pwc

O *playbook* do C-Level: posicionando a segurança no epicentro da inovação

Pesquisa Global Digital Trust Insights 2024

Conteúdo

Apresentação

Segurança no epicentro da inovação: ainda não é o mundo em que vivemos, mas e se fosse?

É verdade que estão em alta o entusiasmo e os orçamentos em relação a programas mais avançados de segurança. Contudo, caminhar em direção à melhoria pode ser um processo lento, havendo até mesmo estagnação.

A **Pesquisa Global Digital Trust Insights 2024** da PwC – que entrevistou 3.876 executivos de negócios, tecnologia e cibersegurança das maiores empresas do mundo, 30% das quais com receitas de US$ 10 bilhões ou mais – mostra um espaço considerável para melhorias na cibersegurança.

Confira estas descobertas: os custos de violações de dados e o número de violações de alto valor seguem em expansão. Embora os ataques a provedores de serviço em nuvem sejam a principal preocupação cibernética, cerca de um terço das empresas não tem um plano de gestão de riscos para enfrentá-los.

Além disso, somente metade relata estar muito satisfeita com suas capacidades tecnológicas em áreas-chave da cibersegurança e mais de 30% não seguem de forma consistente o que deveriam ser práticas-padrão de defesa.

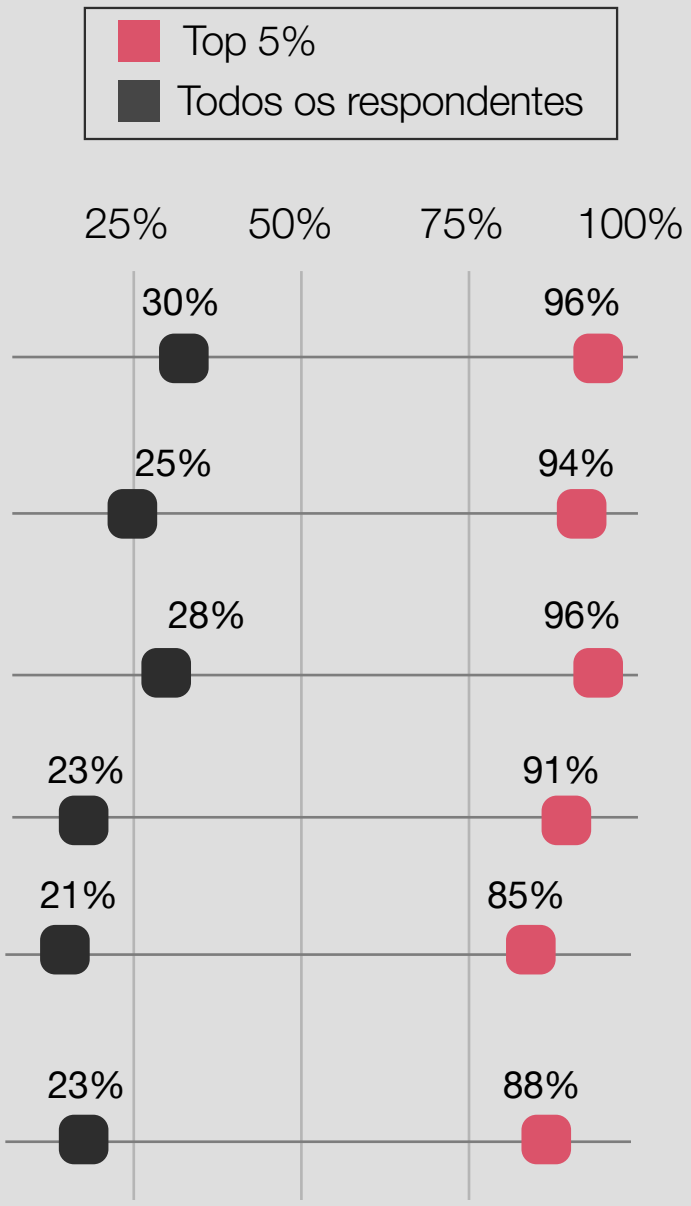
Imagine um mundo com a segurança no epicentro da inovação — um campo onde florescem ideias brilhantes e grandes ambições. Agora imagine o CISO ali, trabalhando para proteger as ambições e os ativos mais valiosos da empresa.

5% parecem estar fazendo justamente isso. Esses executivos (top 5%) — nossos guardiões da confiança digital — estão colhendo benefícios que outros estão perdendo. Eles experimentam menos violações e os ataques que os atingem não são de alto custo.

No caso desses 5%, gerenciar riscos é também mais fácil porque simplificaram suas soluções de segurança. Além disso, eles se posicionaram para ser mais produtivos e crescer mais rapidamente, superando a concorrência à medida que mergulham em novas tecnologias com a confiança de que estão bem protegidos.

Conheça nossos guardiões da confiança digital

Percentual que diz que suas equipes de cibersegurança "normalmente" (80% a 100% do tempo) fazem isso.



Defesa

Respondem rapidamente a ameaças para que a organização possa sair mais forte das disrupções.

Incorporam padrões de privacidade e segurança de dados em produtos, serviços e relacionamentos com terceiros.

Implementam controles em toda a organização para prevenir disrupções cibernéticas graves.

Alocam o orçamento de cibersegurança para os principais riscos da empresa.

Mantêm um relacionamento com o setor público em todos os níveis administrativos para construir resiliência.

Colaboram com outras áreas do negócio que afetam a postura da cibersegurança organizacional (por exemplo, engenharia de software, gestão de produtos, compras, marketing, etc).

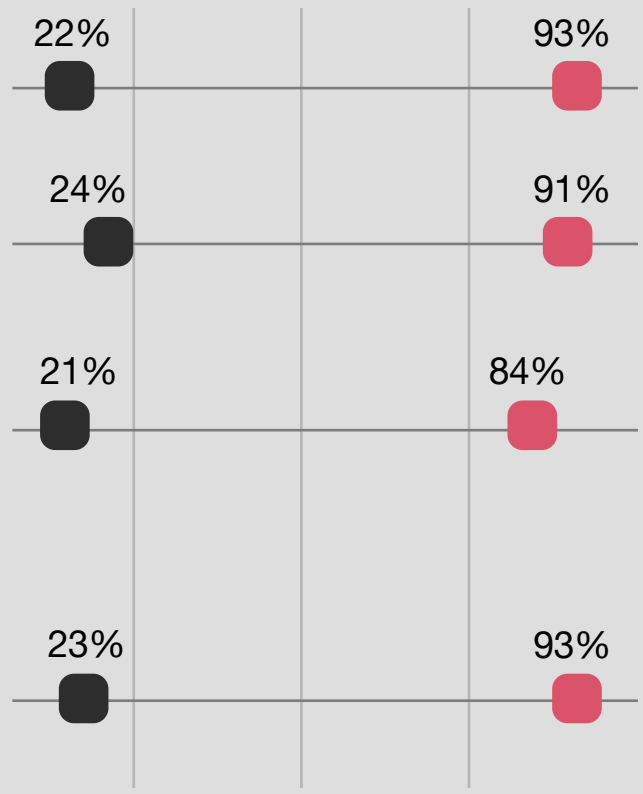
Disposição para o crescimento

Antecipam futuros riscos cibernéticos, considerando o ambiente macro e a estratégia de negócio.

Comunicam as práticas e a estratégia de cibersegurança para ganhar a confiança dos clientes e parceiros.

Aceleram as iniciativas de transformação digital e outras ações de grande dimensão da organização (por exemplo, incorporando segurança e privacidade em novos produtos e serviços).

Trazem insights sobre a exposição a riscos cibernéticos em transformação e medidas de mitigação para o CEO e o Conselho.



Q26. Indique com que consistência a equipe de segurança cibernética da sua organização faz o seguinte.

Base: 3.876 entrevistados.

Fonte: Pesquisa Global Digital Trust Insights 2024.

Salvaguardar a tecnologia e os processos, que estão no centro do negócio, é o mesmo que proteger a empresa. Por essa razão, em 2023, a PwC criou um *playbook* voltado a executivos C-Level para ajudá-los a focar nas perguntas que precisam responder junto com seu CISO.

Atualizamos o *playbook* para 2024 – ano que provavelmente será um divisor de águas, porque a segurança cibernética enfrenta quatro grandes transformações, cada uma das quais potencialmente disruptiva por si só.

- A premente necessidade do C-Level em modernizar e melhorar os investimentos e a infraestrutura tecnológica em um ano de cortes de custos e incerteza macroeconômica.
- O aumento das ameaças cibernéticas híbridas e a crescente dificuldade de definir uma linha divisória entre espionagem e cibercrime que impulsionam a defesa cibernética para o centro da arena da segurança nacional e setorial.
- Uma tecnologia inovadora — a inteligência artificial generativa (GenAI) — que traz novas ameaças, mas que também é uma promessa sem precedentes para a área de defesa.
- A exigência da regulamentação da transparência sobre os incidentes cibernéticos e as práticas de gestão de riscos que podem inaugurar uma nova era de transparência e colaboração.

As empresas estão se reinventando. Os legisladores estão pensando em novas abordagens regulatórias. Seus executivos têm sido igualmente inovadores na forma como protegem a organização? Quão ousados eles podem ser e o que podem fazer de diferente?

9 graus de separação: os *top performers versus* o resto

Os top 5% são:

6x mais propensos a terem implementado iniciativas transformadoras de segurança cibernética, das quais colhem benefícios.

5x mais propensos a estarem muito satisfeitos com suas capacidades tecnológicas cibernéticas.

4x mais propensos a continuamente atualizar seu plano de gestão de riscos para mitigá-los na nuvem.

9x mais propensos a serem maduros em suas práticas de resiliência cibernética.

Os top 5% estão mais propensos a:

Investir mais em cibersegurança. No total, **85% aumentarão seu orçamento em 2024** (contra 79% no geral). Nesse grupo, 19% dizem que vão elevar o valor em 15% ou mais (contra 10% no geral).

Relatar que a **violação cibernética mais prejudicial** dos últimos três anos custou a sua organização menos de US$ 100 mil (28% contra 19% no geral).

Concordar com veemência que sua **empresa desenvolverá novas linhas de negócio com a GenAI** (49% contra 33% no geral).

Planejar a adoção de ferramentas de GenAI para defesa cibernética (44% contra 27%).

Discordar que a GenAI causará um ataque cibernético catastrófico (33% contra 22% no geral).

Fonte: Pesquisa Global Digital Trust Insights 2024.

Uma gestão de riscos cibernéticos pronta para a reinvenção

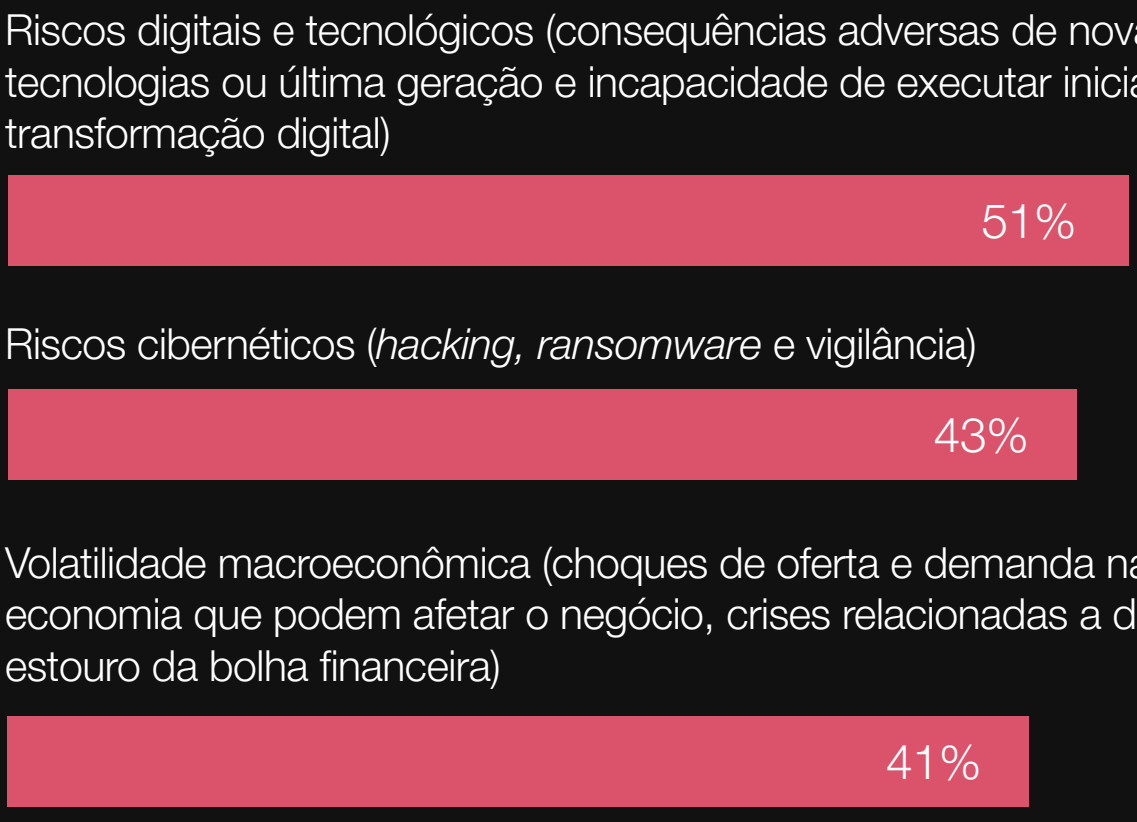
Inovar significa fazer movimentos ousados. Não há nada mais empoderador do que saber que se fez todo o possível para permanecer protegido e que os riscos cibernéticos mais importantes foram avaliados e tratados.

Reduzir riscos cibernéticos é a prioridade máxima de 2024. Após ter caído para a quarta posição na lista dos riscos priorizados do C-Level em nossa 26ª Pesquisa Global Anual de CEOs de 2023, essa questão ocupa, em 2024, a segunda posição – atrás apenas dos riscos tecnológicos. Aliás, para os CEOs, os riscos digitais e tecnológicos são inseparáveis dos cibernéticos.

No ambiente de negócio atual, não dá mais para falar de transformação digital ou reinvenção sem mencionar, ao mesmo tempo, a segurança cibernética. Ataques à nuvem e a dispositivos conectados – duas tecnologias que estão no centro da transformação empresarial hoje – são as ameaças cibernéticas que mais preocupam.

Na lista de prioridades, as digitais lideram de duas formas

Prioridades de mitigação de risco nos próximos 12 meses (ranking dos três primeiros)



As ameaças cibernéticas estão interconectadas. Uma vez que agentes maliciosos invadem sistemas e redes, eles frequentemente causam estragos de todas as maneiras possíveis.

O que pode começar como uma violação à nuvem pode se tornar uma ameaça persistente, já que agentes mal-intencionados se escondem no sistema, coletam dados e procuram formas alternativas de causar dano. Podem também roubar dados, lançar ataques de *ransomware* e, em seguida, vazar essas informações ("*hack and leak*"), mesmo quando o resgate é pago.

Qualquer um desses incidentes seria problemático por si só. Porém, quando acontecem juntos, podem devastar as operações empresariais e a reputação. A má notícia é que grandes violações estão crescendo em número, escala e custo. Passou de 27% em 2023 para 36% a porcentagem dos que relataram custos de US$ 1 milhão ou mais para sua pior violação dos últimos três anos.

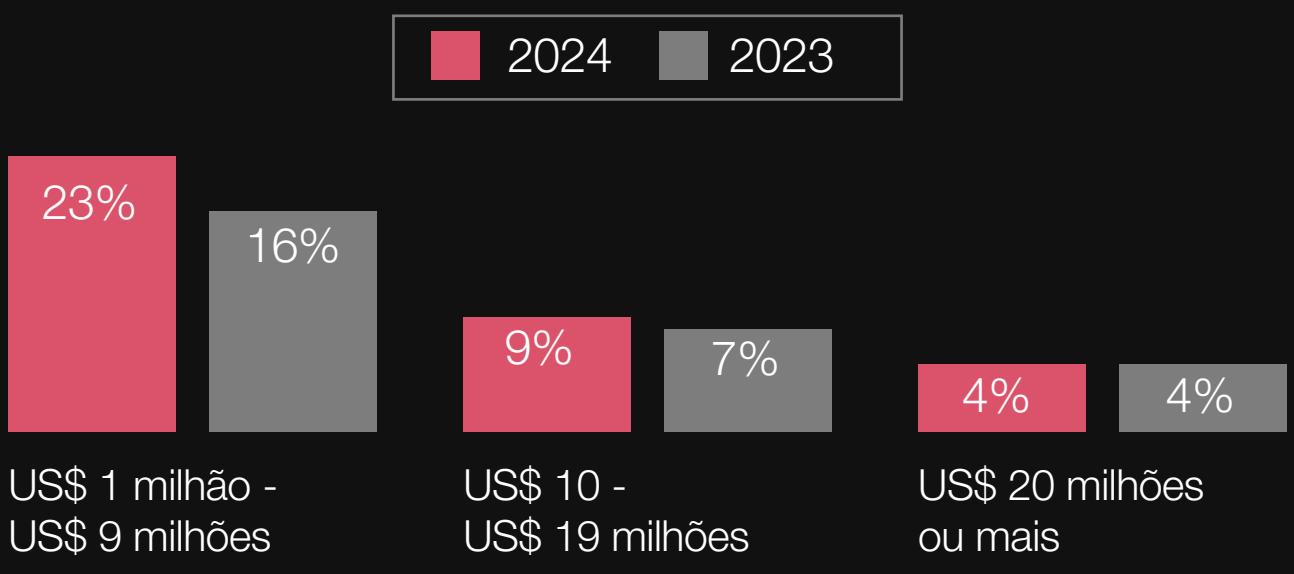
Já o ritmo da inovação e reinvenção dos negócios com o uso de tecnologia não está desacelerando. 40% dos CEOs acham que suas empresas podem não ser mais viáveis economicamente em uma década se seguirem o caminho atual.

O desafio do C-Level é este: a gestão de riscos cibernéticos da sua organização acompanha as transformações?

As violações estão ficando mais caras

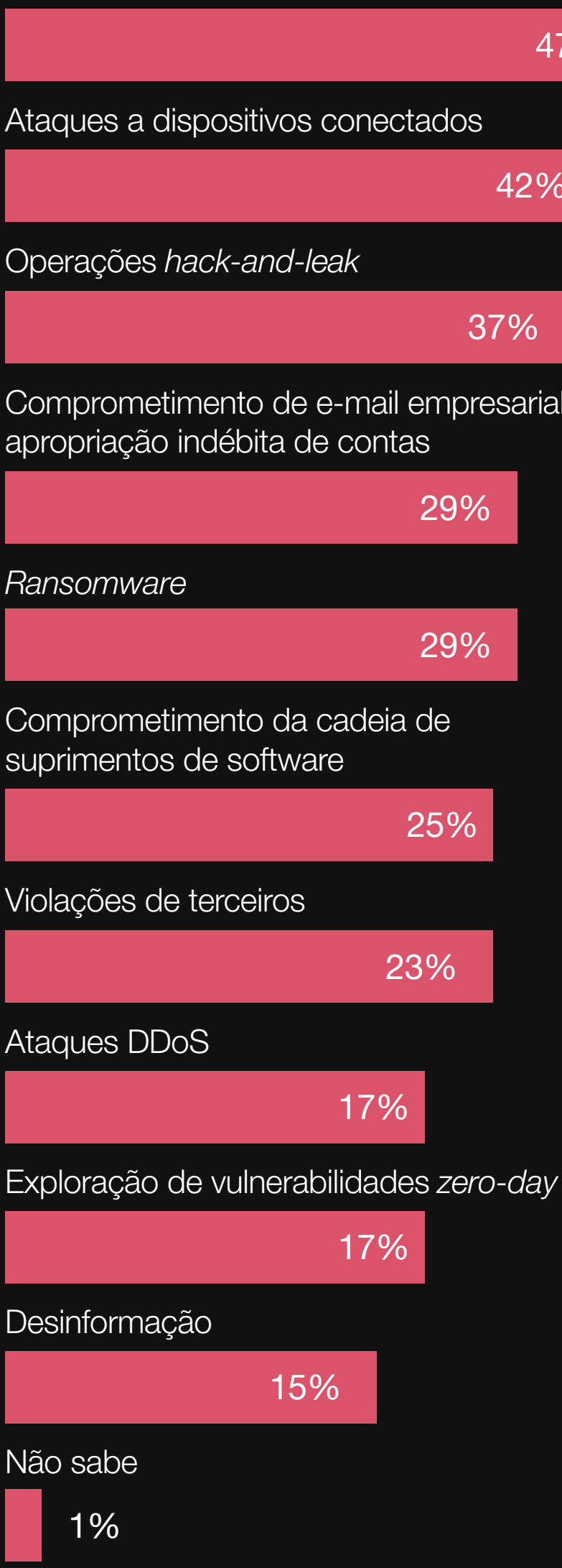
Custos estimados das violações de dados mais prejudiciais às organizações nos últimos três anos

Porcentagem dos que dizem ter tido uma violação de dados de mais de US$ 1 milhão: total de 2024 = 36%, total de 2023 = 27%

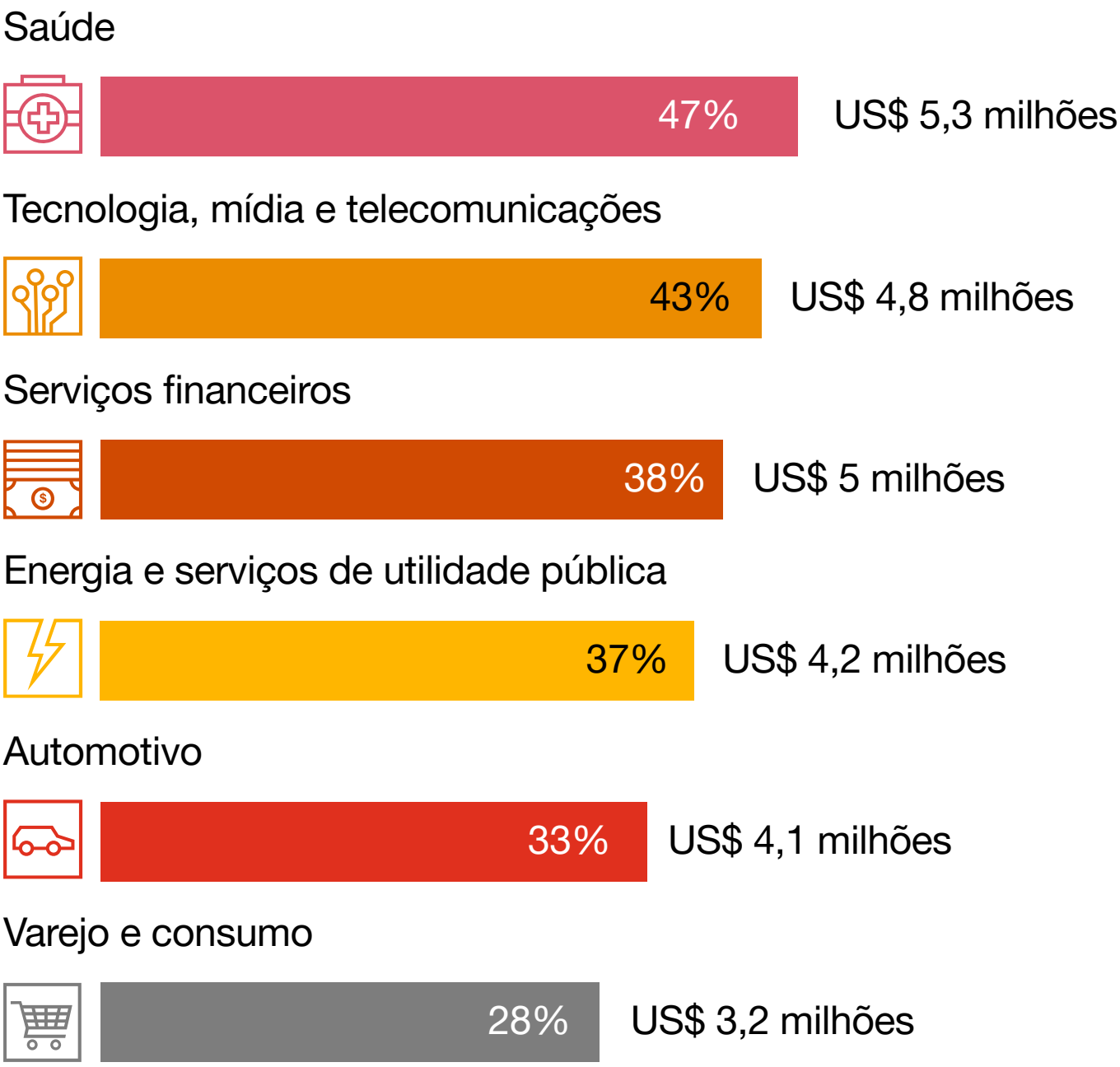


Tudo está conectado, inclusive os ataques cibernéticos

Principais ameaças cibernéticas nos próximos 3 meses



Custo médio das violações em milhões de dólares e porcentagem das fraudes mais prejudiciais, que custam US$ 1 milhão ou mais, por setor



Q5. Pensando na violação de dados mais prejudicial que você sofreu nos últimos três anos, forneça uma estimativa do custo para sua organização.

Base: entrevistados das áreas de segurança e TI e CFO = 1.651.

Fonte: Pesquisa Global Digital Trust Insights 2024.

Simplificação das tecnologias cibernéticas: a ruína dos malfeitores

Modernização e otimização lideram as prioridades de investimento em cibersegurança para 2024. Quase metade (49%) dos líderes apontou como prioritária a modernização da tecnologia, incluindo a infraestrutura cibernética, e 45% citaram a otimização das tecnologias e dos investimentos existentes.

Em 2022, descobrimos que os CEOs estavam muito preocupados que suas organizações se tornassem muito complexas para garantir sua segurança. 32% declararam ter fortalecido seus fornecedores de tecnologia para simplificar e realinhar sua combinação de serviços internos e os que gerenciam externamente.

Em 2024, 44% relatam o uso de um conjunto integrado de soluções de tecnologia cibernética e 39% planejam migrar para um nos próximos dois anos. Quase um quinto (19%) diz que tem à sua disposição muitas soluções cibernéticas e precisa consolidá-las.

Uma superabundância de soluções pontuais pode ser a razão pela qual só 5% dizem estar muito satisfeitos com as capacidades tecnológicas de suas soluções cibernéticas nas oito áreas-chave. Softwares que não trabalham em conjunto podem prejudicar a performance, exigir mais tempo de gestão e impedir a visão geral do que é essencial para gerenciar o risco cibernético.

Quem já foi atingido sabe muito bem. As empresas que sofreram violações de dados custando US$ 1 milhão ou mais, nos últimos três anos, têm maior probabilidade de reconhecer que têm muitas soluções de cibersegurança e precisam integrá-las. Já as empresas que usam conjuntos coesos de soluções cibernéticas conseguem evitar com maior frequência violações grandes e caras.

Os orçamentos de cibersegurança para 2024 visam aproveitar ao máximo as ferramentas existentes

Líderes – Prioridades de investimento em segurança cibernética nos próximos 12 meses (ranking das 3 principais)

Q14b. Quais dos seguintes investimentos você está priorizando ao alocar o orçamento cibernético da sua organização nos próximos 12 meses? (classificado entre os três primeiros).

Base: Empresas entrevistadas = 1925.

Fonte: Pesquisa Global Digital Trust Insights 2024.

Ainda assim, as empresas não estão cortando gastos. Mais de três quartos (79%) declaram que ampliarão seus gastos com segurança cibernética em 2024 (mais que os 64% em 2023), especialmente entre as empresas com receitas de US$ 5 bilhões ou mais.

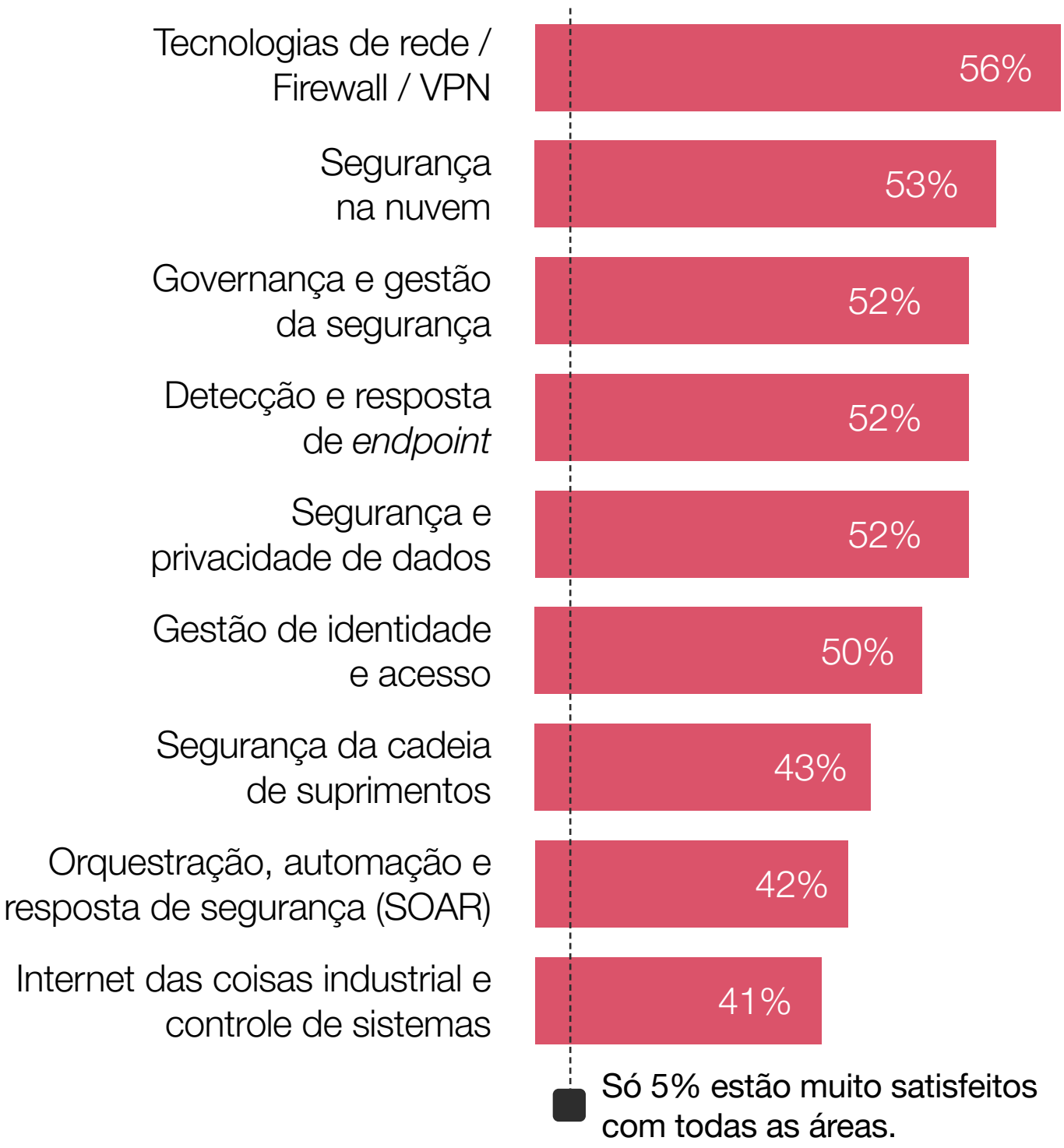
Organizações com receitas de US$ 50 bilhões ou mais, dos setores de tecnologia, mídia e telecomunicações, ou ainda as que projetam uma expansão maior de faturamento em 2024, tendem a ter planos de aumentar seu orçamento em mais de 15%.

Os investimentos em cibersegurança também representam uma proporção maior do orçamento total de TI, tecnologia operacional (OT) e automação. Estamos assistindo a um aumento da média geral de 14% em 2024 contra 11% em 2023.

O desafio do C-Level não é a falta de ferramentas ou investimentos. É, na verdade, descobrir como a organização pode colher seus benefícios. Sua arquitetura de TI é complexa demais para proteger adequadamente a empresa? Os agentes de ameaça encontram *gaps* em sua defesa com facilidade?

Só metade está satisfeita com suas capacidades tecnológicas cibernéticas

Capacidades tecnológicas da empresa em áreas-chave de cibersegurança



Segurança na nuvem: é hora de focar de verdade

O uso de serviços na nuvem sempre esteve relacionado à inovação – permitindo aos desenvolvedores colaborarem não importa onde estejam, adotando formas novas e mais flexíveis de trabalho, criando novos modelos de negócios, conectando tecnologias para ajudar a gerenciar melhor as empresas, fornecendo um serviço superior aos clientes e por aí vai.

Não por acaso, a segurança na nuvem é a preocupação de risco cibernético número 1 de quase metade (47%) das empresas. As formas como agentes mal-intencionados podem invadi-la parecem ser praticamente ilimitadas.

As organizações precisam estabelecer controles em todos os lugares: na identidade e no acesso, na movimentação lateral, nas contas de e-mail, nos portais da internet, nas aplicações, informações proprietárias, interações com clientes, nos sistemas operacionais, dispositivos conectados – e a lista continua.

Segurança da nuvem: principal ameaça e investimento – mas a gestão deixa a desejar

Q19. Até que ponto a sua organização abordou os seguintes desafios com o(s) seu(s) provedor(es) de serviços em nuvem?

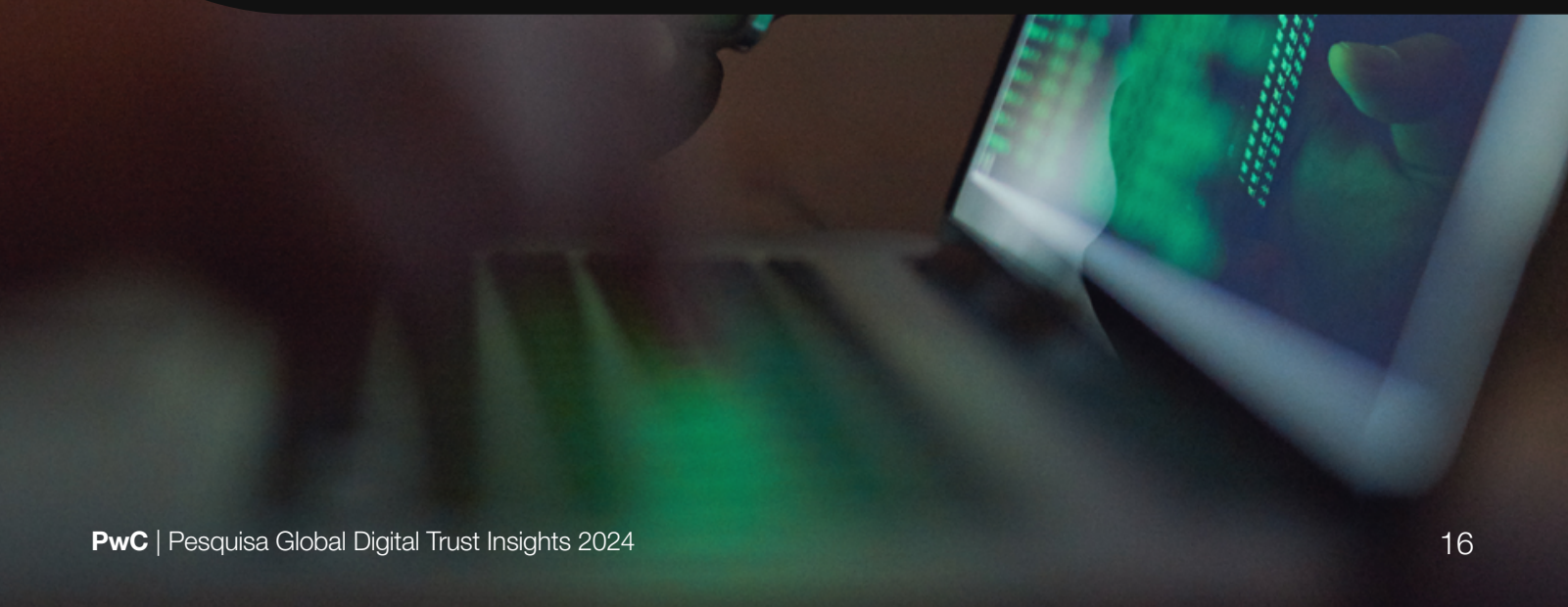
Base: usuários de provedores de nuvem = 3.648.

Fonte: Pesquisa Global Digital Trust Insights 2024.

42% usam mais de uma nuvem, e as preocupações com a segurança aumentam entre usuários de múltiplas (híbridas) nuvens. 54% citam o serviço de nuvem como seu risco de cibersegurança mais urgente.

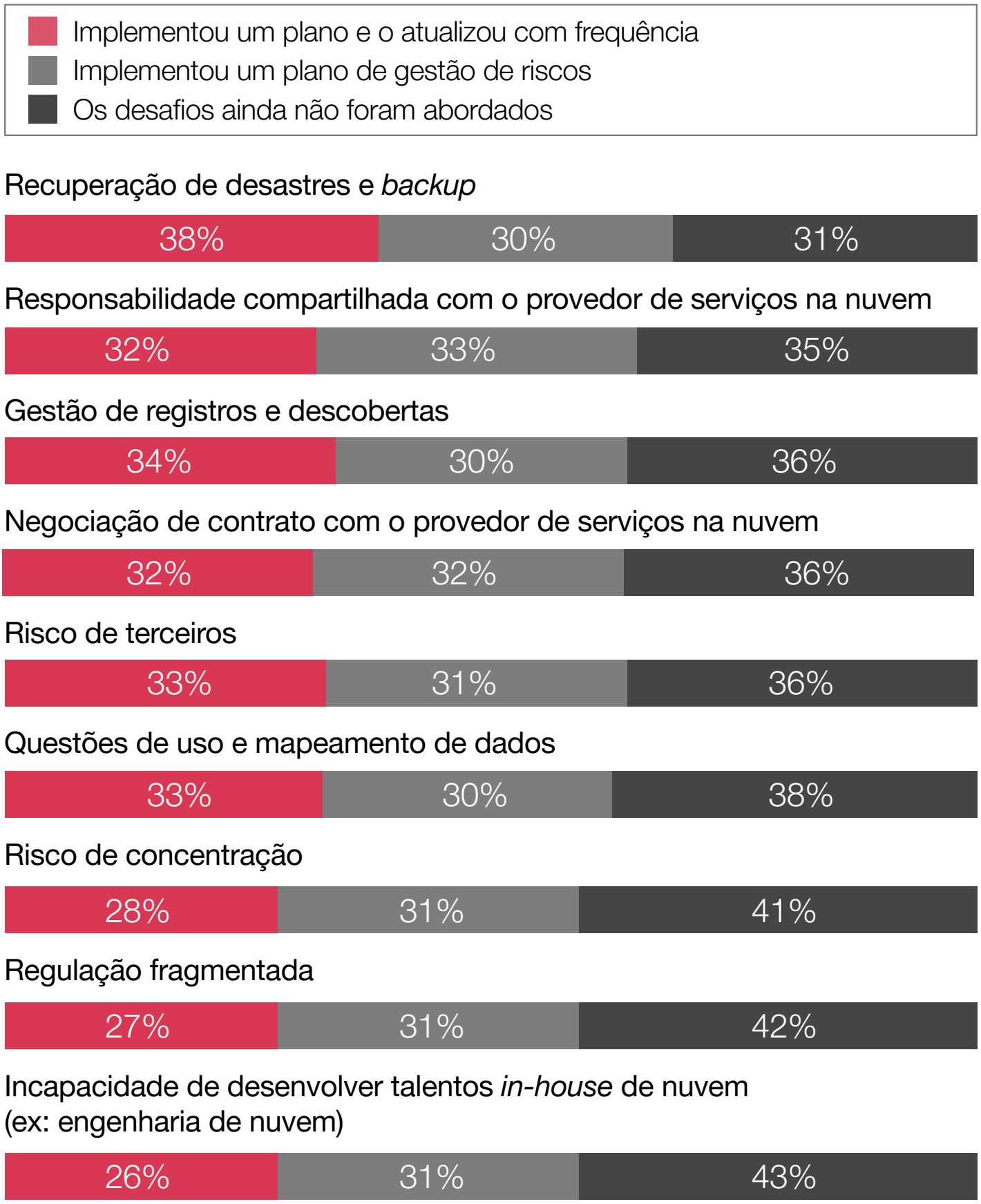
Os usuários do modelo híbrido são também os mais propensos a destacar a nuvem entre suas três prioridades de investimento em segurança este ano (36% contra 33% no geral).

Porém, quase todas as organizações (97%) têm lacunas em seus planos de gestão de risco na nuvem. Somente 3% mantêm planos atualizados que abordam todas as nove áreas de segurança. Além disso, 42% ainda não trataram dos riscos de uma regulação fragmentada, 41% não têm plano para lidar com o risco de concentração e 36% ainda não endereçaram o risco na nuvem de terceiros.



Muitos riscos na nuvem, poucos planos para lidar com eles

Posição da empresa sobre os desafios dos provedores de serviços na nuvem



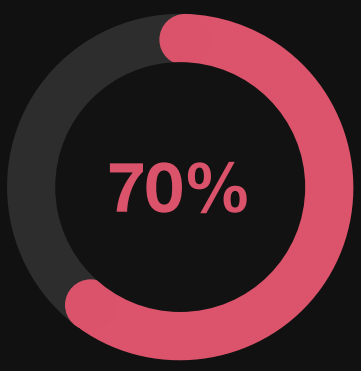
Os 5% melhores líderes — nossos guardiões da confiança digital — estão quatro vezes mais propensos a atualizar continuamente seu plano de gestão de riscos para mitigar os da nuvem. Mas 95% ainda têm muito trabalho pela frente.

O desafio do C-Level é o seguinte: como trabalhar de forma conjunta com seus provedores de segurança na nuvem para avançar na defesa dos pontos de entrada mais importantes para seus sistemas e ativos críticos nesse ambiente?

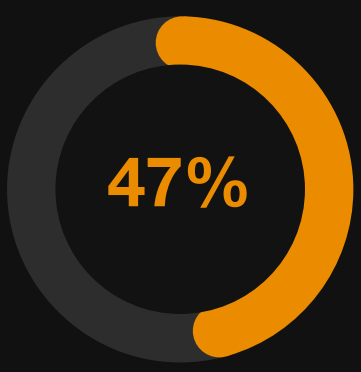
A IA generativa em ascensão para a defesa cibernética

Quase 70% dizem que sua empresa usará a GenAI na defesa cibernética. Essas ferramentas podem ajudar a reduzir a desvantagem das equipes de cibersegurança sobrecarregadas pelo grande número e pela complexidade dos ataques cibernéticos liderados por pessoas – ambos em constante elevação.

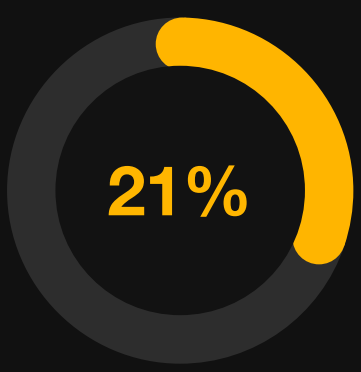
GenAI para a defesa cibernética



Quase 70% dizem que usarão a GenAI para defesa cibernética nos próximos 12 meses



47% já estão usando a GenAI para detecção e mitigação de riscos cibernéticos



21% já estão colhendo os benefícios de seus programas de cibersegurança por causa da GenAI, em poucos meses de uso.

As plataformas estão licenciando seus grandes modelos de linguagem (LLMs) junto com suas soluções tecnológicas cibernéticas. O Microsoft Security Copilot, por exemplo, pretende fornecer recursos de GenAI para a gestão da postura de segurança, resposta a incidentes e elaboração de relatórios. Já o Google anunciou o Security AI Workbench para uso semelhante.

Muitos fornecedores estão forçando os limites da GenAI, testando tudo o que é possível. Pode levar algum tempo até vermos o uso em larga escala desses *defenceGPTs*. Enquanto isso, confira as três áreas mais promissoras para o uso dessa tecnologia na defesa cibernética.

Detecção e análise de ameaças. A GenAI pode ser inestimável para detectar, de forma proativa, a exploração de vulnerabilidades, avaliar com agilidade sua extensão – o que está em risco, o que já foi comprometido e quais são os danos – e então apresentar opções testadas e aprovadas de defesa e remediação.

Pode ajudar também a identificar padrões, anomalias e indicadores de comprometimento que escapam aos sistemas tradicionais de detecção baseados em assinaturas.

Elaboração de relatórios de risco e incidentes cibernéticos. A GenAI pode ainda tornar os relatórios de risco e de incidentes cibernéticos muito mais simples. Com o apoio do processamento de linguagem natural (NLP), pode transformar dados técnicos em um conteúdo conciso que pessoas não-especializadas conseguem entender.

Pode ajudar também com a elaboração de relatórios de resposta a incidentes, inteligência de ameaças, avaliação de risco, auditorias e *compliance* regulatório. Por fim, pode recomendar ações em uma linguagem que qualquer um pode entender, até mesmo traduzindo gráficos confusos em textos simples.

Controles adaptativos. Proteger a nuvem e a cadeia de suprimentos de software requer atualização constante das políticas e dos controles de segurança – uma tarefa que pode ser assustadora.

Os algoritmos de aprendizado de máquina e as ferramentas da GenAI poderão, em breve, recomendar, validar e rascunhar políticas de segurança, além de automatizar controles adaptados ao perfil de ameaça, às tecnologias e aos objetivos empresariais de uma organização.

O desafio do C-Level é o seguinte: como controlar as novas ferramentas sem provocar novos riscos na organização e sociedade? Como usar a GenAI de forma ética e responsável?

Regulamentação: proporcione um lugar seguro para operar e crescer

O senso comum diz que novas regras e regulamentações prejudicam as receitas. No entanto, pelo menos um terço dos líderes da área de cibersegurança acredita que “as proteções que os reguladores estabelecem podem conferir às empresas mais confiança para explorar, experimentar, inventar e competir”. Lidar com as exigências regulatórias pode se tornar uma vantagem competitiva.

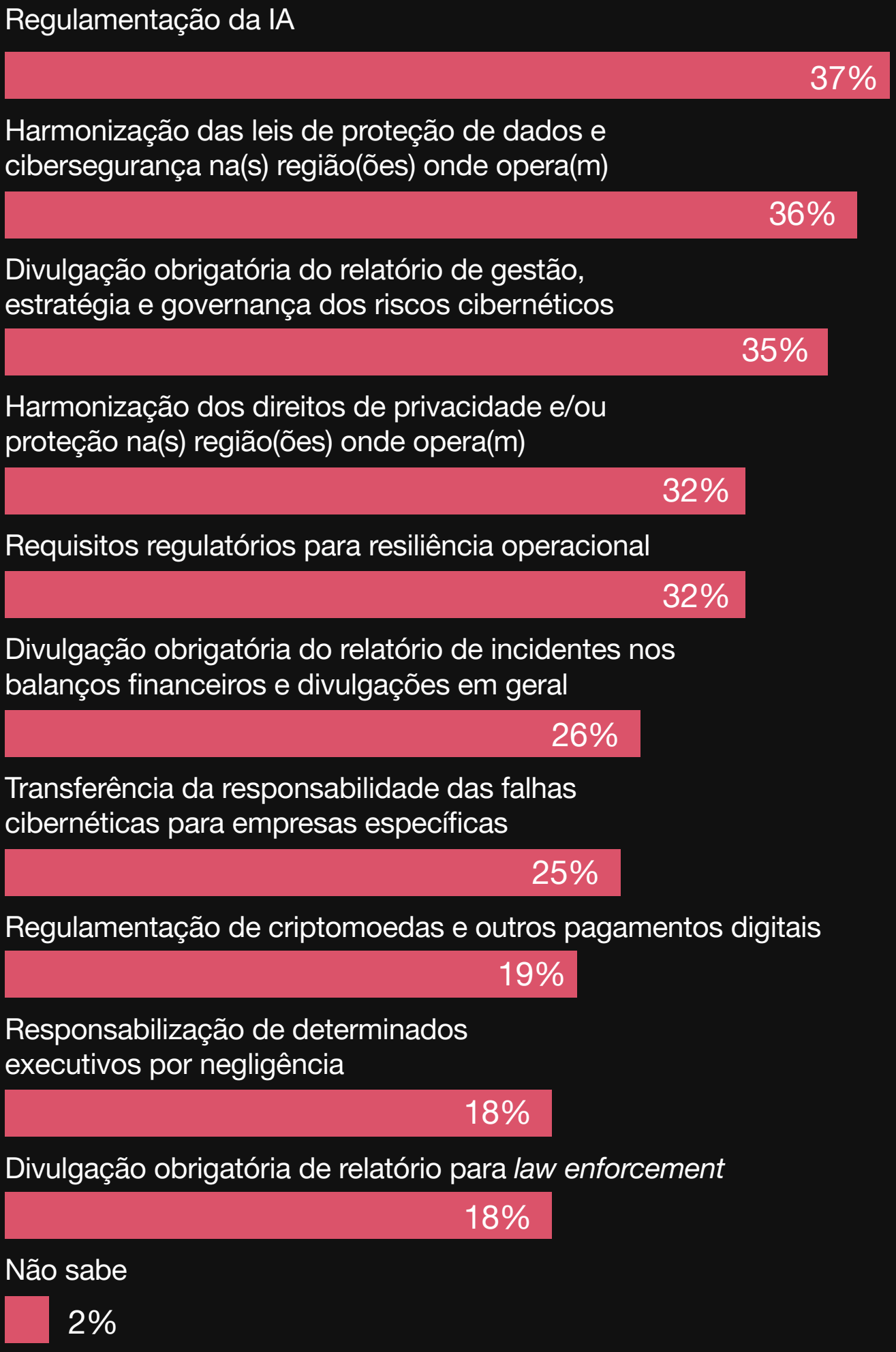
Cerca de um terço dos respondentes concorda que quatro tipos de regulamentação serão mais importantes para garantir o crescimento futuro de suas empresas: a da IA (37%); a harmonização das leis de proteção de dados e cibersegurança (36%); a que trata da elaboração de relatórios obrigatórios para gestão, estratégia e governança dos riscos cibernéticos (35%); e os requisitos de resiliência operacional (32%).

A transparência é a demanda regulatória que continuará a aumentar mundialmente. As novas regras da *Securities and Exchange Commission* (SEC) já determinam a divulgação pública das violações de segurança cibernética e no Brasil a Lei Geral de Proteção de Dados (LGPD) exige a comunicação de incidentes envolvendo dados pessoais, que tenham potencial efeito material sobre as operações e os investidores. As empresas também precisam estar preparadas para as exigências impostas pelos reguladores setoriais, como Banco Central, SUSEP, ONS, ANEEL e outros.

O *Digital Markets Act* e o *Digital Services Act* exigem a transparência nas práticas de dados e na tomada de decisões algorítmicas. Além disso, estão no horizonte regulamentações em relação à IA — incluindo uma Lei de IA da União Europeia em andamento e a regulamentação da GenAI.

Diretrizes regulatórias que poderiam mudar a segurança cibernética

Objetivos e princípios regulatórios com maior impacto para o crescimento futuro da receita da empresa (ranking dos 3 principais)



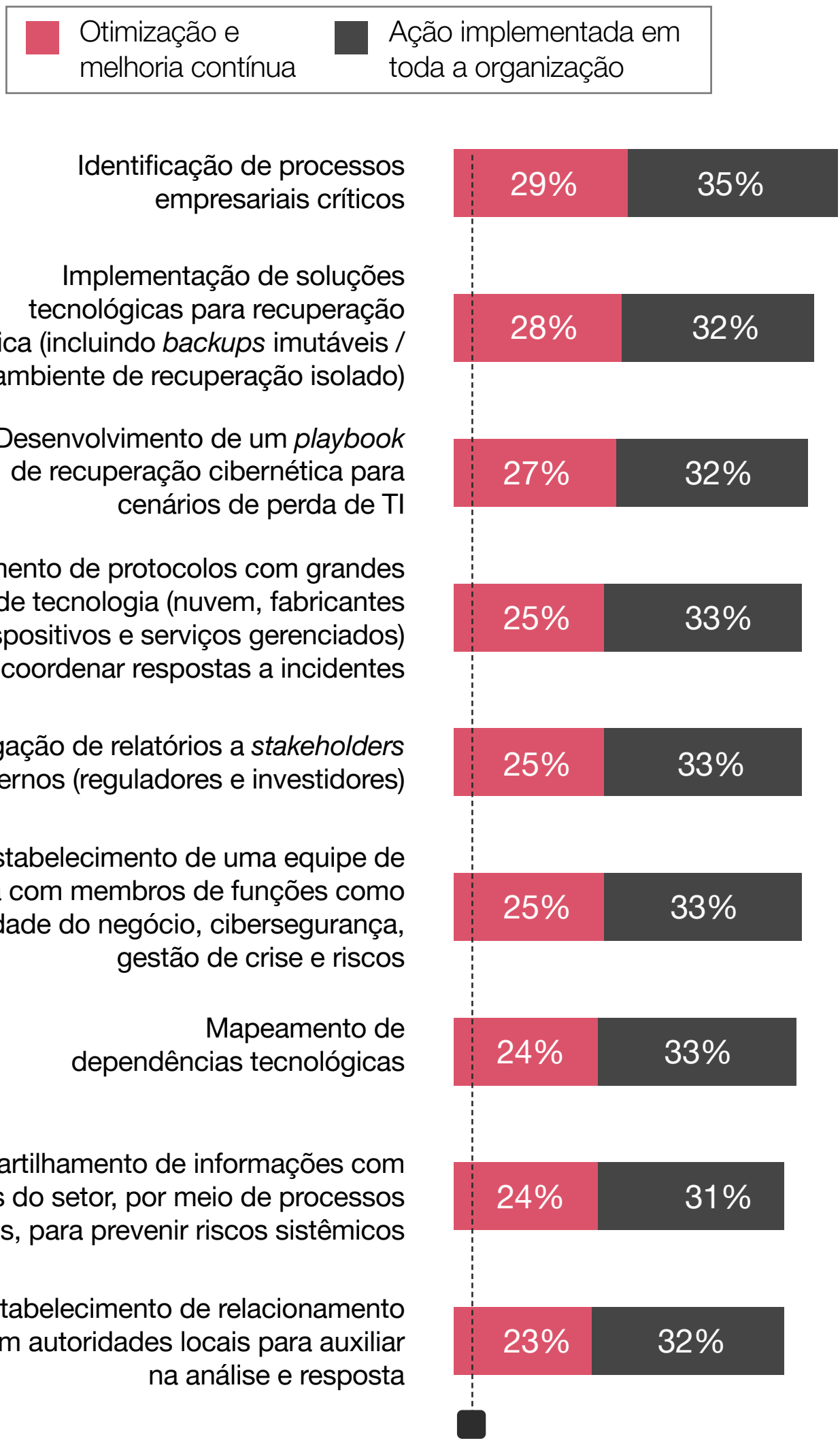
Q24. Quais dos seguintes objetivos e princípios regulatórios propostos terão o maior impacto na capacidade da sua organização de garantir o crescimento futuro das receitas? (classificado entre os três primeiros).

Base: Todos os entrevistados = 3.876.

Fonte: Pesquisa Global Digital Trust Insights, resultados finais, agosto de 2023.

O progresso lento da resiliência cibernética

Grau de implementação de ações-chave para resiliência em segurança cibernética



Somente 2% estão otimizando e melhorando continuamente em todas as áreas.

A resiliência operacional é outro tema importante. Os reguladores sabem que é um grande risco abordar o desafio dos riscos complexos e interrelacionados como acontece frequentemente entre muitas equipes de C-Level – como um exercício isolado que trata o perfil de risco de cada unidade de negócios separadamente.

Novas exigências, como as do Digital Operational Resilience Act, insistirão cada vez mais na promoção de uma resiliência integrada com elementos centrais que tornem a empresa adaptável, flexível e mais forte após cada evento disruptivo.

Cerca de três quartos dos entrevistados esperam que o *compliance* dessas regulamentações exigirá gastos significativos com tempo e dinheiro. Por outro lado, os altos custos e impactos nas receitas podem ser evitados se as organizações se envolverem desde cedo e com frequência nos processos regulatórios — reunindo-se com as autoridades locais, participando de audiências públicas e até ajudando os reguladores a elaborar ou influenciar diretrizes.

O desafio do C-Level é o seguinte: em meio à incerteza regulatória, você consegue abrir espaço para a sua empresa inovar e manter a segurança e a privacidade desde o início? Como você transforma esse novo ambiente regulatório em vantagem competitiva?

O *playbook* do C-Level em 2024: atue para deixar o *cyber-as-usual*

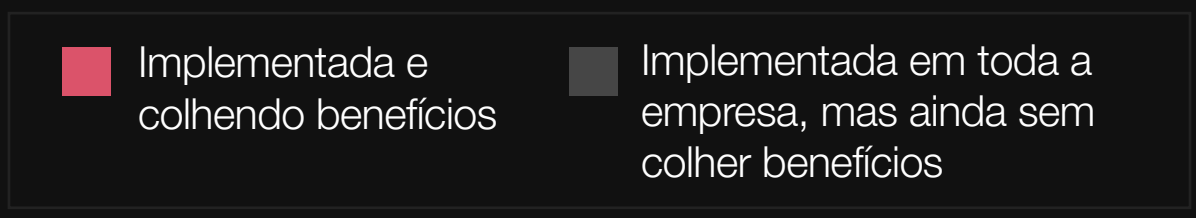
Não se trata mais do *business-as-usual* na sua empresa. A maioria das organizações está presa ao *cyber-as-usual*, como esta pesquisa demonstra bem.

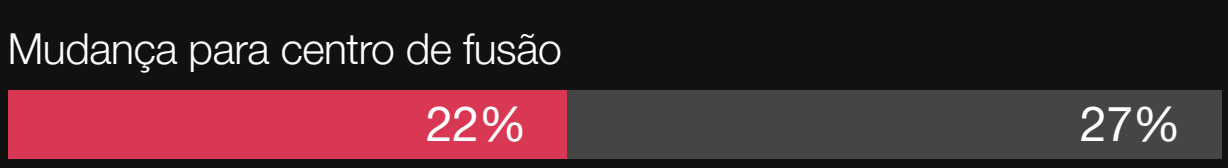
São muitas iniciativas fragmentadas e complexidades tecnológicas sempre em expansão. Um programa de gestão de risco que, com seus *gaps*, é arriscado por si só. Transformações e projetos que não produzem os resultados esperados. Todos esses obstáculos permanecem no caminho de uma segurança cibernética verdadeiramente confiável.

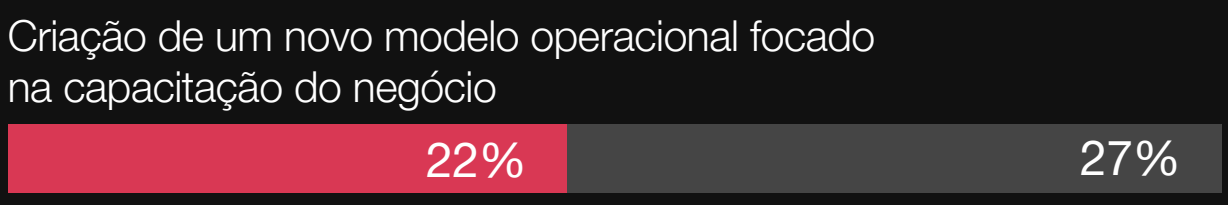
No *playbook* de 2023, identificamos desafios críticos e ainda relevantes que o C-Level deveria tratar em conjunto.

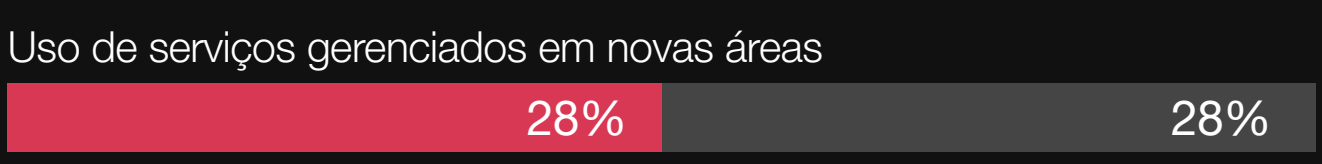
Seu programa de segurança cibernética é focado em *cyber* ou no negócio?

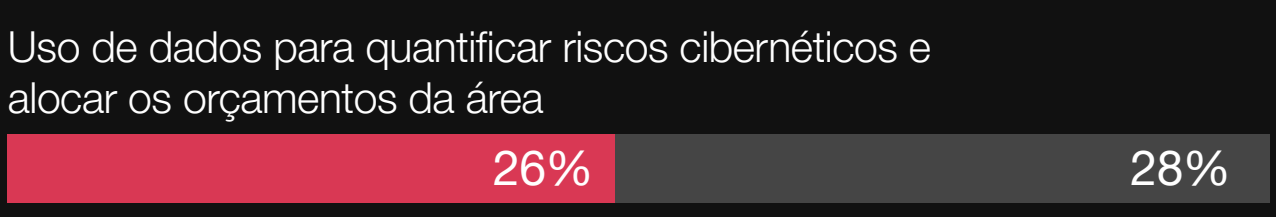
As iniciativas na parte de cima do gráfico são focadas na cibersegurança; na parte inferior, no negócio

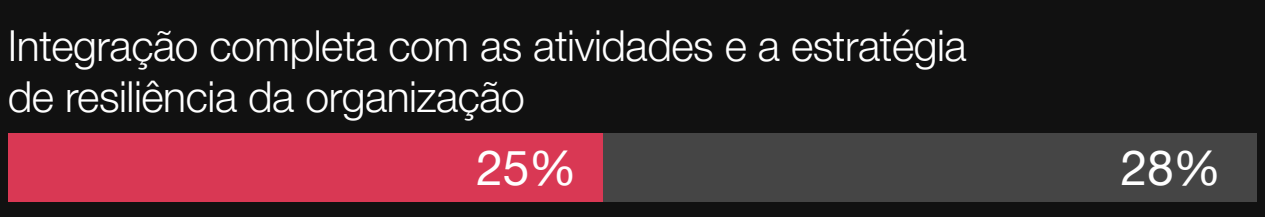












Em 2024, os desafios são estes:

Como líder, você promove a consolidação das tecnologias e gera convergência com a ampliação da eficiência da defesa, visibilidade total dos riscos, adoção das novas capacidades de proteção e o aproveitamento das oportunidades de redução dos atuais custos?

Você dá saltos criativos para finalmente superar os obstáculos que bloqueiam sua empresa de atingir seus objetivos?

Já vemos algumas organizações pensando nas melhores apostas. São muitas as opções.

Qual é o melhor caminho para a sua organização?

Fale uma nova língua.

Estar no epicentro da inovação significa se reunir com suas equipes de liderança onde elas estão para ajudá-las a superar a intimidação que eventualmente possam sentir em relação ao que você faz.

O uso dos jargões da sua área, como paisagem cibernética, superfície de ataque ou mesmo confiança-zero, apenas amplia o mistério para as pessoas de fora.

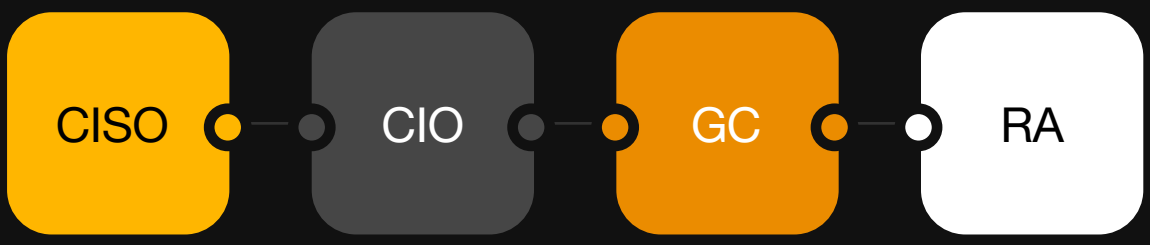
Ouse conversar sobre segurança cibernética em uma linguagem corporativa, de tecnologia, financeira ou do dia a dia. Fale com seus clientes, investidores e parceiros de negócio, nos relatórios anuais de segurança, de forma informativa e engajadora. O uso de um vocabulário mais simples pode ajudar os executivos a lidar com os *trade-offs*, as tensões e o caos que podem acontecer no epicentro da inovação.

Experimente formas novas e ousadas de gerenciar o risco cibernético.

Adote abordagens mais sofisticadas na modelagem dos riscos cibernéticos, como varreduras de potenciais ameaças, usando fórmulas específicas para o setor, a visão e a estratégia de sua empresa. Crie um incentivo de performance atrelada ao risco para todos os funcionários elegíveis a bônus na organização, de modo a construir uma cultura de riscos.

Invente novos jeitos de identificar e fortalecer suas fraquezas, talvez com um programa moderno de recompensa para detecção de erros, que incentive uma investigação de segurança independente. Por fim, adquira e comece a usar uma solução de identidade *cloudfirst*, gerenciada de forma centralizada, para proteger suas metas de expansão empresarial.

Crie barreiras de proteção.



Fale a linguagem da confiança e não apenas a do *compliance* regulatório. Envolva-se cedo e com frequência para ter uma chance maior de influenciar quaisquer regras novas e assegurar que elas vão impulsionar, e não atrapalhar, o sucesso do negócio.

Inteligência artificial, metaverso, criptomoedas e privacidade – esses tópicos regulatórios urgentes podem se beneficiar de sua experiência e seus *insights.*

Libere suas equipes para pensar criativamente (automação, GenAI, serviços gerenciados).

Ter olhos 24 horas por dia é um dos benefícios da automação, da GenAI e dos serviços gerenciados. Outra vantagem é liberar seus times da execução de tarefas rotineiras.

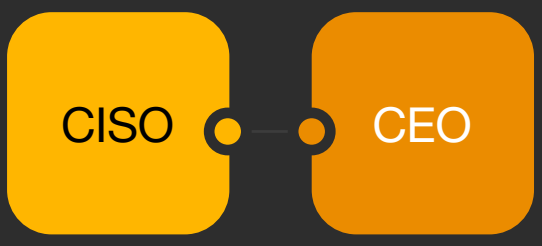
Liberados de atividades tediosas, seus colaboradores podem encontrar tempo e espaço para refletir sobre as novas ameaças cibernéticas em constante evolução e criar formas inovadoras de neutralizá-las.

Dê as boas-vindas à segurança cibernética na alta direção.

A segurança cibernética encabeça os registros de risco da maioria das organizações e em muitas pesquisas corporativas. No entanto, é um assunto recorrente nas reuniões de diretoria? Você recebe informações de qualidade, não apenas sobre riscos e controles cibernéticos, mas também sobre como as principais iniciativas estratégicas impulsionam o crescimento do negócio e da receita?

A segurança fornece a base para tudo o que sua empresa faz – finanças, desenvolvimento, recursos humanos, tecnologia e outras áreas que você provavelmente discute toda vez que acontece uma reunião. Encarar de frente o seu programa de segurança cibernética pode ser um movimento ousado.

Pense como o dono do negócio.



A transformação do negócio é uma coisa, mas a transformação cibernética não é outra. São a mesma coisa. O CISO e o CEO juntos precisam abraçar a cibersegurança como uma iniciativa de toda a empresa, colocando-se no lugar do dono do negócio.

Não gostariam que todos os aspectos — registros financeiros, pesquisas proprietárias, desenvolvimento de aplicativos, dados de clientes e assim por diante — fossem protegidos da visualização ou do uso não autorizado? Não gostariam de proteger a sua marca? A segurança cibernética não poderia impulsionar inovações que economizem os recursos financeiros e ajudem o negócio a crescer? Essa é a razão de ser da cibersegurança.

Sobre a pesquisa

A Global Digital Trust Insights Survey 2024 da PwC foi realizada com 3.876 executivos de negócios, tecnologia e segurança (CEOs, diretores corporativos, CFOs, CISOs, CIOs e líderes C-Level) entre maio e julho de 2023.

Quatro em cada 10 executivos pertencem a empresas com receitas de US$ 5 bilhões ou mais e 30% estão em organizações com receitas de US$ 10 bilhões ou mais.

Os entrevistados atuam em vários setores: manufatura industrial (20%); serviços financeiros (20%); tecnologia, mídia e telecomunicações (19%); varejo e consumo (17%); energia, serviços públicos e recursos naturais (11%); saúde (9%) e serviços estatais e governamentais (3%).

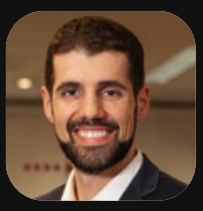
Estão baseados em várias regiões: Europa Ocidental (32%), América do Norte (28%), Ásia-Pacífico (18%), América Latina (10%), Leste Europeu (5%), África (4%) e Oriente Médio (3%).

A Global Digital Trust Insights Survey era conhecida como Global State of Information Security Survey (GSISS). Em seu 26º ano, é a pesquisa anual mais antiga sobre tendências de cibersegurança. É também a maior pesquisa do setor e a única que atrai a participação de vários executivos de negócios, não apenas os de segurança e tecnologia.

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

Contatos

Eduardo Batista
Sócio e líder de Cibersegurança
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

Acesse o site:

www.pwc.com.br

Siga a PwC nas redes sociais