A Lynchpin Media BRAND

CXO priorities

RELATÓRIO DE PRIORIDADES CXO LATAM 2024:

Principais tendências, desafios e prioridades de cibersegurança para os CIOs na América Latina

Um relatório de prioridades do CXO em parceria com paloalto NETWORKS

Conteúdo

Introdução

As mudanças no cenário tecnológico nunca ocorreram tão rapidamente. Ferramentas digitais estão sendo adotadas em todos os setores para transformar a maneira como as empresas operam. No entanto, esse ambiente digital em rápida evolução traz consigo desafios, especialmente em termos de cibersegurança. Desde a necessidade de conformidade (compliance, em inglês), até o surgimento de novas ameaças, os líderes de tecnologia precisam enfrentar um cenário complexo para proteger suas organizações enquanto impulsionam a inovação e o crescimento.

Neste relatório vamos explorar as principais percepções, insights e prioridades dos Chief Information Officers (CIOs) na América Latina, revelando uma ampla gama de preocupações. A governança, o compliance e a demonstração de Retorno Sobre Investimento (ROI, sigla em inglês), surgem como as principais prioridades dos respondentes, enquanto a colaboração e a comunicação entre os executivos são identificadas como elementos cruciais para uma estratégia eficaz de cibersegurança. À medida que as organizações buscam ferramentas digitais para aumentar a lucratividade e a eficiência, o papel do CIO na tomada de decisões e no planejamento estratégico se torna cada vez mais importante.

Nossos dados destacam as principais prioridades para os CIOs em 2024, incluindo o fortalecimento da resiliência de TI, a compreensão e priorização de riscos, além da adoção de tecnologias em nuvem e automação para melhorar as medidas de segurança. Essas prioridades ressaltam a necessidade estratégica das organizações de se adaptarem a um mundo cada vez mais digital e interconectado, enquanto se protegem contra novas ameaças.

O relatório oferece insights valiosos sobre o panorama da cibersegurança para os CIOs em 2024, destacando as prioridades, desafios e oportunidades que os líderes de tecnologia enfrentarão. Ao compreender e abordar essas tendências, as organizações estarão melhor preparadas para navegar nas complexidades da cibersegurança e se posicionar para o sucesso em um ambiente digital em constante evolução.

Visão geral da pesquisa

Para descobrir mais sobre os desafios atuais de cibersegurança e Tecnologia da Informação enfrentados pelos CIOs em organizações na América Latina, realizamos uma pesquisa com CIOs e Líderes de Tecnologia sobre suas experiências e planos em relação aos principais desafios e tendências. Este relatório tem como objetivo apresentar uma visão geral do cenário atual de ameaças, além de explorar tecnologias avançadas e revelar como as organizações planejam priorizar e investir.

Através desta pesquisa, buscamos descobrir:

A correlação entre o papel dos líderes de tecnologia dentro de uma organização, seus padrões de comunicação, principais preocupações e a taxa de colaboração

Como os CIOs esperam que seu papel e suas prioridades mudem para a área de negócios em geral

Práticas rotineiras e a adoção de tecnologias avançadas dentro das organizações

Metodologia

A pesquisa contou com a participação de 200 CIOs e Líderes de Tecnologia

Os três países com maior número de respostas foram **Brasil** (43%), México (23%) e **Argentina** (12%). Outros países que também participaram incluem Chile, Colômbia, Peru, Uruguai, Equador, Costa Rica e Bolívia.

As empresas participantes se dividiram em três principais categorias de tamanho: mais de **50 mil funcionários** (51%), **10 mil a 50 mil funcionários** (37%) e **5 mil a 10 mil funcionários** (6%).

As cinco principais indústrias representadas na pesquisa foram **Manufatura** (25%), **Serviços Financeiros** (15%), **Utilidades e Energia** (10%), **Farmacêutica e Ciências** (9%) e **Atacado e Varejo** (6%)

O que foi descoberto

O PAPEL DO CIO E DA COMUNICAÇÃO

Os CIOs acreditam que, nos próximos cinco anos, enfrentarão uma pressão crescente para se tornarem uma parte essencial na geração de receita da organização (33%), além de uma necessidade de se tornarem uma função mais estratégica dentro da empresa (33%)

A maioria dos entrevistados indicou que, nos próximos 12 meses, dará prioridade à segurança na nuvem, à resiliência cibernética e à gestão de riscos de terceiros

Governança e conformidade (18%) e a demonstração de ROI (13%) são as principais preocupações profissionais para os CIOs na América Latina. As organizações esperam focar nessas áreas para garantir o sucesso em 2024

Para garantir o sucesso, as duas principais áreas que as organizações pretendem priorizar em 2024 são a melhoria da resiliência de TI e organizacional (20%) e a compreensão e priorização dos riscos (15%)

CONTINUAÇÃO

PRIORIDADES DE NEGÓCIOS E CIBERSEGURANÇA DOS CIOS

As três principais prioridades de TI para os próximos 12 meses são: foco na nuvem (21%), melhorias na cibersegurança (21%) e expansão da automação (13%)

Mais de um terço dos entrevistados (37%) já está usando Inteligência Artificial (IA) para simulação de ameaças e previsão de ataques, enquanto 27% a utilizam para detecção e análise de malware

26% dos respondentes estão adotando IA, enquanto 22% têm um entendimento básico dessa tecnologia

Um quarto dos entrevistados afirmou que o papel mais importante da cibersegurança é proteger a empresa e garantir sua continuidade

paloalto NETWORKS

priorities

A Lynchpin Media BRAND

Parte 1

O papel do CIO e da comunicação

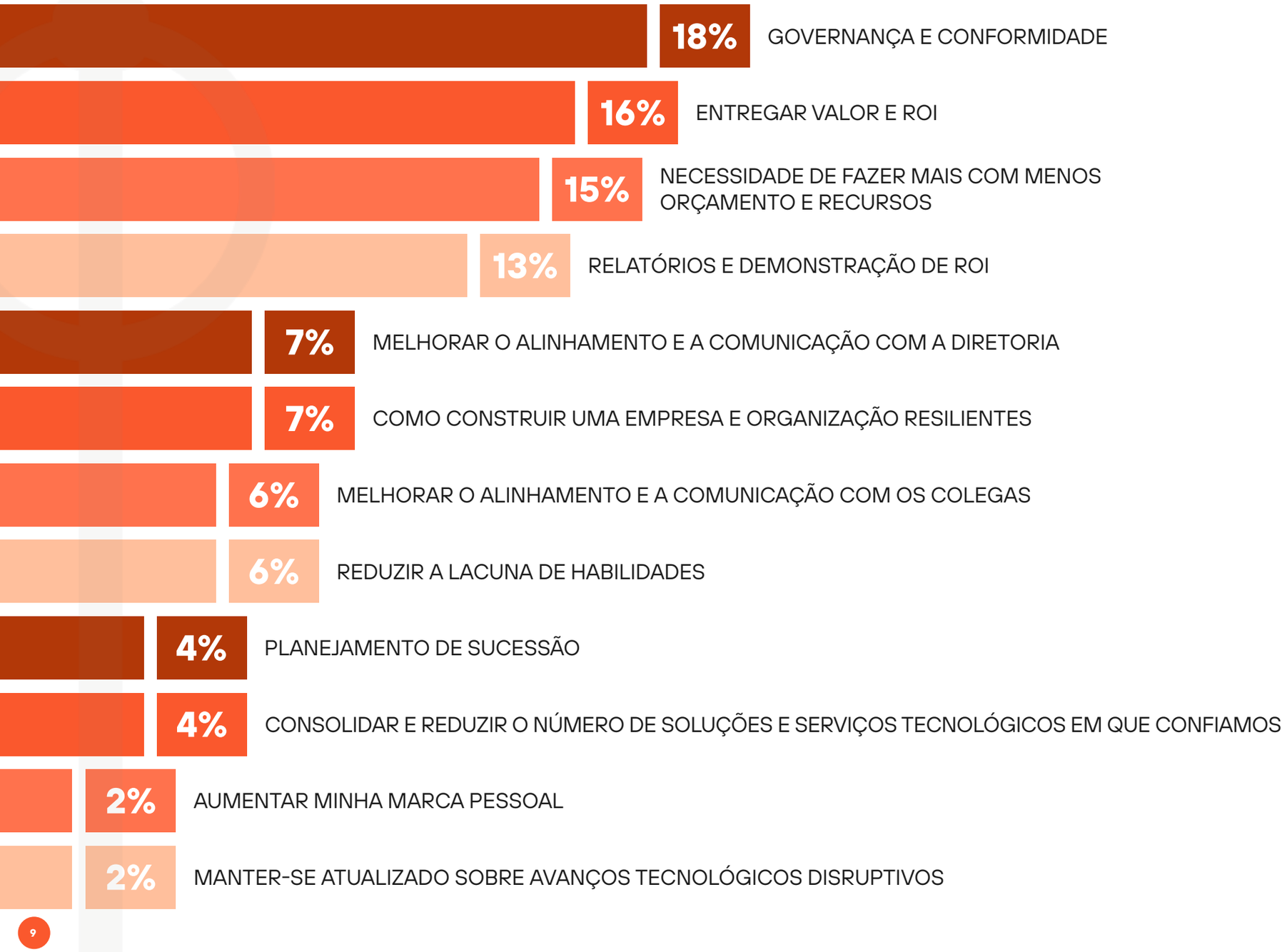
paloalto NETWORKS

priorities

A Lynchpin Media BRAND

1

Quais são suas principais preocupações profissionais no momento?

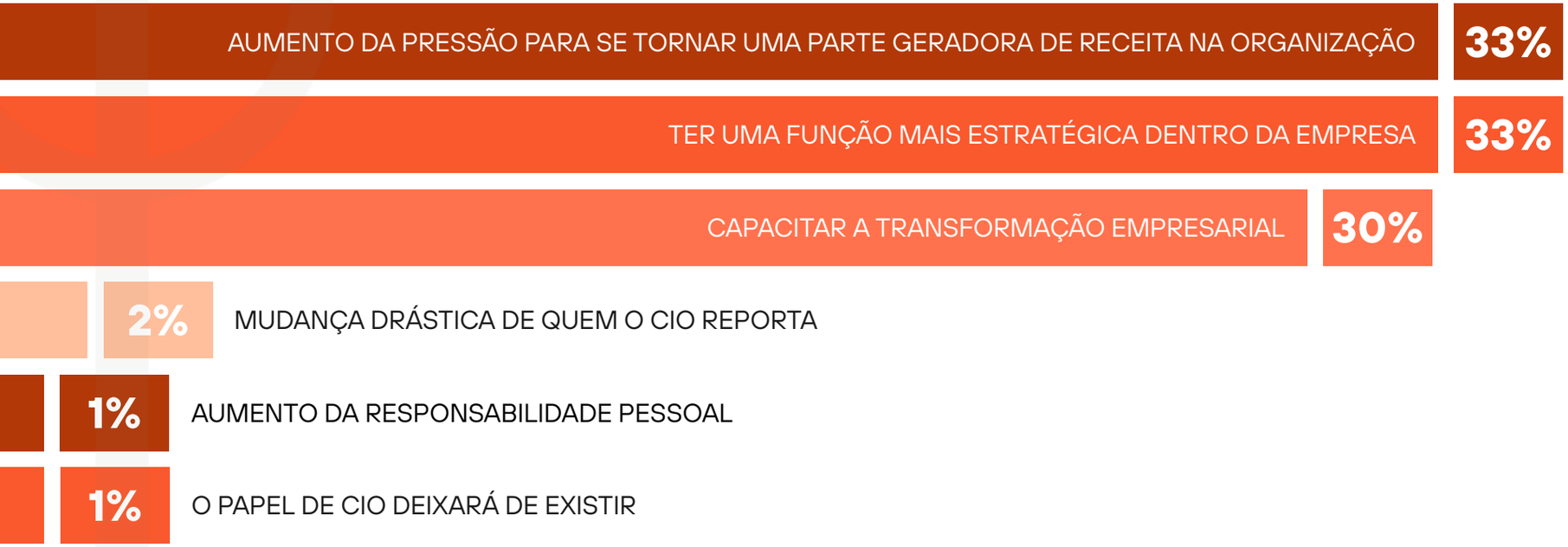


Principais insights:

As preocupações dos CIOs estão distribuídas em várias áreas, mas governança e compliance receberam a maior parcela das respostas, com 18%. Em seguida, entregar valor e ROI (16%) e a necessidade de fazer mais com menos orçamento e recursos (15%) também foram destacadas.

O foco no ROI reflete a pressão que os CIOs enfrentam para garantir que os investimentos em tecnologia possam demonstrar valor real. Governança e compliance estão no topo das prioridades para os líderes de tecnologia, especialmente devido a diretrizes internacionais, como o Digital Operational Resilience Act (DORA, sigla em inglês), o Cyber Resilience Act (CRA, sigla em inglês) e a Diretiva NIS2, além de regulamentações locais que exigem atenção para evitar potenciais penalidades.

Como você acha que seu papel pode mudar nos próximos cinco anos?



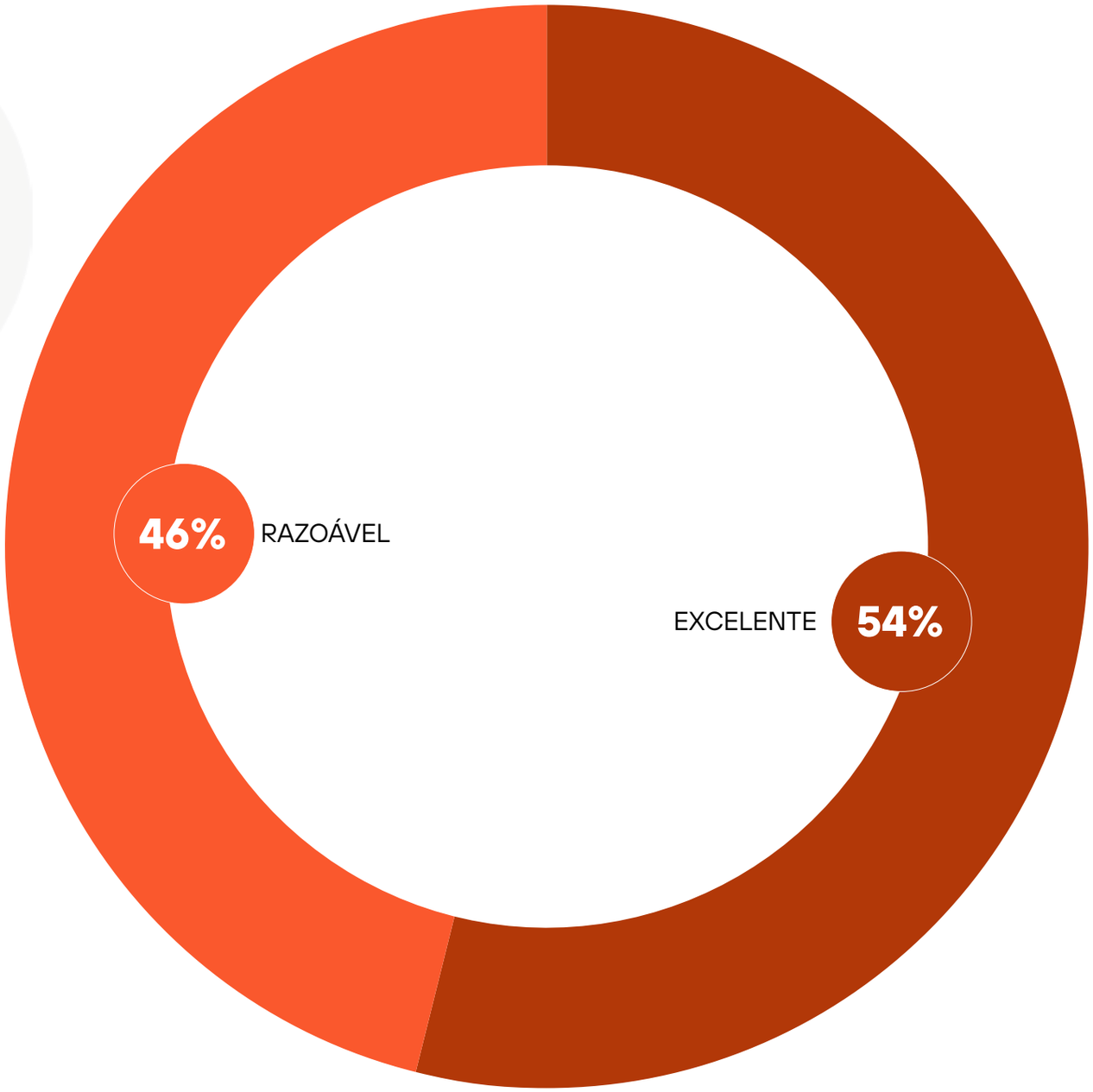
Principais insights:

Os CIOs acreditam que, nos próximos cinco anos, enfrentarão uma pressão crescente para se tornarem uma parte essencial na geração de receita da organização (33%), além de uma necessidade de se tornarem uma função mais estratégica dentro da empresa (33%). Eles também esperam ser responsáveis por impulsionar a transformação dos negócios.

Com as empresas cada vez mais focadas em ferramentas digitais para aumentar a lucratividade e melhorar os processos, os CIOs esperam estar em destaque como os principais responsáveis pelas decisões de investimentos em tecnologia.

3

Como você avaliaria a colaboração entre o seu papel e o restante da alta administração (C-Suite) na sua organização?



AVANÇAR

4

Quais são algumas maneiras de melhorar a colaboração com o restante da alta administração?

Aqui estão as palavras mais mencionadas nas respostas:

"Aproveitar a tecnologia para melhorar a eficiência nas operações."

Principais insights:

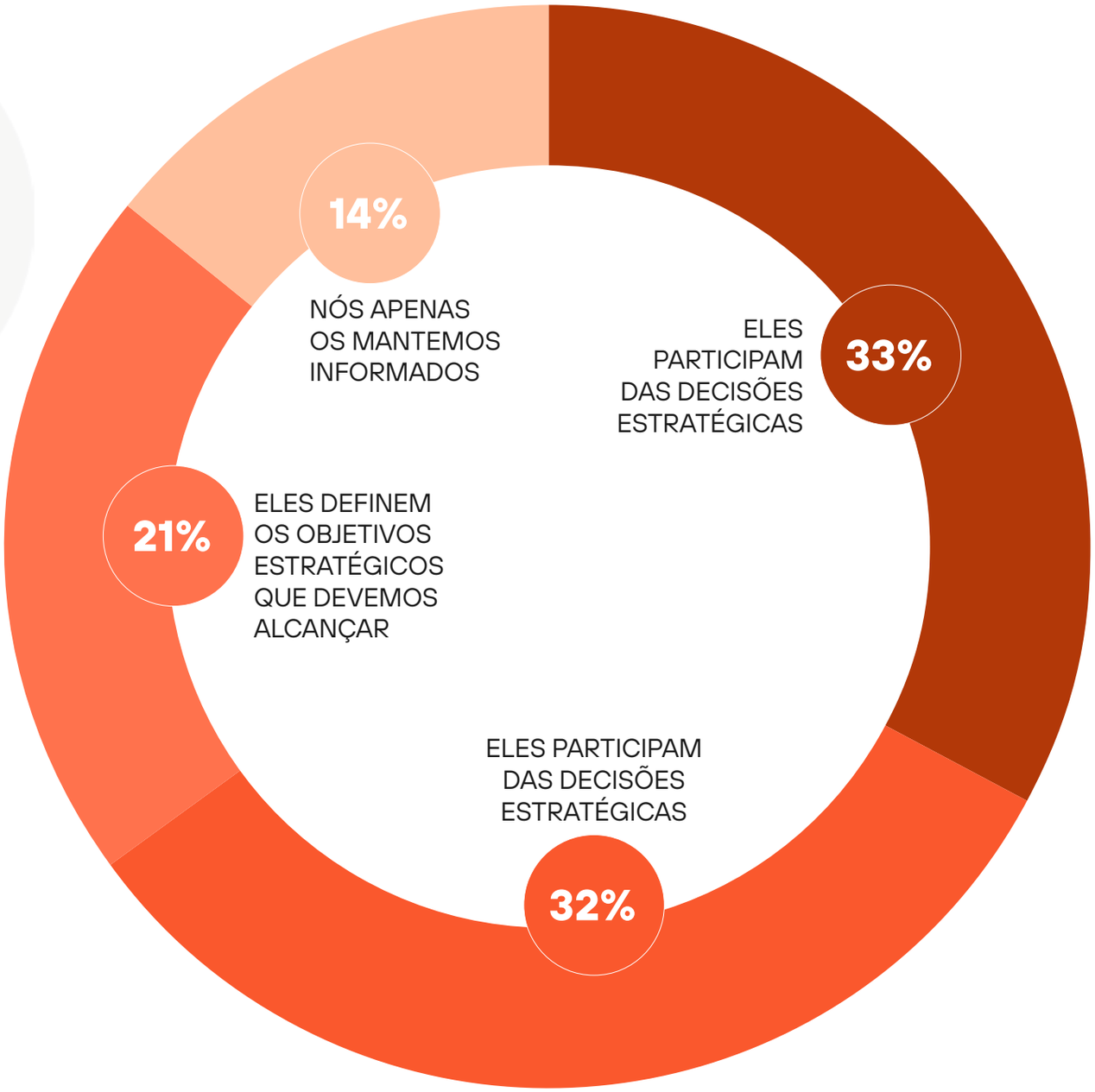
Comunicação e colaboração são fundamentais para a coesão do C-suite, mas nem sempre são garantidas. O sucesso nessa área geralmente depende de uma boa cultura organizacional. Isso é especialmente importante quando se trata de cibersegurança. Nossos dados sugerem que isso é amplamente reconhecido, com mais da metade dos participantes classificando a colaboração entre sua função e o restante da alta administração como "excelente".

No entanto, 46% acreditam que essa colaboração ainda pode melhorar. Algumas sugestões incluem:

- Garantir que as medidas de cibersegurança apoiem o crescimento dos negócios e as iniciativas de sustentabilidade;
- Melhorar a comunicação e o alinhamento para apoiar os esforços de digitalização;
- Aproveitar a tecnologia para aumentar a eficiência operacional;
- Facilitar a colaboração entre diferentes áreas para fortalecer a defesa cibernética e proteger ativos críticos;
- Melhorar a comunicação e a coordenação para impulsionar a Transformação Digital.

5

Quanto a diretoria influencia e direciona a estratégia de cibersegurança da sua organização?



AVANÇAR

paloalto NETWORKS

priorities

A Lynchpin Media BRAND

6

Quais são alguns dos desafios que isso traz para você.

Aqui estão as palavras mais mencionadas nas respostas:

Positivos | 16

Organização | 19

Lidando | 12

Consciência | 19

Escassez | 12

Especialização | 12

Dificuldades | 16

Cibersegurança | 31

Falsos (positivos) | 16

Alerta | 16

Fadiga | 16

Ameaça | 16

Prejudicando | 16

Lacuna | 12

Impedindo | 12

Treinamento | 19

Eficaz | 28

Implementação | 12

Insuficiente | 19

Resposta | 16

> "Sob pressão de requisitos de conformidade e regulamentação, necessitando de ajustes contínuos nas políticas e práticas de segurança."

Principais insights:

As descobertas revelam que a diretoria desempenha um papel importante na definição das estratégias de cibersegurança das organizações. Apenas 14% dos participantes relataram que a diretoria tem um papel passivo, sendo apenas informada sem se envolver necessariamente nos objetivos estratégicos.

Para 33% dos participantes, a diretoria exerce "influência significativa". Já para 32%, a diretoria está envolvida nas decisões estratégicas. Os 21% restantes afirmaram que a diretoria define os objetivos estratégicos. Isso indica que a cibersegurança se tornou uma função essencial do negócio, profundamente integrada na estrutura organizacional.

No entanto, os respondentes mencionaram alguns desafios, incluindo:

- Lidar com a escassez de habilidades e o gap de especialização, o que prejudica a implementação eficaz da estratégia de cibersegurança;
- Falta de conscientização e treinamento adequado em cibersegurança em toda a organização;
- Dificuldades com a saturação de alertas e falsos positivos, dificultando a resposta eficaz às ameaças;
- Resistência à adoção de novas tecnologias em indústrias tradicionais;
- Recursos limitados e alocação de orçamento insuficiente para iniciativas de TI;
- Pressão dos requisitos de compliance e regulamentação, exigindo ajustes contínuos nas políticas e práticas de segurança.

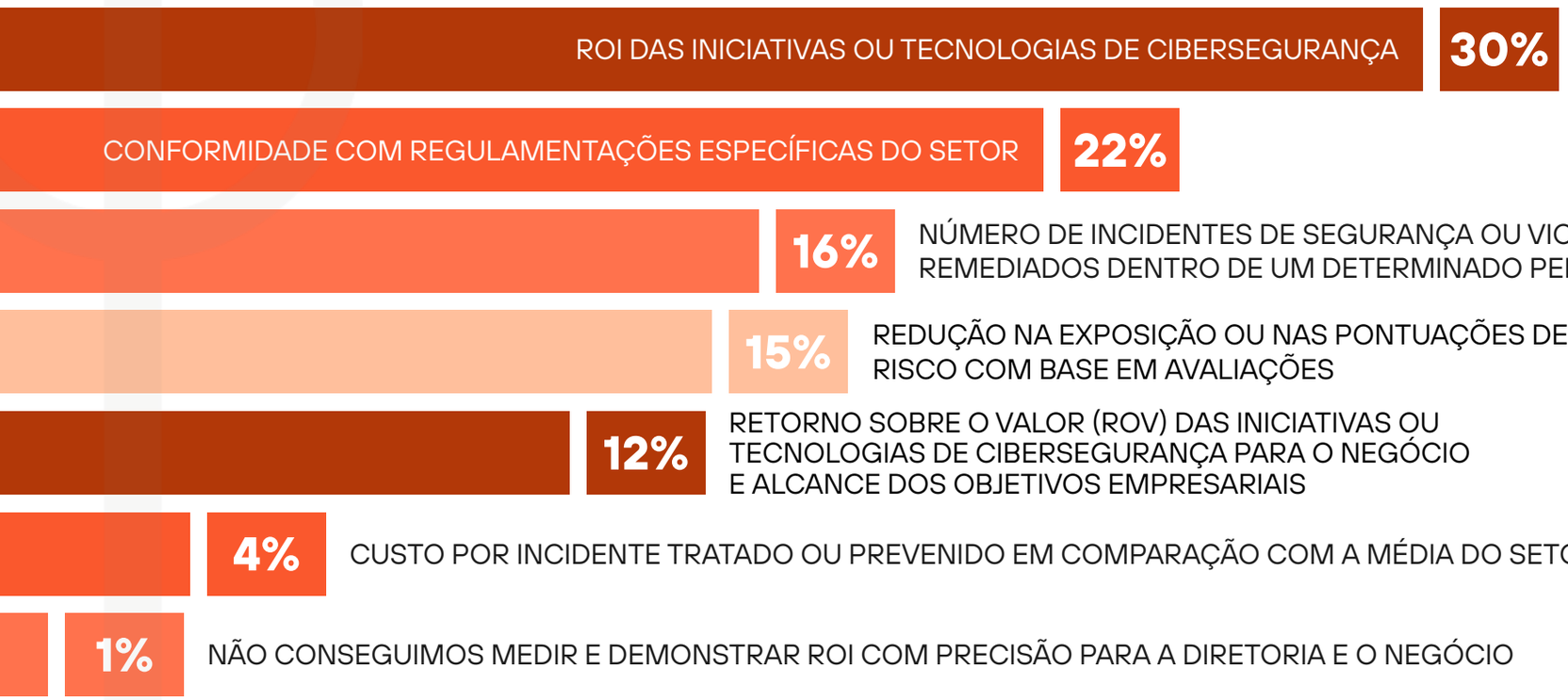
paloalto NETWORKS

priorities

A Lynchpin Media BRAND

7

Quais são algumas das métricas de sucesso que você usa atualmente para avaliar sua postura de segurança e demonstrar valor para o negócio e para a diretoria?



Principais insights:

Sobre as métricas de sucesso usadas para avaliar a postura de segurança e demonstrar valor ao negócio e à diretoria, 22% dos respondentes utilizam a compliance com regulamentações específicas do setor, indicando uma forte adesão a normas regulatórias. Um total de 30% mede o sucesso pelo ROI das iniciativas ou tecnologias de cibersegurança, destacando o aspecto financeiro das decisões de segurança. Redução na exposição ou nas pontuações de risco com base em avaliações é uma métrica de sucesso para 15% dos respondentes, evidenciando uma abordagem proativa na gestão de riscos.

Outras métricas consideradas, embora em menor escala, incluem o custo por incidente tratado ou prevenido em comparação com a média do setor, o número de incidentes de segurança ou violações resolvidos em um determinado período, e o ROV das iniciativas ou tecnologias de cibersegurança para o negócio e o cumprimento dos objetivos empresariais.

paloalto NETWORKS

priorities

A Lynchpin Media BRAND

Parte 2

Prioridades de negócios do CIO

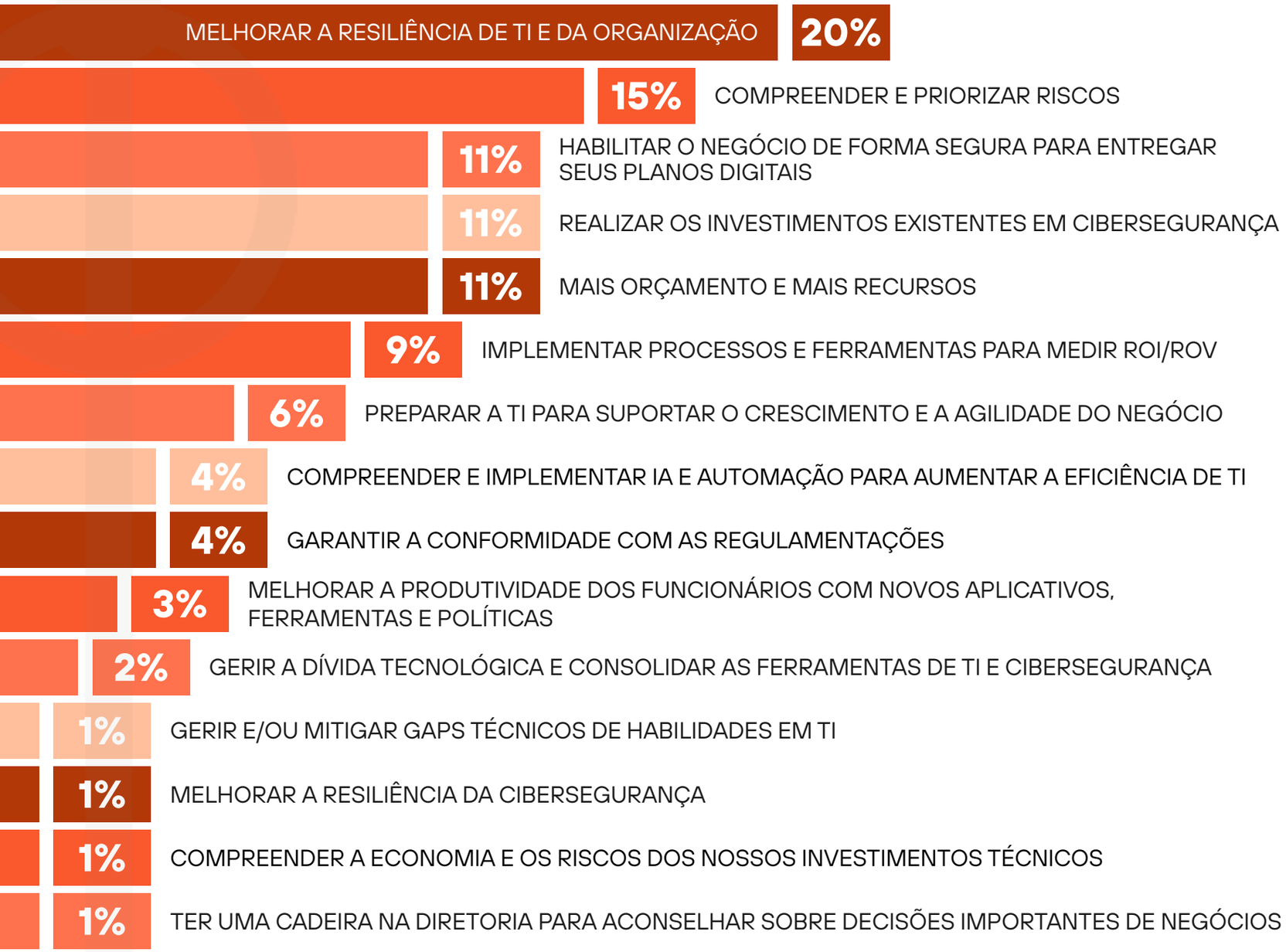
paloalto NETWORKS

priorities

A Lynchpin Media BRAND

8

Quais são as 5 principais coisas que você precisa para garantir o sucesso do seu negócio em 2024



Principais insights:

As cinco principais áreas de foco para garantir o sucesso em 2024 são:

- Melhorar a resiliência de TI e da organização (20%);
- Compreender e priorizar riscos (15%);
- Habilitar o negócio de forma segura para entregar seus planos digitais (11%);
- Realizar os investimentos existentes em cibersegurança (11%);
- Mais orçamento e mais recursos (11%).

Essas prioridades indicam uma forte ênfase na resiliência, Transformação Digital, gestão de riscos, cibersegurança e alocação de recursos como fatores críticos para o sucesso em 2024.

9

Quais são as três principais prioridades de TI da sua organização para os próximos 12 meses?

Principais insights:

As três principais prioridades de TI para os próximos 12 meses são: uso da nuvem (21%); foco e melhorias na cibersegurança (21%); e expansão da automação (13%). Essas prioridades refletem um foco estratégico em melhorar as medidas de segurança, aproveitar tecnologias de nuvem e expandir as iniciativas de automação para impulsionar o crescimento e a resiliência do negócio no cenário tecnológico em constante evolução.

paloalto NETWORKS

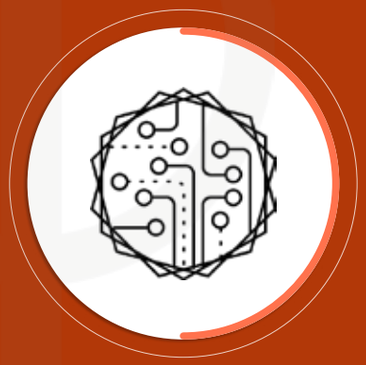
priorities

A Lynchpin Media BRAND

10

Quais tendências tecnológicas você acredita que terão o maior impacto nas suas futuras prioridades de negócios, e quão preparado você está para adotá-las?

IA



26% dos respondentes estão adotando IA

22% têm um entendimento básico de IA

Automação de Cibersegurança

17% têm um entendimento básico

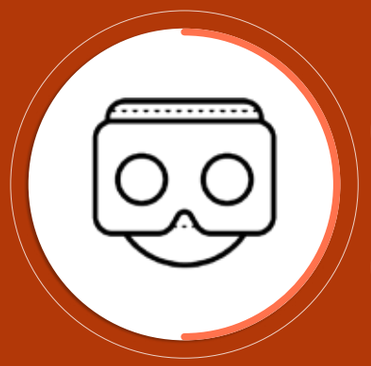
23% precisam de mais informações

Sustentabilidade

28% têm um entendimento básico

26% precisam de mais informações

Realidade Aumentada e Realidade Virtual

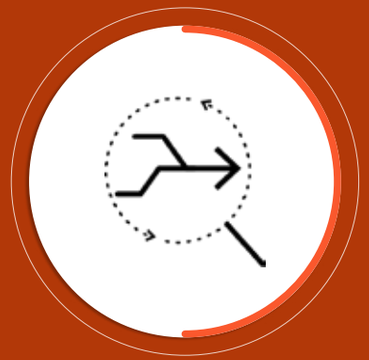


16% estão adotando essas tecnologias

10% têm um entendimento básico

CONTINUAÇÃO

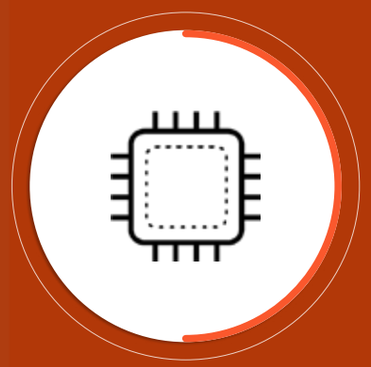
Sistemas Autônomos



25% estão adotando Sistemas Autônomos

23% precisam de mais habilidades

Computação Quântica



12% estão adotando Computação Quântica

15% precisam de mais informações

Ofertas baseadas em serviços

16% precisam de mais informações

15% têm um entendimento básico

paloalto NETWORKS

priorities

A Lynchpin Media BRAND

Parte 3

Prioridades de cibersegurança do CIO

paloalto NETWORKS

priorities

A Lynchpin Media BRAND

11

Qual é o papel mais importante que a cibersegurança desempenha para o sucesso da sua organização?

Principais insights:

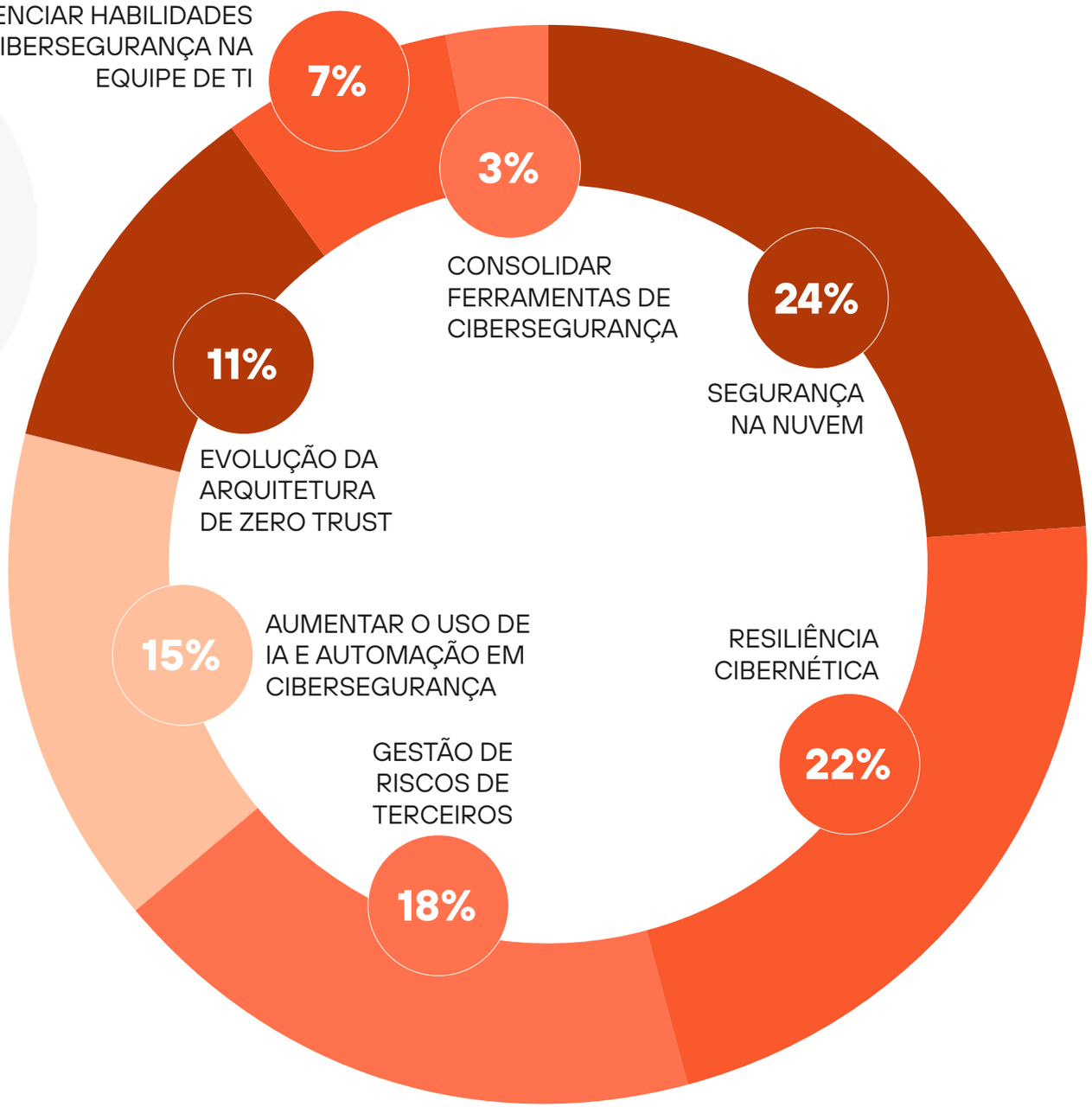
Um quarto dos respondentes destacou que o papel mais importante da cibersegurança é proteger o negócio e garantir sua continuidade. Isso reflete a compreensão de que a cibersegurança robusta é crucial para o sucesso empresarial, não apenas para CISOs, mas para todo o C-suite.

"Proteger e inspirar confiança em clientes e funcionários" foi a escolha de 23% dos respondentes, evidenciando a responsabilidade atribuída à cibersegurança nesse aspecto. Além disso, 21% acreditam que a cibersegurança ajuda as organizações a se adaptarem com segurança às mudanças e a aproveitarem oportunidades digitais.

A mensagem principal aqui é que, sem uma postura de cibersegurança resiliente e firme, a confiança dos clientes será abalada e as organizações terão pouca – ou nenhuma – chance de investir e aproveitar as oportunidades digitais, além de correrem o risco de sair do mercado.

12

Quais são suas três principais prioridades de cibersegurança para os próximos 12 meses?

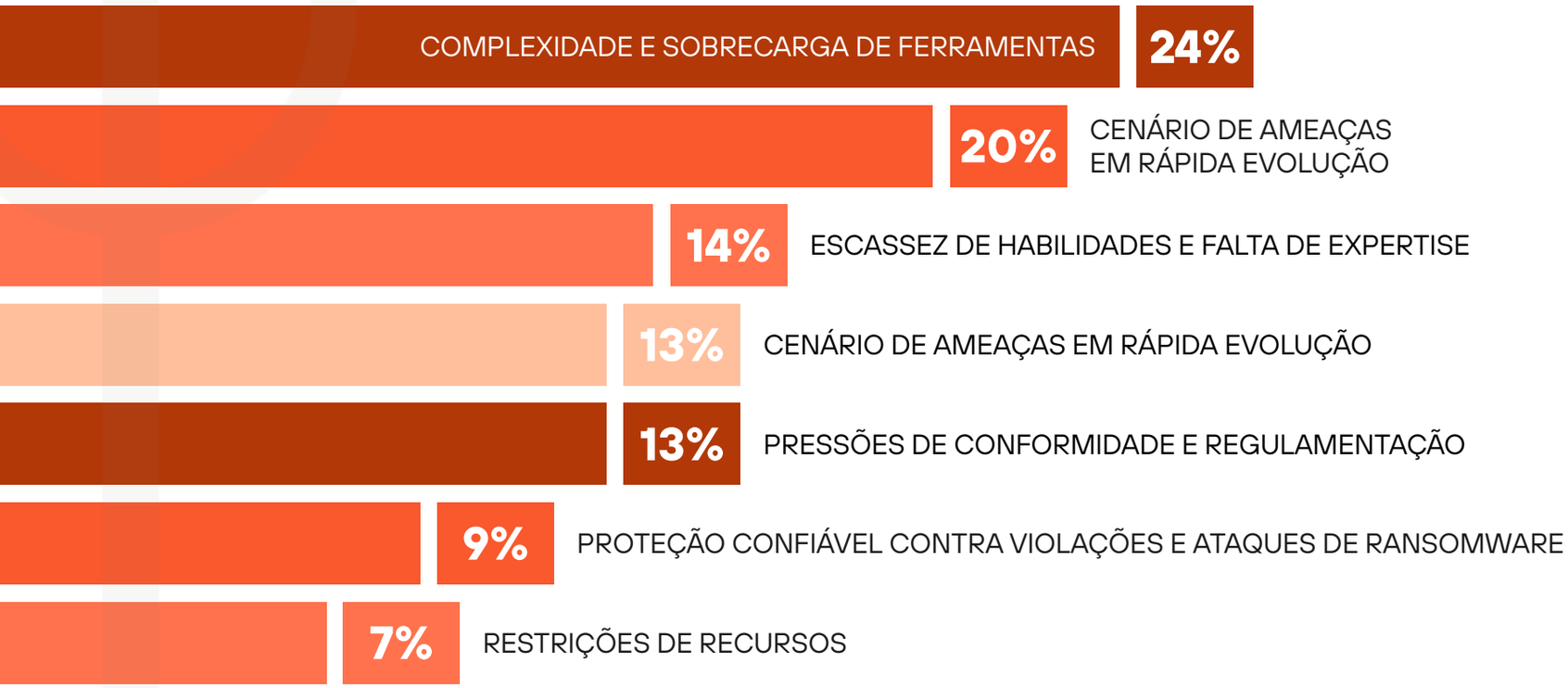


Principais insights:

A maioria dos respondentes planeja priorizar a segurança na nuvem, a resiliência cibernética e a gestão de riscos de terceiros nos próximos 12 meses. Apenas 7% disseram que irão priorizar a gestão de habilidades de cibersegurança dentro da equipe de TI, sugerindo um foco maior no negócio em si do que nas pessoas. Isso pode gerar um debate interessante, considerando que as habilidades e a educação em cibersegurança são fundamentais para o funcionamento de uma organização, sendo crucial que essa área de investimento não seja negligenciada enquanto outras prioridades são abordadas.

13

Quais são os desafios mais comuns que você enfrenta na gestão de suas ferramentas e soluções de cibersegurança?



Principais insights:

Além dos desafios esperados na cibersegurança, como o cenário de ameaças em rápida evolução (20%), a questão das restrições de recursos (7%) foi menos mencionada pelos respondentes em relação aos desafios com ferramentas e soluções. Isso pode sugerir que as organizações estão investindo mais amplamente em recursos como IA e automação para gerenciar esses desafios.

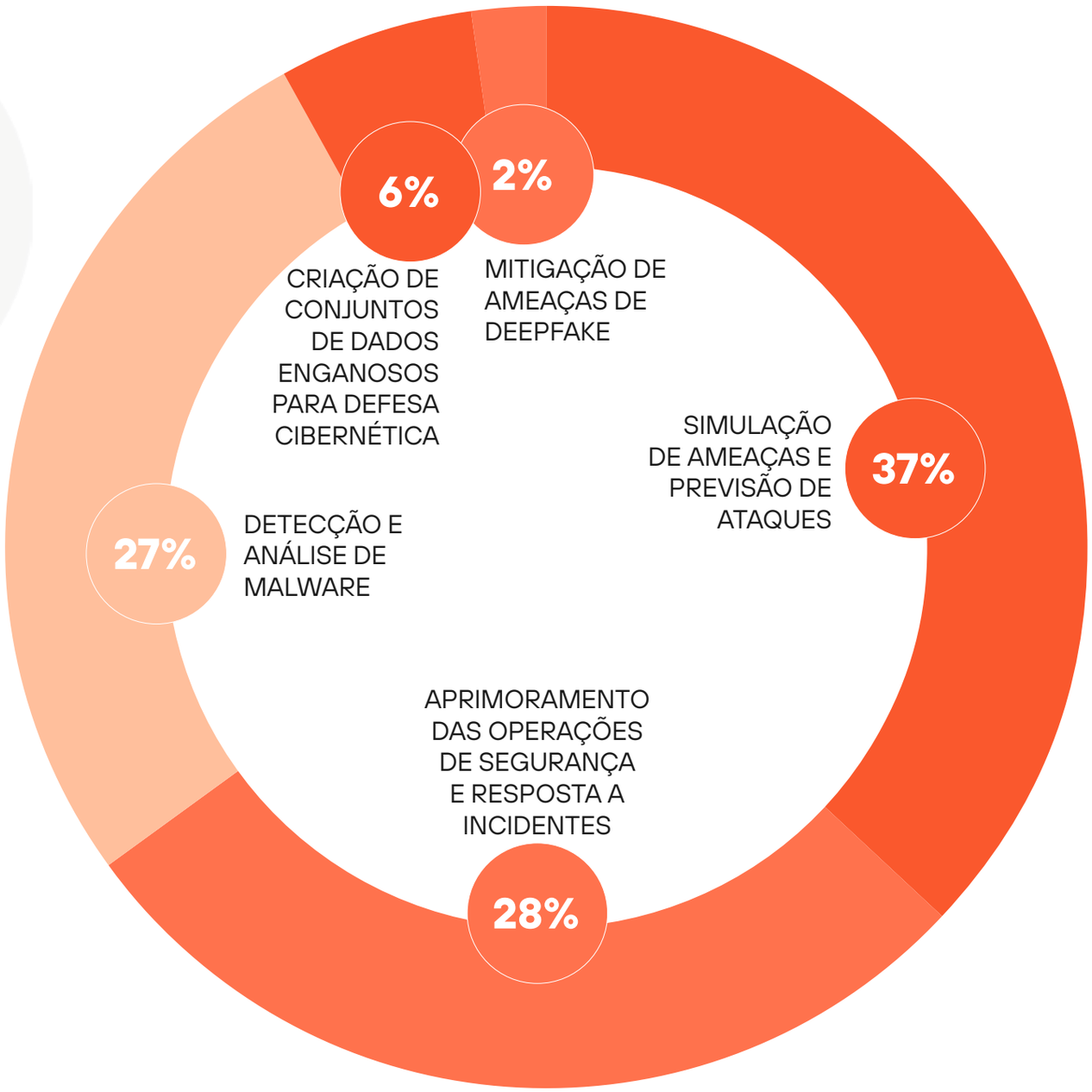
paloalto NETWORKS

priorities

A Lynchpin Media BRAND

14

Você está utilizando IA e automação em alguma das seguintes aplicações para enfrentar o gap de habilidades em cibersegurança?



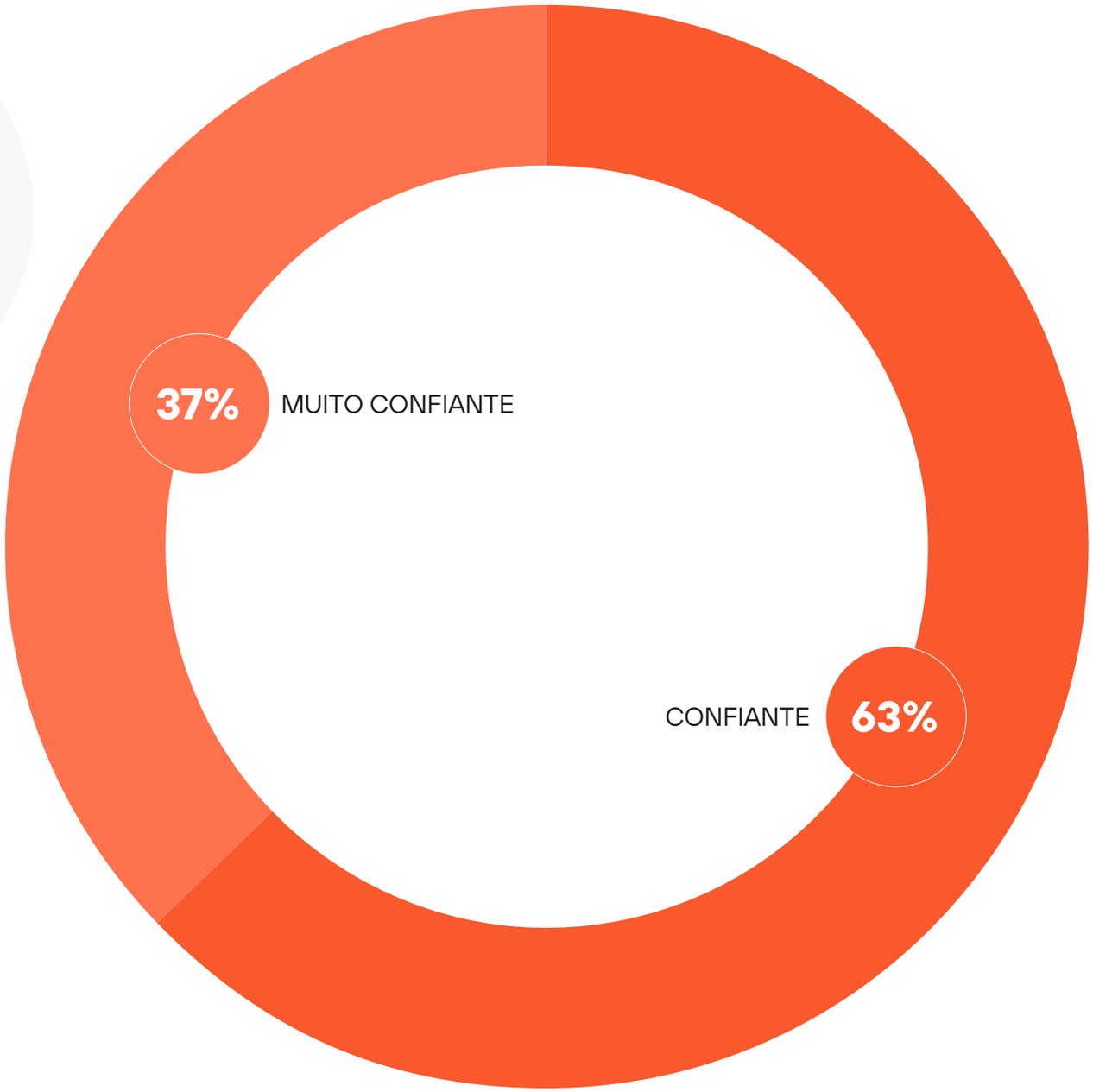
Principais insights:

IA e automação estão dominando o cenário tecnológico, e as organizações estão ansiosas para identificar como usar essas ferramentas para aumentar e simplificar processos. Embora agentes mal-intencionados também estejam utilizando IA para organizar ataques rápidos, há muitos casos em que a automação está fortalecendo as defesas, especialmente em um setor conhecido pela escassez de habilidades.

De fato, mais de um terço (37%) dos respondentes estão usando IA para simulação de ameaças e previsão de ataques, enquanto 27% a utilizam para detecção e análise de malware. Esses resultados mostram como muitas organizações estão usando IA e automação em todo o cenário da cibersegurança, destacando o impacto positivo dessa tecnologia.

15

Em caso de um ataque cibernético, quão confiante você está na capacidade de sua organização de responder e manter as operações de negócios enquanto protege dados críticos?



Principais insights:

Os dados são frequentemente chamados de "o coração pulsante" de uma organização, o que demonstra sua importância e a necessidade de protegê-los. Os respondentes da pesquisa se mostraram "confiantes" (63%) ou "muito confiantes" (37%) em suas habilidades para responder a ataques cibernéticos e manter as operações de negócios enquanto protegem dados críticos, reforçando a convicção de que as organizações estão priorizando a proteção desses dados como parte de sua estratégia. Esses resultados refletem as capacidades empresariais no cenário atual e ajudam a gerar confiança nos clientes.

Conclusão

À medida que os CIOs se preparam para assumir um papel mais estratégico nos próximos cinco anos, seu foco se volta cada vez mais para impulsionar a transformação dos negócios por meio da adoção de tecnologias avançadas. A cibersegurança continua sendo uma preocupação central, com a IA desempenhando um papel crucial na simulação de ameaças, detecção de malware e automação das operações de segurança. A conformidade com regulamentações como DORA, CRA e NIS2 exige ajustes contínuos nas políticas, especialmente na cadeia de suprimentos (suply chain, em inglês).

O aumento do trabalho remoto e a expansão dos dispositivos IoT (Internet of Things, em inglês) fizeram da cibersegurança uma prioridade para o próximo ano. Quase metade dos entrevistados está fortalecendo suas operações de segurança com IA e automação para enfrentar a escassez de habilidades, o que ajuda a inspirar confiança entre os funcionários e proteger funções críticas.

O relatório enfatiza a importância de uma cultura de conscientização e treinamento em cibersegurança, destacando que a adoção de IA para automação e resiliência cibernética está se tornando cada vez mais comum. Tendências como a abordagem “Cloud First”, o foco em cibersegurança e a expansão da automação estão moldando o futuro.

Os CIOs precisam garantir que os investimentos em tecnologia gerem um ROI mensurável, aproveitando ferramentas digitais para aumentar a lucratividade e simplificar processos. A colaboração entre os executivos da C-suite e entre diferentes funções é fundamental para fortalecer as defesas cibernéticas e alinhar os objetivos estratégicos. Em resumo, o relatório destaca a necessidade de estratégias adaptativas para enfrentar os desafios futuros.

CxO Priorities, a Lynchpin Media brand
63/66 Hatton Garden
London, EC1N 8LE

www.cxopriorities.com

Patrocinado por:

3000 Tannery Way
Santa Clara, CA 95054
info@paloaltonetworks.com

www.paloaltonetworks.com