FORTINET
Training Institute

# Déficit de competências em cibersegurança:

Relatório de 2023 de Pesquisa Global da Fortinet

# Conteúdo



# Metodologia

Os resultados deste relatório baseiam-se em respostas obtidas de entrevistas on-line e uma pesquisa por e-mail com 1.855 pessoas responsáveis pela tomada de decisões de TI e cibersegurança, que foi conduzida pela Sapio Research em novembro de 2022. As respostas foram obtidas em 29 locais: África do Sul, Alemanha, Argentina, Austrália, Brasil, Canadá, Cingapura, Colômbia, Coreia do Sul, Emirados Árabes Unidos, Espanha, Estados Unidos, Filipinas, França, Holanda, Hong Kong, Índia, Indonésia, Israel, Itália, Japão, Malásia, México, Nova Zelândia, Reino Unido, República Popular da China, Suécia, Taiwan, e Tailândia.

Os resultados gerais têm uma precisão de ±2,3% em limites de confiança de 95%.

### Porte da empresa

100–499 funcionários **22%**
500–999 funcionários **24%**
1.000–2.499 funcionários **23%**
2.500–4.999 funcionários **16%**
Mais de 5.000 funcionários **15%**

### Gênero

**68%** dos entrevistados eram do sexo masculino
**32%** dos entrevistados eram do sexo feminino

### Total de entrevistados: 1.855

Ásia-Pacífico **30%**
EMEA **27%**
América do Norte **22%**
LATAM **22%**

### Tipo de função

**13%** dos entrevistados ocupavam cargos de gestão
**34%** dos entrevistados ocupavam os cargos executivos seniores mais altos da empresa
**7%** dos entrevistados ocupavam cargos de vice-presidente
**12%** dos entrevistados ocupavam cargos de chefia
**34%** dos entrevistados ocupavam cargos de diretoria

### Setor de negócios

**Setores da empresa — Top 3**

Tecnologia **21%**
Manufatura **16%**
Serviços financeiros **13%**

# Resumo executivo

**Os resultados obtidos no relatório sobre déficit de competências em cibersegurança de 2023** mostram claramente que as organizações estão travando uma difícil batalha contra a ameaça cibernética, o que acaba implicando o aumento de violações, maior demanda por profissionais qualificados e a contínua dificuldade para preencher vagas importantes.

## As violações estão mais frequentes e mais caras

**84%** das organizações foram alvo de **uma ou mais violações** nos últimos 12 meses, um aumento em comparação a 80% em 2021.

**29%** sofreram **cinco ou mais invasões** em comparação a 19% no ano passado.

**48%** sofreram violações nos últimos 12 meses que **custaram mais de US$ 1 milhão** para serem remediadas, o que ultrapassa os 38% em 2021.

## As vagas não ocupadas na área de TI representam um risco à cibersegurança

**68%** das organizações afirmam **enfrentar outros riscos devido à** escassez de habilidades em cibersegurança, o que se mantém alinhado aos 67% observados em 2021.

**56% das empresas têm dificuldades para recrutar** e **54% têm dificuldades para reter** talentos, em comparação com 60% e 52%, respectivamente, em 2021.

**As funções de Operações de segurança e Segurança na nuvem** são as mais difíceis de serem preenchidas.

## Os Conselhos de Administração estão focados em cibersegurança

**93%** dos entrevistados afirmam que seu **conselho questiona quanto à cibersegurança,** o que ultrapassa os 88% em 2021.

Em 2022, **83% dos conselhos sugeriram aumentar o número de funcionários de segurança de TI,** em comparação com 76% em 2021.

## Há uma procura por certificações como comprovação de conhecimento e habilidades em cibersegurança

**90%** dos líderes **preferem contratar pessoas com certificações focadas em tecnologia,** o que ultrapassa os 81% em 2021. **90% também pagariam** para que um funcionário obtivesse uma certificação em cibersegurança.

**72%** dos líderes afirmam que a contratação de pessoas certificadas **aumentou a conscientização e o conhecimento sobre cibersegurança** dentro da empresa.

## Talentos diversificados ajudam a acabar com a lacuna de habilidades, mas nem sempre são fáceis de encontrar

Cerca de **40%** têm **dificuldade em encontrar candidatos qualificados** que sejam mulheres, veteranos militares ou pertencentes a grupos minoritários.

**83%** das empresas têm **metas de contratação de diversidade a curto prazo,** o que fica abaixo dos 89% em 2021.

A quantidade de organizações que confirmaram ter sofrido cinco ou mais violações aumentou 53% entre 2021 e 2022.

INTRODUÇÃO

# Pessoas qualificadas são fundamentais para a cibersegurança

Em 2022, os desafios de cibersegurança se intensificaram globalmente em todos os setores, desde o crescimento exponencial de novas variantes de ransomware até o aumento dos ataques à tecnologia operacional (TO) e o aumento do malware como serviço (MaaS — Malware-as-a-Service). Para muitas empresas, mais do que nunca, esses desenvolvimentos tornam a mitigação do déficit de competências em cibersegurança em suas próprias equipes de TI uma prioridade ainda maior.

Embora as soluções avançadas de cibersegurança continuem a ser essenciais para atender às demandas do cenário de ameaças em rápida mudança, o Relatório de 2023 de Pesquisa Global da Fortinet sobre Déficit de competências em cibersegurança mostra que os líderes também se atentam ao lado humano da equação, buscando entender quais habilidades eles precisam e onde encontrá-las.

O foco no desenvolvimento da capacidade em cibersegurança começa no topo, com mais conselhos de administração questionando quanto à defesa cibernética e recomendando o aumento do número de funcionários de segurança de TI. Isso provavelmente decorre de um reconhecimento de sua responsabilidade de proteger o negócio e, portanto, clientes, parceiros, funcionários e a marca corporativa.

Como mostra este relatório de 2023, as empresas estão buscando recrutar e reter talentos para atender às suas necessidades de cibersegurança, especificamente pessoas com certificações focadas em tecnologia, bem como aquelas de grupos subrrepresentados, incluindo mulheres, pessoas pertencentes a grupos minoritários e veteranos militares.

## O que há de novo em 2023

Esta edição do Relatório de Pesquisa Global da Fortinet sobre Déficit de competências em cibersegurança apresenta comparações ano a ano e análise de tendências com base no feedback de líderes de segurança em todo o mundo. Embora muitos resultados sejam compatíveis nos últimos dois anos, é possível observar algumas diferenças notáveis ao longo do relatório.

Para saber mais sobre a conscientização em cibersegurança dos funcionários, leia nosso relatório complementar: **2023 Security Awareness and Training Global Research Brief**, que será publicado até maio desse ano.

A quantidade de organizações que confirmaram ter sofrido **cinco ou mais violações aumentou 53%** entre 2021 e 2022.

# As violações estão mais frequentes e mais caras

Como previsto pelo FortiGuard Labs da Fortinet, ameaças cibernéticas de todos os tipos se tornaram cada vez mais onipresentes em 2022. Essa disseminação resultou em mais violações do que no ano anterior e em um custo total mais alto de violações para muitas organizações.

## Um grande número de líderes também atribui essas violações, pelo menos em parte, à falta de habilidades em cibersegurança entre os profissionais de TI.

Aparentemente, a grande maioria acredita que o cenário de ameaças só vai piorar. Nos próximos 12 meses, 65% dos entrevistados esperam que o número de ataques cibernéticos aumente. Essa previsão está alinhada com as projeções do FortiGuard Lab, que antecipam o crescimento de muitos tipos de ataques e modelos de negócios de crimes cibernéticos, incluindo o mercado Crime-as-a-Service (CaaS).

Apesar do aumento das violações, 93% dos líderes acreditam que suas empresas estão fazendo tudo o que podem para lidar com o aumento do volume de ataques. Isso pode sugerir incerteza sobre quais outras medidas as organizações podem tomar e, de certa forma, diverge das outras observações sobre as crescentes preocupações do conselho, como a necessidade de certificações para validar as habilidades e conhecimentos e lacunas na conscientização sobre cibersegurança por parte dos funcionários.

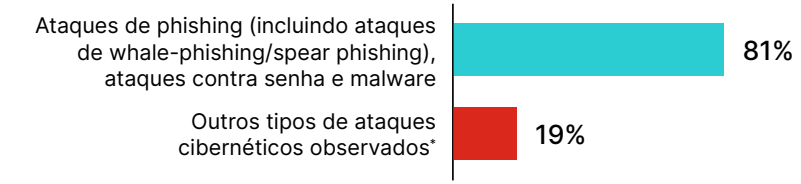
## 81% dos ataques cibernéticos se deram na forma de ataques de phishing, contra senhas e de malware.

### Phishing é o método de ataque mais comum

Em 2022, os entrevistados relataram que ataques de phishing, malware e contra senhas representaram, juntos, a maior parte (81%) dos tipos de ataques apontados pelas organizações entrevistadas em 2022. Particularmente, esses três ataques podem atingir não apenas sistemas, mas também usuários individuais de forma direta. Os esquemas de phishing são especialmente traiçoeiros, pois muitas vezes levam a outros tipos de ataque — malware e engenharia social — que, por sua vez, podem levar a ataques contra senha e web attacks.

Empresas na América do Norte testemunharam uma quantidade significativamente maior de ataques de phishing do que empresas do mesmo ramo na América Latina, que, por sua vez, enfrentou significativamente mais ataques por senha do que empresas do mesmo ramo na Europa, Oriente Médio e África.

**Sua empresa foi alvo de quais tipos de ataques cibernéticos?**




*Refere-se a Web Attacks, ataques de Cavalo de Troia, ataques de ransomware, ataques de DoS e DDoS, ataques de falsificação de DNS, ameaças internas, interpretação de URL, ataques de injeção de SQL, ataques de força bruta, ataques drive-by, ataques de espionagem, ataques de sequestro de sessão, ataques de Cross-site Scripting (XSS), ataques man-in-the-middle (MITM), ataques de aniversário.

**Pergunta feita apenas para aqueles cuja empresa sofreu um ataque cibernético nos últimos 12 meses.

# Uma análise mais a fundo

## Mais empresas foram alvo de violação no ano passado do que em 2021

84% dos entrevistados afirmam que suas empresas foram alvo de uma ou mais violações nos últimos 12 meses, um aumento em comparação 80% no ano anterior.

- 55% sofreram de uma a quatro violações.
- 29% sofreram cinco ou mais violações.
- 7% sofreram nove ou mais, mais do que o dobro do ano passado (3%).

## Houve um aumento notável no custo de violações que ultrapassa a casa de US$ 1 milhão

Quase metade (48%) das empresas que sofreram ao menos uma violação nos últimos 12 meses afirmam que o custo de remediação foi de acima de US$ 1 milhão, o que ultrapassa os 38% em 2021.

- 64% das organizações norte-americanas registram um custo total de violações acima de US$ 1 milhão, o maior de qualquer região.
- 31% das organizações da América Latina registram um custo total de violações acima de US$ 1 milhão, o menor de qualquer região.

64% das organizações norte-americanas registram um custo total de violações acima de US$ 1 milhão, o maior de qualquer região.

## A maioria dos líderes acredita que os ataques aumentarão no futuro

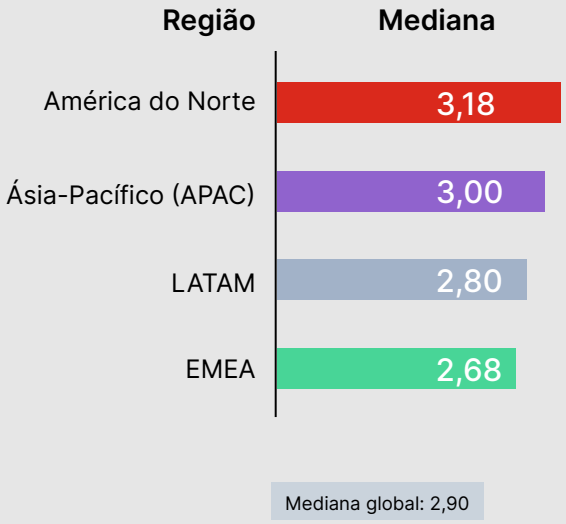
Enquanto a maioria dos entrevistados (65%) espera que os ataques cibernéticos aumentem nos próximos 12 meses, surpreendentes 19% afirmam não esperar nenhum aumento. Dadas as previsões dos analistas que seguem no sentido contrário, essas organizações podem estar vulneráveis, já que, provavelmente, não darão prioridade à preparação da segurança em suas redes, ao recrutamento de TI ou ao desenvolvimento de habilidades cibernéticas na equipe.

- Entrevistados da América do Norte esperam um aumento de 25% nos ataques para o próximo ano.
- Entrevistados da Europa, Oriente Médio e África esperam um aumento um pouco menor de 17%.

# Destaques regionais

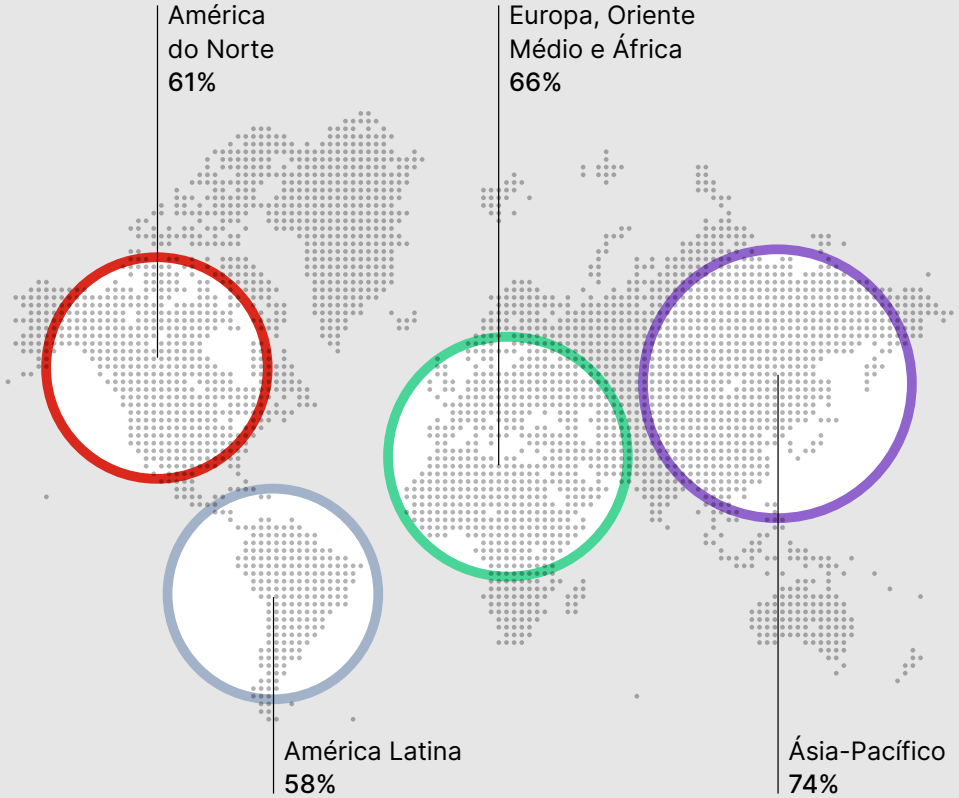
## Organizações norte-americanas relatam o maior número de violações

Em média, os entrevistados na América do Norte afirmam ter sofrido o maior número de violações, enquanto que os da Europa, Oriente Médio e África sofreram o menor número.




## As organizações da região Ásia-Pacífico são mais propensas a esperar um aumento nos ataques

Um número consideravelmente maior de entrevistados na região Ásia-Pacífico acredita que os ataques cibernéticos aumentarão nos próximos 12 meses.



# Os Conselhos de Administração estão focados em cibersegurança

Conforme cresce o número de ameaças cibernéticas e violações, a segurança de TI continua a ganhar destaque no nível de governança, com conselhos de administração fazendo perguntas diretas sobre como as empresas estão se protegendo.

Nos últimos anos, analistas como a McKinsey e publicações como a *Harvard Business Review* destacaram o papel que os conselhos podem desempenhar para ajudar as organizações a fortalecer sua postura de segurança. A crescente superfície de ataque corporativa e a diversificação de ameaças tornaram isso de suma importância, dadas as responsabilidades do conselho para supervisionar o risco à empresa e o gerenciamento da reputação.

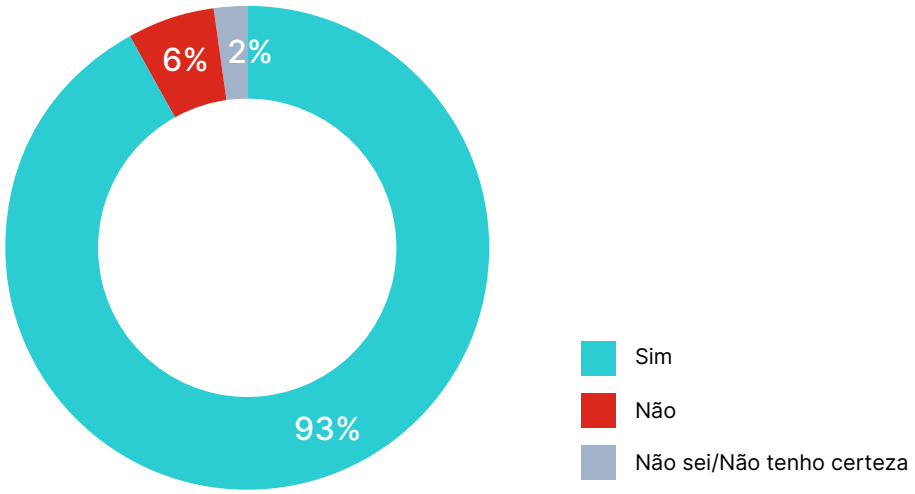
Como resultado, quase todos os líderes entrevistados (93%) afirmam que seus conselhos estão levantando questões de cibersegurança, e a maioria dos conselhos (83%) defende a contratação de mais funcionários de segurança de TI.

83% dos conselhos recomendam aumentar o número de funcionários de segurança de TI.

## Preocupações do conselho crescem junto com o porte da organização

Embora a maioria dos conselhos (93%) esteja fazendo perguntas sobre cibersegurança, essa vigilância é maior (96%) em empresas com 1.000 a 2.499 funcionários.

**Seu conselho de administração está questionando como sua organização está se protegendo contra o aumento dos ataques cibernéticos?**




*Pergunta feita apenas àqueles que são subordinados a ou tem uma linha direta de comunicação com um conselho de administração.

# Uma análise mais a fundo

## Crescem as reocupações do conselho sobre ameaças cibernéticas

Quase todos os líderes (91%) entrevistados são subordinados a ou têm uma linha direta de comunicação com um conselho de administração.

- 93% afirmam que o conselho pergunta como a organização está se protegendo contra o aumento de ataques cibernéticos, o que ultrapassa os 88% em 2021.
- 96% dos conselhos que administram organizações com 1.000 a 2.499 funcionários perguntam sobre cibersegurança.

## O recrutamento de pessoal com a finalidade de fortalecer a segurança é a principal prioridade do conselho

A maioria dos conselhos recomenda a contratação de pessoal de TI e cibersegurança.

- 83% dos líderes afirmam que seus conselhos recomendaram o aumento do número de funcionários de TI e cibersegurança em 2022, o que ultrapassa os 76% em 2021.
- 85% dos conselhos que administram organizações com mais de 5.000 funcionários recomendaram aumentar o número de funcionários de segurança de TI.

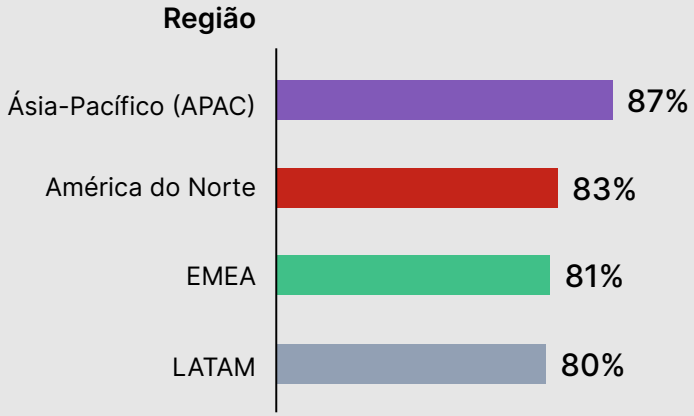
93% dos conselhos estão perguntando como a organização está se protegendo contra o aumento dos ataques de cibersegurança.

# Destaques regionais

## Conselhos em todas as regiões estão preocupados com a cibersegurança

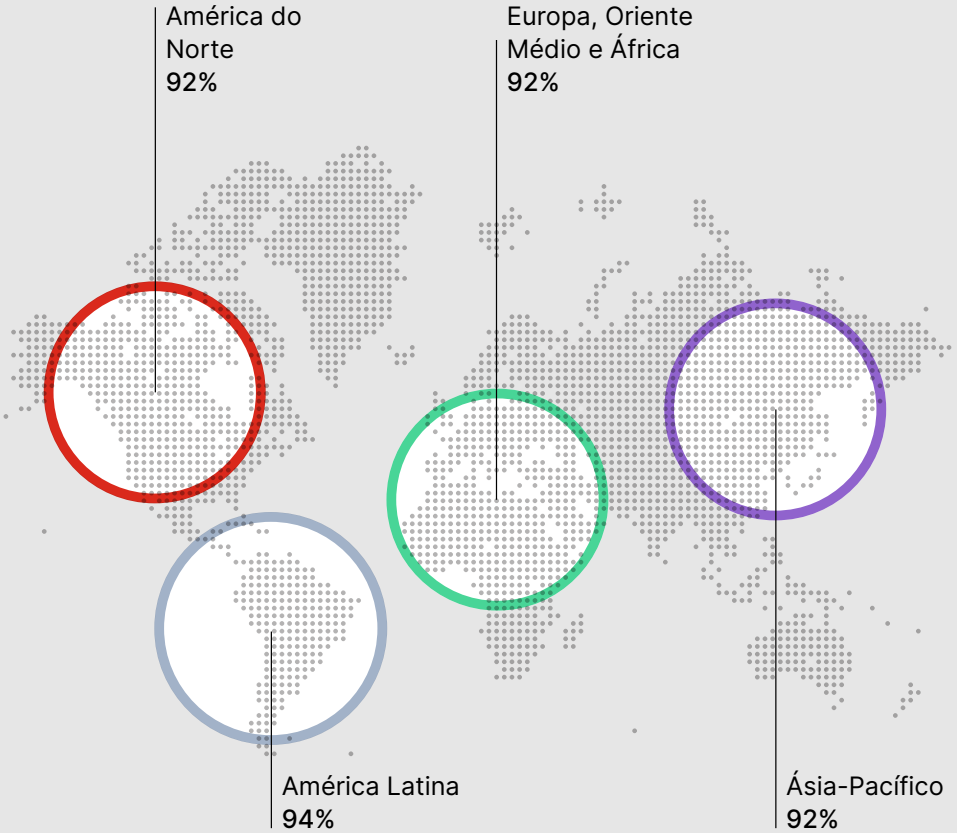
O interesse em proteger as organizações contra ameaças cibernéticas é sistematicamente alto em todo o mundo.

**Seu conselho de administração está sugerindo um aumento da quantidade de pessoas em seu departamento de TI ou de segurança?***




## Conselhos em todas as regiões defendem a contratação de mais funcionários de segurança de TI

Os entrevistados da região Ásia-Pacífico estavam mais propensos a pressionar o aumento do número de funcionários de cibersegurança em 2022.




*Pergunta feita às aqueles cujos conselhos de administração estão questionando como suas organizações estão se protegendo contra o aumento dos ataques cibernéticos.

# Há uma procura por certificações como comprovação de conhecimento e habilidades em cibersegurança

A maioria dos líderes reconhece o valor do conhecimento e das habilidades técnicas especializadas. Oitenta e dois por cento (82%) dos entrevistados afirmam que suas empresas se beneficiariam de certificações de cibersegurança e 90% destacam que pagariam para que um funcionário obtivesse uma certificação em cibersegurança.

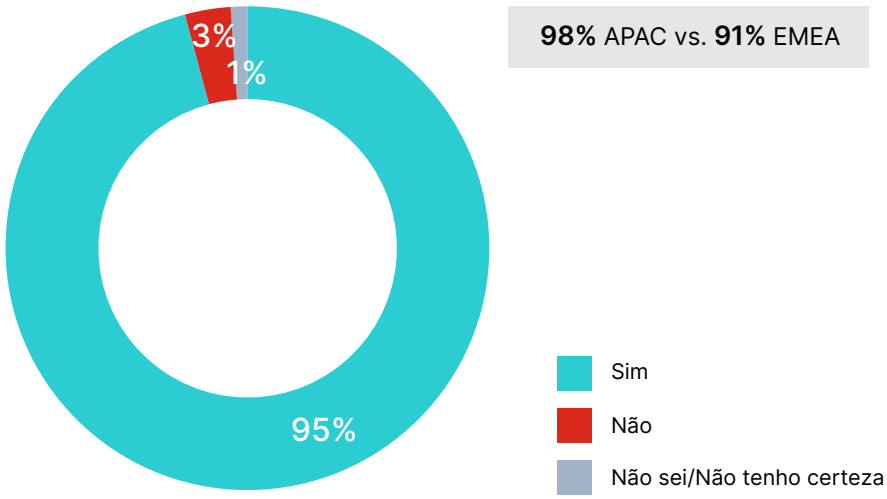
A demanda por profissionais certificados pode estar enraizada na experiência prática, já que a maioria dos líderes possui uma certificação de tecnologia ou trabalha com alguém em sua equipe que tem certificação, o que faz com que entendam melhor o valor que isso representa. Outra hipótese é que, com o crescente cenário de ameaças, os líderes estão deixando menos ao acaso e buscam comprovar que os profissionais que estão retendo ou contratando têm as habilidades de cibersegurança necessárias.

90% dos líderes preferem contratar candidatos com certificações focadas em tecnologia.

## As certificações oferecem benefícios reais

Líderes que possuem certificação em tecnologia, ou têm alguém em sua equipe que possui, afirmam que ter a certificação teve um impacto positivo em sua função ou na função de sua equipe.

**Você acha que a obtenção de certificações focadas em tecnologia teve um impacto positivo em você ou na função de sua equipe?**




*Pergunta feita apenas para aqueles que têm uma certificação focada em tecnologia e/ou equipe com tal certificação.

# Uma análise mais a fundo

## Mais líderes preferem contratar funcionários com certificações focadas em tecnologia

A maioria dos entrevistados (90%) afirma que prefere contratar pessoas com certificações, o que ultrapassa os 81% do ano anterior. Da mesma forma, 90% estariam dispostos a pagar para que os funcionários obtivessem a certificação.

- 84% possuem certificação focada em tecnologia.
- 86% têm alguém na equipe com certificação.
- 73% afirmam que ainda têm dificuldade para encontrar pessoas com certificações focadas em tecnologia, número abaixo dos 78% em 2021.

## As certificações oferecem vantagem tanto para as empresas quanto para as pessoas

Quase todos os líderes (95%) que possuem certificação ou que têm um funcionário certificado em sua equipe tiveram resultados positivos.

- 72% apontam maior conhecimento em cibersegurança.
- 62% apontam melhor desempenho das funções.
- 55% apontam que a certificação acelerou o crescimento de suas carreiras em comparação com 34% em 2021.
- 47% apontam salários mais altos, acima dos 29% em 2021.

## As certificações ocupam uma posição alta ao lado de conscientização, treinamento e soluções de segurança

A classificação próxima de todas as três opções dos entrevistados demonstra que uma abordagem em três frentes pode ser a melhor linha de defesa contra ataques cibernéticos.

- 82% afirmam que sua organização se beneficiaria de treinamento em cibersegurança como certificação.
- 75% afirmam que sua organização se beneficiaria da conscientização e treinamento de cibersegurança para todos os funcionários.
- 71% afirmam que sua organização se beneficiaria de soluções de segurança novas, aperfeiçoadas ou complementares.

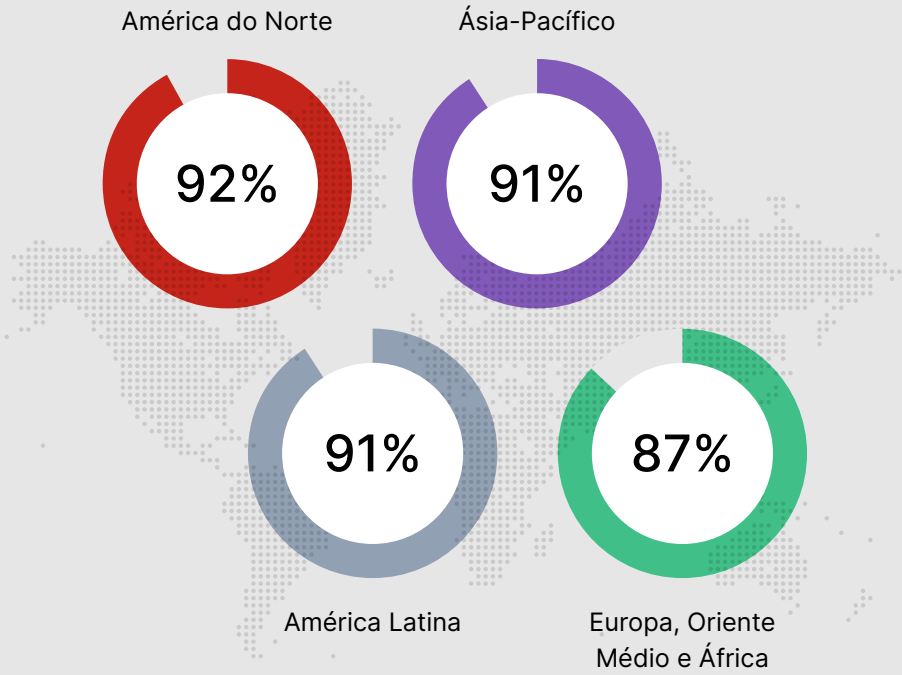
90% dos líderes estariam dispostos a pagar para que os funcionários obtivessem a certificação.

# Destaques regionais

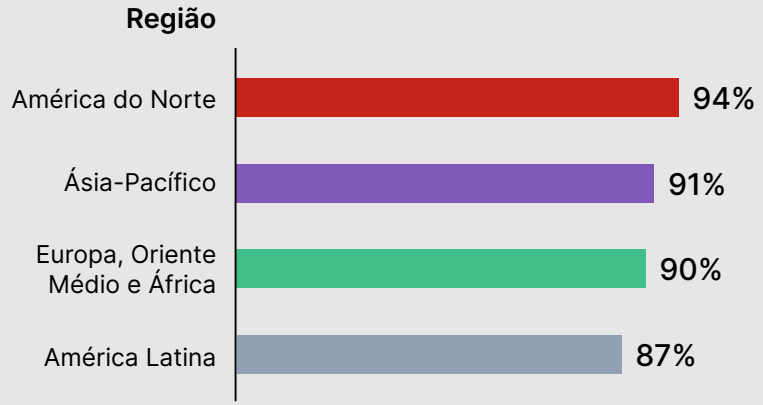
## Empresas do mundo todo reconhecem o valor da certificação

As empresas norte-americanas tiveram o maior número de entrevistados que preferem contratar pessoas com certificações focadas em tecnologia e que estão dispostas a pagar por isso.

**Preferem contratar pessoal certificado**




**Dispostas a pagar para que os funcionários obtenham a certificação**



# As vagas não ocupadas na área de TI representam um risco à cibersegurança

Mais da metade dos líderes afirmam que têm dificuldades para recrutar e reter talentos em cibersegurança, o que acaba provocando a escassez de habilidades que trazem ainda mais riscos cibernéticos para suas organizações.

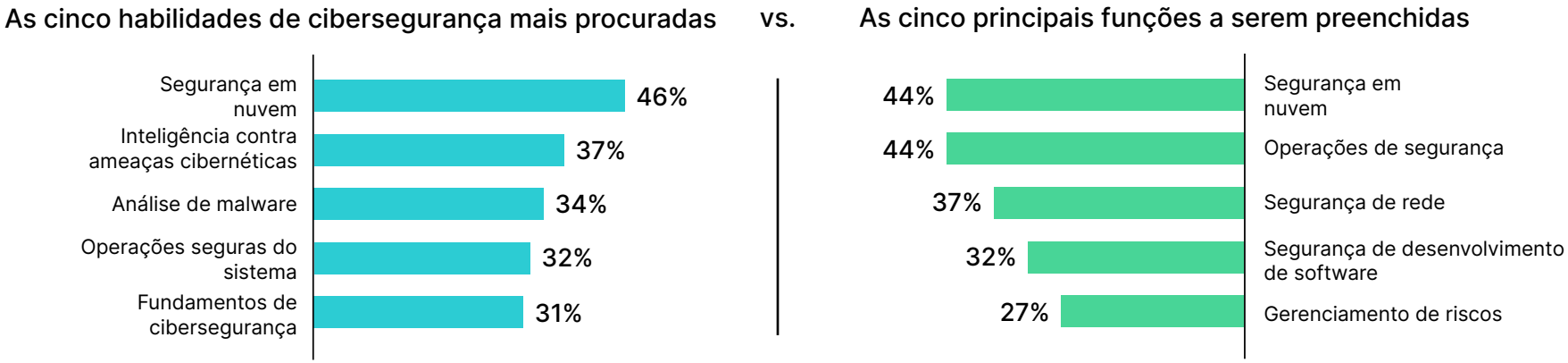
O recrutamento e a retenção são, em essência, desafios equivalentes, sendo as habilidades mais procuradas nas áreas de segurança na nuvem, inteligência contra ameaças cibernéticas e análise de malware. Funções específicas que estão se mostrando difíceis de preencher incluem segurança na nuvem, operações de segurança e segurança de rede.

Dadas as pressões divulgadas que as equipes de cibersegurança estão enfrentando atualmente para acompanhar milhares de alertas diários, gerenciar ferramentas diferentes e proteger um perímetro de rede cada vez mais disperso devido a tecnologias de nuvem e modelos de trabalho híbridos, essa escassez de habilidades é significativa.

68% das organizações afirmam enfrentar outros riscos devido à escassez de habilidades em cibersegurança.

## As habilidades de cibersegurança em nuvem são as mais procuradas.

A segurança na nuvem está no topo da lista das habilidades de cibersegurança mais procuradas e das funções mais difíceis de preencher para as organizações.



# Uma análise mais a fundo

## A falta de cibersegurança aumenta o risco

Sessenta e oito por cento (68%) dos líderes concordam que a escassez de habilidades em cibersegurança traz ainda mais riscos cibernéticos para suas organizações, número parecido com os 67% em 2021.

- 28% concordam totalmente com essa afirmação.
- Apenas 7% discordam totalmente dessa afirmação.

## Recrutamento e retenção são igualmente difíceis

Mais da metade (56%) dos entrevistados afirmam que suas organizações têm dificuldades para recrutar talentos em cibersegurança, um pouco abaixo dos 60% em 2021.

A maioria (54%) aponta que a retenção também é um desafio, um pouco acima dos 52% do ano passado.

- 44% afirmam que as funções de segurança na nuvem e operações de segurança são as mais difíceis de preencher.
- 37% afirmam que as funções de segurança de rede são as mais difíceis de preencher.
- 32% afirmam que as funções de desenvolvimento de software são as mais difíceis de preencher.

## As habilidades em segurança em nuvem são as mais procuradas por quase metade de todas as organizações

Os líderes identificaram as seguintes habilidades como extremamente necessárias para suas organizações.

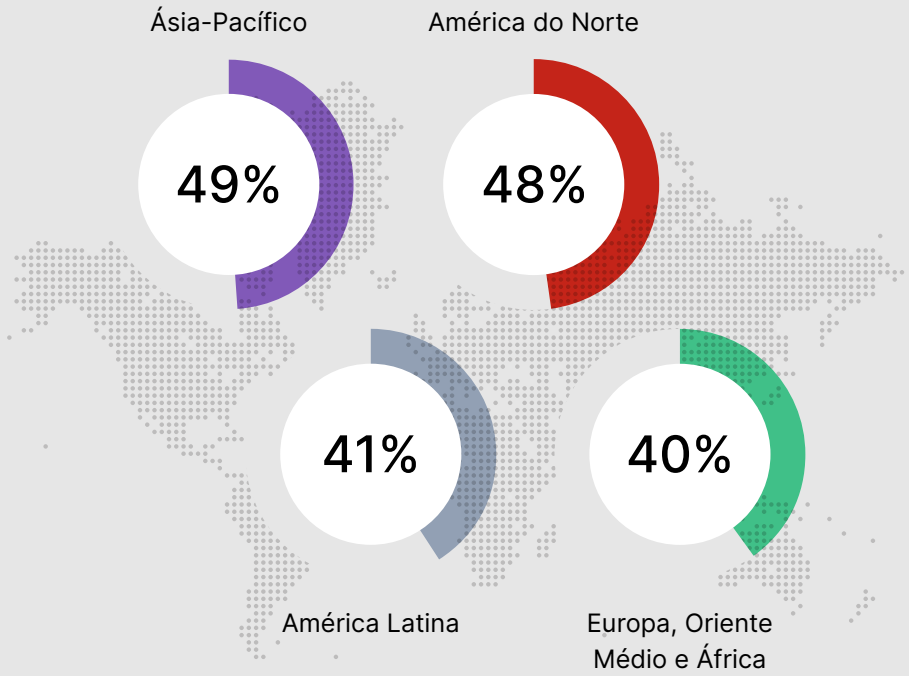
- 46% relatam a demanda por habilidades em segurança na nuvem.
- 37% afirmam que as habilidades em inteligência de ameaças cibernéticas são as mais essenciais.
- 34% afirmam que as habilidades em análise de malware são mais essenciais.

46% relatam a demanda por habilidades em segurança na nuvem.

# Destaques regionais

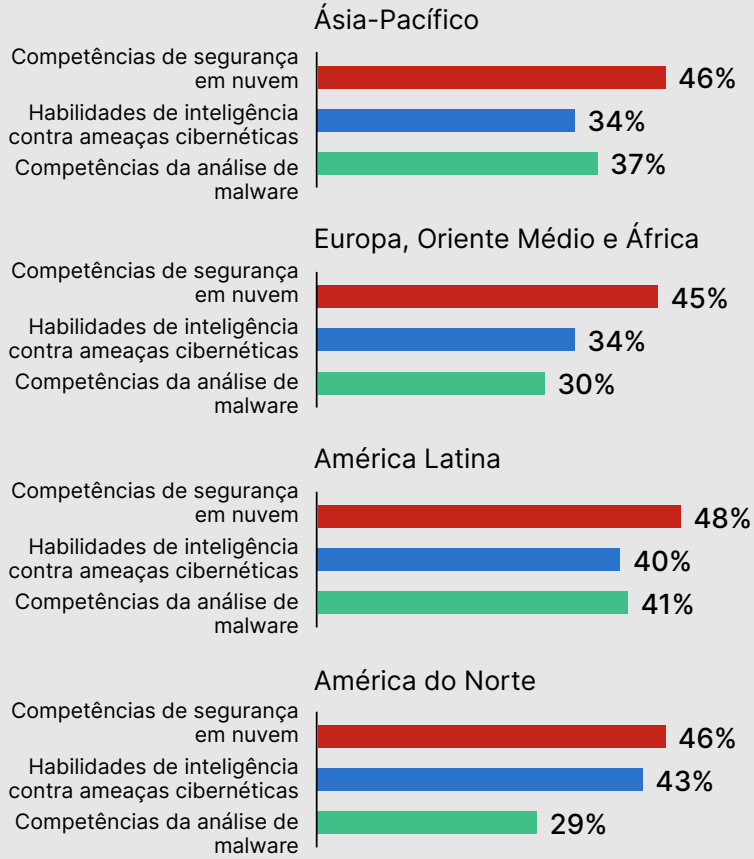
## Algumas regiões têm mais dificuldade em preencher funções de segurança na nuvem

Organizações nas regiões Ásia-Pacífico e América do Norte enfrentam maiores desafios para preencher funções de segurança na nuvem em comparação com empresas do mesmo ramo na América Latina, Europa, Oriente Médio e África.




## Diferentes regiões exigem habilidades diferentes

Enquanto organizações de todas as regiões afirmam que precisam de habilidades em segurança na nuvem, empresas da América do Norte são muito mais propensas a precisarem também de habilidades em inteligência contra ameaças cibernéticas, enquanto que as da América Latina precisam, acima de tudo, de habilidades em análise de malware.



# Talentos diversificados ajudam a atender às demandas em termos de habilidades, mas nem sempre são fáceis de encontrar

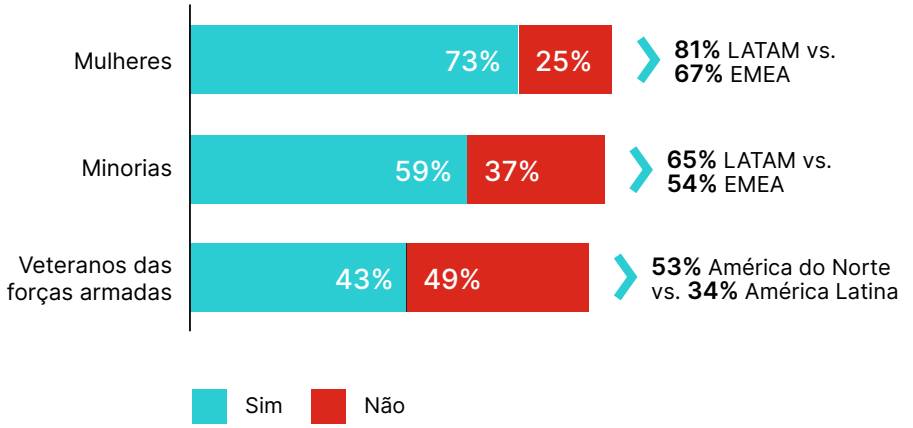
A maioria das organizações (83%) tem metas de diversidade para contratação nos próximos dois a três anos. Projetar a partir de origens de talento historicamente negligenciadas pode ajudar a preencher lacunas de habilidades, expandindo o conjunto geral de potenciais candidatos. No entanto, continua a ser um desafio encontrar pessoas devidamente qualificadas em alguns casos.

As organizações buscam constantemente talentos em cibersegurança de várias origens, em particular, mulheres, grupos minoritários e veteranos militares. Muitas vezes, acredita-se que este último grupo tem o treinamento, orientação e disciplina certos para trabalhar em um contexto de cibersegurança.

Das três origens de talentos, encontrar e contratar mulheres qualificadas é visto como um dos principais desafios pela maioria dos responsáveis pela tomada de decisões de TI, consideravelmente mais difícil do que contratar populações minoritárias e veteranas.

Cerca de 40% das empresas afirmam ter dificuldade em encontrar candidatos qualificados que sejam mulheres, veteranos militares ou pertencentes a grupos minoritários.

**Você tem alguma iniciativa estruturada ou formal de recrutamento que visa especificamente as populações a seguir?**




## Mais iniciativas de recrutamento têm como alvo as mulheres.

Para atrair talentos diversos, muitas organizações mantêm iniciativas de recrutamento voltadas para mulheres (73%) e candidatos de grupos minoritários (59%). No entanto, entre 2021 e 2022, iniciativas parecidas voltadas a veteranos caíram de 51% para 43%.

# Uma análise mais a fundo

## A maioria das organizações tem metas de diversidade, mas tem dificuldade em contratar

Oitenta e três por cento (83%) das empresas entrevistadas têm metas de contratação de diversidade de curto prazo, um pouco abaixo dos 89% em 2021.

- 69% afirmam que a contratação de mulheres é um dos principais desafios, o que se manteve estável em comparação aos 70% em 2021.
- 56% afirmam que contratar pessoas de origens minoritárias é um dos principais desafios, número abaixo dos 61% em 2021.
- 43% afirmam que a contratação de veteranos é um dos principais desafios, número abaixo dos 53% em 2021.

## Parte do desafio é encontrar candidatos qualificados e diversificados

Os entrevistados afirmam que recrutar candidatos qualificados de todos os três grupos subrrepresentados é igualmente desafiador.

A maioria (54%) aponta que a retenção também é um desafio, um pouco acima dos 52% do ano passado.

- 43% apontam a dificuldade em recrutar veteranos qualificados, o que representa uma ligeira queda em comparação aos 45% em 2021.
- 41% afirmam ter dificuldade em recrutar mulheres qualificadas, um aumento significativo em relação aos 30% do ano passado.
- 38% afirmam ter dificuldade em recrutar pessoas qualificadas de origens minoritárias, mesmo número observado no ano passado.

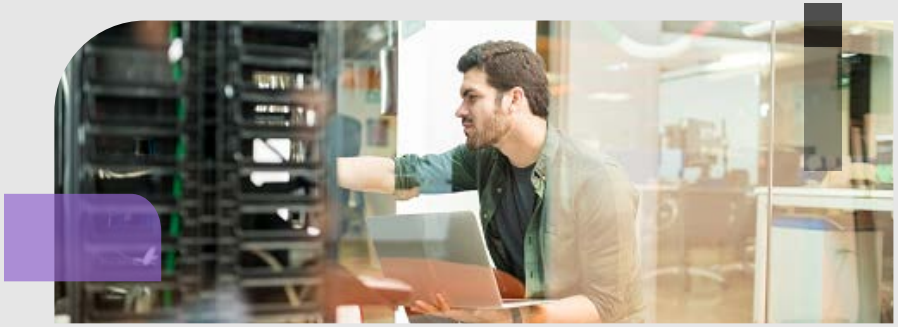
## Apesar dos desafios, a diversidade na contratação já é realidade

Muitas organizações contrataram pessoas de todos os três grupos, especialmente mulheres.

- 89% dos entrevistados contrataram mulheres, aproximadamente o mesmo que no ano passado (88%).
- 68% contrataram pessoas de grupos minoritários, semelhante a 2021 (67%).
- 47% contrataram veteranos militares, uma queda em relação aos 53% do ano anterior.

83% das empresas entrevistadas têm metas de contratação de diversidade a curto prazo, o que fica abaixo dos 89% em 2021.

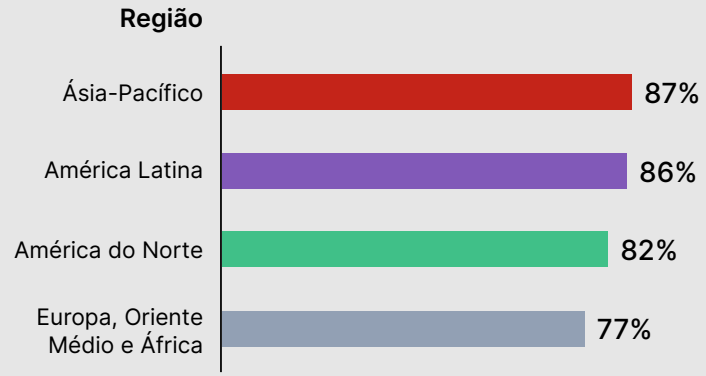
# Destaques regionais



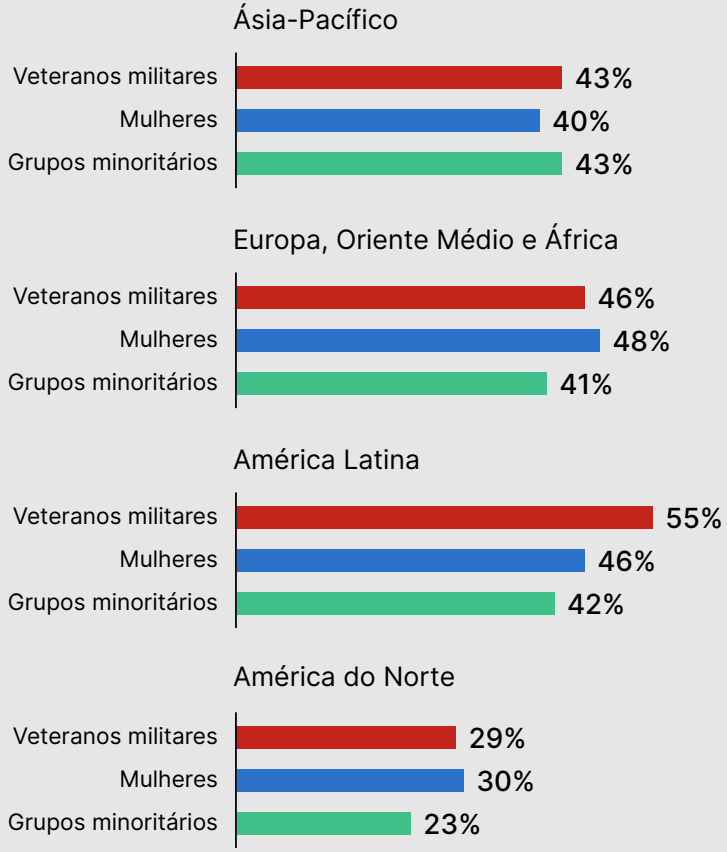
## Em todas as regiões, as organizações enfrentam diferentes desafios de RH

As empresas da região Ásia-Pacífico e da América Latina têm maior probabilidade de ter metas de contratação de diversidade para os próximos dois a três anos. Região por região, a contratação de grupos subrrepresentados é mais difícil.

### Metas de contratação de diversidade por região




### Desafios na contratação de diferentes grupos



# Conclusão

Dado o cenário de ameaças e a incidência de violações que crescem cada vez, é fundamental que as empresas continuem construindo sua defesa de cibersegurança para proteger suas redes, sistemas, dados, clientes, parceiros e funcionários. Ao pensar em suas estratégias de cibersegurança, os líderes devem levar em consideração três fatores:

- **Soluções avançadas** para lidar com ameaças em tempo real em ambientes de TI complexos e distribuídos
- **Equipes especializadas** que têm o conhecimento e as habilidades para gerenciar a cibersegurança de forma eficaz
- **Uma cultura de conscientização cibernética** voltada a cada pessoa da empresa

## Maior interesse dos conselhos de administração

Os conselhos de administração estão prestando mais atenção ao risco cibernético e aos fatores humanos associados, aumentando a discussão sobre o que está sendo feito para mitigar o risco. Conversas específicas sobre o aumento do tamanho das equipes de segurança de TI estão levando as organizações a prestarem mais atenção. É provável que esse maior interesse do conselho leve as organizações a dobrar os esforços para recrutar e reter funcionários qualificados e desenvolver uma estratégia de contratação de habilidades em cibersegurança necessárias e difíceis de encontrar, especialmente com o crescente reconhecimento de que habilidades não atendidas oferecem ainda mais risco para muitas organizações. Líderes que precisam demonstrar aos conselhos que estão cientes da situação atual e futura do cenário de ameaças vão querer se antecipar a essas conversas contínuas.

48% das empresas que sofreram ao menos uma violação nos últimos 12 meses afirmam que o custo de remediação foi de acima de US$ 1 milhão, o que ultrapassa os 38% em 2021.

## Certificações estão no centro das atenções

Seja contratando novos funcionários ou buscando aumentar o conhecimento da atual equipe de segurança de TI, os líderes estão se voltando cada vez mais para certificações para validar habilidades individuais. Programas de certificação bem desenvolvidos visam estabelecer não apenas competências técnicas, mas também uma compreensão mais profunda de como aplicar essas competências no contexto de uma determinada função.

Investir nas pessoas muitas vezes fortalece o compromisso dos funcionários. A Fortinet acredita que, ao investir e desenvolver sua atual equipe de segurança de TI, as organizações podem reduzir os problemas de retenção de talentos. Ao incentivar e apoiar os funcionários a obter ou renovar suas certificações, elas podem aumentar a fidelidade dos funcionários, aumentar a retenção e garantir que as habilidades das pessoas continuem sendo atualizadas.

## Buscando talentos em novos lugares

Expandir o pool de talentos para atrair grupos mais diversos continuará a ser fundamental para que as organizações possam atender às suas necessidades de profissionais. Em 2021, estimava-se que as mulheres representavam apenas um quarto do quadro laboral global de cibersegurança.[3] Embora os grupos minoritários variem de acordo com o país e a região, é fato, em geral, que esses grupos estão subrrepresentados no campo da cibersegurança. Nos EUA, por exemplo, apenas 9% dos especialistas em cibersegurança são negros, 8% são asiáticos e 4% são hispânicos.[4]

Veteranos militares muitas vezes têm a vantagem de já terem uma mentalidade de defesa e serem bem treinados para aprender novas habilidades e transitar de função. A indústria tem muito a ganhar atraindo pessoas desse grupo e desenvolvendo seus treinamentos e habilidades atuais — tanto técnicas quanto soft skills.

## A cultura corporativa é importante

Além das tecnologias e especialistas em cibersegurança, os líderes têm outra ferramenta poderosa para se proteger: uma cultura de cibersegurança interna robusta. Os líderes podem cultivar uma cultura sólida aumentando a conscientização dos funcionários sobre a necessidade de uma boa integridade da cibersegurança. Para saber mais sobre a conscientização em cibersegurança dos funcionários, leia nosso relatório complementar: 2023 Security Awareness and Training Global Research Brief, que será publicado até maio desse ano.

A boa notícia é que ainda há progresso sendo feito no combate ao crime cibernético, e as organizações que estão comprometidas em fortalecer sua postura de segurança não estão sozinhas. Desde a iniciativa Partnership Against Cybercrime (PAC) do Fórum Econômico Mundial até a NATO Industry Cyber Partnership e o MITRE Engenuity Center for Threat-Informed Defense, muitos órgãos governamentais estão engajados na proteção de empresas contra ameaças cibernéticas. Nós da Fortinet estamos orgulhosos de ser um contribuinte ativo para muitas dessas iniciativas.

[3] Tayo Bero, "Cybersecurity is a red-hot career choice — why aren't more women working in this space?" The Globe and Mail, 24 de agosto de 2022.
[4] Ben Allen, "Minorities and the Cybersecurity Skills Gap," Forbes, 30 de setembro de 2022.

# Sobre a Fortinet

A Fortinet (NASDAQ: FTNT) tem sido essencial na evolução da cibersegurança e na convergência de rede e segurança. Nossa missão é proteger pessoas, dispositivos e dados em todos os lugares, e hoje fornecemos cibersegurança em todos os lugares que você precisa com o maior portfólio integrado de mais de 50 produtos de nível empresarial.

Mais de meio milhão de clientes confiam nas soluções da Fortinet, que estão entre as mais implantadas, mais patenteadas e mais validadas do setor.

O Fortinet Training Institute, um dos maiores e mais amplos programas de treinamento do setor, dedica-se a disponibilizar treinamento em cibersegurança e novas oportunidades de carreira para todos. O FortiGuard Labs, a organização de inteligência e pesquisa de ameaças de elite da Fortinet, desenvolve e utiliza tecnologias de aprendizado de máquina e IA de ponta para fornecer aos clientes proteção oportuna e de primeira categoria, além de inteligência de ameaças acionável. Saiba mais em www.fortinet.com, no Fortinet Blog e no FortiGuard Labs.

FORTINET
Training Institute

www.fortinet.com


Março de 2023

# Resumo executivo

**Os resultados obtidos no relatório sobre déficit de competências em cibersegurança de 2023** mostram claramente que as organizações estão travando uma difícil batalha contra a ameaça cibernética, o que acaba implicando o aumento de violações, maior demanda por profissionais qualificados e a contínua dificuldade para preencher vagas importantes.

## As violações estão mais frequentes e mais caras

**84%** das organizações foram alvo de **uma ou mais violações** nos últimos 12 meses, um aumento em comparação a 80% em 2021.

**29%** sofreram **cinco ou mais invasões** em comparação a 19% no ano passado.

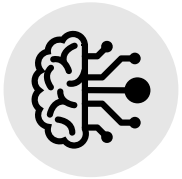
**48%** sofreram violações nos últimos 12 meses que **custaram mais de US$ 1 milhão** para serem remediadas, o que ultrapassa os 38% em 2021.

## As vagas não ocupadas na área de TI representam um risco à cibersegurança

**68%** das organizações afirmam **enfrentar outros riscos devido à** escassez de habilidades em cibersegurança, o que se mantém alinhado aos 67% observados em 2021.

**56% das empresas têm dificuldades para recrutar** e **54% têm dificuldades para reter** talentos, em comparação com 60% e 52%, respectivamente, em 2021.

**As funções de Operações de segurança e Segurança na nuvem** são as mais difíceis de serem preenchidas.



## Os Conselhos de Administração estão focados em cibersegurança

**93%** dos entrevistados afirmam que seu **conselho questiona quanto à cibersegurança,** o que ultrapassa os 88% em 2021.

Em 2022, **83% dos conselhos sugeriram aumentar o número de funcionários de segurança de TI,** em comparação com 76% em 2021.

## Há uma procura por certificações como comprovação de conhecimento e habilidades em cibersegurança

**90%** dos líderes **preferem contratar candidatos com certificações focadas em tecnologia,** o que ultrapassa os 81% em 2021.

**90% também pagariam** para que um funcionário obtivesse uma certificação de cibersegurança.

**72%** dos líderes afirmam que a contratação de pessoas certificadas **aumentou a conscientização e o conhecimento sobre cibersegurança** dentro da empresa.

## Talentos diversificados ajudam a acabar com a lacuna de habilidades, mas nem sempre são fáceis de encontrar

Cerca de **40%** têm **dificuldade em encontrar candidatos qualificados** que sejam mulheres, veteranos militares ou pertencentes a grupos minoritários.

**83%** das empresas têm **metas de contratação de diversidade a curto prazo,** o que fica abaixo dos 89% em 2021.