Resiliência cibernética

Como superar os desafios diante da expansão dos ataques

Pesquisa Global Digital Trust Insights 2025

pwc

Resultados da DTI 2025

Apenas 2%

dos participantes no mundo adotaram ações de resiliência cibernética em todas as áreas de sua organização.

Menos de 50%

dos CISOs no Brasil e no mundo estão extremamente envolvidos em atividades relevantes de negócios.

As regulamentações de cibersegurança ajudaram

89%

das organizações no Brasil. E 78% no mundo.

As empresas precisam fortalecer sua resiliência cibernética diante da expansão da superfície de ataque causada por avanços em inteligência artificial (IA), dispositivos conectados e tecnologias de nuvem, além de um cenário regulatório em constante evolução.

Apesar da ampla conscientização sobre os desafios dessa empreitada, ainda existem vulnerabilidades importantes. Para proteger suas organizações, os executivos devem tratar a cibersegurança como prioridade constante na agenda corporativa, integrando-a a cada decisão estratégica e promovendo a colaboração entre os líderes executivos.

A **Pesquisa Global Digital Trust Insights 2025** da PwC, realizada com 4.042 executivos de negócios e tecnologia de 77 países, incluindo o Brasil, revelou deficiências importantes que as empresas precisam corrigir para alcançar a resiliência cibernética nas seguintes áreas:

Implementação da resiliência cibernética

Apesar das crescentes preocupações com os riscos cibernéticos, apenas 2% dos executivos globais entrevistados afirmam que suas empresas executaram ações de resiliência cibernética em todas as áreas avaliadas na pesquisa.

Preparação

As organizações se sentem menos preparadas para lidar com as ameaças cibernéticas mais preocupantes, como riscos relacionados à nuvem e violações de terceiros.

Participação dos CISOs

Apenas cerca de metade dos executivos no Brasil e no mundo dizem que seus CISOs estão extremamente envolvidos no planejamento estratégico, nos relatórios ao conselho e na supervisão das implantações tecnológicas.

Confiança no *compliance* regulatório

CEOs e CISOs/CSOs apresentam níveis diferentes de confiança na capacidade da empresa de cumprir as regulamentações, especialmente em relação à IA, resiliência e infraestrutura crítica.

Medição do risco cibernético

Embora os executivos reconheçam a importância de medir o risco cibernético, globalmente menos da metade o faz de maneira eficaz e apenas 15% no Brasil e no mundo medem o impacto financeiro dos riscos cibernéticos de forma significativa.

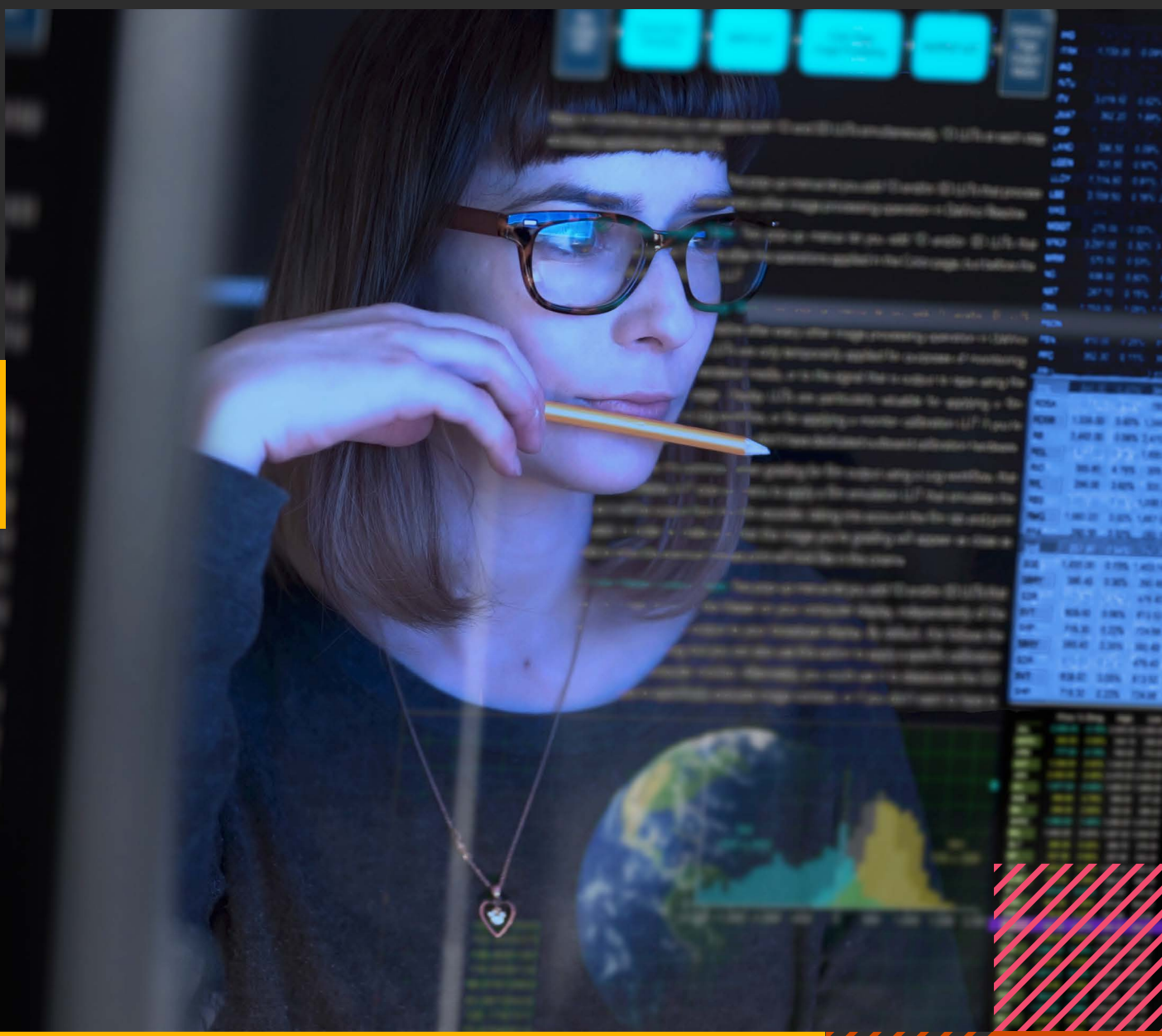
Tudo isso aponta para a necessidade de melhorar a colaboração entre os executivos da alta administração e fazer investimentos estratégicos para fortalecer a resiliência cibernética.

Ao abordar essas questões e tornar a cibersegurança uma prioridade de negócios, os executivos podem construir um futuro mais seguro. Os CISOs, especificamente, podem impulsionar esse processo ao compartilhar insights baseados em tecnologia e traduzir as prioridades cibernéticas em termos empresariais (custo, oportunidade, risco).

Tecnologias disruptivas trazem ainda mais dinamismo para o setor de cibersegurança. Estamos lidando com a necessidade de mudar processos mais rapidamente para acompanhar a inovação dos negócios. O fortalecimento da resiliência cibernética da sua organização precisa ser uma prioridade em meio ao contexto de riscos relacionados à inteligência artificial, a tecnologias de nuvem e ao cenário regulatório que tem acompanhado a agilidade das novas tecnologias.”

Eduardo Batista,
sócio e líder de Cibersegurança e Privacidade

Conteúdo



Como enfrentar as ameaças cibernéticas: estratégia unificada de preparação

65%

dos executivos de tecnologia no Brasil classificam o risco cibernético como o mais importante a ser mitigado, em comparação com 46% dos executivos de negócios. No mundo, os percentuais são semelhantes: 66% x 48%.

Menos de 56%

dos brasileiros classificam os riscos relacionadas à nuvem como a ameaça cibernética que mais preocupa (42% no mundo).

Top 2

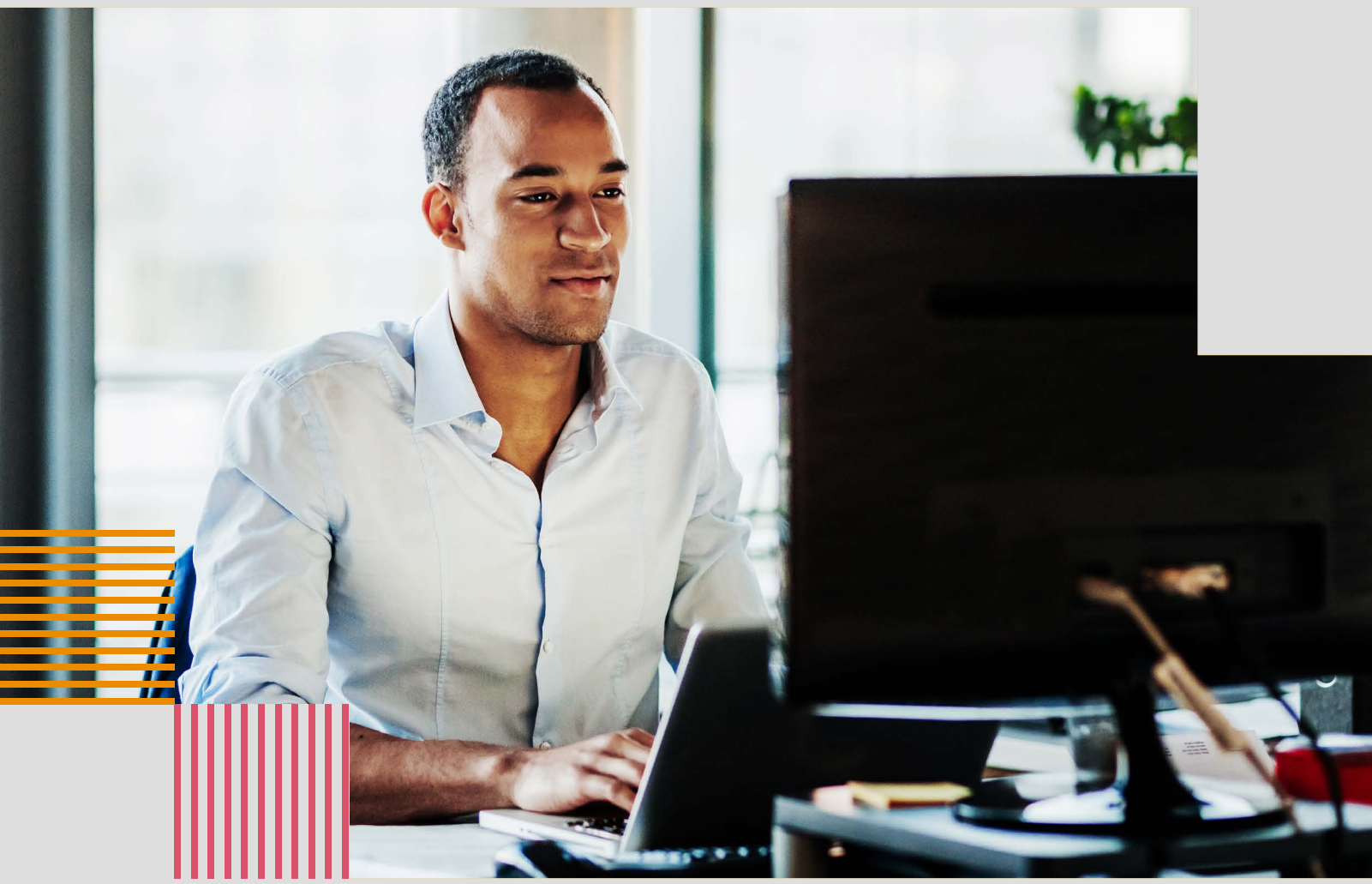
Os ataques relacionados à nuvem e a produtos conectados são aqueles que os executivos de segurança se sentem menos preparados para enfrentar.

À medida que o cenário de cibersegurança evolui, as organizações enfrentam ameaças cada vez mais voláteis e imprevisíveis. A expansão da superfície de ataque – impulsionada pela maior dependência de recursos como nuvem, IA, dispositivos conectados e terceiros – exige uma abordagem ágil e abrangente para garantir a resiliência. Alinhar as prioridades e a preparação organizacional é fundamental para manter a segurança e a continuidade dos negócios.

Despreparados para as ameaças mais preocupantes

As maiores preocupações das organizações são justamente aquelas para as quais elas estão menos preparadas. As quatro principais ameaças – relacionadas a nuvem, violações de terceiros, operações de *hack-and-leak* e ataques a produtos conectados – são também as que os executivos de segurança se sentem menos aptos a enfrentar. Essa deficiência ressalta a urgência de investimentos melhores e capacidades de resposta mais robustas.

Além disso, há uma diferença de percepção entre os executivos de segurança e o restante da organização, com CISOs e CSOs mais propensos a incluir o *ransomware* entre suas três principais preocupações. Isso reflete seu papel, mais focado em cibersegurança e TI, e seu maior entendimento das vulnerabilidades. É um cenário que reforça a importância de uma melhor troca de informações entre as lideranças para alinhar as prioridades.

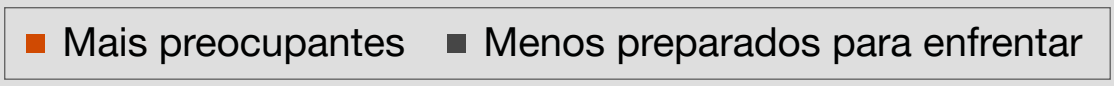


Preocupação com ameaças cibernéticas e a preparação para enfrentá-las

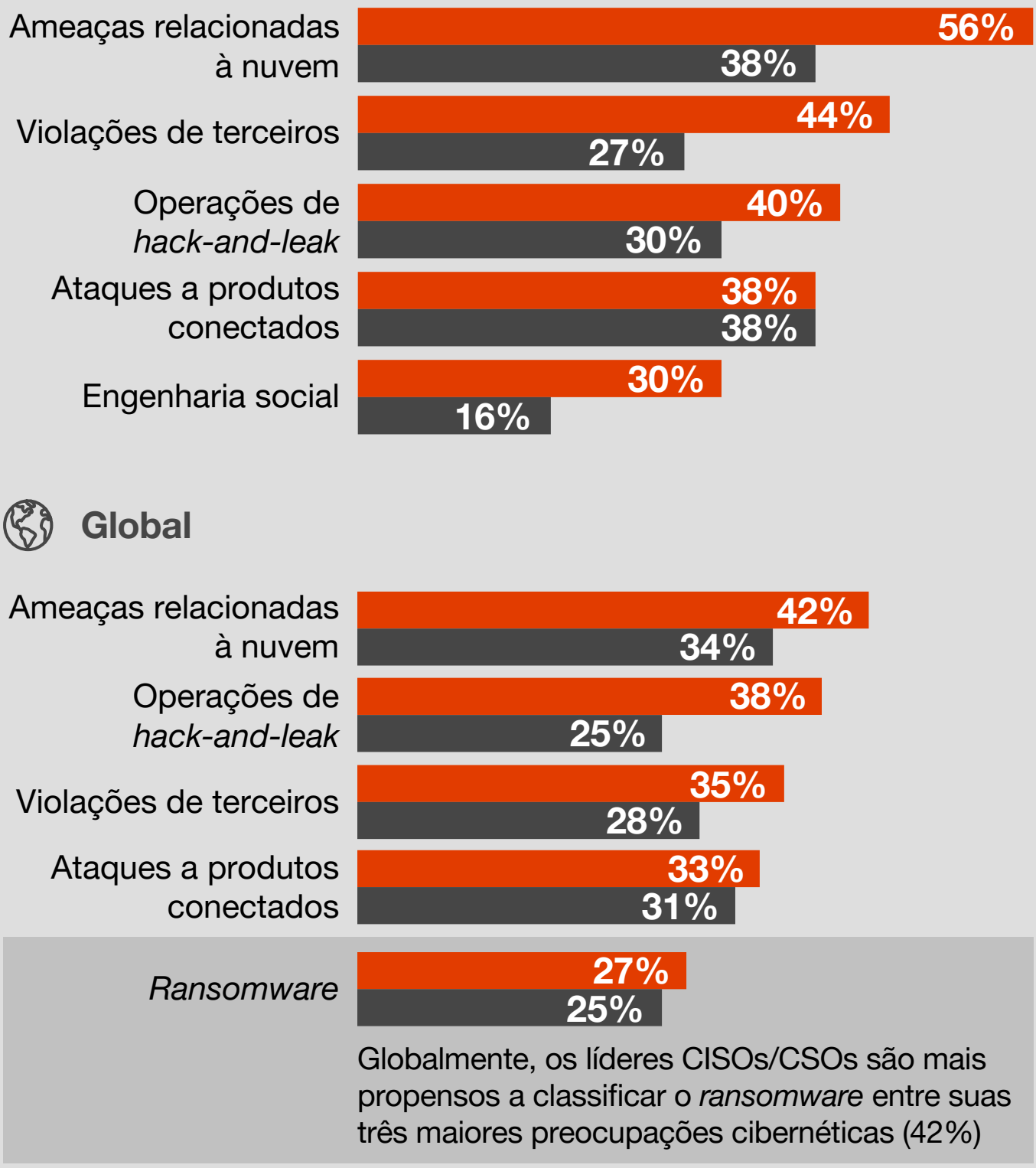
(% dos participantes que classificaram as alternativas entre as três primeiras)

Pergunta: nos próximos 12 meses, com quais das seguintes ameaças cibernéticas sua organização está mais preocupada (por exemplo, riscos para a marca, perda dos negócios ou disrupção dos negócios, *compliance*)? Selecione e classifique até três opções, sendo 1 a maior prioridade de mitigação.

Pergunta: Nos próximos 12 meses, quais das ameaças cibernéticas você acha que sua organização está menos preparada para enfrentar? Selecione e classifique até três opções, sendo 1 a área que sua organização está menos preparada para enfrentar.



Brasil



Global

Globalmente, os líderes CISOs/CSOs são mais propensos a classificar o *ransomware* entre suas três maiores preocupações cibernéticas (42%)

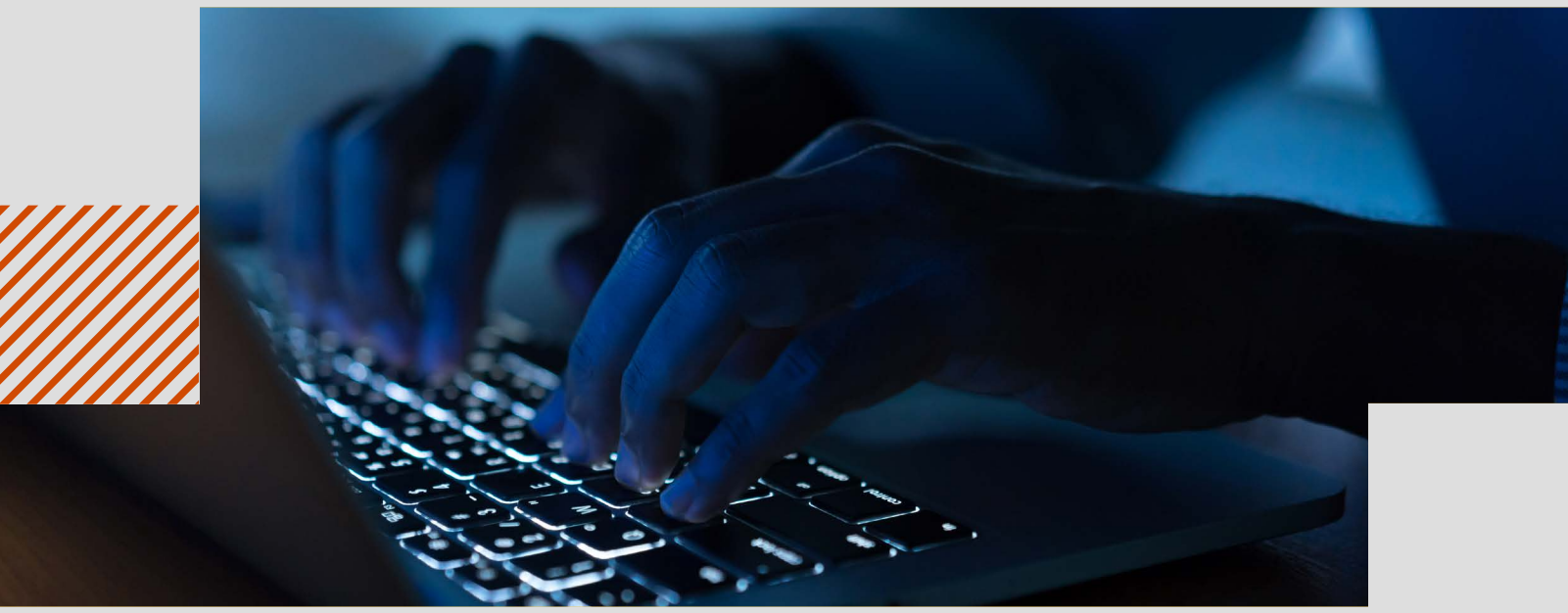
Alerta

Uma estratégia de investimento cibernético orientada por ameaças é indispensável. Priorize investimentos nos riscos cibernéticos mais urgentes e analise cuidadosamente como os recursos estão sendo alocados, considerando pessoas, processos e capacidades de defesa.

Descompasso estratégico: prioridades de negócios e tecnologia

Executivos de negócios e de tecnologia priorizam riscos diferentes. Enquanto os de negócios estão mais preocupados com a inflação, os de tecnologia classificam os riscos cibernéticos como sua maior prioridade – provavelmente devido à sua proximidade com o cenário de ameaças cibernéticas.

Mesmo assim, quase metade dos executivos de negócios ainda coloca os riscos cibernéticos entre suas três maiores preocupações, o que ressalta a importância crítica deles. Essa percepção comum representa uma oportunidade para os CISOs conectarem a agenda de cibersegurança à agenda de negócios.

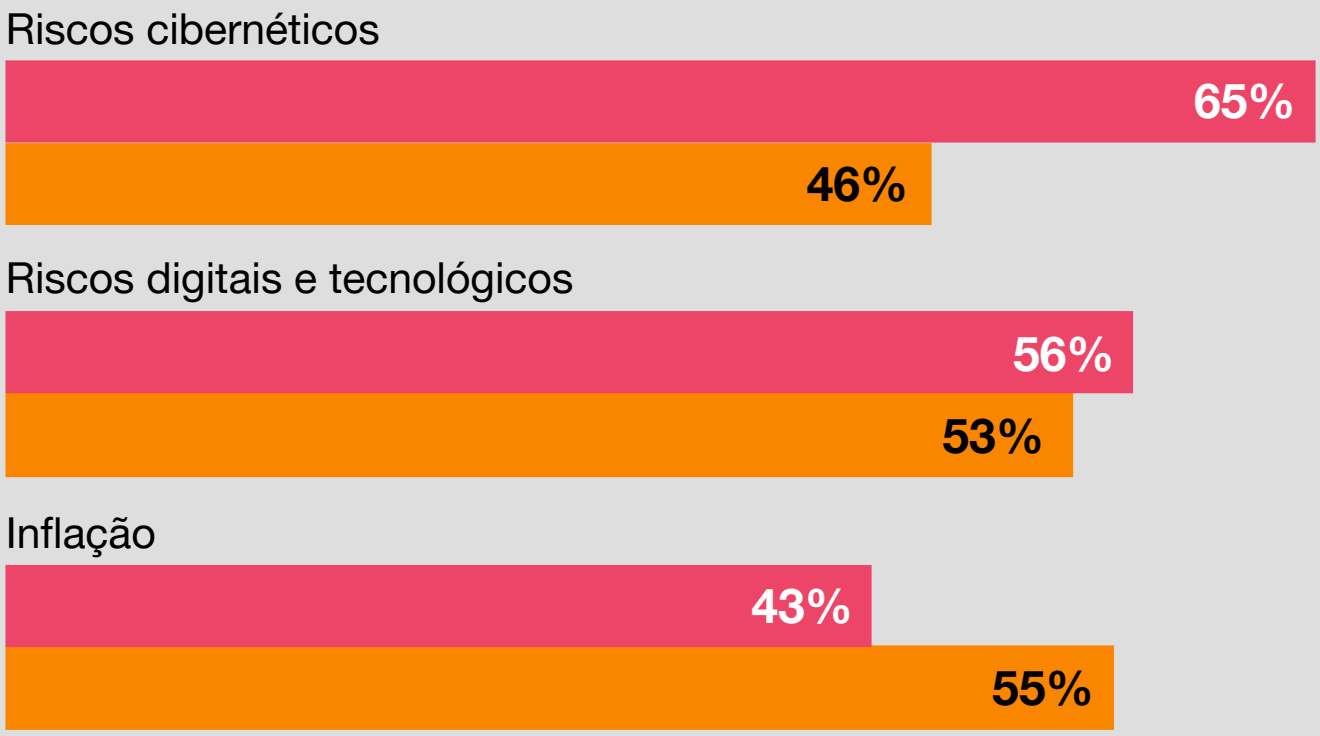


Prioridades de mitigação de riscos para líderes de negócios e de tecnologia

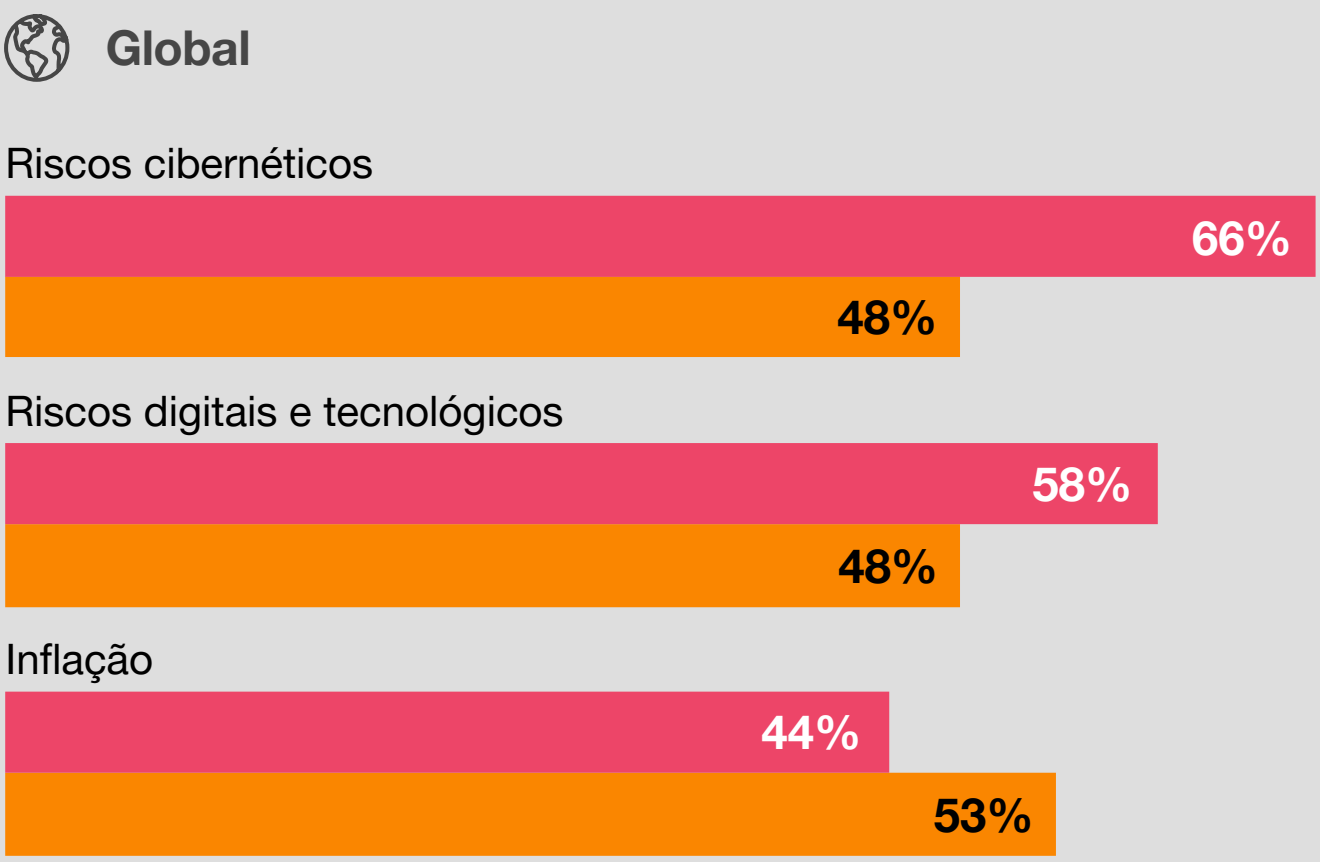
(% dos participantes que classificaram as alternativas entre as três primeiras)

Pergunta: quais dos seguintes riscos sua organização está priorizando para mitigação nos próximos 12 meses? Selecione e classifique até três opções, sendo 1 a maior prioridade para mitigação.

Brasil



Global



Alerta

Para os executivos de negócios e tecnologia, é hora de buscar alinhamento. Equilibre a priorização dos riscos cibernéticos com as pressões econômicas para ajudar a proteger os ativos e criar resiliência. Avaliações regulares entre as diferentes áreas garantirão que estratégia e prioridades permaneçam alinhadas.

Custo médio global de uma violação de dados supera US$ 3 milhões

No Brasil, 32% dos executivos afirmam que a violação de dados mais prejudicial dos últimos três anos custou à sua organização pelo menos US$ 1 milhão (no mundo, são 27%). Globalmente, o resultado é semelhante ao da pesquisa do ano passado em organizações de todos os tamanhos e na maioria das regiões e setores. No geral, estima-se que o custo médio de uma violação de dados seja de US$ 3,32 milhões.

As organizações de melhor desempenho no mundo – aquelas que relataram maior probabilidade de adotar de forma consistente práticas de cibersegurança de alta qualidade – tiveram menos incidências de violações de dados nos últimos três anos.

Essas organizações de alto desempenho geralmente são maiores e exibem rápido crescimento, com orçamentos de cibersegurança que devem aumentar 15% ou mais no próximo ano. Isso indica que a maturidade dos programas de cibersegurança e o aumento do financiamento estão correlacionados a uma maior resiliência.

Ação recomendada para a liderança

À medida que as organizações enfrentam um cenário de ameaças mais sofisticado, é importante que os executivos da alta administração assumam um papel proativo na avaliação dos riscos atuais e emergentes. Ao alinhar as estratégias de cibersegurança com os objetivos mais amplos do negócio, os executivos podem preparar melhor suas organizações para gerenciar riscos e fortalecer a resiliência.

CISO: enfatize para o restante da alta administração as ameaças que mais expõem o negócio a riscos, especialmente se for necessário redirecionar os investimentos.

CIO e CTO: com base em conversas com os executivos encarregados de riscos, avalie como determinadas ameaças podem comprometer a segurança da informação e da infraestrutura de maneira geral, e quais ameaças representam os maiores obstáculos à resiliência.

CFO: obtenha uma compreensão mais profunda do CISO e CRO sobre as principais prioridades de gestão e investimento em cibersegurança.

CEO: reúna-se regularmente com o CRO e CISO para entender os vetores de ameaça que mais preocupam. Garanta que esteja recebendo relatórios frequentes sobre os esforços atuais de mitigação de ameaças.

Conselho de administração: compreenda os principais riscos cibernéticos da organização e faça perguntas difíceis à gestão. Como os riscos estão sendo mitigados? Temos planos e recursos suficientes para abordar proativamente os riscos e responder caso um incidente ocorra?

Alerta

Priorize estratégias holísticas de mitigação de riscos que abranjam prevenção, detecção, resposta e recuperação. Compreenda os impactos mais amplos de uma violação – além do prejuízo financeiro – para desenvolver resiliência verdadeira.

Como equilibrar oportunidades e riscos das novas tecnologias

68%

dos executivos de segurança no Brasil dizem que a IA generativa aumentou sua superfície de ataque no último ano (67% no mundo).

85%

aumentaram seus investimentos em IA generativa nos últimos 12 meses (78% no mundo).

80%

aumentaram seus investimentos em gestão de riscos e governança de IA (72% no mundo).

Embora o rápido avanço da IA generativa esteja trazendo novas oportunidades em diversos setores, ele também leva a riscos de cibersegurança. Quando as organizações adotam a IA generativa e outras tecnologias emergentes, a alta direção deve tratar de vetores de ataque mais complexos e imprevisíveis, obstáculos de integração e a natureza ambivalente da IA generativa, que pode ser usada tanto para a defesa quanto para o ataque cibernético. Esses desafios estão acompanhados por relevantes questões legais e de dados, que podem dificultar a implementação e governança da IA generativa.

Uma superfície de ataque crescente

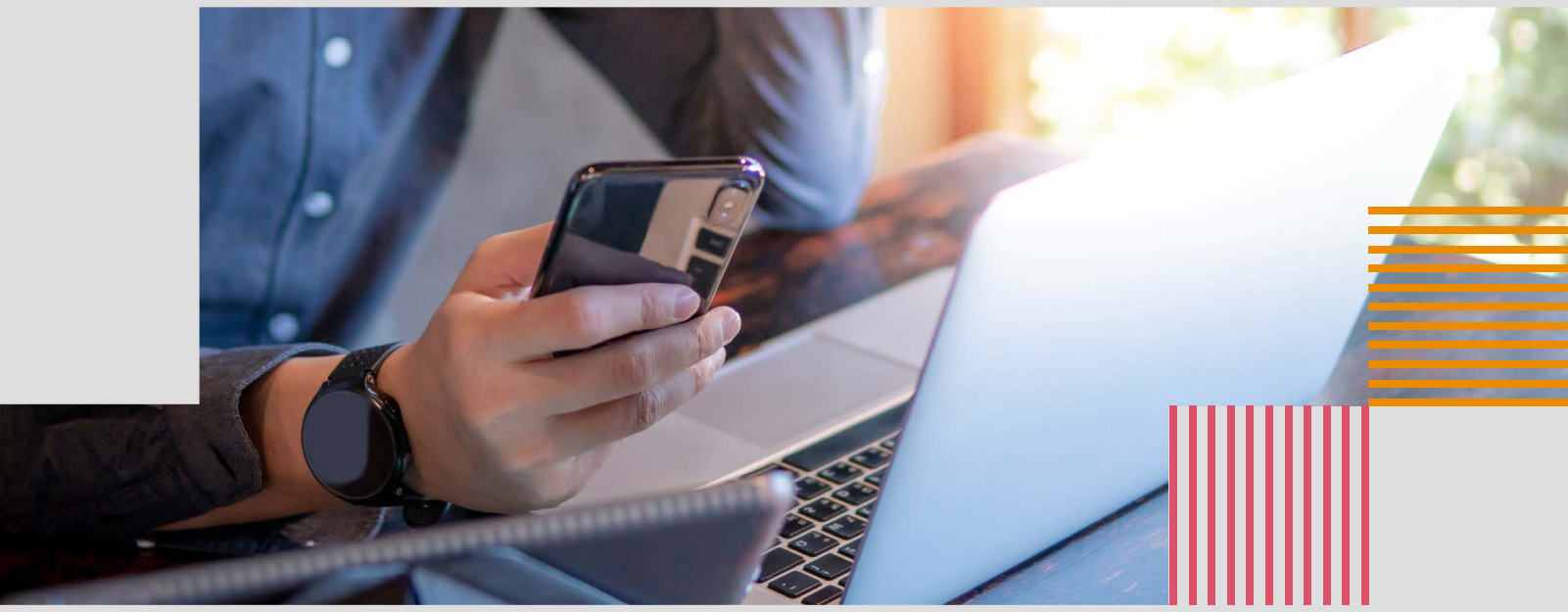
Executivos de segurança relatam que a IA generativa (68% no Brasil e 67% no mundo) e as tecnologias de nuvem (66% em ambos os recortes) ampliaram a superfície de ataque cibernético no último ano, tornando as empresas mais vulneráveis a ameaças sofisticadas.

A IA generativa também pode reduzir as barreiras de entrada para agentes de ameaças menos experientes, permitindo que eles criem ataques de *phishing* eficazes e *deepfakes* em grande escala. Isso está em linha com as conclusões da nossa 27ª Global CEO Survey, na qual 74% dos CEOs no Brasil (64% globalmente) concordam que a IA generativa provavelmente aumentará o risco de cibersegurança em suas organizações.

O uso da IA generativa também traz à tona preocupações sobre integridade de dados, privacidade e *compliance*, enquanto as empresas lidam com um cenário regulatório em mudança.

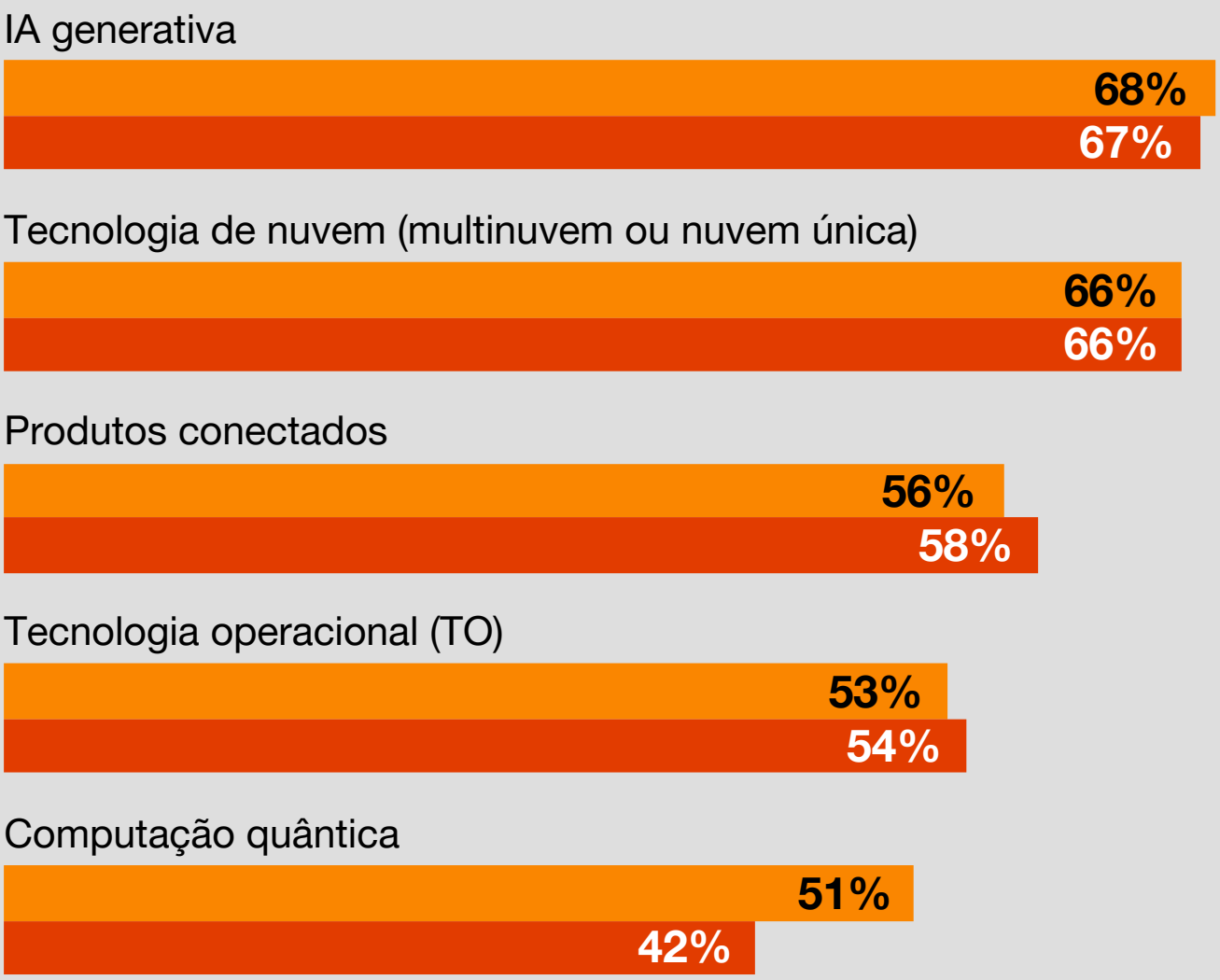
Outras tecnologias, como dispositivos conectados e tecnologia operacional (TO), também estão ampliando a superfície de ataque, com impacto em setores como produção industrial, saúde e energia.

O aumento da interconexão entre dispositivos torna a segurança desses sistemas cada vez mais desafiadora. Além disso, embora a computação quântica ainda esteja distante, 51% dos executivos de segurança no Brasil (42% no mundo) já relataram a necessidade de enfrentar vulnerabilidades decorrentes dessa tecnologia.



Tecnologias que afetam a superfície de ataque cibernético*

Pergunta: em que medida as seguintes tecnologias afetaram a superfície de ataque cibernético no ambiente de TI da sua organização nos últimos 12 meses? (respondida apenas por líderes de segurança).



Alerta

A avaliação contínua de novas vulnerabilidades, o investimento em medidas avançadas de segurança e o fortalecimento da colaboração entre as equipes de tecnologia, segurança, risco e jurídica são questões fundamentais. Ao se manterem preparadas para essas ameaças, as empresas podem proteger melhor seus ativos críticos e manter a confiança dos *stakeholders*.

*Porcentagem combinada dos participantes que selecionaram “aumento significativo” ou “ligeiro aumento”.

Usando a IA generativa para defesa cibernética: oportunidades e desafios

Embora a IA generativa esteja aumentando a superfície de risco a ataques cibernéticos para a maioria das organizações, os executivos também estão usando essa mesma tecnologia para defesa cibernética. As três principais maneiras de aproveitar a IA generativa são:

- detecção e resposta a ameaças;
- inteligência de ameaças; e
- detecção de *malware/phishing*.

No entanto, apesar dessas oportunidades, as organizações enfrentam vários obstáculos ao incorporar a IA generativa em suas estratégias de defesa cibernética.

Brasil	Global	
43%	39%	Dificuldade de integração com sistemas e processos existentes
40%	39%	Falta de confiança dos *stakeholders* internos na IA generativa
37%	38%	Controles internos e gestão de riscos insuficientes
35%	37%	Ausência de políticas internas padronizadas que regulem seu uso

Alerta

A IA generativa tem potencial para transformar suas defesas cibernéticas, mas isso só acontecerá se você superar os desafios de integração, confiança e governança, aplicando práticas responsáveis de IA. Caso contrário, você corre o risco de ficar para trás na corrida contra os agentes de ameaças.

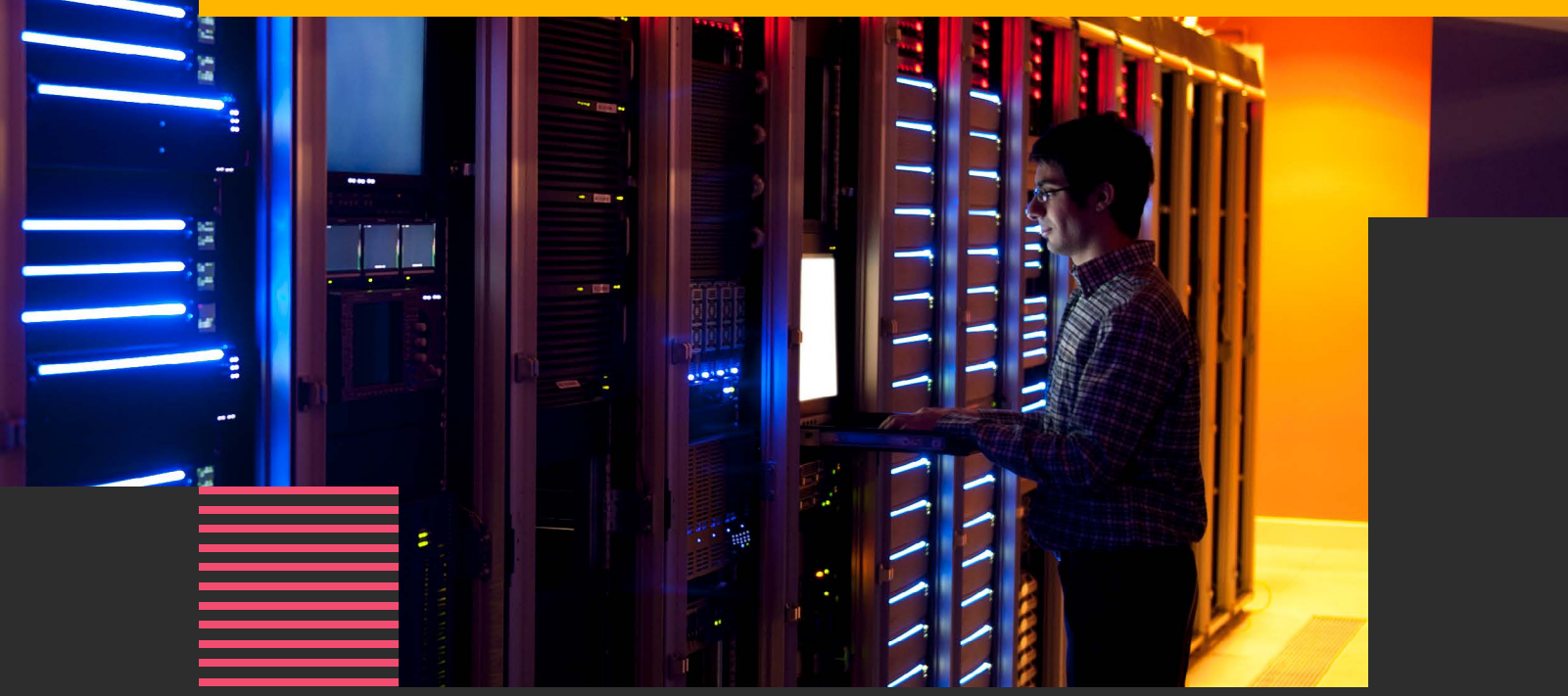
IA generativa lidera as prioridades de investimento em cibersegurança

Reconhecendo os riscos cibernéticos crescentes, 85% dos executivos brasileiros (78% no mundo) aumentaram seus investimentos em IA generativa, com foco especial em governança. Esse investimento ressalta a importância de gerenciar tanto as capacidades quanto os riscos da IA generativa.

As empresas também estão começando a investir na preparação para a era quântica. Mesmo que a adoção ainda leve alguns anos, já há uma necessidade crescente de desenvolver tecnologias resistentes à computação quântica e medidas de segurança pós-quântica para combater futuras ameaças que essa tecnologia pode representar se for mal utilizada.

Alerta

Investir em IA generativa é apenas o começo. Avance ainda mais aproveitando o potencial inexplorado de outras tecnologias, como soluções resistentes à computação quântica, para que suas defesas superem as ameaças em constante evolução.



Ação recomendada para a liderança

Com as tecnologias emergentes redefinindo o panorama da cibersegurança, é fundamental que os executivos da alta direção assumam um papel ativo em orientar suas organizações sobre as oportunidades e os riscos que essas inovações apresentam.

CISO: impulsione a padronização em todo o ambiente tecnológico para integrar a IA nas defesas cibernéticas. Aplique direitos de acesso individualmente para identificar possíveis vetores de ataque.

CIO e CTO: elabore uma avaliação de impacto da IA para orientar os executivos sobre as áreas nas quais o investimento e a implementação são mais estratégicos. Prepare as plataformas para garantir escalabilidade conforme o uso da IA generativa aumenta.

CFO: trabalhe em conjunto com o CISO para priorizar a segurança e a confidencialidade da proteção de dados financeiros.

CDO (diretor de dados): melhore seus protocolos de governança de dados e avalie os riscos de privacidade de dados em conformidade com as leis de privacidade e a orientação dos reguladores.

Diretor e assessor jurídico: colabore com outras equipes de riscos e conformidade para prevenir usos indevidos de dados e possíveis exposições legais.

Um mundo cibernético cada vez mais regulado: as empresas estão preparadas?

100%

dos brasileiros relatam que as regulamentações de cibersegurança incentivaram o aumento de seus investimentos em segurança cibernética nos últimos 12 meses (96% no mundo).

89%

acreditam que as regulamentações ajudaram a questionar, melhorar ou ampliar sua postura de segurança cibernética (78% no mundo).

13 p.p.

é a diferença de confiança entre CISOs/CSOs e CEOs globais em relação ao *compliance* com as regulamentações de IA e resiliência.

Os *frameworks* regulatórios exigem que as empresas passem a cumprir rapidamente uma crescente gama de requisitos. Um aumento nas novas regulamentações – Digital Operational Resilience Act (DORA), Cyber Resilience Act, AI Act, Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), Singapore Cybersecurity Act, entre outras – ressalta a urgência com que as organizações precisam alinhar suas práticas a essas expectativas cada vez maiores.

Ao enfrentar essas exigências, as empresas se deparam com uma diferença significativa de confiança entre CISOs/CSOs e CEOs sobre a viabilidade de alcançar um *compliance* total. Superar esses desafios é fundamental para desenvolver uma postura de cibersegurança sólida e em *compliance* com os requisitos, capaz de resistir ao escrutínio regulatório e às novas ameaças.

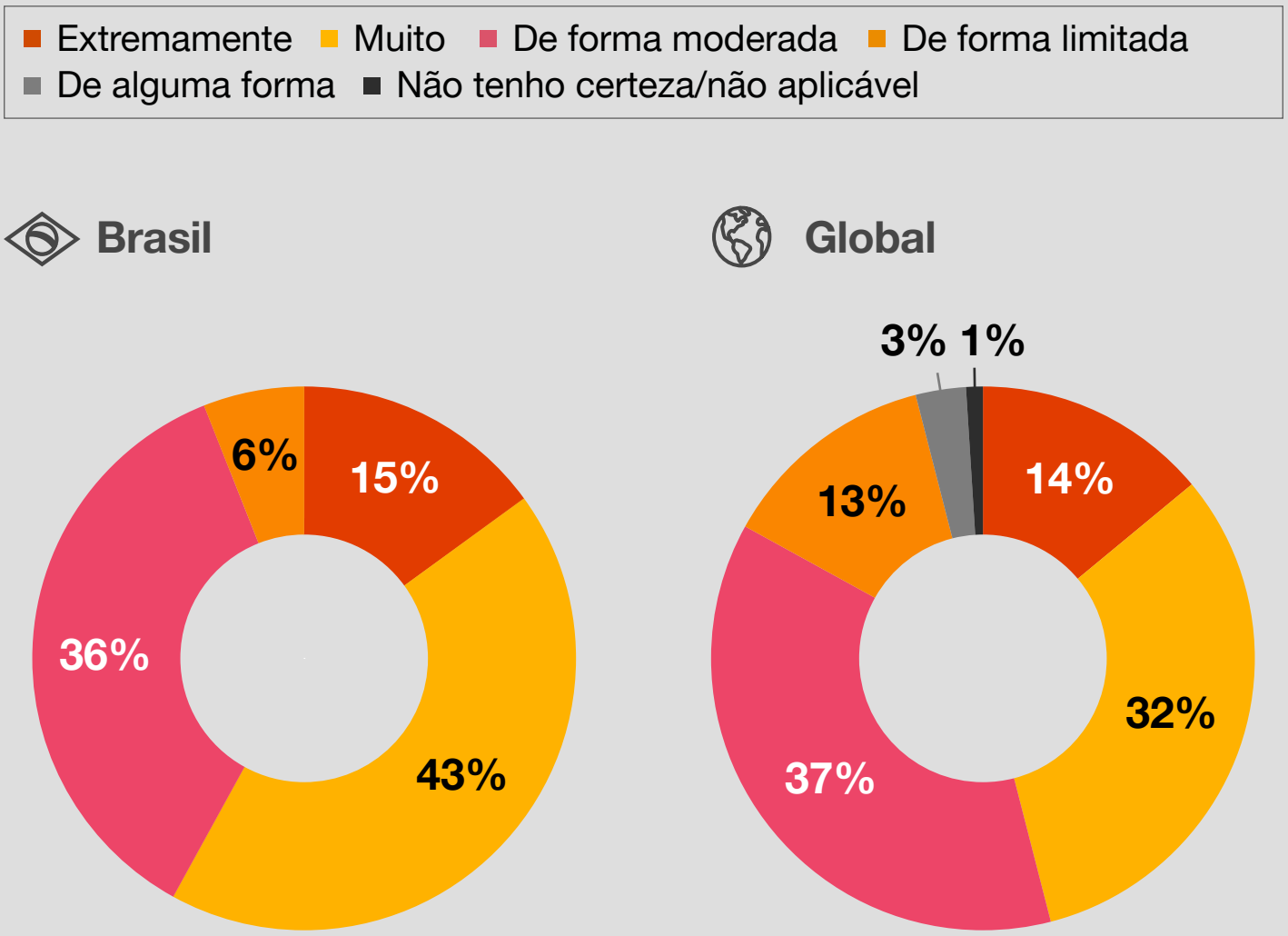
Regulamentações de cibersegurança estão impulsionando mudanças positivas

As regulamentações de cibersegurança estão se mostrando um importante fator de incentivo para investimentos em segurança cibernética, com 100% dos executivos brasileiros reconhecendo que as exigências regulatórias os levaram a melhorar suas medidas de proteção (96% no mundo).

Além disso, 89% acreditam que as regulamentações ajudaram a questionar, fortalecer ou ampliar suas práticas de cibersegurança (78% no mundo). Isso indica que, apesar dos desafios de *compliance*, as regulamentações estão ajudando a fortalecer as capacidades de cibersegurança em vários setores.

Impacto das regulamentações no aumento dos investimentos em segurança cibernética

Pergunta: em que medida, se houver, as regulamentações de cibersegurança aumentaram o investimento em cibersegurança da sua organização nos últimos 12 meses? (apenas líderes de segurança e CFOs).



Impacto positivo nas organizações

Pergunta: qual declaração, se houver, reflete melhor o impacto das novas regulamentações de cibersegurança em sua organização nos últimos 12 meses?

As regulamentações de cibersegurança **ajudaram 89%** das organizações no **Brasil**.

34%

Desafiaram nossa organização a fortalecer o atual programa de gestão de riscos cibernéticos, processos e abordagens de governança.

31%

Levaram à avaliação de serviços gerenciados de cibersegurança para atender às exigências regulatórias.

16%

Ajudaram a estabelecer diretrizes para a inovação tecnológica e os esforços de transformação.

8%

Ajudaram a impulsionar a resiliência ao exigir um *framework* abrangente para o setor.

24%

15%

20%

19%

E **78%** no **mundo**.

Alerta

Empresas que cumprem os requisitos regulatórios tendem a fortalecer seus *frameworks* de segurança e a assumir uma postura mais firme diante das ameaças emergentes. O *compliance* não deve ser visto apenas como formalidade, mas sim como uma oportunidade de desenvolver resiliência de longo prazo e confiança na relação com os *stakeholders*.

Gap de confiança: CISOs estão menos seguros do que CEOs em relação ao *compliance* cibernético

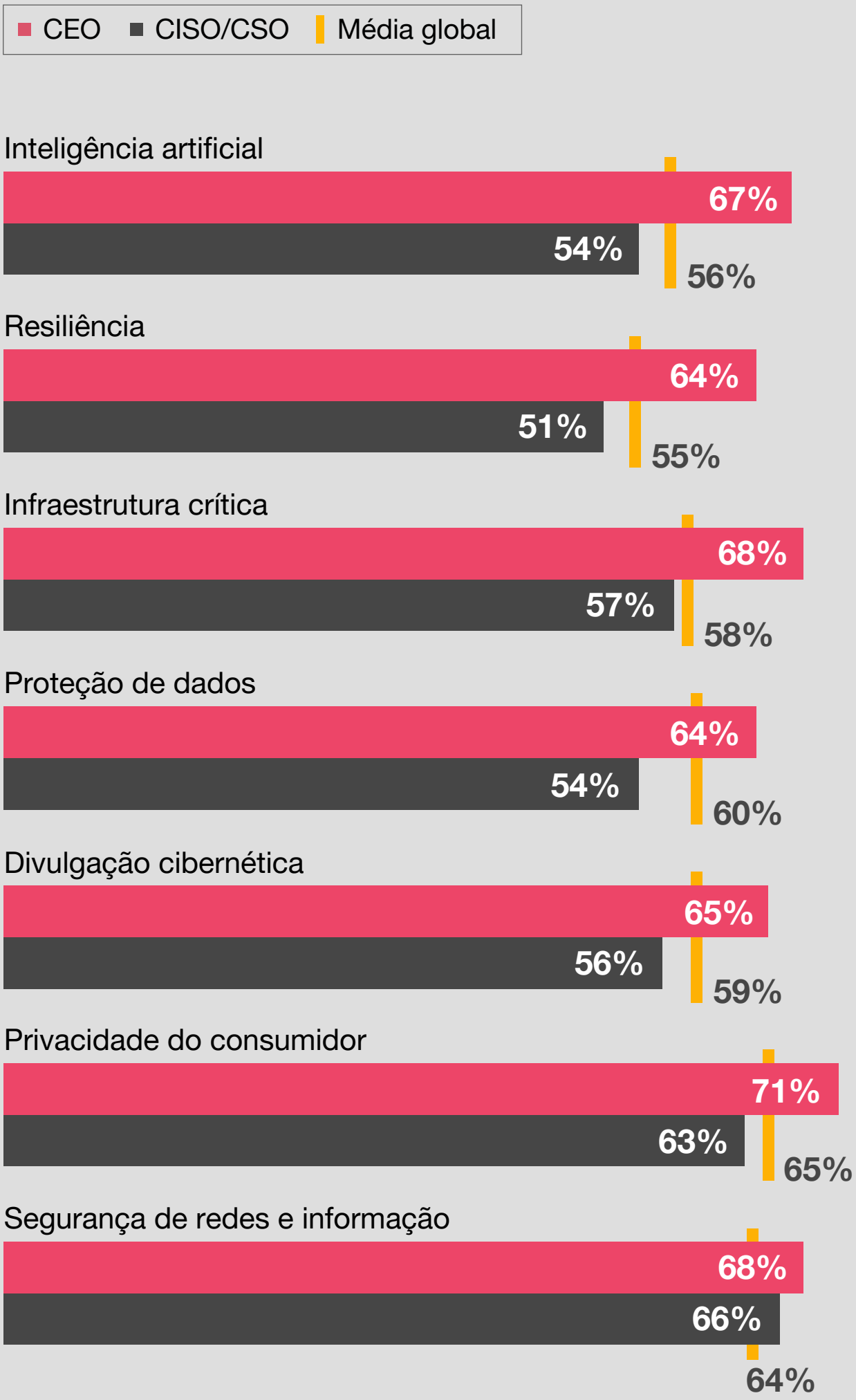
Embora a percepção seja que as regulamentações de cibersegurança estão beneficiando as organizações, há uma diferença significativa na confiança entre CEOs e CISOs/CSOs quanto à capacidade de cumprir essas regulamentações. As maiores divergências dizem respeito ao *compliance* com requisitos relacionados à IA, resiliência e infraestrutura crítica. Os CISOs, que lidam diretamente com a cibersegurança, estão menos otimistas que os CEOs quanto à capacidade da organização de cumprir essas exigências regulatórias.

Por estarem mais familiarizados com as dificuldades operacionais diárias, limitações de recursos e possíveis vulnerabilidades que podem comprometer o *compliance* cibernético, os CISOs devem comunicar esses riscos de forma mais eficaz à equipe de liderança. O que os impede? Possíveis barreiras seriam a falta de envolvimento dos CISOs nas decisões estratégicas e a dificuldade de justificar o nível de investimento necessário para a gestão de riscos cibernéticos.

Confiança no *compliance* regulatório da organização

(% de CEO x CISO/CSO que demonstram alta confiança)

Pergunta: quão confiante você está na capacidade da sua organização de cumprir os seguintes tipos de regulamentações que podem ser aplicáveis à(s) localidade(s) em que opera?



Alerta

Eliminar essa lacuna de confiança exige melhor alinhamento e comunicação entre os executivos de segurança e a alta direção. Os CEOs devem garantir que os CISOs não apenas sejam ouvidos, mas também tenham os recursos e o apoio necessários para cumprir as exigências regulatórias. Os CISOs, por sua vez, precisam fornecer insights baseados em dados e apresentar um argumento sólido de negócios para tornar o *compliance* uma prioridade estratégica.

Ação recomendada para a liderança

Com os requisitos regulatórios continuando a influenciar o cenário da cibersegurança, é essencial que os executivos da alta direção se antecipem às questões de *compliance*, utilizando as regulamentações como um motor para a inovação. Alinhar as equipes de segurança, as funções de risco e a liderança executiva é fundamental para garantir a prontidão de *compliance* e promover melhorias estratégicas.

CISO e CRO: envie relatórios frequentes aos outros líderes executivos sobre a situação das regulamentações que impactam diretamente as necessidades específicas do setor ou da localidade. Além disso, trabalhe para implementar processos de gestão de mudanças tecnológicas e regulatórias.

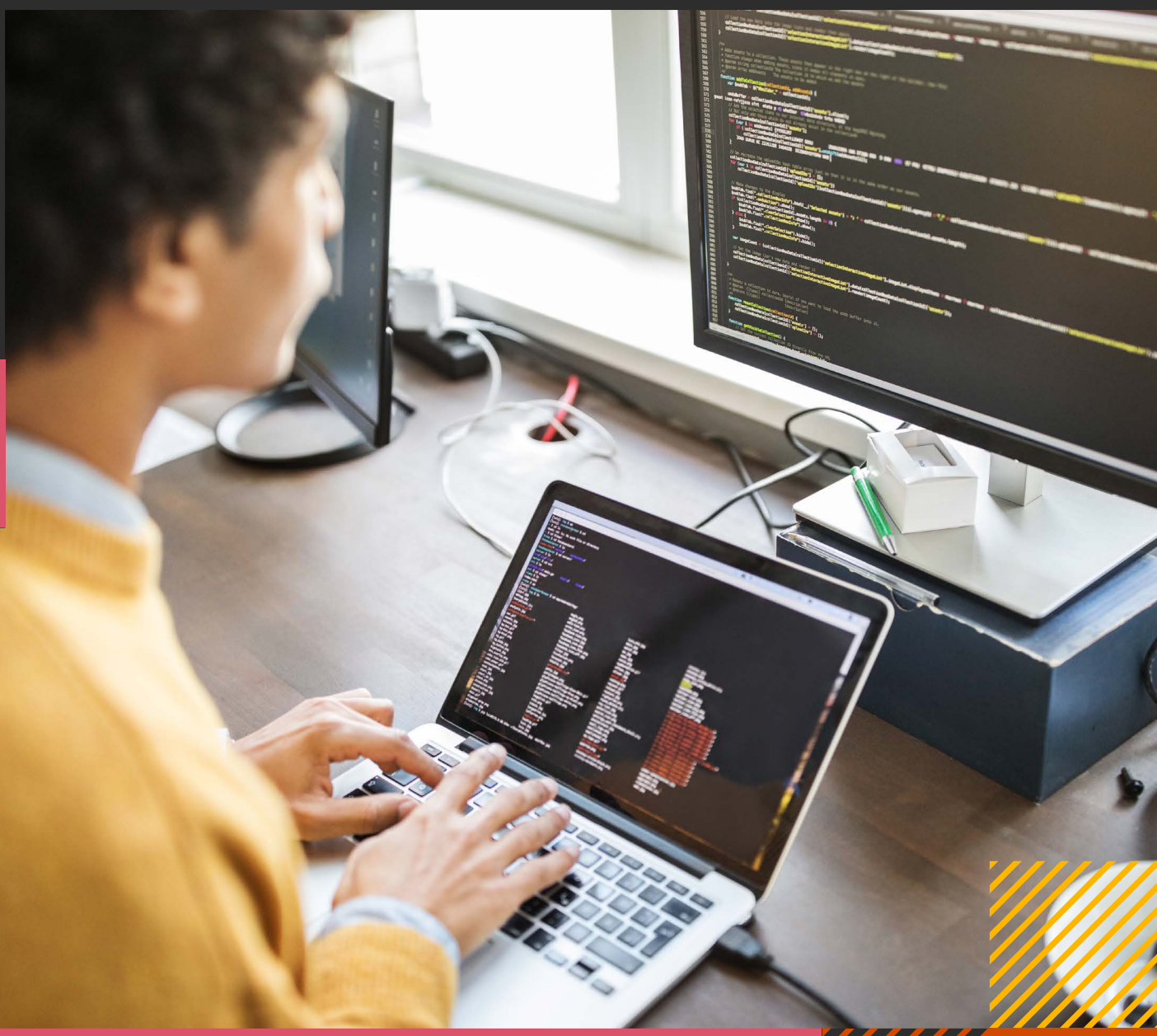
CFO: verifique a precisão, completude e justificativa de todas as divulgações regulatórias sobre a gestão de riscos cibernéticos e a postura do programa. Desenvolva uma compreensão clara da materialidade e do impacto específico de um incidente cibernético, incorporando a quantificação de riscos cibernéticos para avaliar e comunicar com precisão os riscos potenciais.

CEO: compreenda as responsabilidades de supervisão para orientar os esforços de *compliance*, incluindo a coordenação necessária entre diferentes unidades de negócios. Identifique perguntas-chave para fazer aos CISOs a fim de eliminar lacunas de conhecimento sobre a postura de *compliance*.

Diretor de *compliance*: mantenha-se atualizado sobre os requisitos de *compliance* regulatório e colabore com o CISO e o CRO para incorporar medidas de *compliance* e monitoramento de forma proativa, a fim de confirmar periodicamente a conformidade.

Diretor e assessor jurídico: defina o grau adequado de detalhamento para atender às exigências de relatórios de programas cibernéticos, mantendo o equilíbrio entre transparência e confidencialidade.

Conselho: mantenha-se atualizado sobre novas exigências regulatórias e solicite informações da administração sobre as medidas proativas que estão sendo tomadas como preparação para novas exigências. Compreenda a abordagem da administração para avaliar e divulgar incidentes cibernéticos.



Potencial da quantificação de riscos cibernéticos: principais desafios para as organizações

15%

apenas medem, em profundidade, o impacto financeiro dos riscos cibernéticos no Brasil e no mundo.

96%

dizem que alocar recursos para áreas de maior risco é altamente importante (87% no mundo).

37%

afirmam que problemas de dados são um dos principais desafios enfrentados ao quantificar o impacto financeiro do risco cibernético (44% no mundo).

Com as ameaças cibernéticas evoluindo rapidamente em escopo e sofisticação, a quantificação de risco cibernético se tornou uma ferramenta essencial que as organizações não podem ignorar. No entanto, apesar de seus benefícios amplamente reconhecidos, vários desafios (como problemas de qualidade dos dados e confiabilidade dos resultados) têm impedido uma adoção mais ampla.

Medir o risco cibernético é essencial, mas esse processo ainda é limitado

Embora a maioria dos executivos concorde que avaliar o risco cibernético é crucial para priorizar investimentos em segurança (95% no Brasil e 88% no mundo) e alocar recursos nas áreas de maior risco (96% no Brasil e 87% no mundo), apenas 15% das organizações no Brasil e no mundo o fazem em profundidade (por exemplo, com quantificação extensiva de riscos cibernéticos, uso de automação e relatórios abrangentes).

Entre as organizações que medem o risco, 79% dos executivos brasileiros (73% no mundo) afirmam utilizar avaliações de postura de segurança para quantificar o risco residual, considerando a eficácia de controles-chave, como *compliance* com a remediação de vulnerabilidades, revisões de acesso de usuários e a conclusão de treinamentos. No entanto, a adoção de práticas mais abrangentes de quantificação de risco cibernético ainda permanece limitada.

Benefícios da quantificação de riscos cibernéticos

Pergunta: indique a importância dos seguintes aspectos para a sua organização na quantificação do risco cibernético (apenas respostas “muito” e “extremamente importante”).

Brasil	Global	
98%	88%	Ajudar a avaliar e comunicar os riscos cibernéticos de acordo com a tolerância a riscos definida
96%	87%	Ajudar a alocar recursos nas áreas de maior risco
95%	88%	Ajudar a priorizar investimentos em segurança cibernética
95%	86%	Demonstrar o valor do programa de gestão de riscos cibernéticos
92%	84%	Medir e comparar ameaças e incidentes de forma equitativa

Alerta

Está na hora de explorar plenamente o potencial da quantificação de riscos cibernéticos. A diferença entre reconhecer sua importância e implementar medidas eficazes representa uma oportunidade desperdiçada, que já não pode ser ignorada.

Organizações que não quantificam seus riscos cibernéticos, ou que ainda não aprimoraram essa competência, estão perdendo valiosas informações estratégicas, especialmente no que diz respeito à fundamentação das decisões do conselho e à alocação de recursos.

Quais são as barreiras para uma implementação mais ampla?

Questões relacionadas a dados, incerteza quanto ao escopo e preocupações legais estão entre os principais obstáculos à implementação da quantificação de risco cibernético.

A falta de confiança quanto à precisão dos resultados da quantificação é outro fator. Além disso, a adoção é dificultada pela lacuna entre o que os executivos seniores esperam e o que os CISOs entregam, já que medir o risco cibernético exige alinhamento entre os executivos de segurança e o apetite da organização aos riscos.

Desafios na quantificação do impacto financeiro do risco cibernético

Pergunta: quais desafios, se houver, sua organização enfrentou ao quantificar o impacto financeiro potencial do risco cibernético? Selecione e classifique até três opções, sendo 1 o maior desafio.

Brasil	Global	
54%	43%	Preocupações legais ou regulatórias
38%	45%	Incerteza quanto ao escopo pretendido dos resultados da quantificação de riscos
37%	44%	Problemas com dados
38%	38%	Confiabilidade e credibilidade dos resultados da quantificação de riscos

Alerta

As barreiras para a adoção e o uso da quantificação de riscos cibernéticos podem estar atrasando o progresso. As organizações não podem se dar ao luxo de permitir que esses desafios prejudiquem a tomada de decisões críticas. É importante enfrentar esses obstáculos de forma direta, estabelecer confiança na quantificação de riscos cibernéticos e integrá-la completamente ao processo estratégico.

Ação recomendada para a liderança

Estabelecer um sistema confiável de quantificação de riscos cibernéticos é essencial para tomar decisões bem fundamentadas e priorizar investimentos estratégicos. Ao medir o risco com precisão, os executivos podem alinhar os esforços de cibersegurança com os objetivos mais amplos do negócio.

CISO: avalie começar de forma modesta, com um objetivo específico em mente. Aproveite as informações já disponíveis em sua organização (por exemplo, eficácia dos controles, maturidade, dados de incidentes ou perdas). Novas ferramentas podem ajudar na quantificação de riscos, mas não são uma exigência. Defina seu programa e procure tecnologias que apoiem o que você planejou.

CISO e CRO: mostre aos executivos os resultados mais impactantes da medição de risco financeiro obtidos por meio de ferramentas e práticas de quantificação. Esses exemplos podem ajudar a convencer a liderança a priorizar e alocar os recursos corretos para as áreas de maior risco.

CEO: trabalhe em conjunto com o CISO e o CRO para obter uma compreensão mais profunda do valor estratégico da quantificação de riscos cibernéticos e dos potenciais custos e oportunidades perdidas por não medir esses riscos.

Conselho: compreenda os métodos que sua organização atualmente usa para avaliar o risco cibernético. Cobre da gestão um plano para implementar a quantificação de risco de forma mais ampla, a fim de melhorar a avaliação e os relatórios sobre a postura de risco cibernético da empresa.

Investindo na resiliência e promovendo a confiança

84%

dos brasileiros esperam que seu orçamento de cibersegurança aumente no próximo ano (77% no mundo).

39%

dos executivos de negócios priorizam a proteção de dados e a confiança neles como o principal investimento em cibersegurança para o próximo ano (48% no mundo).

50%

dos executivos de tecnologia priorizam a segurança na nuvem como o principal investimento em cibersegurança para o próximo ano (34% no mundo).

Com a crescente relevância da cibersegurança como prioridade corporativa, as organizações estão reconhecendo seu valor como fator estratégico e oportunidade de melhorar sua reputação e confiança. Em resposta, muitas estão aumentando seus orçamentos de cibersegurança, com ênfase especial na proteção e confiança dos dados. Investindo de maneira estratégica nessas áreas, as empresas não apenas aumentam sua resiliência, mas também se destacam positivamente perante seus clientes e o mercado.

Orçamentos de cibersegurança devem crescer no próximo ano

Os orçamentos de cibersegurança permanecem estáveis em relação ao ano anterior, globalmente, com organizações menores alocando uma porcentagem maior de seus recursos em comparação às maiores. Isso provavelmente indica um esforço das pequenas organizações para avançar em áreas nas quais as grandes empresas já realizaram investimentos significativos.

As grandes organizações, embora preocupadas com ameaças emergentes e resiliência, adotam uma abordagem mais cautelosa para seus investimentos, provavelmente por já terem estruturas de segurança mais consolidadas.

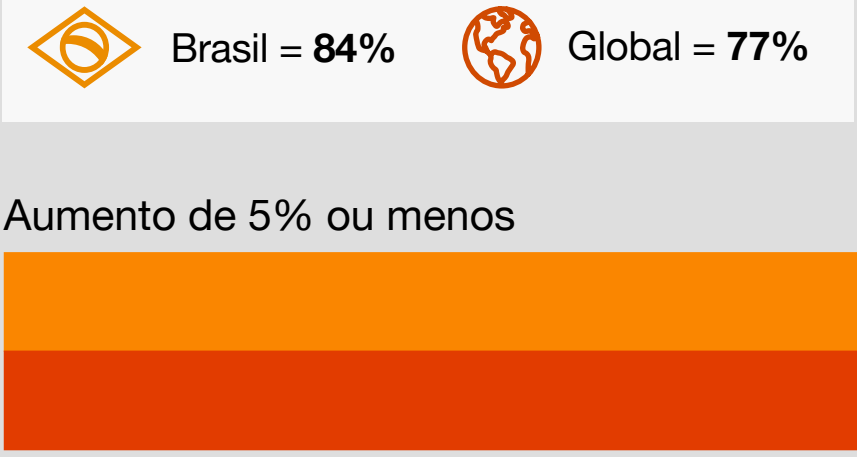
No Brasil, 84% dos executivos esperam que o orçamento de cibersegurança de suas organizações aumente no próximo ano, em comparação com 77% no mundo. Globalmente, a expectativa de aumento é maior na América do Norte (82%) e no setor de tecnologia, mídia e telecomunicações (TMT).

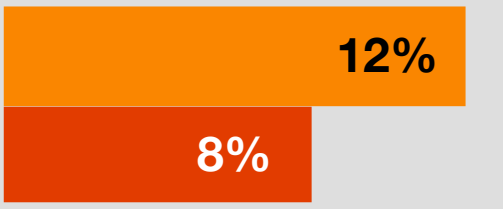
Mudança no orçamento de cibersegurança em 2025

Pergunta: como o orçamento de cibersegurança da sua organização mudará em 2025?

Esperam aumento do orçamento de cibersegurança em 2025:

Brasil = **84%** Global = **77%**





Alerta

Após um ano de manutenção dos orçamentos, é essencial alinhar o aumento planejado nos gastos com os riscos atuais e futuros, garantindo que cada dólar contribua para fortalecer a resiliência e preparar a organização para o cenário de ameaças em constante evolução.

Investindo no que mais importa: confiança nos dados e segurança na nuvem caminham juntas

Nos próximos 12 meses, as empresas no Brasil estão priorizando a modernização da tecnologia e a segurança na nuvem acima de outros investimentos em cibersegurança – no mundo, os investimentos em proteção/confiança nos dados têm mais destaque. É importante que as empresas compreendam que proteger informações sensíveis é crucial para manter a confiança dos *stakeholders* e a integridade da marca.

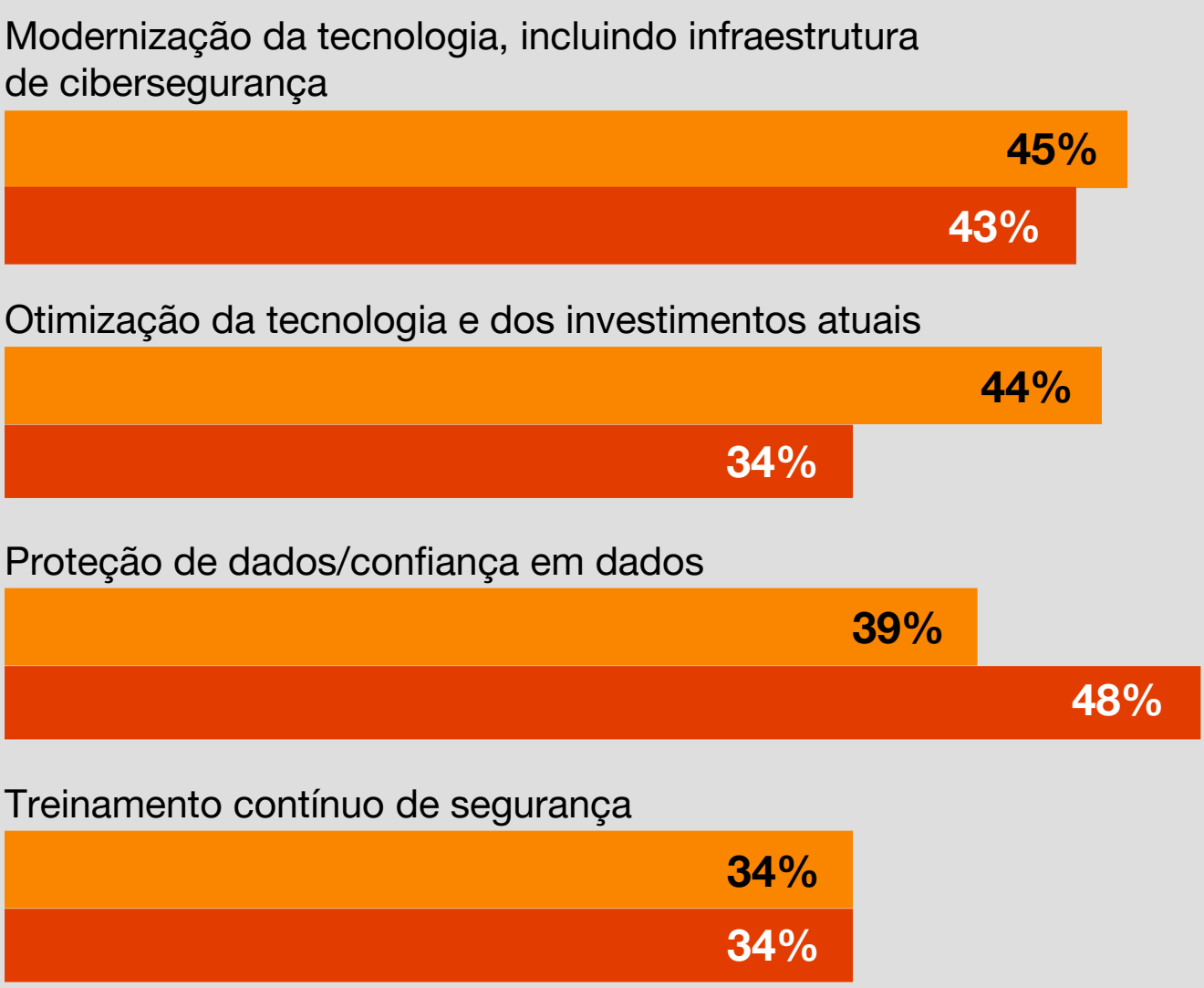
Executivos de negócios e tecnologia classificam suas prioridades de forma diferente, com base em suas áreas específicas de responsabilidade.

Executivos de negócios no Brasil afirmam que a modernização e otimização tecnológica é sua principal prioridade (45%), seguida pela otimização da tecnologia e dos investimentos atuais (44%).

Já para os executivos de tecnologia brasileiros, a segurança na nuvem continua sendo a principal prioridade (50%), seguindo a mesma tendência do ano passado. IA generativa e aprendizado de máquina são a segunda prioridade (38%).

Prioridades de investimento em cibersegurança para executivos de negócios

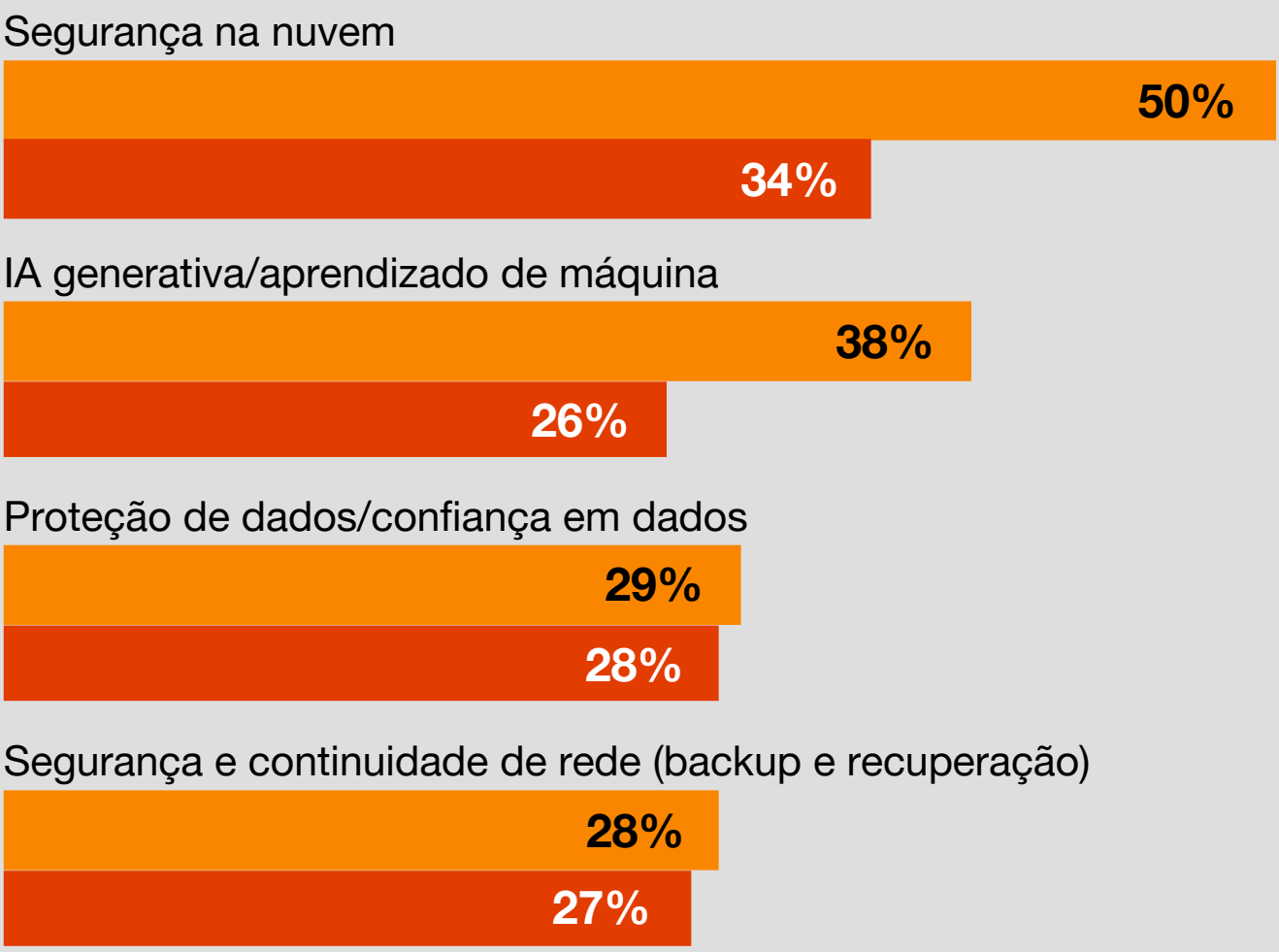
(% dos participantes que classificaram as alternativas entre as três primeiras)



Prioridades de investimento em cibersegurança para líderes de tecnologia

(% dos participantes que classificaram as alternativas entre as três primeiras)

Pergunta: quais dos seguintes investimentos, se houver, você está priorizando ao alocar o orçamento de cibersegurança da sua organização nos próximos 12 meses? Selecione e classifique até cinco opções, sendo 1 a maior prioridade de alocação do orçamento de cibersegurança.

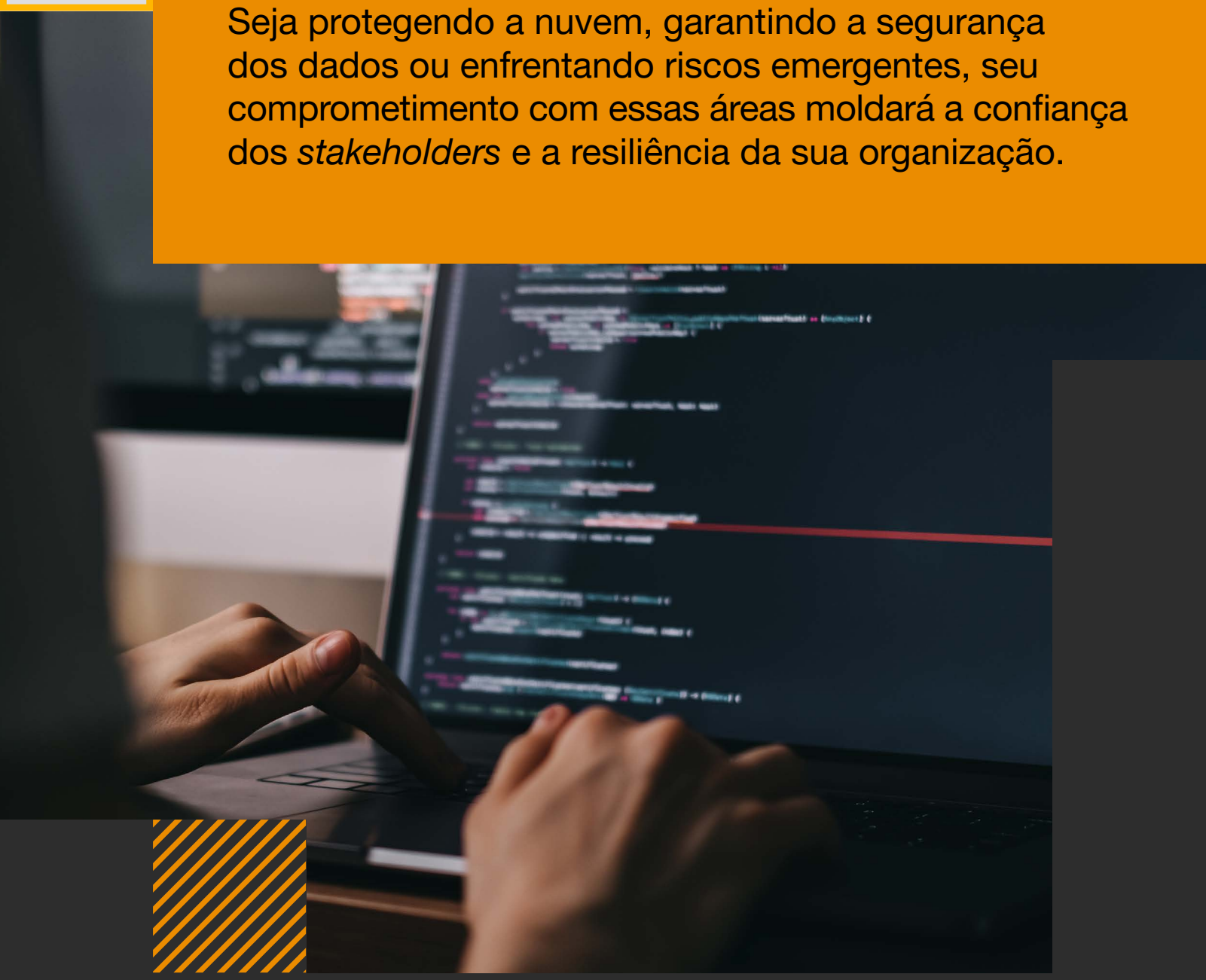


Por que a segurança na nuvem continua a exigir atenção?

Apesar de anos de investimento, a rápida adoção de tecnologias em nuvem, a consolidação dos grandes provedores de nuvem e o aumento de configurações híbridas e multinuvem concentraram os riscos no ambiente da nuvem. Essa concentração aumenta o impacto potencial de erros de configuração de acesso a dados, violações de dados e desafios de integração. À medida que os agentes de ameaças evoluem, as estratégias de segurança na nuvem também precisam evoluir, o que torna crucial o investimento contínuo para mitigar esses riscos crescentes.

Alerta

Investir em cibersegurança é investir em confiança. Seja protegendo a nuvem, garantindo a segurança dos dados ou enfrentando riscos emergentes, seu comprometimento com essas áreas moldará a confiança dos *stakeholders* e a resiliência da sua organização.



Cibersegurança e confiança: o novo diferencial competitivo

As organizações estão enxergando a cibersegurança cada vez mais como um fator-chave de diferenciação para obter vantagem competitiva: 64% dos brasileiros mencionam a integridade e a lealdade da marca (49% no mundo) e 63% citam a confiança do consumidor (57% no mundo) como áreas de influência.

À medida que as ameaças cibernéticas aumentam, uma postura forte em cibersegurança não significa apenas proteção – é também a construção de uma reputação na qual clientes e *stakeholders* possam confiar. Sendo a confiança essencial, as empresas que priorizam a cibersegurança estão mais bem posicionadas para se destacar como líderes tanto em segurança quanto em integridade.

Posicionando a cibersegurança como uma vantagem competitiva

(% dos participantes que selecionaram "Em grande medida")

Pergunta: em que medida sua organização posiciona a cibersegurança como vantagem competitiva nas seguintes áreas?

Alerta

Sua cibersegurança não está apenas protegendo dados. Ela protege sua marca. Em um cenário competitivo, a confiança é tudo. Fortaleça suas medidas de segurança agora para ajudar sua organização a se destacar como líder em integridade de dados.

Ação recomendada para a liderança

Com a expectativa de crescimento dos investimentos em cibersegurança, é fundamental que cada membro da alta administração alinhe suas estratégias aos riscos mais urgentes da organização. Os executivos devem realizar investimentos que não apenas solucionem as vulnerabilidades atuais, mas também construam confiança e resiliência.

CIO, CTO e CISO: traduza para o CFO o argumento de negócio em prioridades de investimento na proteção de dados e segurança na nuvem. Tome como base o valor comercial dos principais resultados (por exemplo, reduzir o tempo de recuperação de dados de missão crítica ou aplicar *patches* em um sistema).

CFO: determine o valor comercial da proteção de dados e da segurança na nuvem para conquistar a confiança dos *stakeholders* e tomar decisões de investimento em cibersegurança mais bem fundamentadas.

CDO: colabore com executivos de tecnologia, segurança e finanças para identificar as prioridades mais essenciais de segurança e integridade de dados que guiarão a estratégia de investimento em segurança da informação e nuvem. Confirmar a qualidade e a prontidão dos dados é necessário para aumentar os investimentos em segurança.

Sua liderança e estratégia cibernética estão promovendo uma verdadeira resiliência?

Apenas 2%

dos participantes no mundo adotaram ações de resiliência cibernética em todas as áreas da organização.

Apenas 21%

costumam alocar o orçamento cibernético para os principais riscos da organização (no Brasil e no mundo).

56%

dos CISOs no Brasil estão amplamente envolvidos no planejamento estratégico de investimentos cibernéticos (49% no mundo).

Para gerenciar as ameaças futuras, não basta apenas fazer investimentos – as organizações também devem melhorar sua abordagem de liderança e estratégia cibernética. Desde esforços de resiliência defasados até falhas na participação dos CISOs em decisões estratégicas, há áreas claras nas quais é preciso fazer um alinhamento estratégico.

Para alcançar esse objetivo, as organizações devem seguir as melhores práticas de cibersegurança de seus pares de melhor desempenho. Elas também precisam avançar além das ameaças conhecidas, implementando uma abordagem ágil e segura desde a concepção do negócio, buscando construir confiança e resiliência duradoura.

Uma implementação parcial não é suficiente

Apesar da crescente preocupação com o risco cibernético, a maioria das empresas enfrenta dificuldades para adotar plenamente a resiliência cibernética em práticas essenciais. Uma análise de 12 ações de resiliência envolvendo pessoas, processos e tecnologia indica que menos da metade dos executivos acredita que suas organizações implementaram totalmente alguma dessas ações.

Mais preocupante ainda, apenas 2% no mundo afirmam que todas as 12 ações de resiliência foram implementadas na organização. Isso deixa uma vulnerabilidade evidente – sem resiliência em toda a empresa, as organizações permanecem perigosamente expostas às ameaças crescentes que podem comprometer toda a operação.

Esperam aumento do orçamento de cibersegurança em 2025:

Criar uma equipe de resiliência com integrantes de funções como continuidade dos negócios, cibersegurança e gestão de crises e riscos.

Desenvolver um plano de recuperação cibernética para cenários de perda de TI.

Mapear dependências tecnológicas.

Implementação de ações de resiliência cibernética em toda a organização

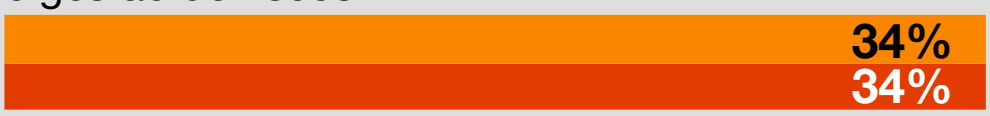
Pergunta: até que ponto sua organização está implementando ou planejando implementar as seguintes ações de resiliência cibernética?

Brasil Global

Pessoas

Criação de conexões com as autoridades locais para buscar apoio na análise e resposta

Criação de uma equipe de resiliência com integrantes de funções como continuidade dos negócios, cibersegurança, gestão de crises e gestão de riscos



Relatórios para *stakeholders* externos (reguladores, investidores)

Processos

Definição de protocolos com provedores de tecnologia para coordenar respostas a incidentes

Compartilhamento de informações com pares do setor, por meio de processos formais, para prevenir riscos sistêmicos

Desenvolvimento de um plano de recuperação cibernética para cenários de perda de TI

Realização de exercícios e simulações

Identificação de processos críticos de negócios

Tecnologia

Implementação de soluções de recuperação cibernética (incluindo backups imutáveis)

Mapeamento de dependências tecnológicas

Implementação de ferramentas para aumentar a visibilidade dos ativos de tecnologia operacional (TO)

Implementação de computação quântica para defesa e resiliência cibernética

Alerta

A falta de resiliência cibernética deixa sua organização vulnerável. Adote uma abordagem integrada e abrangente, fortalecendo tecnologia, processos e capacitando pessoas para transformar suas defesas e se antecipar aos desafios futuros.

A resiliência cibernética é uma prioridade. Por que tantas empresas ainda estão atrasadas em áreas críticas?

Muitas organizações ainda não acompanham as melhores práticas em cibersegurança. Apenas cerca de um em cada cinco executivos afirma aplicar essas práticas de forma consistente. Por exemplo, somente 19% antecipam riscos cibernéticos futuros (20% no mundo) e apenas 21% direcionam o orçamento de cibersegurança para os principais riscos da organização (no Brasil e no mundo). Esse atraso pode ser causado por diversos fatores, como a falta de visão estratégica, recursos limitados ou uma abordagem reativa para a cibersegurança.

Comportamentos que a equipe de cibersegurança de uma organização “geralmente” realiza

% dos participantes que responderam “Geralmente” (81-100% do tempo)

Pergunta: indique com que frequência a equipe de cibersegurança da sua organização realiza as seguintes atividades.

Brasil Global

Aplica controles e responde rapidamente a ameaças para que nossa organização possa resistir a crises cibernéticas graves

Colabora com outras áreas do negócio que afetam a postura de cibersegurança da organização

Fornece insights sobre a exposição a riscos cibernéticos em evolução, mudanças regulatórias e medidas de mitigação para o CEO e o conselho

Aloca o orçamento de cibersegurança para os maiores riscos da organização

Antecipa futuros riscos cibernéticos considerando ambiente macro, tecnologia emergente e estratégia de negócios

Acelera iniciativas digitais e outras grandes transformações de nossa organização (por exemplo, projetando segurança e privacidade em novos produtos e serviços)

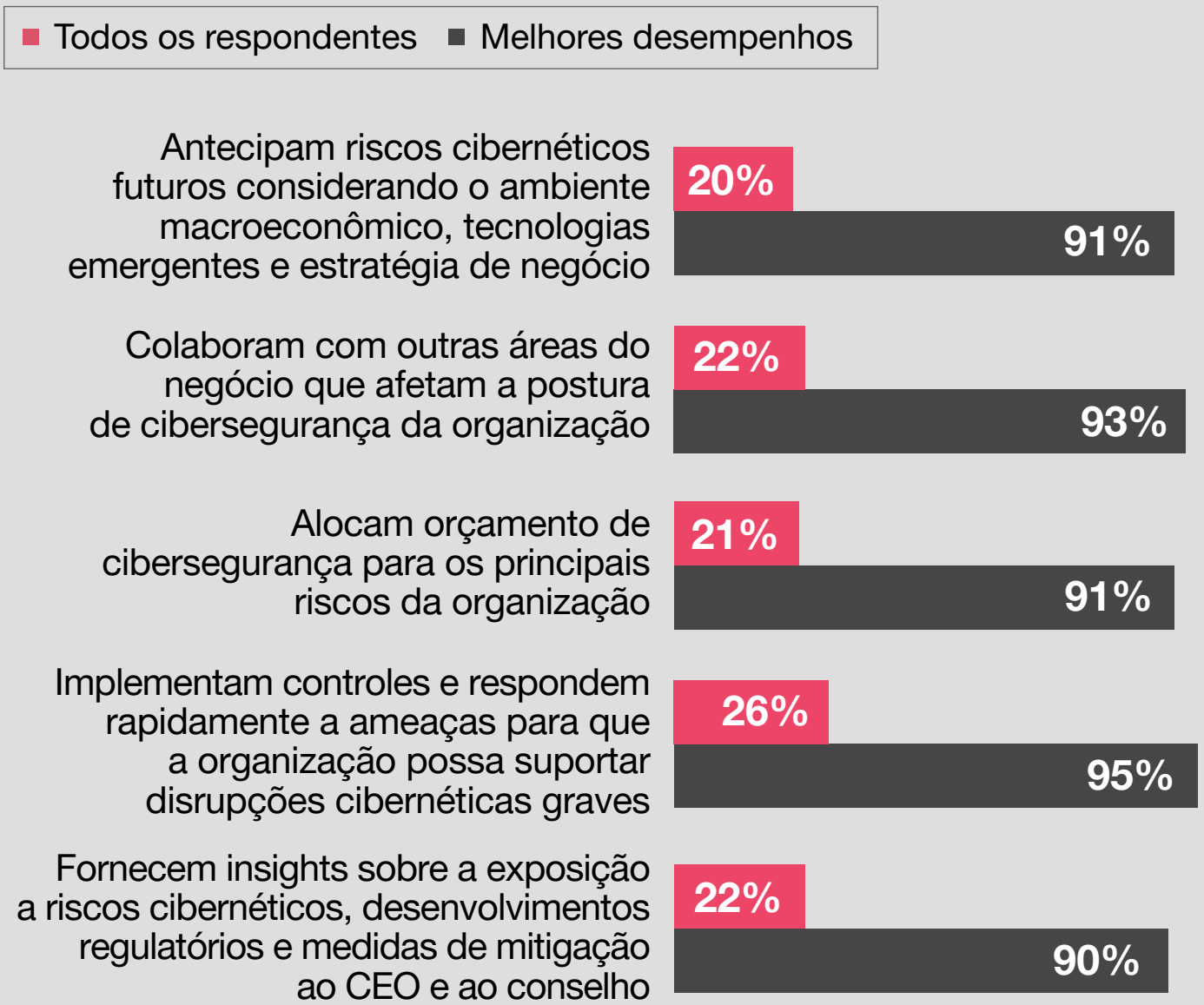
Os líderes com melhor desempenho se destacam de forma consistente e significativa

Analisamos essa questão mais a fundo para identificar um grupo de executivos de alto desempenho que “geralmente” exibe esses comportamentos. Globalmente, existe uma diferença de 69 pontos percentuais ou mais em todos os comportamentos entre esses líderes e o total de nossos respondentes. Os executivos de melhor desempenho demonstram maior confiança na capacidade de suas organizações de cumprir regulamentações e já implementaram ações cruciais de resiliência em toda a empresa.

Diferença de comportamento entre as equipes de cibersegurança de melhor desempenho e a média de todas as equipes

% dos participantes que responderam “Geralmente” (81-100% do tempo)

Pergunta: indique com que frequência a equipe de cibersegurança da sua organização realiza as seguintes atividades.

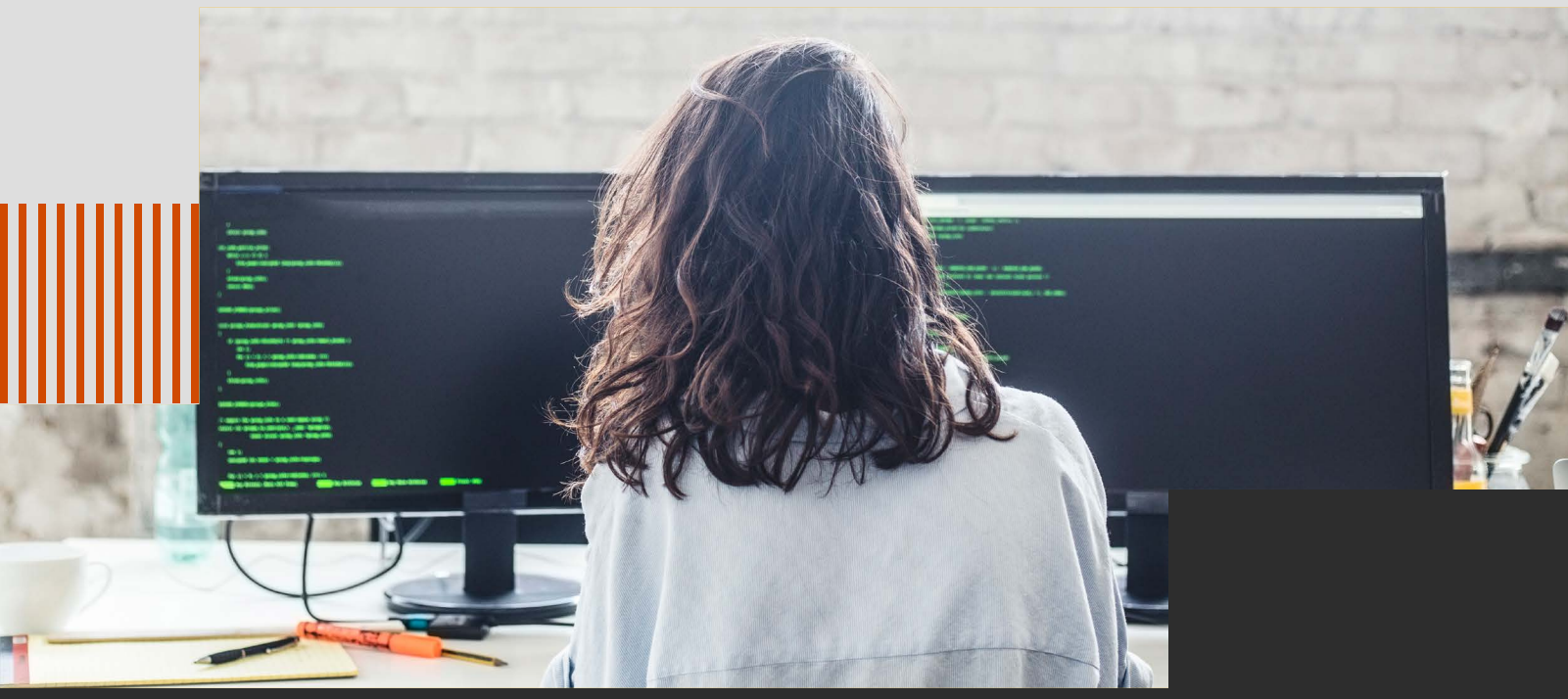


Alerta

Para eliminar essa lacuna, as organizações devem passar de estratégias reativas de cibersegurança para abordagens proativas. Isso envolve antecipação mais precisa de riscos, alocação estratégica de recursos e um compromisso sólido com a melhoria contínua.

Prioridades estratégicas: agilidade, confiança e segurança para os *stakeholders*

Nos próximos 12 meses, 31% dos executivos brasileiros planejam trabalhar na redução do tempo de resposta a incidentes e interrupções (36% no mundo). Outros objetivos importantes são aumentar a confiança na capacidade da liderança de gerenciar ameaças, ampliar o uso de serviços cibernéticos gerenciados e melhorar a experiência de clientes e funcionários. Esses objetivos refletem um esforço mais amplo para, além de acelerar a mitigação de riscos, construir confiança e proteger clientes e funcionários.



Alerta

Respostas rápidas não são apenas um objetivo – são uma necessidade. Reações demoradas a ameaças podem custar mais do que apenas tempo: elas podem corroer a confiança e causar sérias crises para o negócio. Agilidade e confiança na liderança devem ser prioridades inegociáveis.

Elevando o papel do CISO: alinhando estratégia com segurança

Muitas organizações perdem oportunidades importantes por não envolverem completamente seus CISOs em iniciativas-chave. No Brasil, cerca de metade dos executivos afirma que seus CISOs estão amplamente envolvidos no planejamento estratégico para investimentos em cibersegurança, relatórios ao conselho e supervisão de implementações tecnológicas – no mundo, os resultados são ligeiramente inferiores. Essa lacuna deixa as organizações vulneráveis a estratégias desalinhadas e posturas de segurança mais fracas.

Envolvimento amplo do CISO nas atividades de negócios

Pergunta: qual o envolvimento do CISO da sua organização nas seguintes áreas?

Alerta

Garanta que o seu CISO participe das discussões estratégicas. As visões dele são essenciais para uma abordagem proativa da cibersegurança como um risco estratégico para o negócio. Integrá-lo ao mais alto nível de decisão permite que sua organização alinhe a proteção de ativos críticos com o fortalecimento da resiliência.

Ação recomendada para a liderança

A liderança eficaz em cibersegurança demanda visão estratégica e o alinhamento de toda a organização. Cada executivo tem um papel fundamental em promover esse alinhamento, seja integrando o CISO nas decisões-chave ou priorizando os esforços de resiliência.

CISO: apresente ao restante da alta liderança os motivos pelos quais é essencial que o CISO esteja envolvido na estratégia, no planejamento e na supervisão da mitigação de riscos cibernéticos e da estratégia de resiliência.

CEO, CFO e CIO: participe de avaliações e exercícios de resiliência cibernética para compreender melhor as lacunas e os desafios que os CISOs podem enfrentar ao integrar melhores práticas, padrões e controles.

Conselho: mantenha-se informado sobre o desenvolvimento dos programas de risco cibernético, especialmente no que diz respeito à exposição a riscos e ameaças cibernéticas da organização, para cumprir responsabilidades crescentes de supervisão e governança.

Sobre a pesquisa

A **Pesquisa Global Digital Trust Insights 2025** é um levantamento realizado com 4.042 executivos de negócios e tecnologia, entre maio e julho de 2024. Um quarto dos executivos representa grandes empresas com receitas de US$ 5 bilhões ou mais. Os respondentes atuam em diversos setores, como indústria e serviços (21%); tecnologia, mídia e telecomunicações (20%); serviços financeiros (19%); varejo e consumo (17%); energia e serviços de utilidade pública (11%); saúde (7%) e governo (4%).

Os respondentes são de em 77 países, com a distribuição regional da seguinte forma: Europa Ocidental (30%), América do Norte (25%), Ásia-Pacífico (18%), América Latina (12%), Europa Central e Oriental (6%), África (5%) e Oriente Médio (3%).

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

Em seu 27º ano, é a pesquisa anual mais antiga sobre tendências em cibersegurança. Também é a maior do setor de cibersegurança e a única que conta com a participação de altos executivos de negócios, e não apenas de executivos de segurança e tecnologia.

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

Contatos

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

Fernando Mitre
Sócio
fernando.mitre@pwc.com

Joana Mendes
Sócia
joana.mendes@pwc.com

Larissa Escobar
Sócia
larissa.escobar@pwc.com

Magnus Santos
Sócio
magnus.santos@pwc.com

Maressa Juricic
Sócia
maressa.juricic@pwc.com

Rafael Cortes
Sócio
cortes.rafael@pwc.com

pwc

Acesse o site:

www.pwc.com.br

Siga a PwC nas redes sociais