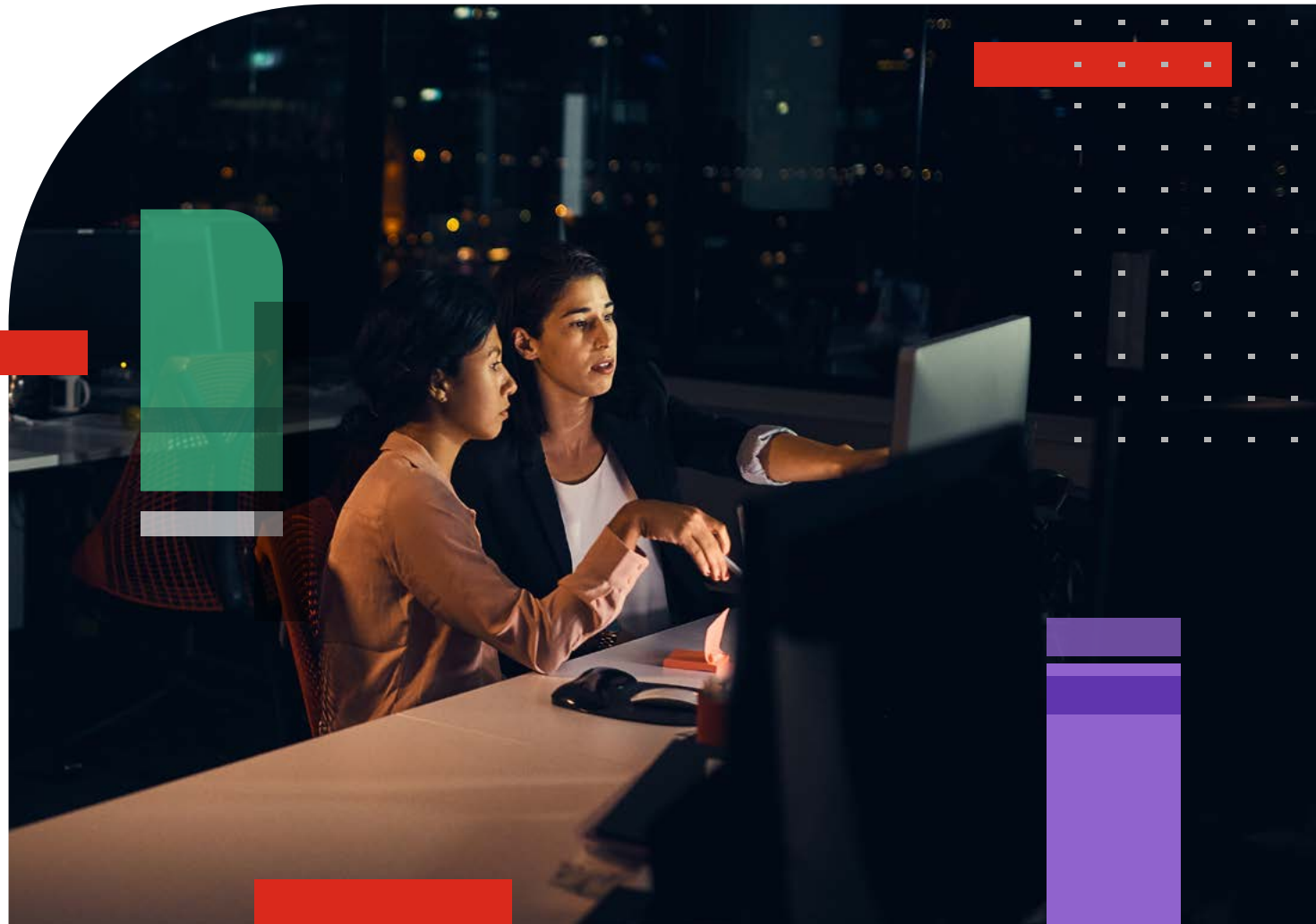
FORTINET
Training Institute

Conscientização e treinamento em segurança de 2023

Resumo da pesquisa global



Conteúdo

Metodologia

Os resultados deste relatório baseiam-se em uma entrevista on-line e uma pesquisa por e-mail com 1.855 pessoas responsáveis pela tomada de decisões de TI e cibersegurança, que foram realizadas pela Sapio Research em novembro de 2022. As respostas foram coletadas em 29 locais: África do Sul, Alemanha, Argentina, Austrália, Brasil, Canadá, Colômbia, Coreia do Sul, Emirados Árabes Unidos, Espanha, Estados Unidos, Filipinas, França, Hong Kong, Índia, Indonésia, Israel, Itália, Japão, Malásia, México, Nova Zelândia, Países Baixos, Reino Unido, República Popular da China, Singapura, 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 — **25%**
500–999 funcionários — **23%**
1.000–2.499 funcionários — **23%**
2.500–4.999 funcionários — **15%**
Mais de 5.000 funcionários — **14%**

Gênero

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

Total de entrevistados: 1.855

APAC **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

21% Tecnologia
16% Fabricação
13% Serviços financeiros

INTRODUÇÃO

Foco no elemento humano da cibersegurança

À medida que os ataques cibernéticos se intensificam, cada vez mais organizações reconhecem a necessidade de ter uma sólida cultura de segurança entre todos os funcionários. Essa força de trabalho com conscientização cibernética é um elemento adicional necessário para uma equipe de segurança qualificada e experiente e para o uso de soluções avançadas de cibersegurança. Os funcionários que sabem como praticar uma boa higiene cibernética são cada vez mais considerados como uma linha de defesa crucial.

O reforço das defesas cibernéticas será importante em 2023, à medida que as organizações enfrentam um cenário de ameaças em constante evolução. O FortiGuard Labs da Fortinet prevê um crescimento explosivo nos crimes cibernéticos como serviço (CaaS); uso de aprendizado de máquina para lavagem de dinheiro; explorações de crimes cibernéticos em ambientes de realidade aumentada, virtual e mista; e malware de limpeza de dados.

Essa previsão ressalta a natureza crítica da conscientização e do treinamento em cibersegurança dos funcionários, e é por isso que a Fortinet está se concentrando nesses tópicos com este *Resumo da pesquisa global sobre conscientização e treinamento em segurança de 2023*. As páginas a seguir destacam algumas das principais preocupações e ações que estão sendo tomadas pelos líderes em todo o mundo, com base nos resultados da pesquisa anual apresentados no Relatório de pesquisa global sobre o déficit de competências em cibersegurança da Fortinet.

Resumo executivo

Os funcionários podem ser seu ponto mais vulnerável ou sua defesa mais poderosa.

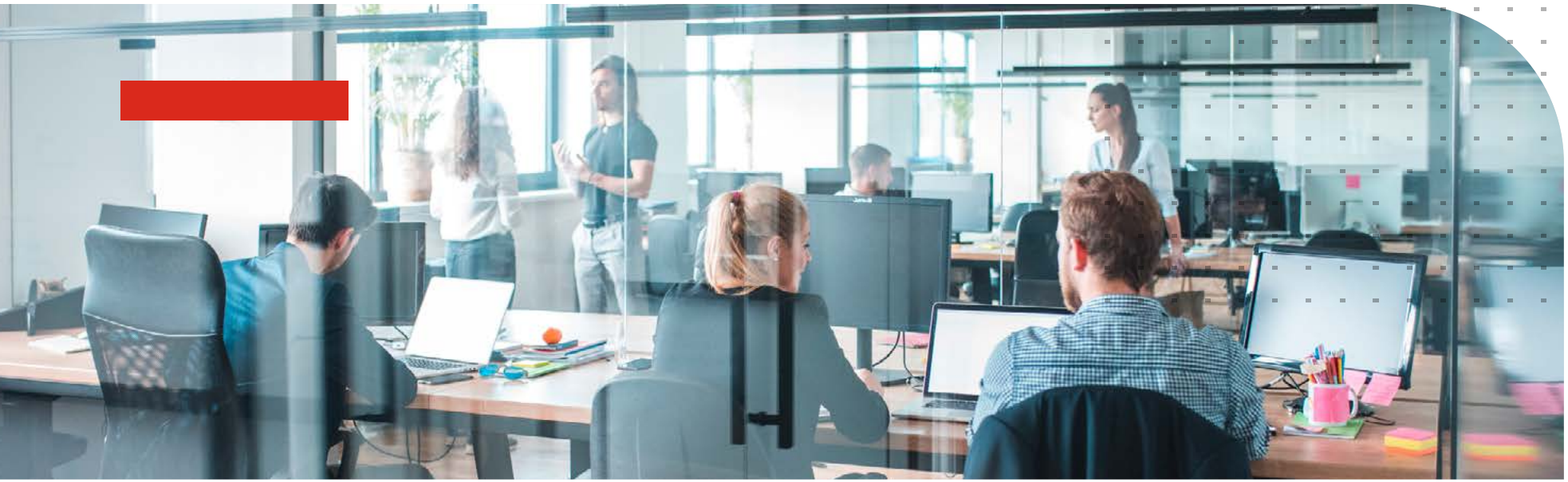
81% das organizações pesquisadas enfrentaram **ataques de malware**, **phishing**, **e senha no** ano passado, muitos deles direcionados diretamente aos usuários.

Falta consciência sobre cibersegurança aos funcionários, mesmo com o treinamento atual.

56% dos líderes acreditam que seus **funcionários têm conhecimento insuficiente** no que diz respeito à conscientização sobre cibersegurança.

A cibersegurança é uma prioridade crescente para os conselhos corporativos.

93% dos conselhos de administração estão questionando as **defesas cibernéticas de suas organizações**.



81% dos ataques cibernéticos ocorreram na forma de ataques de phishing, ataques de senha e ataques de malware.

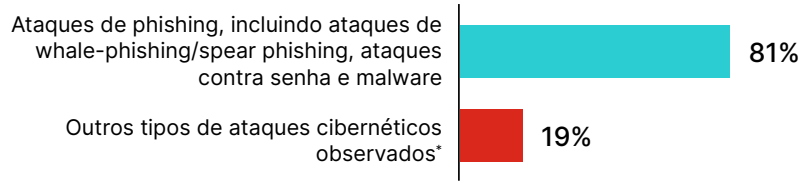
Os funcionários podem ser seu ponto mais vulnerável ou sua defesa mais poderosa

Quase todas as organizações pesquisadas sofreram pelo menos uma violação de cibersegurança nos últimos 12 meses e, em quase um terço delas, houve cinco ou mais violações. Uma característica comum de muitos dos ataques cibernéticos ocorridos em 2022 é que eles visavam os usuários diretamente, como esquemas de phishing, ou capitalizavam a fraca higiene cibernética para comprometer senhas e credenciais.

Embora o malware tenha sido o tipo mais comum de ataque usado nos últimos 12 meses, o phishing pode ser o mais insidioso, muitas vezes abrigando outros tipos de ataques sob o disfarce de e-mails amigáveis, mensagens de texto e links da Web. Outros tipos relatados de ataques direcionados a funcionários incluíram ataques de senha, spear phishing e whale phishing (também conhecido como ataque baleeiro).

Com o custo de violações excedendo US$ 1 milhão para quase metade das organizações respondentes, capacitar os funcionários para reconhecer, evitar e relatar ameaças cibernéticas é fundamental.

Ataques mais comuns relatados pelas organizações



*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.

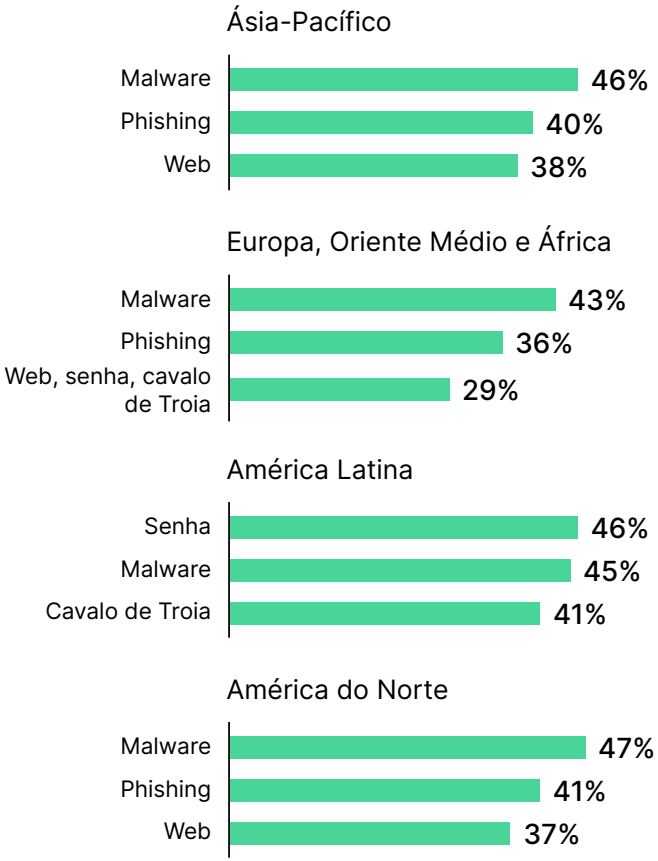
Uma análise mais a fundo

- **84%** das organizações pesquisadas sofreram **pelo menos uma violação de cibersegurança** nos últimos 12 meses, frente a 80% no ano anterior.
- **29% sofreram cinco ou mais**, frente aos 19%.
- E **7% sofreram mais de 9**, frente a apenas 3%.
- **65%** dos líderes esperam um **aumento médio de 20% nos ataques cibernéticos** nos próximos 12 meses.

Destaques regionais

Os ataques mais comuns variam de acordo com a região.

As organizações em cada região do mundo têm um perfil de ataque ligeiramente diferente.



Diferentes setores enfrentam diferentes volumes de ataques de malware.

A pesquisa FortiGuard Labs 2022 mostra que os volumes de ataques variam de acordo com o setor e a região. Para esta pesquisa, a FortiGuard Labs separou a Europa e o Oriente Médio da África.

Setor	
Serviços financeiros	
Região com maior volume	Europa e Oriente Médio (**63,1%**)
Região com menor volume	América latina (**1,8%**)
Serviços de saúde	
Região com maior volume	Ásia-Pacífico (**62%**)
Região com menor volume	África (**2,6%**)
Serviços de segurança gerenciados	
Região com maior volume	Europa e Oriente Médio (**46,6%**)
Região com menor volume	Ásia-Pacífico (**1,8%**)
Varejo e hotelaria	
Região com maior volume	Ásia-Pacífico (**38,8%**)
Região com menor volume	África (**8,6%**)
Petróleo e gás	
Região com maior volume	Europa e Oriente Médio (**49,1%**)
Região com menor volume	Ásia-Pacífico (**18,9%**)

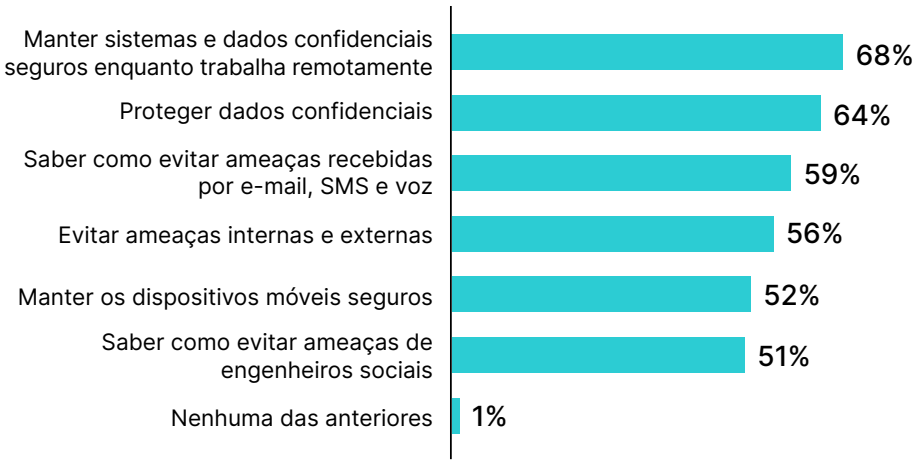
Falta consciência sobre cibersegurança aos funcionários, mesmo com o treinamento atual

Oitenta e cinco por cento dos líderes afirmam que sua organização tem um programa de conscientização e treinamento em segurança, mas mais da metade acredita que ainda falta conhecimento sobre cibersegurança a seus funcionários.

Essa desconexão parece sugerir que os programas de treinamento em vigor não são tão eficazes quanto poderiam ser, que as práticas de higiene cibernética são aplicadas de forma inconsistente ou que o treinamento não é suficientemente reforçado, o que os analistas consideram fundamental para construir uma cultura de cibersegurança eficaz.

Os líderes afirmam que proteger dados e sistemas confidenciais ao trabalhar remotamente é o aspecto mais importante da conscientização sobre cibersegurança para os funcionários, sendo que a proteção de dados confidenciais em geral vem logo em seguida.

Onde a conscientização sobre cibersegurança é mais importante



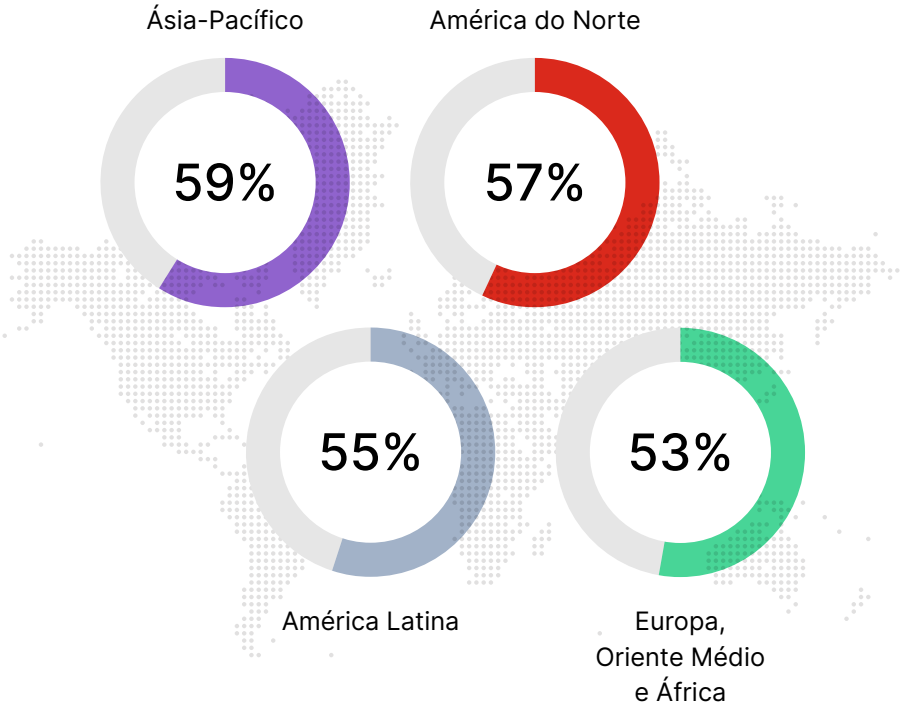
Uma análise mais a fundo

- **56%** dos líderes acreditam que seus **funcionários têm conhecimento insuficiente** no que diz respeito à conscientização sobre cibersegurança, frente a 52% em 2021. Isso ocorre apesar de **85%** terem um **programa de conscientização e treinamento em cibersegurança** em vigor.
- **73%** das organizações **que não têm programas de treinamento** estão à procura de um, o que representa um aumento de 66% em relação a 2021.
- **93%** dos líderes acreditam que uma maior conscientização dos funcionários sobre cibersegurança ajudariam a **reduzir os ataques cibernéticos**.
- **59%** dos líderes afirmam que é adequado que os funcionários **dediquem de uma a três horas por ano em treinamento em cibersegurança**.
- **68%** dos líderes afirmam que o mais importante é que os funcionários saibam **como manter dados e sistemas confidenciais seguros enquanto trabalham remotamente**.

Destaques regionais

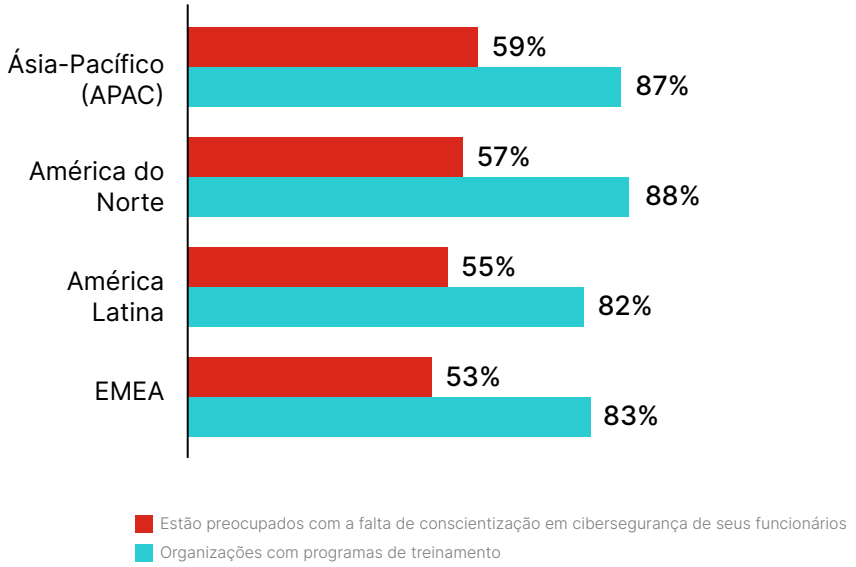
As preocupações com a conscientização sobre cibersegurança são semelhantes em todas as regiões.

A preocupação é ligeiramente maior na região Ásia-Pacífico e menor na Europa, Oriente Médio e África.



O treinamento é comum, mas as lacunas persistem.

É interessante observar que, embora mais da metade dos líderes em todas as regiões acredite que falte conscientização em cibersegurança, a maioria das empresas oferece programas de treinamento.



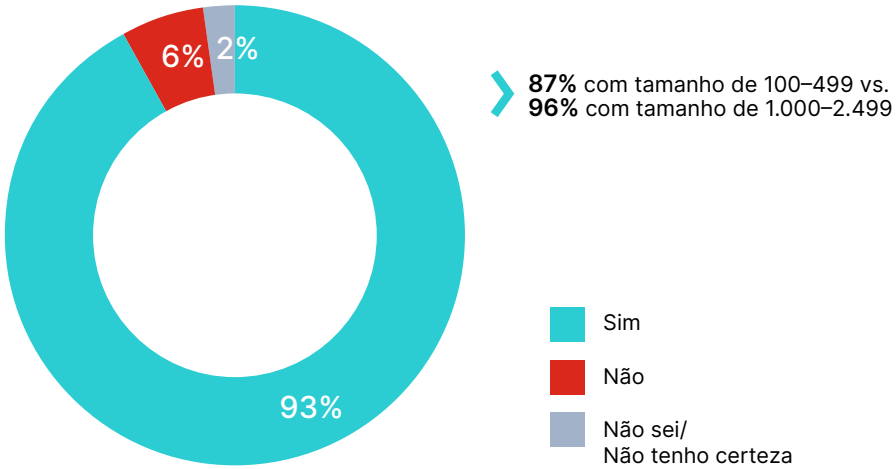
A cibersegurança é uma prioridade crescente para os conselhos de administração

93% dos líderes com acesso direto ao conselho de administração afirmam que os respectivos conselhos estão questionando sobre as defesas cibernéticas da organização.

É razoável considerar isso como um sinal de que os conselhos levam a sério suas responsabilidades de gerenciar riscos corporativos e proteger a marca, e que estão cientes do aumento de ataques e violações.

Uma vez que muitos ataques visam usuários, parece provável que os conselhos vejam, ou logo verão, que a conscientização sobre cibersegurança dos funcionários é uma parte crítica da "equação da defesa". Noventa e três por cento dos líderes acreditam que o aumento da conscientização sobre cibersegurança dos funcionários ajudaria a diminuir a ocorrência de ataques cibernéticos.

Os conselhos de administração estão perguntando sobre a cibersegurança



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

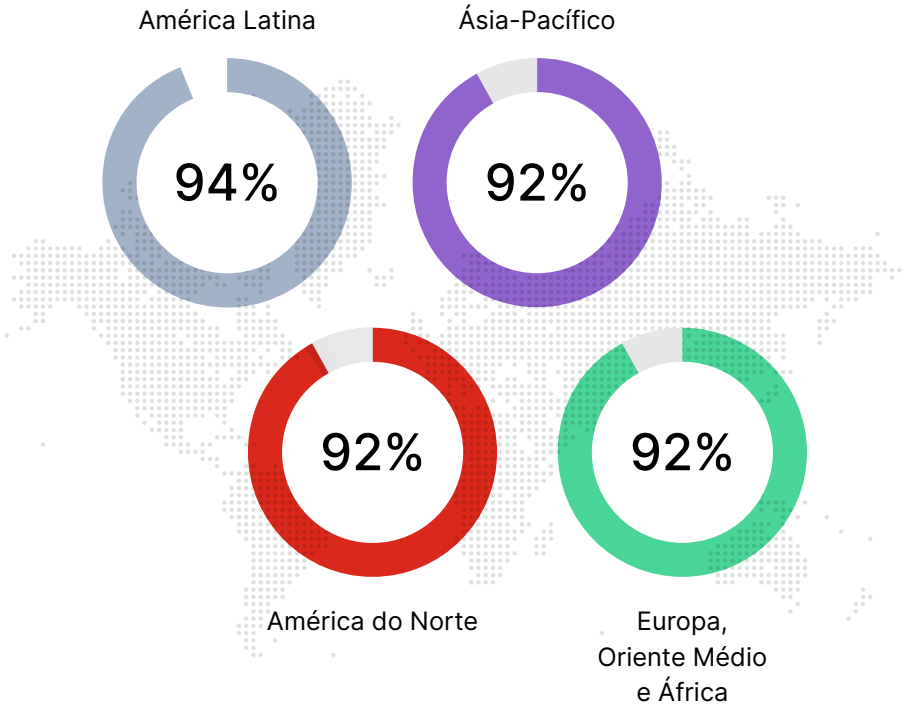
Uma análise mais a fundo

- **O interesse do conselho na cibersegurança está aumentando, de 88% para até 93%** nesta pesquisa atual, conforme relatado no *Relatório sobre o déficit de competências em cibersegurança 2022 da Fortinet*.
- **O interesse do conselho na segurança é muito consistente em todos os setores**, embora um pouco maior em serviços financeiros, saúde e telecomunicações (94–95%) do que em educação, mídia e entretenimento (88%).

Destaques regionais

Conselhos de todas as regiões estão perguntando sobre a cibersegurança.

Os resultados da pesquisa mostram níveis semelhantes de preocupação entre os conselhos em todo o mundo.



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

Conclusão

Com 84% dos líderes relatando pelo menos uma violação cibernética nos últimos 12 meses, e quase metade citando um custo total de violações acima de US$ 1 milhão, é fundamental que as organizações continuem fortalecendo suas defesas cibernéticas. As organizações precisam desenvolver uma abordagem de cibersegurança abrangente, que inclua soluções sofisticadas e automatizadas; equipes de especialistas; e — como mostram os resultados da pesquisa — um programa eficaz de conscientização e treinamento em cibersegurança.

Os funcionários são uma linha de defesa essencial.

Como muitos dos tipos mais comuns de ataques cibernéticos, como esquemas de phishing, certas formas de malware e ataques por senha, visam diretamente os usuários, a baixa conscientização em cibersegurança dos funcionários provavelmente enfraquece significativamente a postura geral de segurança das organizações. Por outro lado, programas eficazes de conscientização e treinamento em cibersegurança podem melhorar a postura de segurança, adicionando camadas extras de proteção à organização. Os líderes parecem reconhecer isso, já que 93% deles responderam que acreditam que um melhor treinamento e conscientização dos funcionários ajudaria a diminuir a frequência de ataques cibernéticos.

Treinamento requer reforço.

Os programas de conscientização e treinamento em cibersegurança são métodos amplamente reconhecidos de reforçar a cultura cibernética dos funcionários. Não surpreende o fato de que a maioria das organizações tenha programas em vigor. No entanto, mais da metade de todos os líderes entrevistados ainda está preocupada com a falta de conscientização em cibersegurança de seus funcionários. Uma avaliação crítica dos programas de conscientização e treinamento de segurança pode revelar oportunidades para abordar o elemento humano da cibersegurança de forma mais eficaz, reduzindo assim o risco geral. Tomar medidas para garantir que os programas cubram suficientemente uma ampla gama de tópicos de maneira prática, e para garantir que a aprendizagem seja reforçada com lembretes e verificações, deve ajudar a melhorar os resultados do treinamento.

Os conselhos de administração estão focados em cibersegurança.

Com um programa de treinamento sólido, as organizações podem aumentar a conscientização sobre riscos cibernéticos dos funcionários e capacitá-los a defender a organização, estabelecendo as bases para uma cultura de cibersegurança forte e preparada. Isso pode repercutir nos conselhos de administração corporativos que, como mostram os resultados da pesquisa deste ano, estão cada vez mais preocupados com a cibersegurança e provavelmente se concentrarão no elemento humano de agora em diante, reconhecendo que tal elemento desempenha um papel essencial na proteção dos interesses comerciais e da reputação da marca corporativa.

As organizações sabem que precisam de soluções avançadas de cibersegurança e que as certificações de tecnologia geram os recursos de cibersegurança de suas equipes de TI. Até o momento, a conscientização dos funcionários pode não ter recebido toda a atenção que merece, mas pode ser fundamental na luta contra os ataques cibernéticos nos próximos anos.

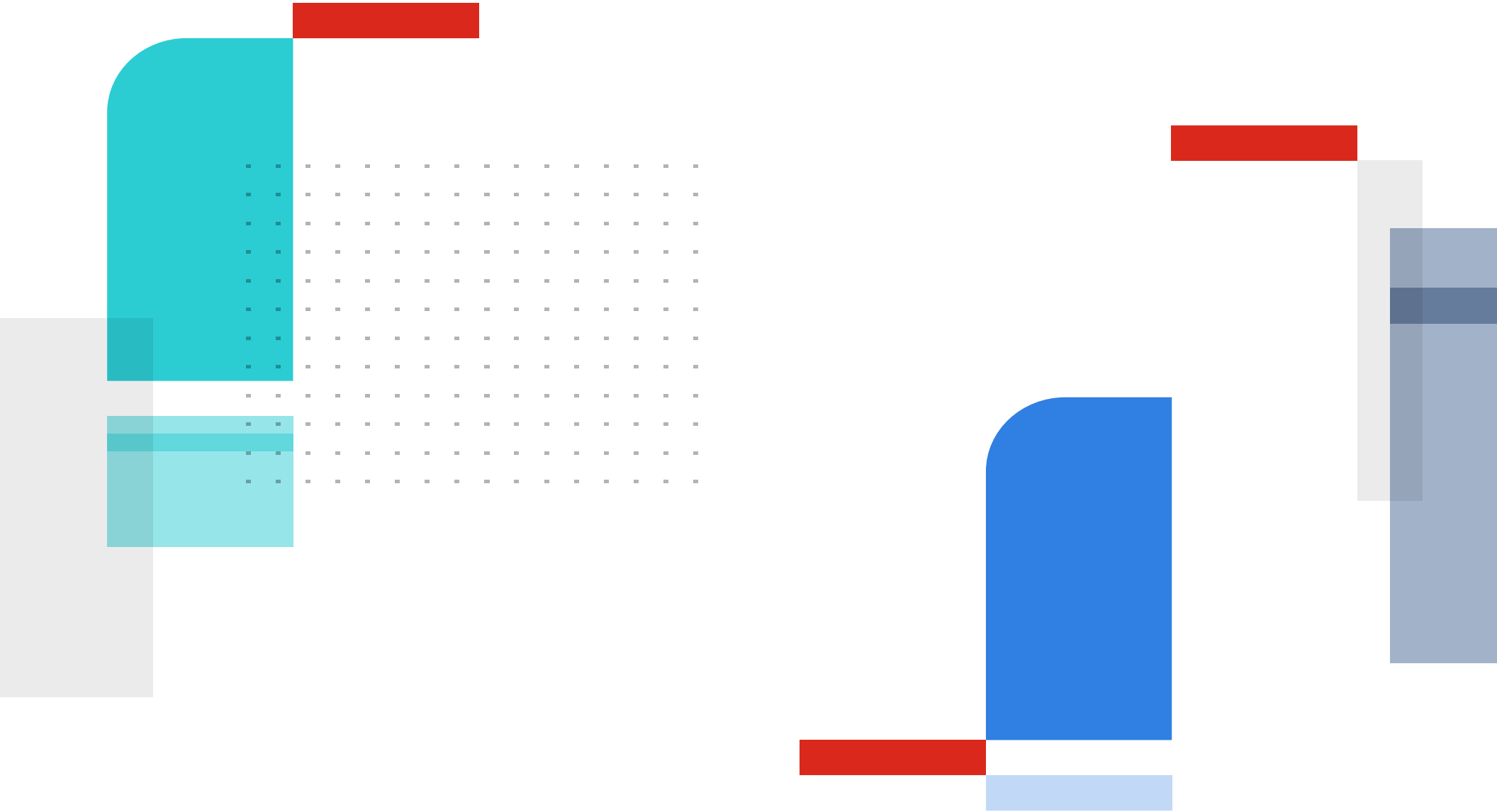
Obtenha uma visão mais ampla e detalhada das necessidades e desafios de cibersegurança das organizações no Relatório de pesquisa global sobre o déficit de competências em cibersegurança 2023 da Fortinet.

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 https://www.fortinet.com, no Fortinet Blog, e FortiGuard Labs.



FORTINET

Training Institute

www.fortinet.com

Maio de 2023