança este ano

No Brasil, 61% dos CEOs (51% no mundo) dizem que exigirão um plano de gerenciamento de risco cibernético para cada importante mudança operacional ou nos negócios. E mais da metade afirma que vai liderar iniciativas relevantes, como simplificar a cadeia de suprimentos e eliminar produtos que enfraquecem a postura de cibersegurança da empresa.

CEOs de empresas que sofreram violações no passado estão ainda mais determinados a mudar suas operações de cibersegurança. Eles querem mais informações para poder supervisionar melhor os programas de cibersegurança. Mais de 35% no mundo priorizam três áreas para obter melhores relatórios:

- Avaliações e práticas de gestão do risco cibernético
- Planos de continuidade de negócios e de resiliência no caso de um incidente cibernético
- Um painel para monitorar os principais indicadores de riscos cibernéticos

Já no Brasil, 40% dos CEOs estão concentrados na estratégia de cibersegurança (e seu alinhamento com a estratégia geral da empresa) e no programa de gestão de riscos cibernéticos de terceiros.

Mensagem ao CEO

Grandes mudanças podem ser a maneira mais eficaz de melhorar a postura de cibersegurança – e só o CEO pode fomentá-las. Você tolera complexidades desnecessárias e evitáveis em suas operações e tecnologias? Isso precisa mudar.

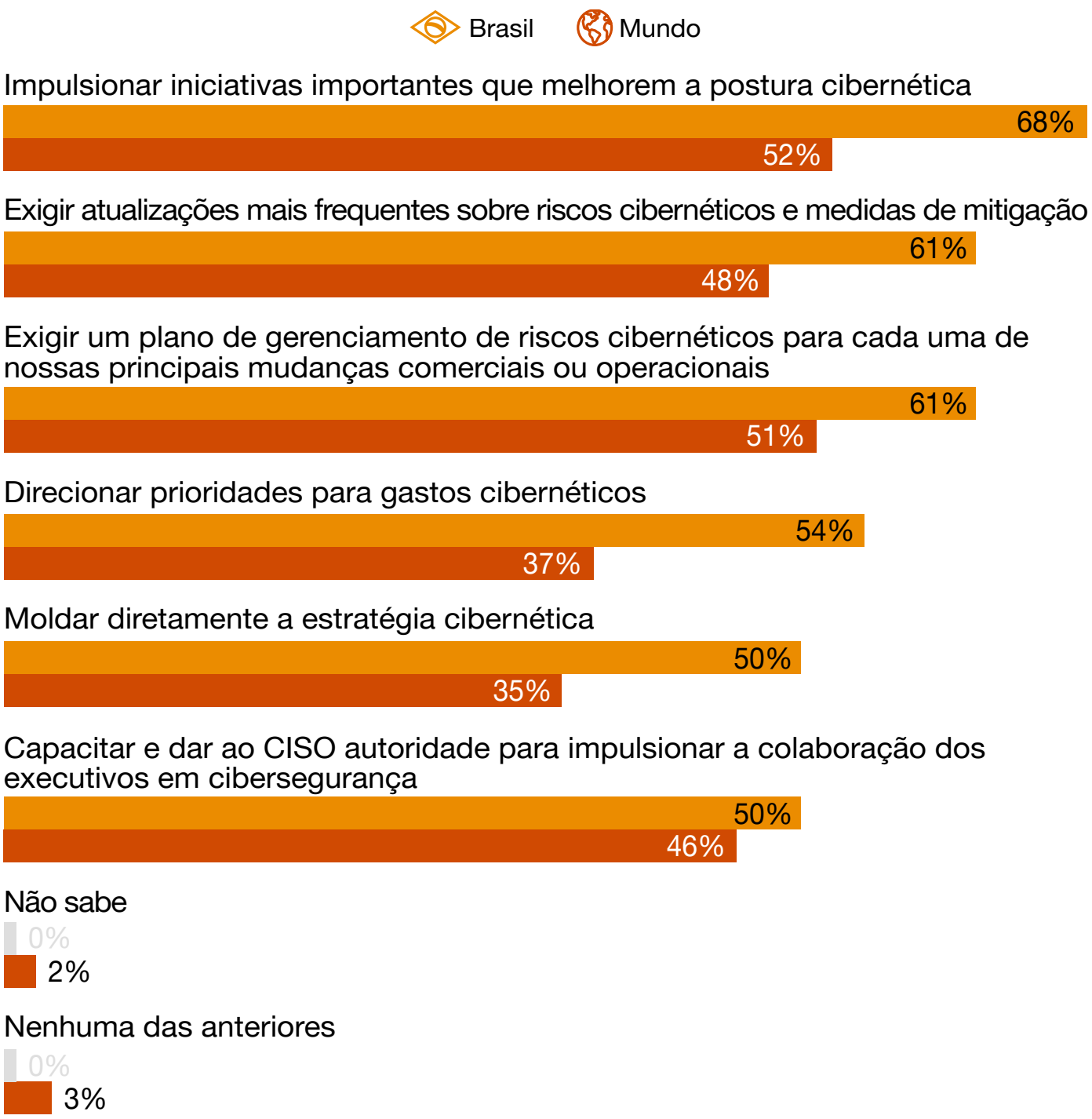
Muitas vezes, as investigações após uma grande violação cibernética revelam mais fraquezas sistêmicas do que tecnológicas, causadas pela falta de foco dos líderes em abordar vulnerabilidades já identificadas pelas equipes. Você está pronto para apoiar uma mudança estratégica? Essa pode ser a forma mais eficaz de fazer correções.

Talvez a falta de conexão entre os altos executivos ou entre funções de negócio e cibernéticas freie seus esforços de crescimento, como um aplicativo para o consumidor, uma nova linha de negócios com base em inteligência artificial, a expansão para um novo mercado ou o uso da Internet das Coisas industrial em sua fábrica.

O CEO deve usar a sua influência para inspirar mudanças estratégicas e criar uma frente unida contra ataques. É importante reunir a alta administração em torno da ideia de que o caminho seguro pode realmente ser o mais fácil para o sucesso dos negócios. “São crescentes as ameaças e as necessidades de segurança da organização”, afirma Cíntia Scovine Barcelos, do Bradesco. “Devemos priorizar as ações com base no risco, trazendo mais automação ao modelo de segurança, desde a detecção e análise até a remediação.”

Assuntos cibernéticos em que os CEOs planejam se envolver pessoalmente

P: Quais das seguintes ações, se for o caso, você pretende realizar nos próximos 12 meses para se envolver em questões de segurança cibernética em sua organização?



Os conselhos podem incentivar a elaboração de relatórios cibernéticos mais precisos para melhorar a governança

Os conselhos estão mais engajados com a cibersegurança à medida que suas empresas enfrentam riscos crescentes. Globalmente, 54% dizem que sua organização assumiu mais riscos cibernéticos com a expansão da digitização e 44% relatam um aumento nas violações cibernéticas em seu sistema desde 2020.

Eles reconhecem que é um desafio manter em dia a cibersegurança. Hoje, menos da metade dos entrevistados no mundo que fazem parte do conselho diz que o órgão em que atua exerce a governança sobre os riscos cibernéticos “de forma muito eficaz” em seis áreas - ver gráfico na página 29. Por exemplo, 37% dizem que compreendem de forma “muito eficaz” as causas e efeitos dos riscos cibernéticos, enquanto 43% dizem o mesmo sobre a supervisão do alinhamento da gestão de riscos cibernéticos às necessidades do negócio. Apenas 9% dos entrevistados do conselho dizem que seu conselho exerce a governança sobre o ciberespaço “de forma muito eficaz” em todas as áreas.

Mas o futuro da supervisão cibernética pode ser diferente. Os conselheiros estão dispostos a dedicar tempo para aprender sobre a atividade cibernética. Eles dizem que as medidas a seguir os ajudarão a fazer um trabalho melhor na gestão da cibersegurança em 2023:

- Aumento da frequência de reuniões com foco em questões cibernéticas (73% no Brasil e 47% no mundo)
- Relatórios aprimorados sobre práticas, melhorias e incidentes cibernéticos (60% no Brasil e 44% no mundo)
- Treinamento interno do conselho pelos gestores (57% no Brasil e 47% no mundo)
- Inclusão de um membro no conselho com experiência cibernética (60% no Brasil e 42% no mundo)

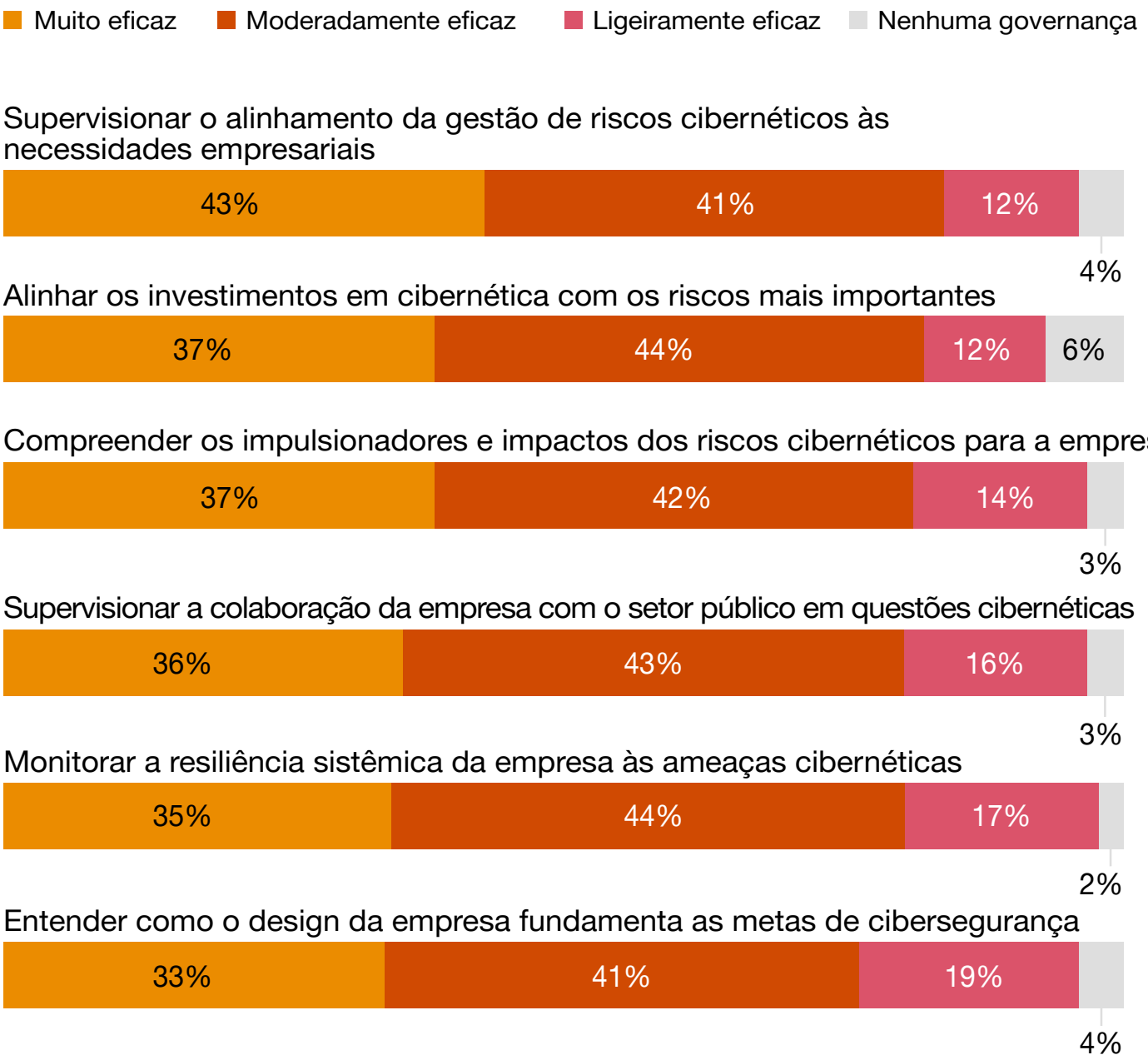
Os CISOs e os demais líderes podem ajudar os conselhos a se familiarizar com a cibersegurança, especialmente nestas principais melhorias que os conselhos gostariam de ver nos relatórios cibernéticos:

- Um painel de indicadores para ajudar os membros do conselho a entender os principais riscos cibernéticos para a organização com métricas relevantes
- A estratégia de cibersegurança da organização e como ela está alinhada com a estratégia geral do negócio
- Os planos de continuidade de negócios, contingência e recuperação em caso de incidente cibernético

“Para administrar melhor as questões cibernéticas, é preciso considerar enviar relatórios que transmitam confiança e contenham informações sobre o gerenciamento dos riscos cibernéticos relacionados aos movimentos estratégicos da organização”, comenta Cinthia Scovine Barcelos. A cibersegurança não é um estado final, “avalie como a empresa está evoluindo em sua postura cibernética e capacidade de defesa contra novas ameaças”.

Os conselhos sabem que precisam administrar melhor as questões cibernéticas

Avaliação da governança do conselho de administração quanto aos seguintes aspectos da cibersegurança:



“O CISO deverá ter uma influência cada vez maior nas organizações à medida que as iniciativas de transformação digital avançarem e for preciso atender às demandas de cibersegurança de ambientes em constante mudança. A nova era de transparência cibernética exige que os CISOs consigam apresentar informações de uma maneira que o conselho, a alta administração e os investidores entendam para poderem agir. Para isso, a estratégia de comunicação precisa ser diferente do jargão cotidiano da cibersegurança.”

Magnus Santos
Sócio da PwC Brasil

A nova era da transparência cibernética

Os *stakeholders* clamam por mais informações sobre como as empresas gerenciam sua exposição ao risco cibernético. Os reguladores querem ter visão das práticas de cibersegurança adotadas para proteger os cidadãos contra fraudes e perda de privacidade, ajudar os investidores a tomar melhores decisões e evitar disrupções.

Os investidores procuram divulgações consistentes e comparáveis para que possam aplicar seu dinheiro em empresas que atendam às suas necessidades. Afinal, incidentes cibernéticos podem afetar o valor das ações – temporária ou permanentemente.

As pessoas sabem como seus dados e privacidade são vulneráveis a violações cibernéticas. Os parceiros de negócios querem que seus dados e outros ativos estejam seguros. Esses *stakeholders* precisam entender o quanto podem confiar na capacidade das empresas e de sistemas inteiros de resistir às crescentes ameaças cibernéticas.

A alta administração vê uma vantagem em toda essa transparência. No Brasil, 91% dos altos executivos (79% no mundo) concordam que a divulgação obrigatória de incidentes cibernéticos, com formatos comparáveis e consistentes, é necessária para conquistar a confiança do mercado.

Os CISOs podem posicionar suas equipes para trabalhar com o CFO, o conselho e outros altos executivos para ajudar a traduzir a estratégia e as práticas em uma narrativa precisa, coesa e convincente sobre as atividades de gerenciamento de risco cibernético da empresa.

Visão da liderança

José Luiz França
BISO de Redes da Neoenergia

É necessário ter executivos de cibersegurança com conhecimento do negócio, equilibrando as decisões e desdobrando estratégias com o *Board*. Em grandes empresas, a diversidade de temas torna necessária a distribuição de papéis entre diferentes responsáveis para garantir a efetividade nas ações.

Na Neoenergia, por exemplo, temos os negócios de redes (distribuição e transmissão), renováveis e liberalizados, cada uma com suas particularidades e sensibilidades, com isso, adotamos a estratégia de ter BISOs (*Bussiness Information Security Officer*) distintos por negócio, priorizando demandas e investimentos alinhados à estratégia de cada um.

Em paralelo, existe uma questão visível do volume e da sofisticação das quadrilhas com uma grande motivação financeira para fazer os ataques. O profissional de cibersegurança precisa estar de prontidão sempre, envolvido em uma reciclagem contínua, e estar muito motivado para ser criativo.

Nenhuma organização está completamente protegida e precisamos ter humildade para entender que temos que nos esforçar muito mais. A mensagem ao mercado é clara: competidores reais e potenciais precisam criar fóruns e se aliar para lidar com esse cenário, que muda rapidamente. As empresas, que estão em um mesmo mercado e são competidoras, devem se aliar contra esse “inimigo comum”. Devemos estar unidos.

na nuvem

“Nosso plano de segurança na nuvem é tão ágil quanto nosso negócio na nuvem?” Diretores de Tecnologia da Informação (CIOs) e CISOs deveriam estar fazendo essa pergunta.

As ameaças que exploram a nuvem aumentaram em quase 40% das organizações participantes da pesquisa no Brasil e no mundo. Enquanto isso, quase dois terços dos altos executivos dizem que não mitigaram totalmente os riscos da adoção da nuvem.

As notícias não são todas negativas. Metade dos CISOs, CIOs e CTOs diz ter evoluído no gerenciamento de credenciais, permissão de recursos, configurações de segurança na nuvem e gerenciamento de API.

Mas apenas 19% estão “muito confiantes” que sua organização protegeu adequadamente as potenciais brechas usadas para violar a segurança na nuvem. É comum que o CIO ou CTO e sua equipe de DevOps se sintam ansiosos – ou pressionados – para aproveitar a agilidade, velocidade e colaboração que o trabalho na nuvem oferece.

Nesse caso, eles talvez permitam que os desenvolvedores criem projetos em um ambiente de nuvem antes da implementação de medidas de segurança ou da migração de sistemas existentes para a nuvem, planejando protegê-los apenas posteriormente.

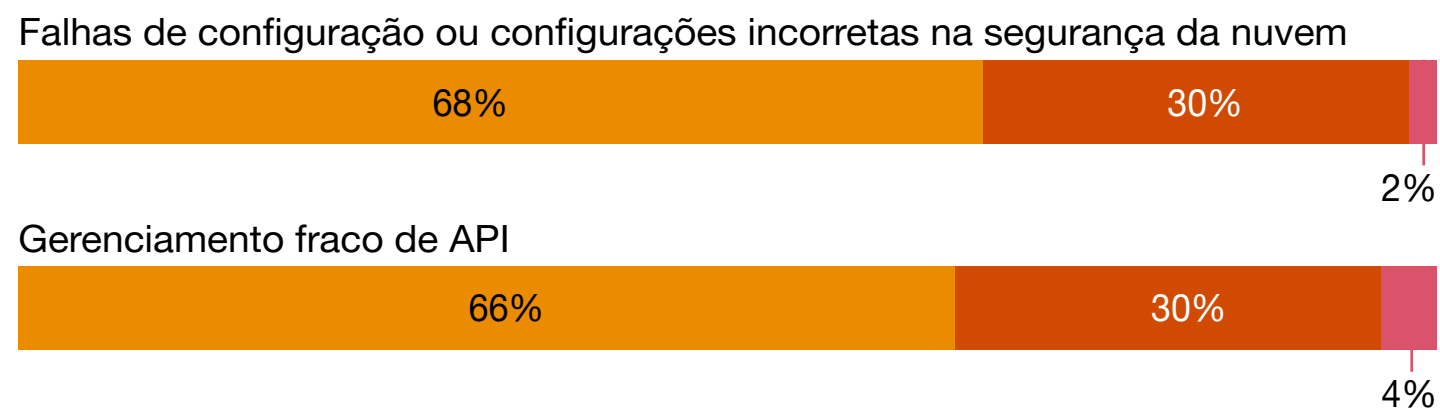
Essas equipes podem contornar o CISO para impedir a abordagem metódica e de segurança que o executivo certamente aconselharia. No mundo digital acelerado, as empresas sabem que precisam de velocidade para atingir seus objetivos. Quando agilidade e velocidade são os objetivos, quem precisa de freios?

As iniciativas de segurança na nuvem estão valendo a

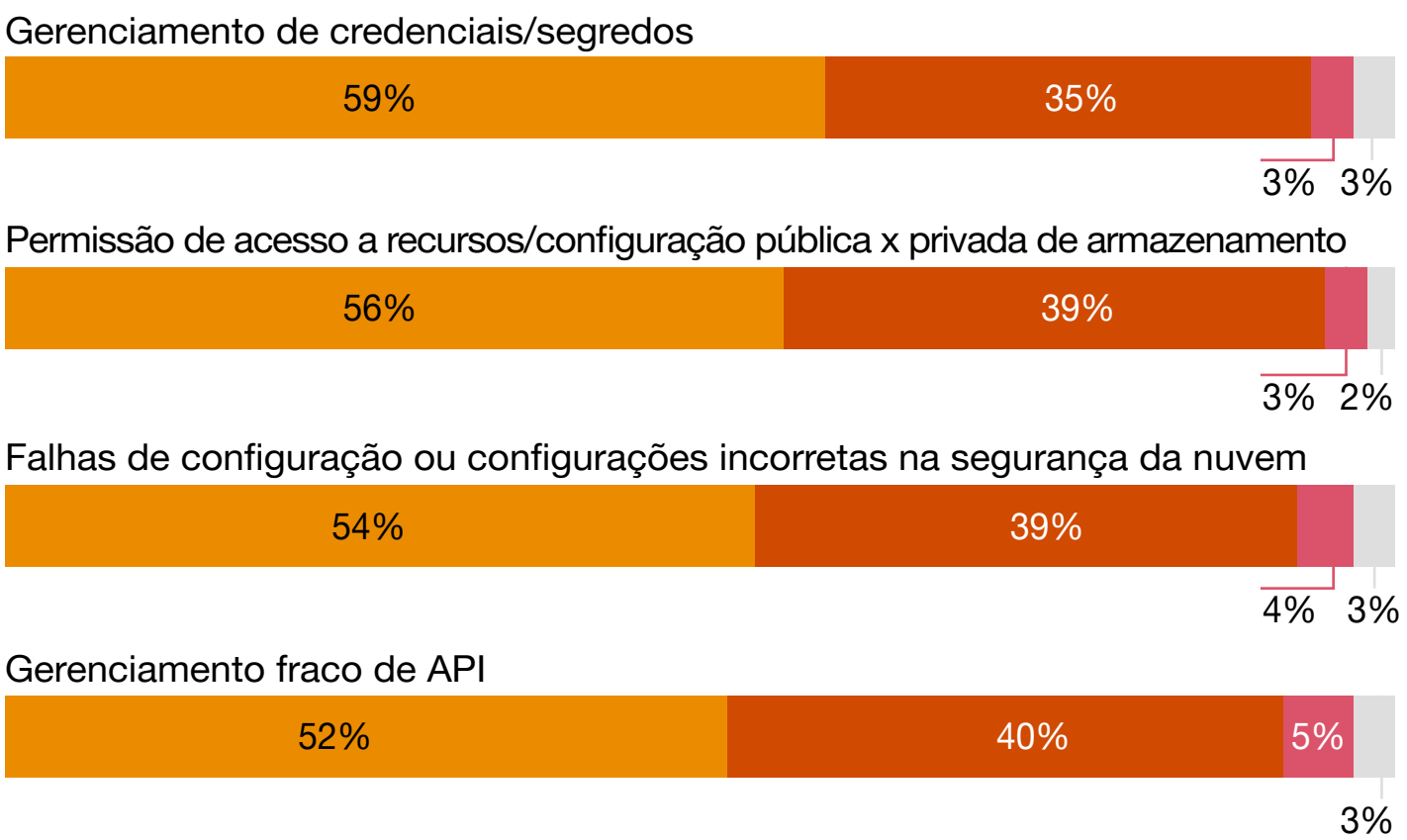
pena, mas ainda há muito trabalho a fazer

Nível de confiança na capacidade da organização de se proteger adequadamente contra motivos para violações de segurança na nuvem:

Brasil



Mundo



Base: CIOs, CISOs, CTOs e outros altos executivos de TI e segurança (1.253 no mundo | 47 no Brasil)

Mas a governança coesa é fundamental, especialmente em um ambiente multinuvem em que cada provedor de serviços tem diferentes habilidades e requisitos de segurança. Com lançamentos frequentes de novos recursos e atualizações, o ambiente de nuvem da empresa muda continuamente.

Em 2023, é preciso projetar uma arquitetura de segurança abrangente que inclua todas as plataformas de nuvem que a empresa está usando. Reúna todos os controles de segurança da organização para protegê-los em um único local e com o máximo de automação possível.

Crie ferramentas de infraestrutura como código (*IaC*, na sigla em inglês) e DevSecOps para definir automaticamente as verificações de segurança corretas em todas as plataformas em nuvem.

Os CISOs podem fornecer aos desenvolvedores serviços de segurança em nuvem fáceis de usar e em conformidade com as políticas de segurança da organização. Construir uma API de criptografia para uso dos desenvolvedores, por exemplo, pode acelerar o lançamento dos aplicativos no mercado e assegurar que a criptografia use protocolos aprovados pela empresa.

Mensagem para CIOs e CTOs

Forme alianças com o CISO e sua equipe DevSecOps. Adote o paradigma *shift left* e comece a implementar mecanismos de segurança antes de começar a usar a nuvem ou o mais rápido possível.

Desenvolvimento rápido e controles fortes podem ser indissociáveis. As empresas líderes projetam e administram controles que operam na velocidade rápida e ágil do DevOps, e não no ritmo lento frequentemente associado à supervisão. Nessas organizações, todos ganham. Para proteger seu *back-end, front-end*, a Internet das Coisas e as tecnologias operacionais, trabalhe com o CISO para bloquear seus ambientes em nuvem.

Nesse cenário, de acordo com José Luiz França, “o profissional de cibersegurança precisa ter algumas necessidades muito claras: conhecimento técnico e proficiência, além de uma habilidade de conseguir juntar as peças para poder se antecipar a fraudes”. Tem que ter a “sua caixa de ferramentas bem montada”, mas também a criatividade para imaginar como elas poderiam ser usadas de uma forma mais inteligente.

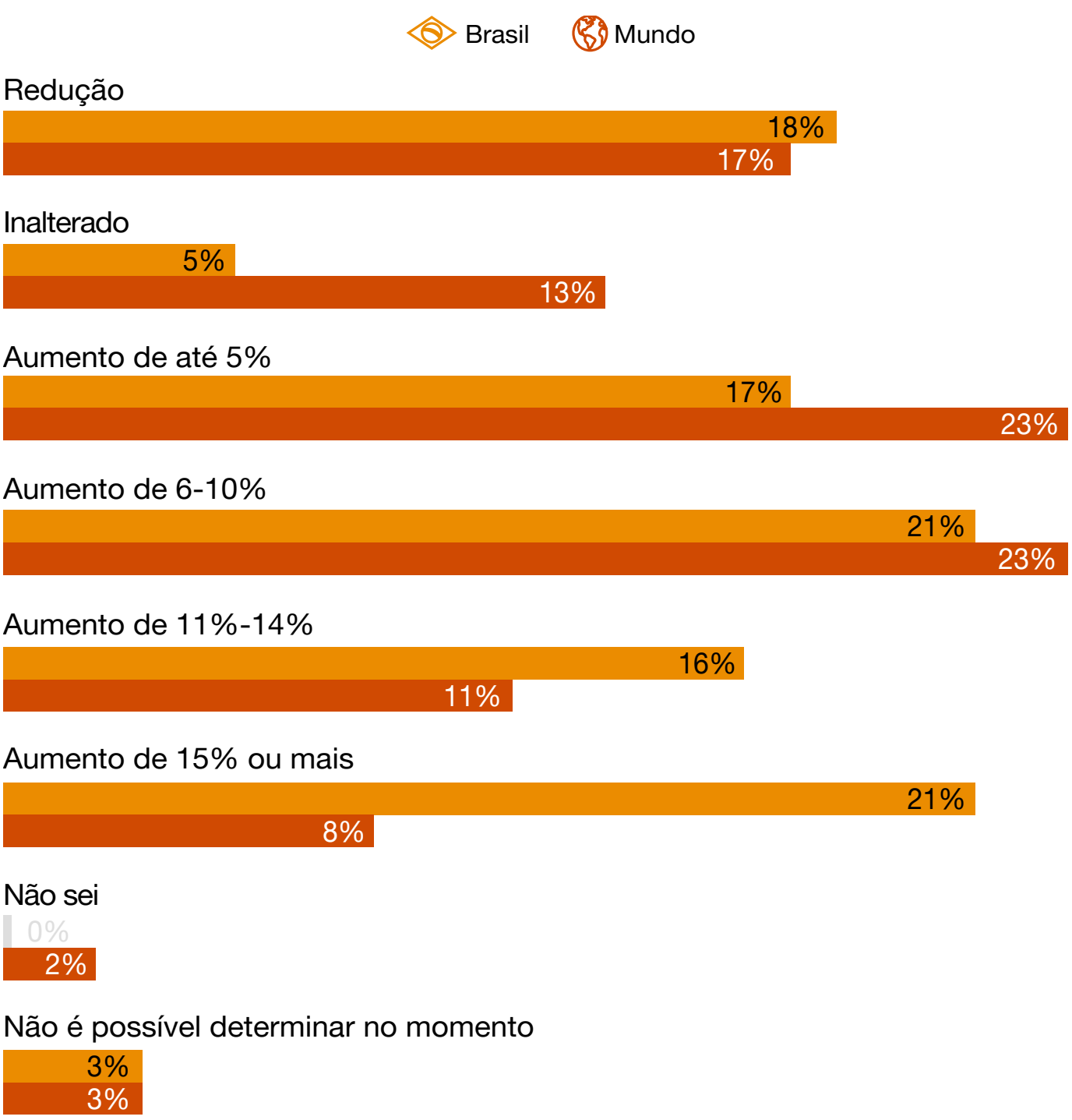
CFOs e CISOs devem levar a sério os riscos e o retorno do investimento cibernético

As empresas continuam a elevar seus gastos com cibersegurança. No Brasil, 75% dos altos executivos (65% no mundo) dizem esperar um aumento dessas despesas em 2023, em comparação com 83% (69% no mundo) em 2022.

Mas o aumento dos orçamentos cibernéticos não está ocorrendo no mesmo ritmo de 2022. Enquanto 45% das empresas no Brasil (26% no mundo) esperavam que os gastos cibernéticos aumentassem mais de 10% em 2022, no próximo ano, 37% (19% globalmente) acreditam que esse ritmo de aumento será mantido.

Não surpreende que as organizações que sofreram violações sejam muito mais propensas a dizer que aumentariam seus gastos com cibersegurança em 2023: 68% no mundo, em comparação com 55% das outras. E entre as empresas maiores (com receitas anuais superiores a US$ 1 bilhão), 10% disseram que seus gastos cibernéticos aumentariam 15% ou mais.

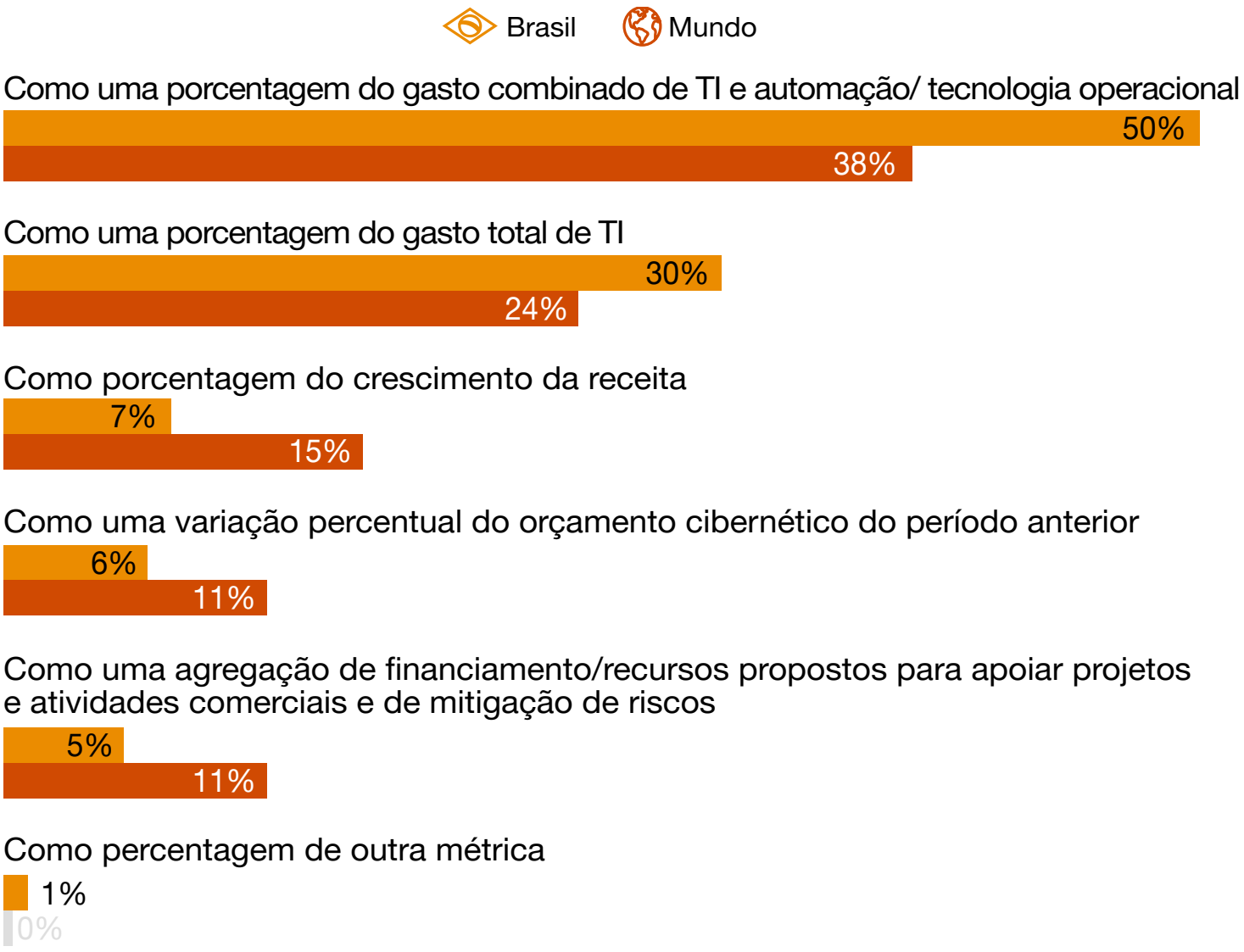
Como o orçamento cibernético das empresas está mudando para 2023



Base: executivos de negócios e tecnologia (3.522 no mundo | 109 no Brasil)

As empresas estão adotando uma abordagem mais expansiva ao fazerem o orçamento para a área cibernética. Metade dos CEOs, CFOs e CISOs no Brasil (38% no mundo) dizem que suas empresas agora financiam a cibersegurança com uma porcentagem de todos os gastos com tecnologia, incluindo tecnologia operacional e automação. Outros 7% no Brasil (15% no mundo) dizem que o orçamento de cibersegurança é uma porcentagem da receita.

Como as organizações definem seus orçamentos cibernéticos



Base: CEOs, CFOs, CISOs, CIOs, CTOs e outros executivos em finanças, segurança, funções de TI (2.498 no mundo | 86 no Brasil)

Muitos também começaram a mudar sua estratégia de investimento cibernético. Globalmente, mais da metade dos participantes diz que, “em grande medida”, está escolhendo como gastar em cibersegurança de acordo com sete parâmetros-chave:

55% **Alinhamento com a estratégia de negócios**

55% **Reflexo das prioridades cibernéticas**

55% **Geração de valor para a organização**

52% **Equilíbrio entre necessidades imediatas e de longo prazo**

51% **Fundamentação na quantificação de riscos**

51% **Alinhamento com o apetite a riscos da organização**

51% **Boa alocação contra os riscos que a organização enfrenta**

Vimos essa mudança começando em nossa pesquisa de 2021, em que 50% dos altos executivos no mundo disseram que queriam ver os orçamentos refletindo melhor a estratégia de negócios, 44% queriam um processo orçamentário melhor e 44% queriam quantificar os riscos.

Menos de 8%, no entanto, indicaram que fizeram essa mudança em todas as áreas. Os entrevistados de organizações maiores eram muito mais propensos a dizer que evoluíram na forma como investem: 60% disseram que seus gastos apoiam a estratégia de negócios, por exemplo.

Modernização da tecnologia

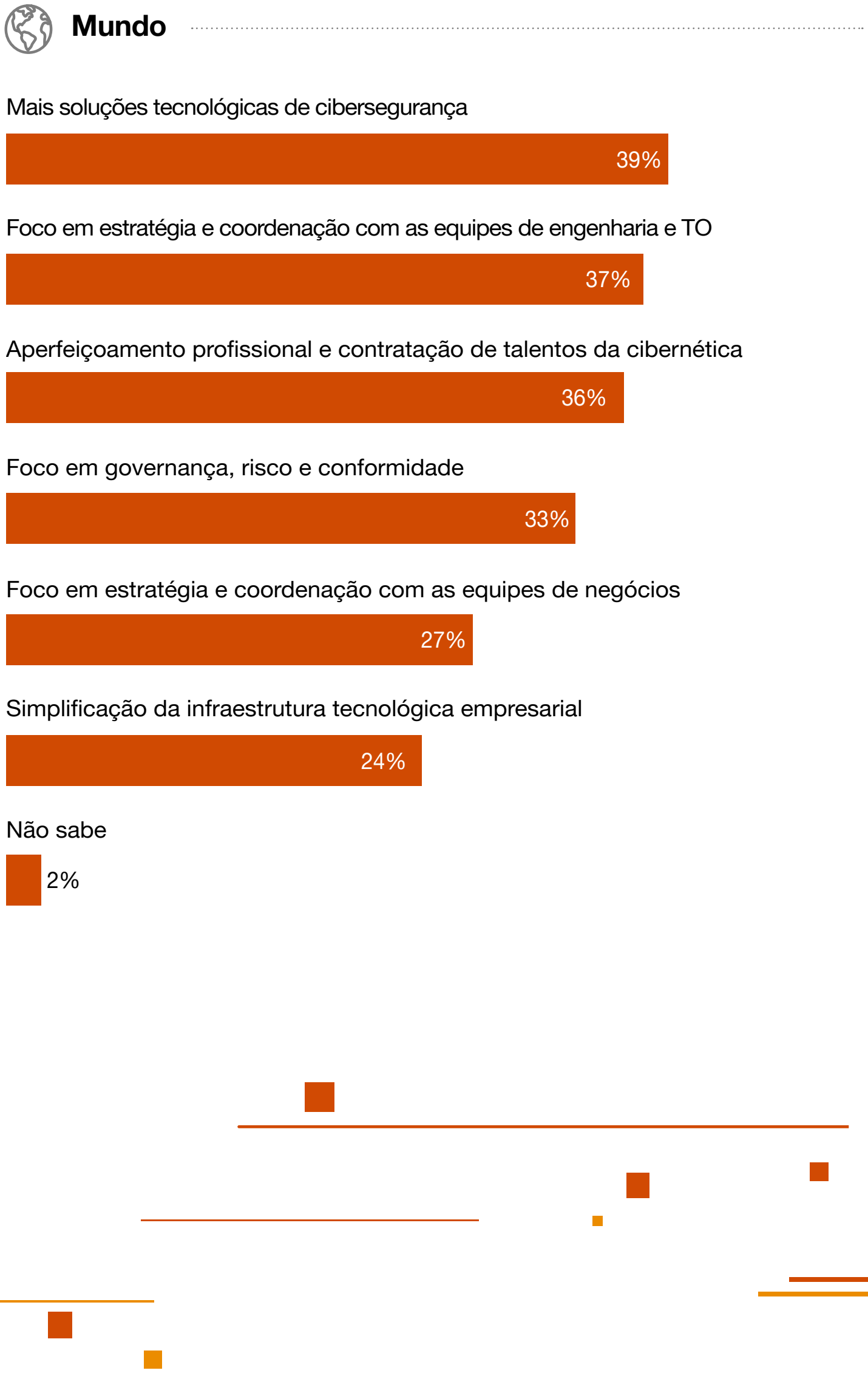
As soluções de tecnologia cibernética estão no topo da lista de áreas que os CFOs consideram essenciais para melhorar a postura digital de suas organizações. A modernização ainda é um problema em muitas organizações, especialmente quando se trata de tecnologia operacional. Recursos desatualizados e o gerenciamento de vulnerabilidades são as principais barreiras para melhorar a segurança da tecnologia operacional, dizem CISOs, CIOs e CTOs.

A complexidade também continua sendo uma grande preocupação. Simplificar e consolidar o portfólio de software é uma das prioridades para 2023 entre os entrevistados que sofreram violações nos últimos três anos. Novamente, nossos resultados da pesquisa Global Digital Trust Insights de 2022 previram essa tendência: 77% dos participantes no Brasil (75% no mundo) disseram que seus dados, tecnologias e outras operações eram muito complexos e causavam preocupações quanto a riscos cibernéticos.

É revelador que outro foco importante entre as empresas violadas seja eliminar o déficit técnico – o custo de buscar atalhos no desenvolvimento por questões de velocidade. Para as demais empresas, entretanto, esse aspecto está no fim da lista de objetivos de transformação cibernética.

Áreas em que os CFOs querem mais recursos para melhorar a postura cibernética de suas organizações nos próximos 12 meses

Mundo



Mensagem aos CFOs

Você está certo em perguntar: “Estamos gastando o suficiente e nas áreas certas? Estamos reduzindo o risco cibernético de nossos investimentos para o nível certo?” À medida que as soluções de tecnologia proliferam, você precisará trabalhar com o CISO para elaborar um plano geral a fim de proteger sua organização em vários níveis, além de simplificar e agilizar o software da sua empresa. Lembre-se de sua implantação inicial na nuvem – as cargas de trabalho que foram migradas para a nuvem usando o modelo *lift and shift*. Elas também contribuem para o seu déficit técnico.

A natureza aberta da nuvem também exige que as organizações ajustem seus parâmetros de confiança para zero. Você precisará de um plano abrangente para fazer uma transição para arquiteturas de confiança zero. Em nossa pesquisa, 40% dos CISOs no Brasil (36% no mundo) dizem que começaram a implementar componentes de confiança zero; outros 26% (25% no mundo) começarão nos próximos dois anos.

De acordo com José Luiz França, da Neoenergia, “ao modernizar e simplificar a TI, é preciso perguntar como cada valor gasto a mais pode reduzir o risco cibernético. As empresas que compreendem os custos pensam na segurança desde a etapa de desenvolvimento da solução – e economizam”.

COOs e CISOs se unem para planejar defesas contra ataques crescentes à cadeia de suprimentos e à tecnologia operacional

A cadeia de suprimentos é um ponto focal para ameaças cibernéticas e de outros tipos, pressões competitivas e macroeconômicas e preocupações com ESG. Globalmente, 56% dos CROs e COOs dizem que estão extremamente ou muito preocupados com sua capacidade de resistir a ataques à cadeia de suprimentos.

Apenas cerca de um quarto concorda fortemente que sua força de trabalho da área de operações tem as habilidades digitais necessárias ou que investiu o suficiente para impedir que ataques cibernéticos perturbem a cadeia de suprimentos.

Eles temem que sua capacidade de controlar essas ameaças esteja parcialmente nas mãos de terceiros mal equipados para protegê-los. Apenas um quinto concorda fortemente que seus parceiros e fornecedores terceirizados agiram ou investiram o suficiente para evitar perturbações na cadeia de suprimentos por ataques cibernéticos; 13% discordam.

Tecnologias operacionais: mais e melhores soluções são necessárias

Apenas cerca de um terço de todos os entrevistados da pesquisa no mundo diz ter mitigado totalmente os riscos associados à convergência de tecnologia operacional e TI ou os riscos decorrentes do aumento do uso da Internet das Coisas.

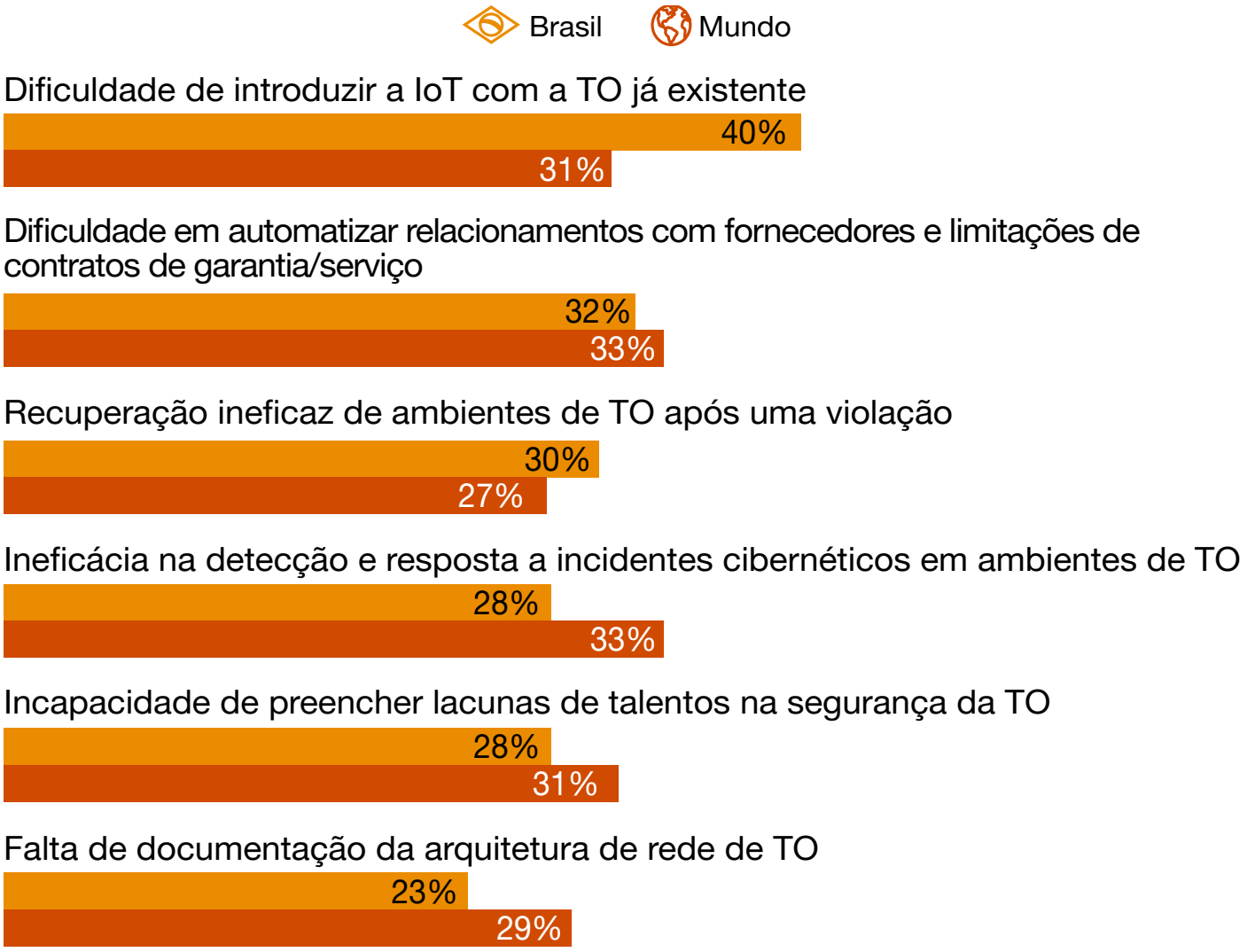
Outra área de preocupação para COOs e CROs é a segurança da tecnologia operacional. Com a sofisticação das tecnologias e soluções de tecnologia operacional – como o uso de inteligência artificial e aprendizado de máquina para aumentar a automação em fábricas, por exemplo – as organizações enfrentam dificuldades para manter suas operações seguras e protegidas.

Não são apenas os CROs e COOs que veem esses desafios. CISOs e CIOs também estão cientes deles. Há, no entanto, diferenças no que cada um considera o maior obstáculo para ter operações modernas e totalmente seguras.

- Ambos os grupos dizem que ter soluções tecnológicas inadequadas é o principal obstáculo para melhorar a tecnologia operacional. Eles também querem soluções que abordem especificamente a segurança dessa área.
- Para CISOs/CIOs, o principal obstáculo vem do uso de software desatualizado e de ferramentas de gerenciamento de vulnerabilidades. Ao todo, 27%, incluindo os CROs, dizem que isso é um problema.
- Ao mesmo tempo, os CROs/COOs acham que é necessária uma abordagem mais ampla para o risco cibernético de tecnologia operacional – que considere não apenas os riscos comerciais e financeiros, mas também os de saúde, segurança e meio ambiente. Para eles, o fato de essas preocupações não estarem recebendo a mesma atenção tem um papel primordial em dificultar as melhorias em tecnologia operacional.

Visão de CISOs, CIOs, CTOs

P: Quais são os desafios mais importantes para melhorar a tecnologia operacional em sua organização? Classifique os cinco primeiros.



Visão de CROs e COOs

Mundo

Recursos insuficientes para embasar as estratégias de gerenciamento de riscos de TI e TO da nossa empresa

Dificuldade em automatizar relacionamentos com fornecedores e limitações de contratos de garantia/serviço

Ineficácia na detecção e resposta a incidentes cibernéticos em ambientes de TO

Falta de responsabilidade claramente definida pela segurança de TI e TO

Recuperação ineficaz de ambientes de TO após uma violação

Incapacidade de preencher lacunas de talentos na segurança da TO

Falta de documentação da arquitetura de rede de TO

Dificuldade de introduzir a IoT com a TO já existente

Mensagem aos COOs

Com a digitização das operações corporativas, você reconhece a importância de trabalhar com equipes de cibersegurança para manter tudo seguro – e de fazer mais para compensar as deficiências entre parceiros e fornecedores terceirizados.

Suas equipes de risco, auditoria interna e conformidade talvez já estejam trabalhando com equipes de cibersegurança em várias tarefas cibernéticas: metade dos CROs/COOs no mundo diz que essas equipes monitoram e priorizam os riscos regularmente; um terço faz isso às vezes.

Esse trabalho em equipe está valendo a pena: 79% dos entrevistados disseram que sua equipe cibernética fez progressos na proteção da tecnologia operacional durante o ano passado. Quase 75% dizem ter visto uma melhor colaboração entre equipes de cibersegurança e de tecnologia operacional – certamente não é coincidência.

Mas os ataques à cadeia de suprimentos e à tecnologia operacional não estão entre as principais ameaças prováveis, o que pode criar uma certa complacência. Permaneça vigilante: vimos este ano o que pode acontecer quando as empresas baixam a guarda em relação à cadeia de suprimentos de software, e os ataques à tecnologia operacional estão aumentando. Agentes de ameaças cibernéticas que buscam formas de entrar em sistemas geralmente visam o ponto de menor resistência; não deixe sua área ser esse ponto.

Trabalhe ativamente com o CISO para que suas equipes colaborem nas questões sobre tecnologia operacional e segurança da cadeia de suprimentos, desde tarefas diárias, como monitoramento, até aquelas mais abrangentes, incluindo governança. Pergunte como você pode aumentar a resiliência a perturbações ou atrasos em sua cadeia de suprimentos, assim como a ataques aos sistemas de tecnologia operacional. E trabalhe com seu CIO para estabelecer um processo de envio de planos de gerenciamento de riscos cibernéticos sempre que fizer uma grande mudança em suas operações.

CROs e CISOs respondem ao risco com resiliência

“Risco” é a palavra de ordem na área cibernética hoje. Cada vez mais, as equipes de cibersegurança estão trabalhando em conjunto com as de riscos, auditoria interna e conformidade, um sinal de que a segurança cibernética está ocupando seu devido lugar como prioridade de gerenciamento de riscos corporativos.

Um número crescente de CROs, diretores de auditoria (CAEs) e diretores de conformidade reconhece que cibernética significa negócios. No mundo, metade dos entrevistados disse que as equipes cibernéticas estão “sistematicamente” monitorando e priorizando riscos em conjunto com essas outras funções. Aproximadamente outro terço faz isso algumas vezes.

No mundo:

50% **Monitoram riscos sistematicamente**

50% **Priorizam riscos**

49% **Têm um entendimento geral de como os riscos cibernéticos se encaixam no gerenciamento de riscos corporativos**

49% **Relatam eventos ao conselho**

48% **Respondem a ataques cibernéticos e violações em conjunto**

45% **Aplicam um modelo comum de governança de dados**

44% Desenvolvem uma visão comum dos riscos e ameaças em todo o ecossistema

44% Quantificam riscos

43% Fornecem aos líderes das unidades de negócios (responsáveis pelos riscos) as ferramentas para gerenciar melhor os riscos nas linhas de frente/operações

41% Aplicam um modelo comum de governança digital

40% Seguem um modelo operacional para a divisão de responsabilidades entre funções de risco e cibernéticas

Aqueles que têm uma violação no histórico de sua empresa tendem muito mais a fornecer sistematicamente uma resposta conjunta a invasões cibernéticas – 50%, em comparação a 38% das empresas não violadas no mundo.

A abordagem “um por todos, todos por um” ao risco cibernético não acontece com tanta frequência como pode parecer à primeira vista. Apenas 7% no mundo dizem que as equipes cibernéticas trabalham sistematicamente com outras funções de riscos em todas as atividades relacionadas a riscos. Os CROs/COOs têm trabalho a fazer nessa área.

CROs e COOs tendem a aplaudir o desempenho das equipes cibernéticas e de privacidade de suas organizações. Quase metade diz que essas equipes estão indo incrivelmente bem no atingimento de metas importantes, como a implementação de controles para evitar sérias disrupções – o que é fundamental para a resiliência dos negócios. No entanto, apenas 5% dos CROs/COOs acham que as áreas de cibersegurança e privacidade atendem a todas as expectativas “de maneira excepcional”.

Visão da liderança

Robson Costa
CISO da Azul Linhas Aéreas

Resiliência é o quanto somos velozes para recuperar um ambiente depois de uma disrupção. É imprescindível trabalhar com outras áreas da organização, além da segurança da informação. Todos os setores devem estar preparados para o momento crítico da crise, colocando o tema a todo momento no Comitê de Segurança.

Um grande desafio é encontrar o equilíbrio entre o que vai ao mercado e o que vamos considerar como proteção do ambiente, ou seja, ter a visibilidade de que um risco está presente a todo momento. Há débitos técnicos que devem ser considerados na ação que a companhia tomará, que muitas vezes tem uma data para acontecer, como o evento da semana *Black Friday*. Com segurança da informação, a companhia é colocada em um posicionamento de risco e incidentes, enquanto os produtos estão à venda. É importante ter a área de segurança junto com a de negócios, dividindo informações em tempo real com os executivos, expondo os riscos e informando como é o trabalho de mitigação. A partir do momento que o negócio está sob controle, torna-se mais simples.

O executivo é um grande acelerador da cultura de segurança da informação. A empresa tem que conseguir tratar a comunicação desse tema de uma forma que os todos consigam entender facilmente. O diálogo constante é essencial, é a melhor forma de se manter alerta nas questões que ocorrem dentro e fora da empresa. É preciso melhorar a observação dos incidentes vinculados aos negócios, ter um ecossistema em que se consiga compartilhar informação sobre eles e criar critérios de proteção.

Testes de resiliência em 2023

“A vida é o que acontece enquanto você faz outros planos”, diz o ditado. Isso também vale para os negócios.

Resiliência significa ser capaz de permanecer no caminho certo mesmo quando surgem problemas inesperados: um ataque cibernético catastrófico, uma recessão global, uma nova crise sanitária ou o ressurgimento da covid-19 e a inflação subindo.

Essas são as principais preocupações de nossos entrevistados para os próximos 12 a 24 meses. Mas poucos parecem prontos para lidar com elas facilmente.

É preciso adotar uma abordagem que envolva “todos os riscos” para identificar fontes de disrupção diante do ambiente de risco atual. No entanto, apenas 7% dos altos executivos no mundo dizem que estão adotando abordagens verdadeiramente integradas e holísticas para lidar com as cinco principais capacidades que definem a resiliência.

A boa notícia para os CROs/COOs é que 62% no mundo estão tratando o risco de forma holística. Mas em todas as outras áreas – resposta a incidentes, continuidade de negócios, recuperação de desastres – aproximadamente metade das organizações parece tratar cada violação como um caso isolado, em vez de aplicar as lições aprendidas com as várias competências essenciais de resiliência.

“Em 2023, a Azul trabalhará fortemente a questão do mapeamento mais rígido do ambiente e faremos uma revisão com nossos parceiros, uma vez que é imprescindível que estejam envolvidos. Temos várias empresas com SaaS (sigla em inglês para *Software* como Serviço), que precisam estar nesse contexto”, diz Robson Costa.

Fragmentada ou expansiva: qual é sua abordagem para a resiliência organizacional?

P: Para cada par de afirmações, qual delas melhor descreve a abordagem e a capacidade de resiliência cibernética atual da sua organização?

Brasil

Leva em conta sistemas e operações críticos e de alta prioridade necessários para a continuidade das operações — 55%

Leva em conta elementos secundários e terciários, não apenas sistemas e processos críticos e de alta prioridade, dos quais a organização depende — 45%

Tem uma postura reativa a disrupções, invocando planos após o incidente e concentrando-se na recuperação para retornar às operações de negócios após uma falha ou incidente — 45%

Adota uma abordagem proativa e preventiva, assumindo que os incidentes ocorrerão e incorporando capacidades de resiliência para suportar uma possível disrupção — 55%

Aborda a recuperação e a continuidade dos negócios de forma independente com equipes individuais de plataforma e serviço — 43%

Coordena e integra formalmente a continuidade dos negócios/recuperação de desastres, gerenciamento de crises, preparação para incidentes/resposta e inteligência de ameaças — 57%

Concentra-se em cenários isolados de risco e em como abordar a recuperação para aquela disrupção específica — 39%

Desenvolve uma ampla compreensão dos riscos que as empresas enfrentam atualmente e de como continuar as operações em meio a riscos simultâneos em toda a empresa — 61%

Usa planos e processos individuais predefinidos projetados para responder a disrupções específicas — 33%

Promove um modelo operacional integrado e ágil que pode dar conta de uma série diversificada de eventos disruptivos — 67%

Mundo

Leva em conta sistemas e operações críticos e de alta prioridade necessários para a continuidade das operações

Leva em conta elementos secundários e terciários, não apenas sistemas e processos críticos e de alta prioridade, dos quais a organização depende

Usa planos e processos individuais predefinidos projetados para responder a disrupções específicas

Promove um modelo operacional integrado e ágil que pode dar conta de uma série diversificada de eventos disruptivos

Aborda a recuperação e a continuidade dos negócios de forma independente com equipes individuais de plataforma e serviço

Coordena e integra formalmente a continuidade dos negócios/recuperação de desastres, gerenciamento de crises, preparação para incidentes/resposta e inteligência de ameaças

Tem uma postura reativa a disrupções, invocando planos após o incidente e concentrando-se na recuperação para retornar às operações de negócios após uma falha ou incidente

Adota uma abordagem proativa e preventiva, assumindo que os incidentes ocorrerão e incorporando capacidades de resiliência para suportar uma possível disrupção

Concentra-se em cenários isolados de risco e em como abordar a recuperação para aquela disrupção específica

Desenvolve uma ampla compreensão dos riscos que as empresas enfrentam atualmente e de como continuar as operações em meio a riscos simultâneos em toda a empresa

Base: 3.522 (Mundo) | 109 (Brasil)

Mensagem aos CROs

Os cenários de 2023 exigem que a alta administração e o conselho trabalhem juntos.

As violações são inevitáveis. Uma boa resposta – que limita bastante os danos que os agentes de ameaças podem causar – é, em grande parte, resultado do trabalho feito por você para estabelecer uma base cibernética forte e resiliente.

Cada vez mais, as autoridades financeiras de todo o mundo colaboram para testar a resiliência das instituições financeiras. E a orientação e fiscalização regulatória começam a se expandir para além dos serviços financeiros.

Você, em parceria com os CISOs, deve defender o CEO e o conselho: a verdadeira resiliência organizacional requer muita coordenação entre todos os integrantes da alta administração, e eles precisam apontar o caminho.

Os CEOs podem precisar de um estímulo para sair da zona de conforto, especialmente se estiverem em estado de inércia. Eles talvez acreditem que não precisam agir porque a empresa já tem planos de gerenciamento de crises, continuidade de negócios ou recuperação de desastres. Mas até que ponto esses planos estão coordenados? A organização testou? A organização pode se recuperar dentro do prazo estabelecido como objetivo?

Reveja seu apetite ao risco para conhecer seus limites de resiliência – o significado específico de “resiliência” depende parcialmente da tolerância e do apetite ao risco de uma organização. Reveja os planos de crise, continuidade de negócios e recuperação de desastres e monte um plano de resiliência empresarial coeso. Fique em sintonia com os altos executivos para estabelecer uma abordagem coordenada que mantenha a empresa no caminho certo se, e quando, surgirem problemas.

A colaboração em segurança de dados e proteção de privacidade é urgente

As empresas estão aderindo ao uso de dados para entender melhor o que os clientes desejam e satisfazê-los. Os dados agora são parte integrante da transformação digital centrada no cliente.

Um terço dos CMOs, CDOs e CPOs no mundo diz que sempre usa dados para monitorar o *feedback* do cliente e criar experiências personalizadas. Mais de um quarto usa dados para encontrar segmentos mal atendidos e expandir seus negócios.

Para capturar valor duradouro dessa transformação, as empresas precisam processar e gerenciar dados e algoritmos de forma inteligente e eficiente. Ao mesmo tempo, devem abordar questões de ética pública e privacidade e cumprir os padrões regulatórios.

Mas quantas estão realmente levando a sério o consentimento dado pelo cliente e a privacidade dele? As abordagens de gerenciamento e governança de dados relatadas pelos altos executivos são reveladoras, mas não surpreendem.

Percentual de organizações que sempre coletam e usam dados de clientes para os seguintes objetivos

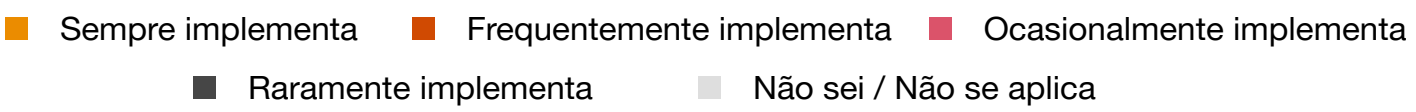
Mundo

Base: CDOs, CPOs, CMOs e altos executivos de funções voltadas para o cliente (412 no mundo)

A segurança e a privacidade dos dados são o calcanhar de aquiles de muitas organizações

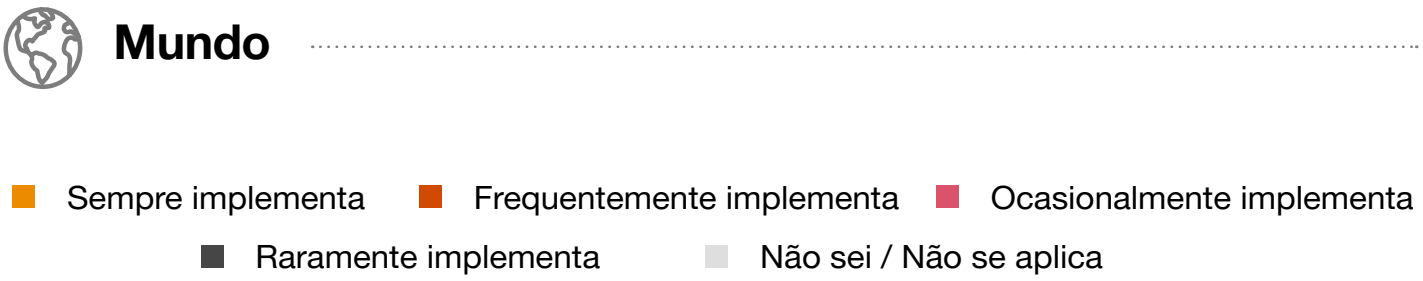
P: Em uma escala de 1 a 10, até que ponto sua organização mitigou os riscos de segurança cibernética associados a cada um dos itens a seguir nos últimos 12 meses?

Brasil



Base: 3.522 (Mundo) | 109 (Brasil)

Mundo



Base: 3.522 (Mundo) | 109 (Brasil)

Mais de 40% no Brasil dizem que podem usar dados de clientes sem consentimento expresso

Metade no Brasil e 54% no mundo nem sempre examinam todos os terceiros e parceiros com quem compartilham dados de clientes. Percentual semelhante pode lançar às vezes novos produtos e serviços sem uma avaliação de segurança e privacidade de dados.

Cerca de metade no Brasil (quase 60% no mundo) diz que nem sempre verifica padrões obscuros na maneira como projeta os aplicativos que seus clientes usam. Na prática, 61% dos executivos no Brasil (50% no mundo) dizem que a falta de segurança e governança é o principal obstáculo ao maior uso de dados para tomada de decisões – à frente de falta de acessibilidade de dados (57%), precisão (48%) e usabilidade (43%).

No mundo, menos de 30% dos CMOs, CDOs, CPOs e CISOs concorda fortemente que seu programa ou equipe cibernética e de privacidade:

27%	Dá a eles segurança na sua capacidade de nutrir confiança
25%	Ajuda a função de marketing a cumprir com eficiência e eficácia os regulamentos
24%	Permite que eles reflitam sobre quaisquer contrapartidas entre segurança e privacidade, de um lado, e crescimento lucrativo, de outro
24%	Dá a eles uma vantagem competitiva no mercado
21%	Dá a eles uma vantagem competitiva com os clientes

Mensagem para CDOs e CPOs

Você sabe que precisa fazer um trabalho melhor para controlar os dados e proteger a privacidade. Entre as empresas identificadas na pesquisa Market Winners 2022 da PwC, tratar os dados de clientes para conquistar mais confiança e compartilhar termos de privacidade de dados em uma linguagem mais amigável são os principais planos de investimento em cibersegurança para os próximos dois anos.

Os benefícios potenciais de uma estratégia de negócios que prioriza a privacidade são enormes: fidelidade do cliente, maior consentimento para usar seus dados e aumento da satisfação do cliente. Mas o risco de esforços desconexos também é enorme. As responsabilidades se sobrepõem entre os altos executivos – CISO, CDO e CPO – que podem liderar as tarefas de governança de dados e proteção de privacidade.

No entanto, as posições de CDO e CPO não existem na maioria das organizações. Apenas 21% das 2.500 maiores empresas do mundo têm um CDO no nível da alta administração. E essas empresas se concentram em alguns setores (seguros, bancos e mídia e entretenimento) e regiões (as Américas), de acordo com o nosso estudo de 2021 sobre diretores de dados. Globalmente, 42% dos CDOs não são membros da alta administração.

Como você pode controlar e proteger os dados de clientes para que a empresa continue a usá-los de forma privada e segura? Comece com os responsáveis pela governança. Formule seus objetivos e entenda as diferentes responsabilidades e as transferências de controle. O CDO, o CPO e o CISO devem criar e trabalhar em um manual que aborde todas as dimensões importantes de segurança e privacidade de dados, incluindo governança, acessibilidade e precisão.

CISOs e CHROs estão rompendo com velhos modelos

A perda de talentos é um problema crescente para 39% dos CISOs, CIOs e CTOs no mundo. Para outros 15%, ela atrapalha o progresso em relação às metas cibernéticas.

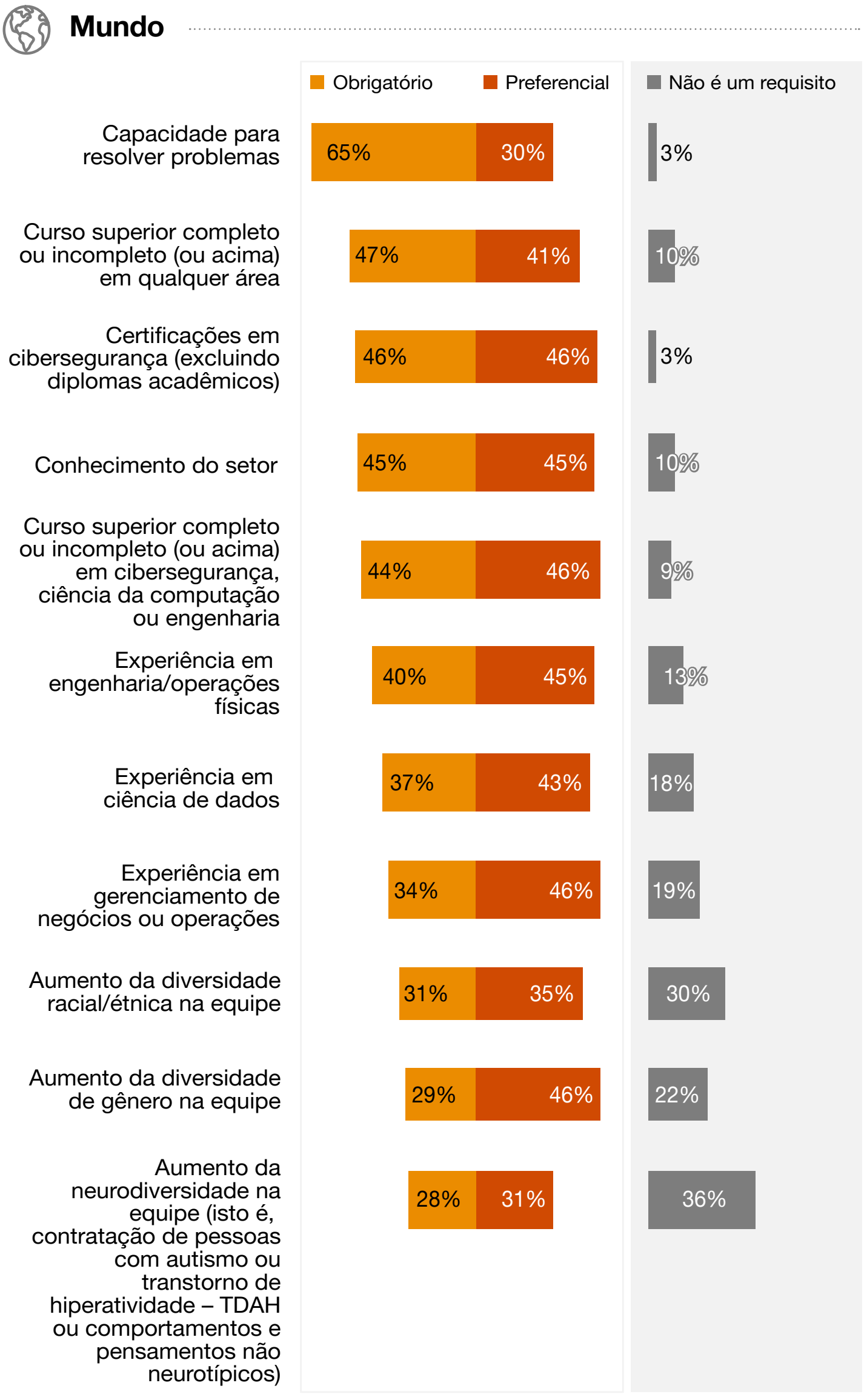
Possivelmente como resposta a esse problema, CISOs e CHROs estão rompendo com velhos modelos para poder preencher posições na área cibernética mais rapidamente e reter talentos.

Eles ampliam os parâmetros de recrutamento, reconhecendo que algumas características – como habilidades de resolução de problemas – são, no mínimo, tão importantes como certificações e diplomas técnicos.

Essa nova mentalidade pode ampliar o leque de candidatos. Um diploma de graduação (ou nível superior) em qualquer área já supera um diploma de graduação em cibernética, ciência da computação ou engenharia como requisito. Para cerca de 10%, ele nem sequer é necessário. Quando os candidatos se equiparam em todas as outras qualificações, a diversidade de gênero dita a preferência.

Ao contratar sua equipe de cibersegurança, até que ponto você considera as seguintes características em sua decisão final de contratação?

Mundo



Base: CDOs, CPOs, CMOs e altos executivos de funções voltadas para o cliente (412 no mundo)

Para eliminar a lacuna de talentos, os CISOs globais elegem três abordagens como as mais eficazes:

45% **Requalificação**

41% **Incentivos de contratação, como bônus de entrada**

36% **Serviços gerenciados para cibersegurança**

Protegendo seus serviços gerenciados

Entre as prioridades de investimento cibernético em 2023, os serviços de segurança gerenciados perdem apenas para a segurança de rede. Cerca de metade dos CISOs no mundo implementou totalmente uma série de medidas para gerenciar seus riscos em relação a terceiros.

Ao todo, 57% relatam ter desativado contas de provedores de segurança gerenciados (MSP, na sigla em inglês) que não estão mais gerenciando a infraestrutura. Além disso, 45% impõem a autenticação de múltiplo fator em todos os serviços e produtos. Mas ainda há trabalho a fazer: apenas 2,2% implementaram todas as práticas de segurança que faziam parte da nossa enquete.

As empresas estão encontrando maneiras de usar cada vez mais serviços gerenciados com segurança

P: Pensando no uso de serviços gerenciados de cibersegurança, até que ponto sua empresa implementou as seguintes medidas para gerenciar os riscos associados ao uso de pessoal externo para preencher lacunas em seus talentos e recursos de cibernética?

Mundo

Base: 278 entrevistados que selecionaram serviços gerenciados como uma das principais abordagens eficazes para solucionar a lacuna de talentos cibernéticos.

Mensagem aos CHROs

Enquanto a rotatividade de funcionários aumenta em vários mercados, os temores de recessão deixam as empresas ansiosas em relação a seus planos de contratação. Em meio à incerteza, elas podem adiar iniciativas, especialmente quando sabem que precisam tentar algo novo para evitar a crise marcada por fenômenos de demissão voluntária em massa descritos como “grande demissão” e “demissão silenciosa”.

Os CISOs e executivos das áreas de risco devem ajudar os CHROs a avaliar os efeitos cumulativos e os riscos operacionais em cascata da perda de talentos. Independentemente das soluções criativas adotadas para reter e contratar talentos, os altos executivos também precisam ajudar a gerenciar os riscos de reputação.

Pergunte quais habilidades você realmente precisa ter em seu programa cibernético, atualize sua forma de recrutamento, dê incentivos aos talentos e ofereça trilhas de crescimento que os estimulem a ficar na empresa. A dependência da organização em relação a serviços gerenciados e outros recursos externos só tende a aumentar. Adicione medidas de cibersegurança aos contratos.

“A capacidade de atrair e reter os melhores talentos é uma das tarefas mais importantes dos líderes de segurança cibernética hoje. É preciso entender bem as necessidades cibernéticas mais importantes do negócio e saber incentivar e medir o desenvolvimento de talentos com mentalidade mais de transformação para enfrentar desafios do que de manutenção do status quo existente.”

Maressa Juricic
Sócia da PwC Brasil

Cenários para exemplificar a necessidade de colaboração da liderança

Selecionamos três tipos de eventos cibernéticos mais preocupantes para os altos executivos. Embora a compreensão das táticas e técnicas nesses cenários possa exigir conhecimento técnico especializado, deve ficar claro que as consequências de cada um deles se estendem a áreas que os executivos de operações, finanças, dados e gerenciamento de riscos corporativos precisam abordar.

O plano de ação para cada executivo da alta administração não é rígido. Na verdade, ele ilustra os vários ângulos que devem ser abordados para elaborar uma resposta completa e duradoura a um ataque. Na área cibernética, um executivo não comprometido é um ponto vulnerável.

Preparado para diferentes cenários

De que forma os cenários que as organizações enfrentarão em 2023 testarão a capacidade dos altos executivos de trabalharem juntos em situações de crise para evitar disrupções nos negócios?

O ataque cibernético catastrófico é a preocupação número um quase unânime. Apenas os CFOs o classificam em segundo lugar, depois de recessão global e ao lado de temores em relação à outra crise sanitária, como o ressurgimento da covid-19.

Esses cenários exigem que a alta administração e o conselho trabalhem juntos, mas a cibersegurança pode ser o único problema que requer o engajamento de todos em busca de uma solução – e é também um problema sobre o qual se pode dizer que a organização tem algum controle.

Dois terços dos executivos no Brasil e no mundo consideram o cibercriminoso o agente de ameaças mais importante para sua organização no próximo ano. Os ataques cibernéticos são um negócio próspero e proporcionam carreiras lucrativas para os cibercriminosos.

Ferramentas de cibercrime como serviço e prontas para uso permitem que criminosos executem uma variedade de ataques lucrativos com mais facilidade. As operações de *ransomware*, por exemplo, agora são executadas como um negócio, o principal operador “aluga” o *ransomware* de afiliados. Os cibercriminosos podem implantar *ransomware* alugado em larga escala em vários alvos.

Desde 2021, o grupo PwC Threat Intelligence também observou o aumento de “*quartermasters* comerciais”, empresas que vendem ferramentas de crimes cibernéticos – como *spyware*, ataques de dia zero e outros tipos de *malware* – para mais clientes em muitos países.

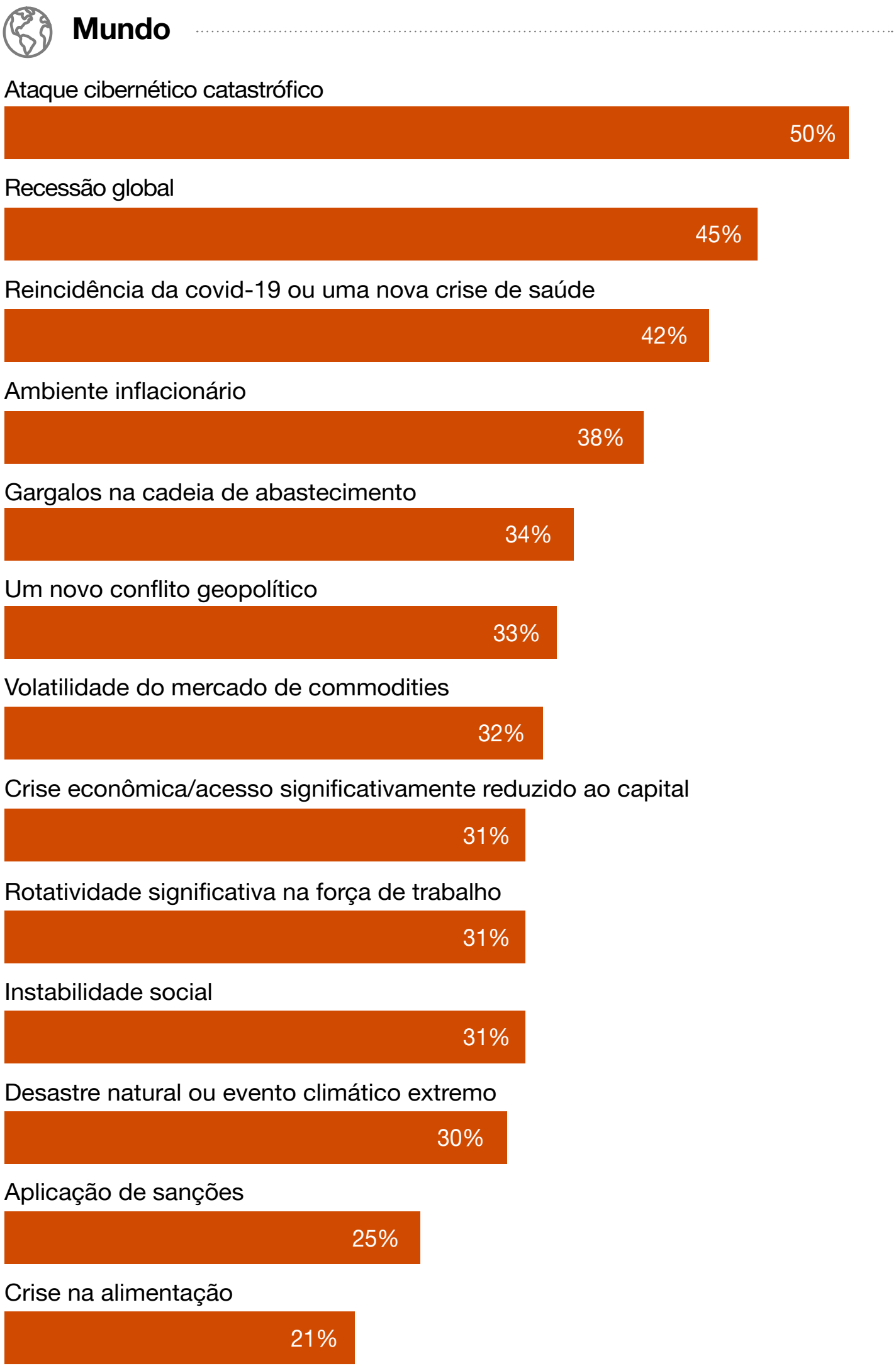
Essas operações globais tornam mais fácil iniciar uma vida de crimes cibernéticos: os agentes de ameaças não precisam mais desenvolver seu próprio *malware*. Ao mesmo tempo, o *malware* distribuído dificulta a identificação dos culpados.

Essas ferramentas disponíveis comercialmente são eficazes contra uma ampla gama de alvos, incluindo servidores públicos e executivos do setor privado. Organizações que consideram esses tipos de ameaças como fora de seu perímetro precisam rever sua posição.

Ataque cibernético lidera uma ampla gama de ameaças percebidas

P: Pensando nos riscos gerais para sua organização nos próximos 12 a 24 meses, classifique os cinco principais cenários que você está incorporando a seus planos de resiliência organizacional.

Mundo



Cenário 1: ataques que exploram a nuvem

36%
no Brasil (38% no mundo) esperam ataques mais sérios via nuvem em 2023

A violação:

Os invasores exploram uma configuração incorreta no aplicativo hospedado na nuvem da empresa e roubam dados de usuários para vender no mercado negro.

Consequências:

Notificações dispendiosas para os titulares dos dados. Uma possível ação coletiva contra a empresa. Danos à reputação da empresa.

O que deu errado:

Segurança inadequada, nenhuma defesa em profundidade, erros de código, testes inadequados de código escrito e de biblioteca, dados criptografados incorretamente.

Como trabalhar em conjunto para uma melhor defesa:

- **CIO:** habilite o DevSecOps no desenvolvimento de aplicativos e testes completos de pré-lançamento. Corrija configurações incorretas de usuários e implantações automatizadas.
- **CISO:** estabeleça e aplique políticas e procedimentos para proteger aplicativos, testes de vulnerabilidade e penetração, *patches* regulares, monitoramento contínuo de conformidade e monitoramento de eventos e incidentes de segurança.
- **CTO:** exija que provedores de serviços em nuvem e terceiros forneçam *dashboards* e ferramentas para detectar configurações incorretas em seus ambientes.
- **CDO:** verifique se seus aplicativos estão em conformidade com os requisitos de privacidade e se os dados do cliente são particionados e criptografados para melhor proteção. Coloque em prática soluções que criptografam dados em repouso, em trânsito e durante o uso.

Cenário 2: ataques à tecnologia operacional

39%
no Brasil (29% no mundo) esperam um aumento nos ataques à tecnologia operacional

A violação:

Um sistema de produção é afetado por um evento de *ransomware* devido a vulnerabilidades em sistemas operacionais legados.

Consequências:

A produção é interrompida quando os sistemas afetados são desligados para evitar que os danos se espalhem. Os impactos se disseminam pela cadeia de suprimentos.

O que deu errado:

Hackers exploram vulnerabilidades não corrigidas para injetar *ransomware*. As vulnerabilidades exploradas já haviam sido corrigidas em sistemas corporativos, mas, como faltam recursos de gerenciamento, monitoramento e detecção de *patches* para os sistemas legados, as vulnerabilidades permaneceram não detectadas.

Como trabalhar em conjunto para uma melhor defesa:

- **CIO:** com o CISO e o CTO, mapeie convergências e interdependências críticas entre sistemas de TI e de tecnologia operacional.
- **CISO:** trabalhe com o CIO e o CTO para exigir a separação entre a TI e a tecnologia operacional, desenvolva uma zona de destino segura que impeça o acesso direto à tecnologia operacional e treine os funcionários em funções adequadas de acesso e resposta a incidentes.
- **CTO:** com o CISO e o CIO, crie um plano para aplicação de *patches* e monitoramento de *endpoints*.
- **CRO:** desenvolva metodologia para avaliar o risco cibernético no ambiente de tecnologia operacional. Inclua cenários e ensaie procedimentos de resposta a incidentes que associem os processos de resposta da TI e tecnologia operacional.
- **COO:** considere a cibersegurança no processo de aquisição de seus sistemas de controle industrial, na contratação de provedores de nuvem e na definição de contratos com provedores de serviços externos.

Cenário 3: *ransomware*

45%

dos executivos de segurança e TI esperam que os ataques de *ransomware* continuem aumentando

A violação:

Um médico empregado abre um documento em um e-mail de *phishing*, ativando *malware*.

Consequências:

Interrupção do serviço e desligamento quase completo das redes.

O que deu errado:

O software antivírus executou regras desatualizadas que falharam na detecção do *malware* incorporado no anexo malicioso. A falta de autenticação multifatorial permitiu que os invasores obtivessem acesso inicial. Sem serem notados na rede corporativa por semanas, os cibercriminosos realizaram o reconhecimento da rede e acabaram por comprometer uma conta de administrador de domínio, adquirindo privilégios elevados para lançar o *malware* que desligou grande parte da infraestrutura de TI principal e comprometeu *backups*.

Como trabalhar em conjunto para uma melhor defesa:

- **CEO:** apoie o treinamento de conscientização sobre segurança em toda a organização.
- **CIO:** revise as conexões entre os sistemas de TI e o ambiente de saúde.
- **CTO:** avalie a vulnerabilidade de dispositivos médicos em um cenário de ataque a dispositivos.
- **COO:** ajude o CIO e o CISO a dimensionar os efeitos na segurança do paciente em cenários semelhantes.
- **CISO:** elimine os *gaps* de segurança entre as operações de TI e de assistência médica.
- **CDO:** trabalhe com o COO, o CISO e o CPO para avaliar danos causados por roubo/corrupção de dados de clientes.
- **CRO:** faça testes de resiliência com equipes de crise e continuidade de negócios/recuperação de desastres.
- **CFO:** trabalhe com o CISO e o CIO nas divulgações para os reguladores e o público. Analise os gastos cibernéticos, incluindo seguro cibernético, com o CISO e o CIO, considerando as vulnerabilidades descobertas. Defina sua política de pagamento de *ransomware*.
- **Conselho:** obtenha informações sobre o exercício de simulação feito pela diretoria como preparação para um ataque de *ransomware*. Confirme quando o conselho será informado sobre um incidente cibernético ou ataque de *ransomware*.

Para ver um exemplo de revisão de um evento de *ransomware* pós-incidente, consulte: Ataque cibernético Conti no HSE.

Sobre a pesquisa

A pesquisa **Global Digital Trust Insights 2023** foi realizada com 3.522 executivos de negócios, tecnologia e segurança (CEOs, conselheiros, CFOs, CISOs, CIOs e integrantes da alta administração) em julho e agosto de 2022.

- As mulheres representam 31% da amostra.
- 52% dos entrevistados são executivos de grandes empresas (US$ 1 bilhão ou mais em receitas); 16% estão em empresas com receita de US$ 10 bilhões ou mais.
- Vários setores estão representados: produção industrial (24%), tecnologia, mídia, telecomunicações (21%), serviços financeiros (20%), varejo e mercados de consumo (18%), energia, serviços públicos e recursos (9%), saúde (5%) e governo e setor público (3%).
- Os entrevistados estão localizados em várias regiões: Europa Ocidental (31%), América do Norte (28%), Ásia-Pacífico (18%), América Latina (12%), Europa Oriental (5%), África (4%) e Oriente Médio (3%).

A **Global Digital Trust Insights Survey** era antes conhecida como Global State of Information Security Survey (GSISS).

A PwC Research, o centro de excelência global da PwC para pesquisa e insights de mercado, realizou esta pesquisa.

Contatos

Eduardo Batista
Sócio e líder de *Cybersecurity*
eduardo.batista@pwc.com

Maressa Juricic
Sócia
maressa.juricic@pwc.com

Fernando Mitre
Sócio
fernando.mitre@pwc.com

Rafael Cortes
Sócio
rafael.cortes@pwc.com

Magnus Santos
Sócio
magnus.santos@pwc.com

Joana Mendes
Sócia
joana.mendes@pwc.com

Larissa Escobar
Sócia
larissa.escobar@pwc.com

Edgar D'Andrea
Sócio
edgar.dandrea@pwc.com

pwc

www.pwc.com.br

PwC Brasil @PwCBrasil PwC Brasil @PwCBrasil PwC Brasil @PwCBrasil