3ª EDIÇÃO

vantico

Inside Pentesting

2019

Sumário

Mensagem da **Vantico**

Em 2025 observamos o desenvolvimento e a consolidação de muitas tendências que emergiram nos últimos anos.

A IA se tornou parte do cotidiano tanto das empresas quanto dos adversários, exigindo novas camadas e estratégias de proteção. Supply chain (cadeia de fornecedores) permaneceu sendo um ponto crítico, causando profundo impacto operacional e milhões de dólares em prejuízo no mundo todo.

Também foi o ano em que comprovamos, na prática, que adequação a compliance não traz proteção real. Somente testes constantes e evidências técnicas são capazes de criar um programa de segurança eficaz e resiliente.

A combinação entre o fator humano e a inteligência artificial se mostra uma peça fundamental do quebra-cabeça que vem sendo construído para 2026.

Neste e-book, reunimos os aprendizados que coletamos em centenas de testes, avaliações e revisões, além da expertise de nossa equipe para analisar possíveis tendências e pontos de atenção.

A **Vantico** segue ao seu lado para enfrentar esta nova fase das ameaças cibernéticas.

Kaique Bonato
CEO da Vantico

Sumário Executivo

Compreender os dados e antecipar tendências é essencial para se preparar com eficiência para 2026.

Neste material, você irá encontrar as conclusões extraídas por nossos especialistas após centenas de testes conduzidos pela Vantico e meses de pesquisa em diferentes fontes.

Isso nos permitiu reconhecer padrões, mapear frequência e impacto, e identificar as principais tendências em evolução.

Este e-book é um apoio para as decisões do board, e um guia estratégico para profissionais de TI e segurança da informação. Use-o de forma complementar às métricas e ao contexto do negócio para transformar riscos em ações.

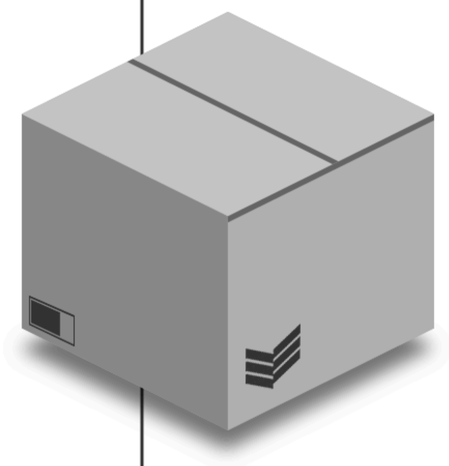
Cibersegurança em 2025

1. Phishing e Engenharia Social
2. Compliance vs. Segurança
3. Supply chain de alto impacto
4. Despreparo no uso de IA
5. Esgotamento dos profissionais de segurança

Tendências para 2026

1. IA como sistema operacional dos atacantes (+ fator humano em destaque)
2. Gestão de identidades no centro
3. Resiliência como métrica fundamental
4. Riscos de Supply Chain se acentuam
5. Ransomware causará mais estragos

Tipos de Pentests Executados em 2025



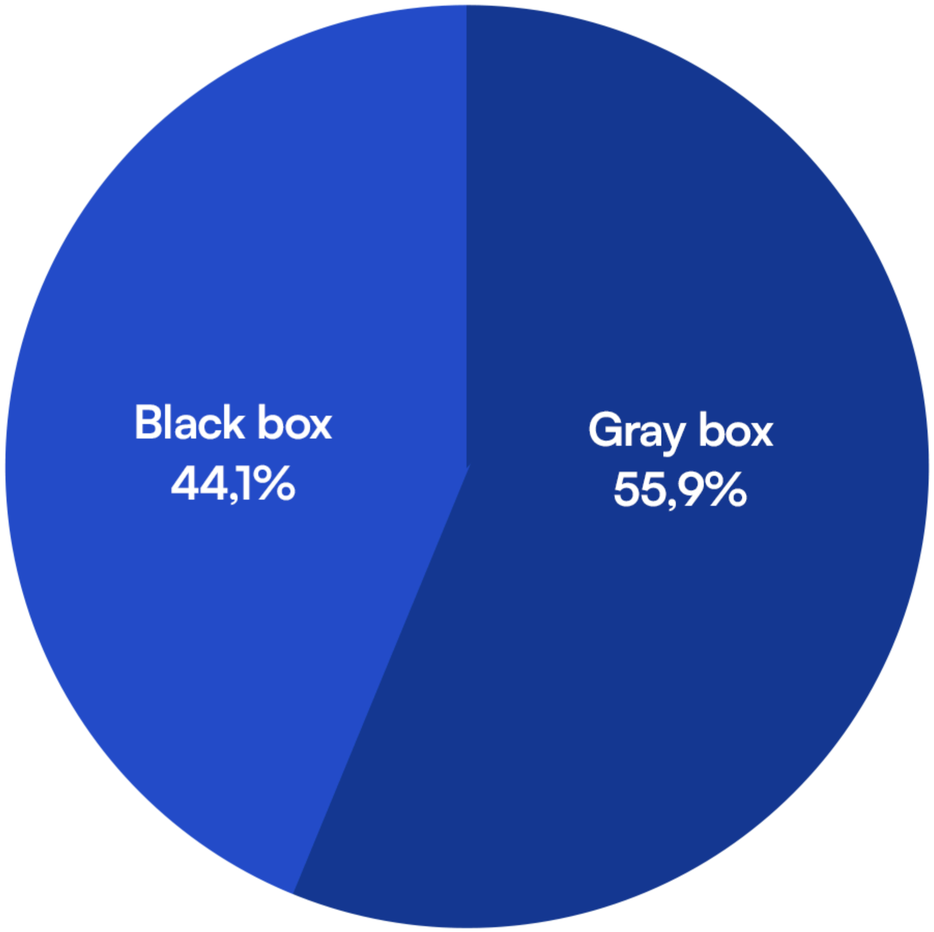
Gray box

- Execução em áreas específicas do ativo (interna e externa)
- Usa credenciais de acesso
- Fornece informações limitadas sobre estrutura/sistema
- Foi usado em 55,9% dos Pentests de 2025 ↑

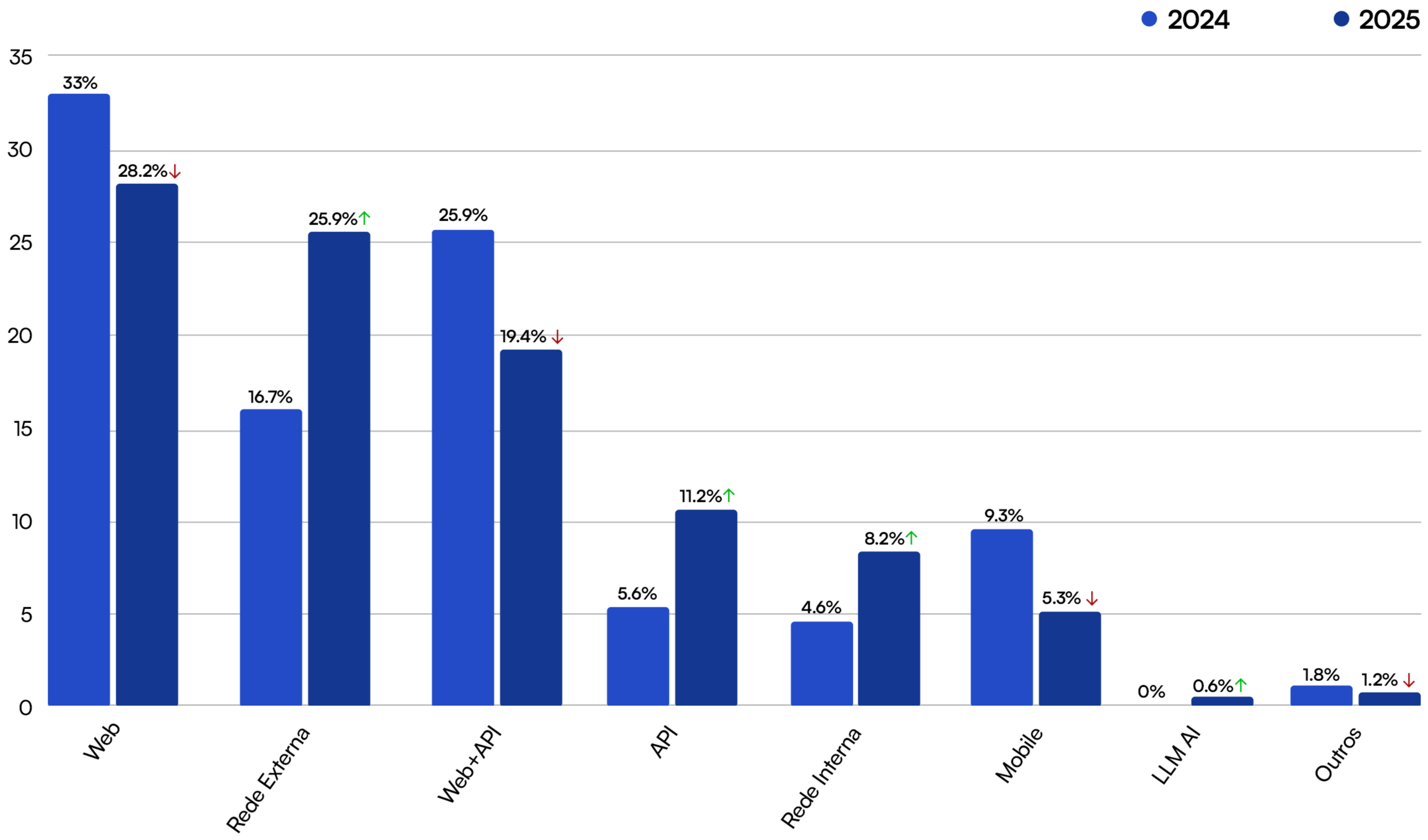
Black box

- Execução de forma externa
- Sem credenciais de acesso
- Sem informações sobre estrutura/sistema
- Foi usado em 44,1% dos Pentests de 2025 ↓

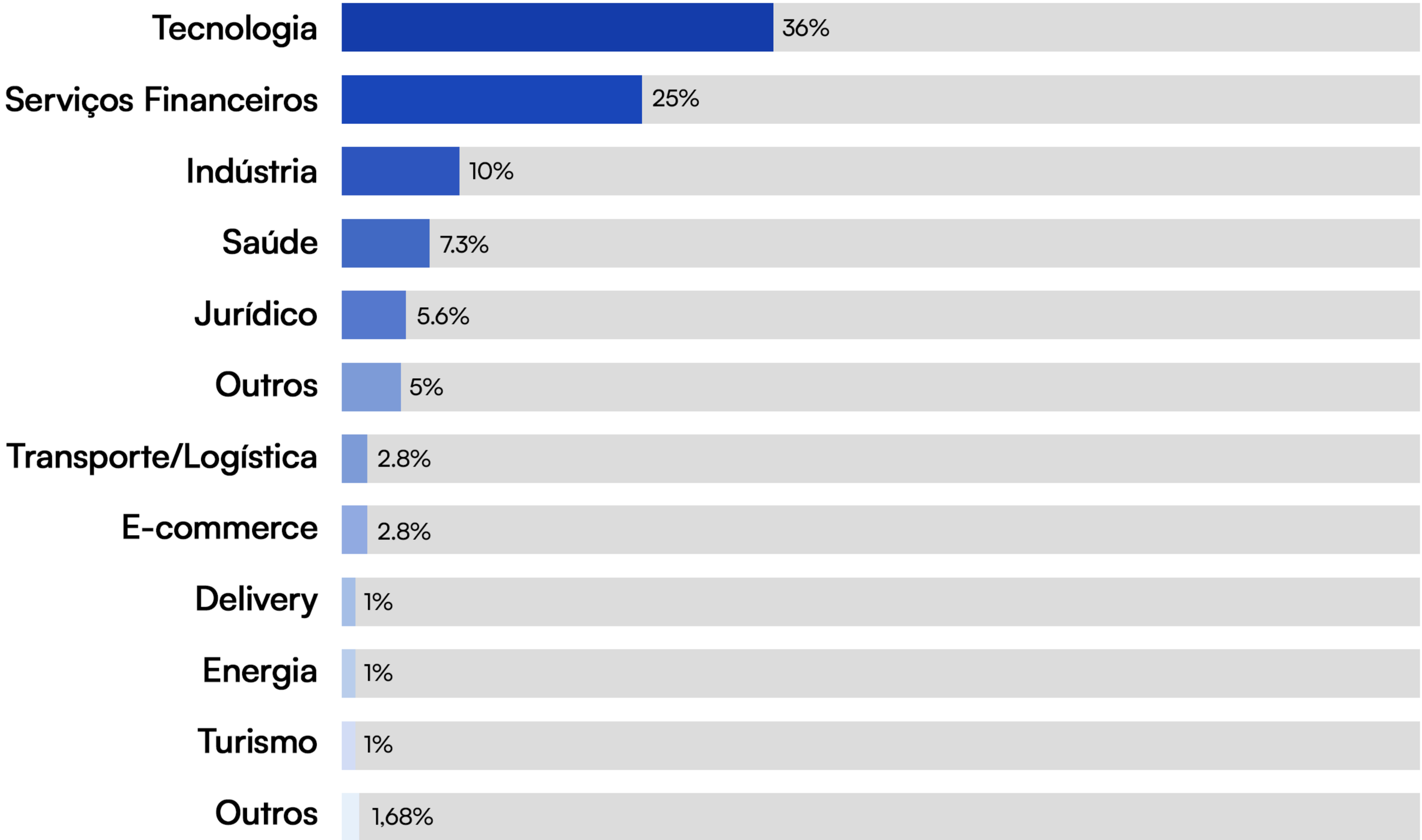
Contagem de credenciais



Principais ativos testados em 2025



Setores em que a Vantico atuou



5 principais falhas identificadas

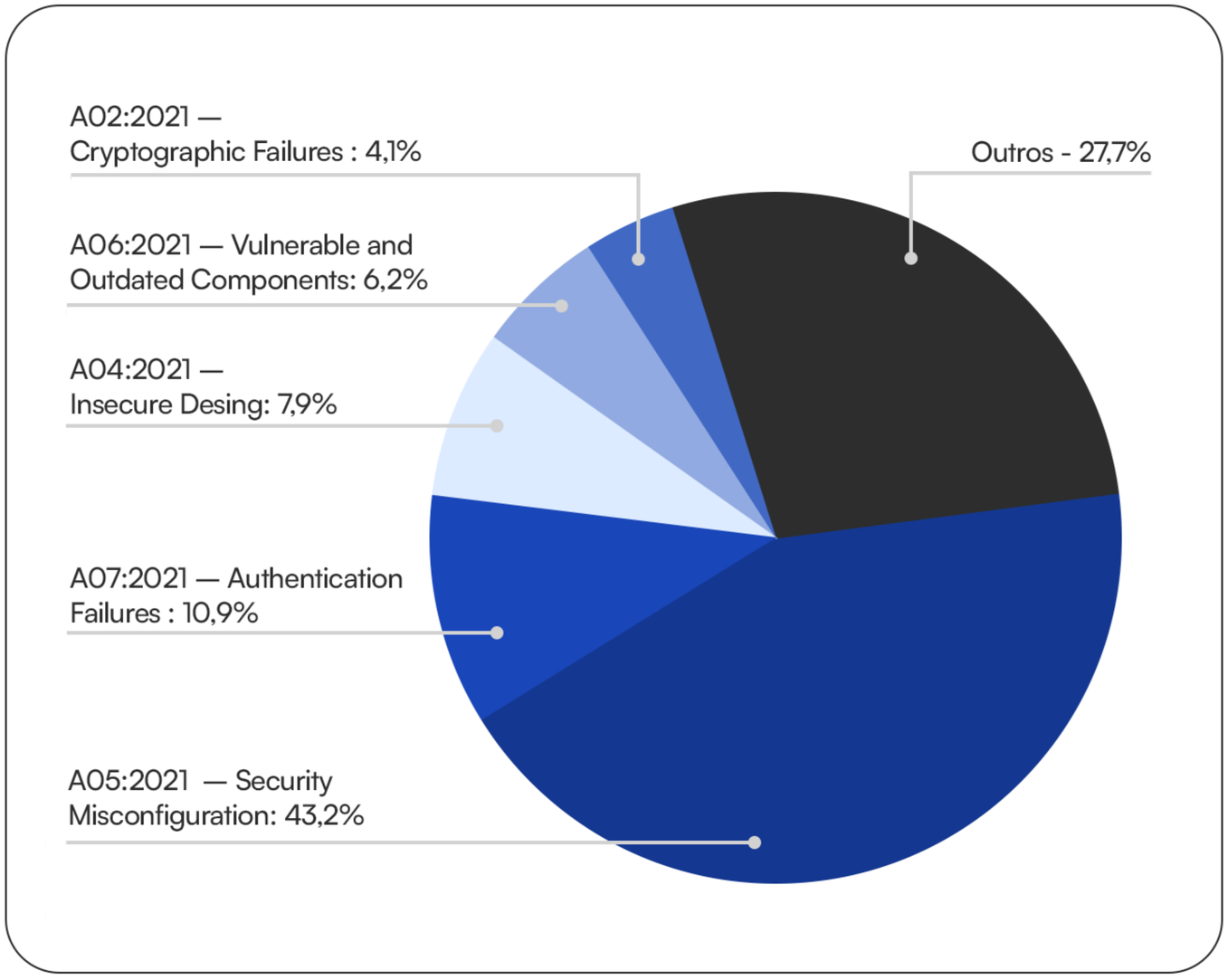
1. A05:2021
   Security Misconfiguration (43.2%)

2. A07:2021
   Authentication Failures (10.9%)

3. A04:2021
   Insecure Design (7.9%)

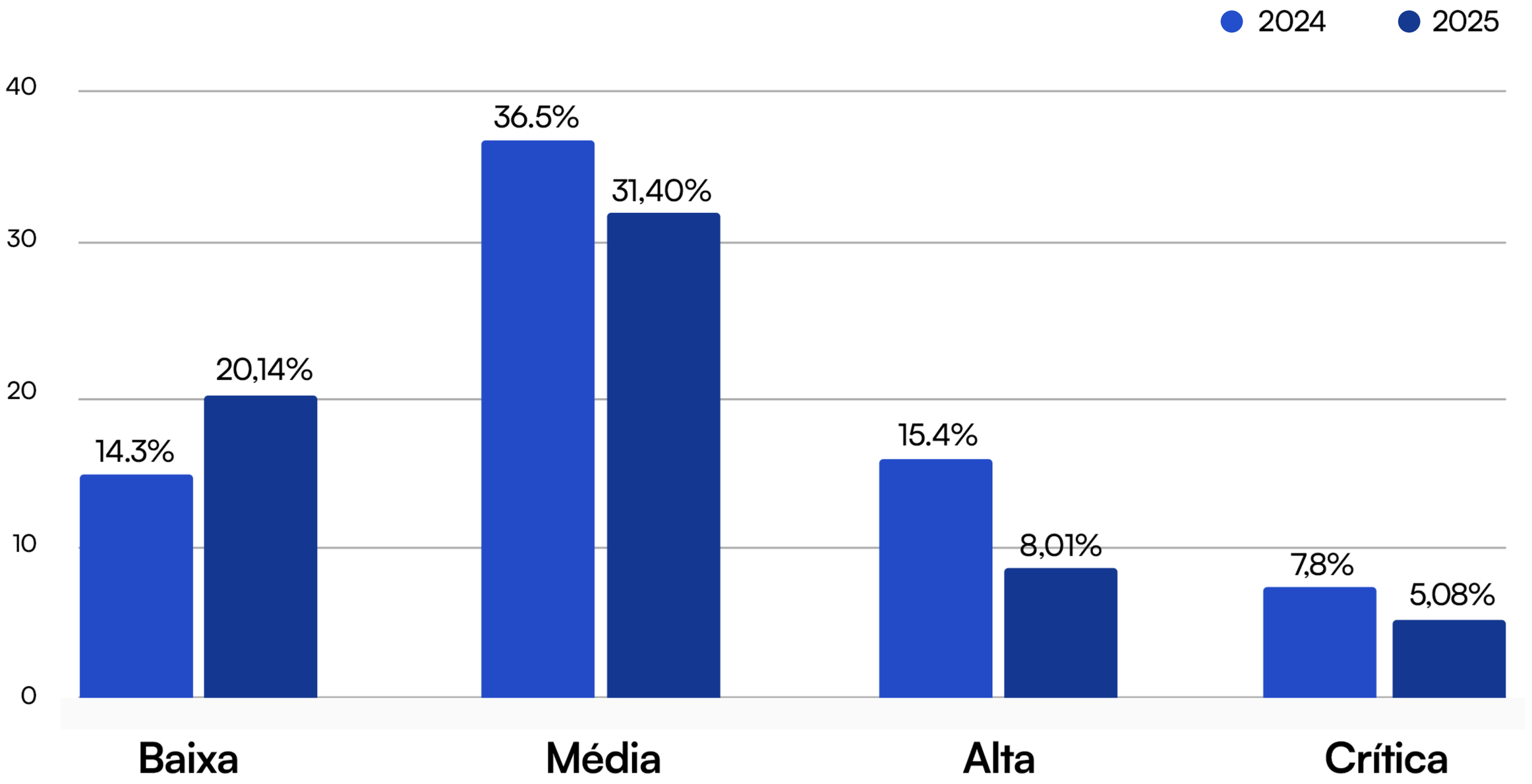
4. A06:2021
   Vulnerable and Outdated Components (6.2%)

5. A02:2021
   Cryptographic Failures (4.1%)

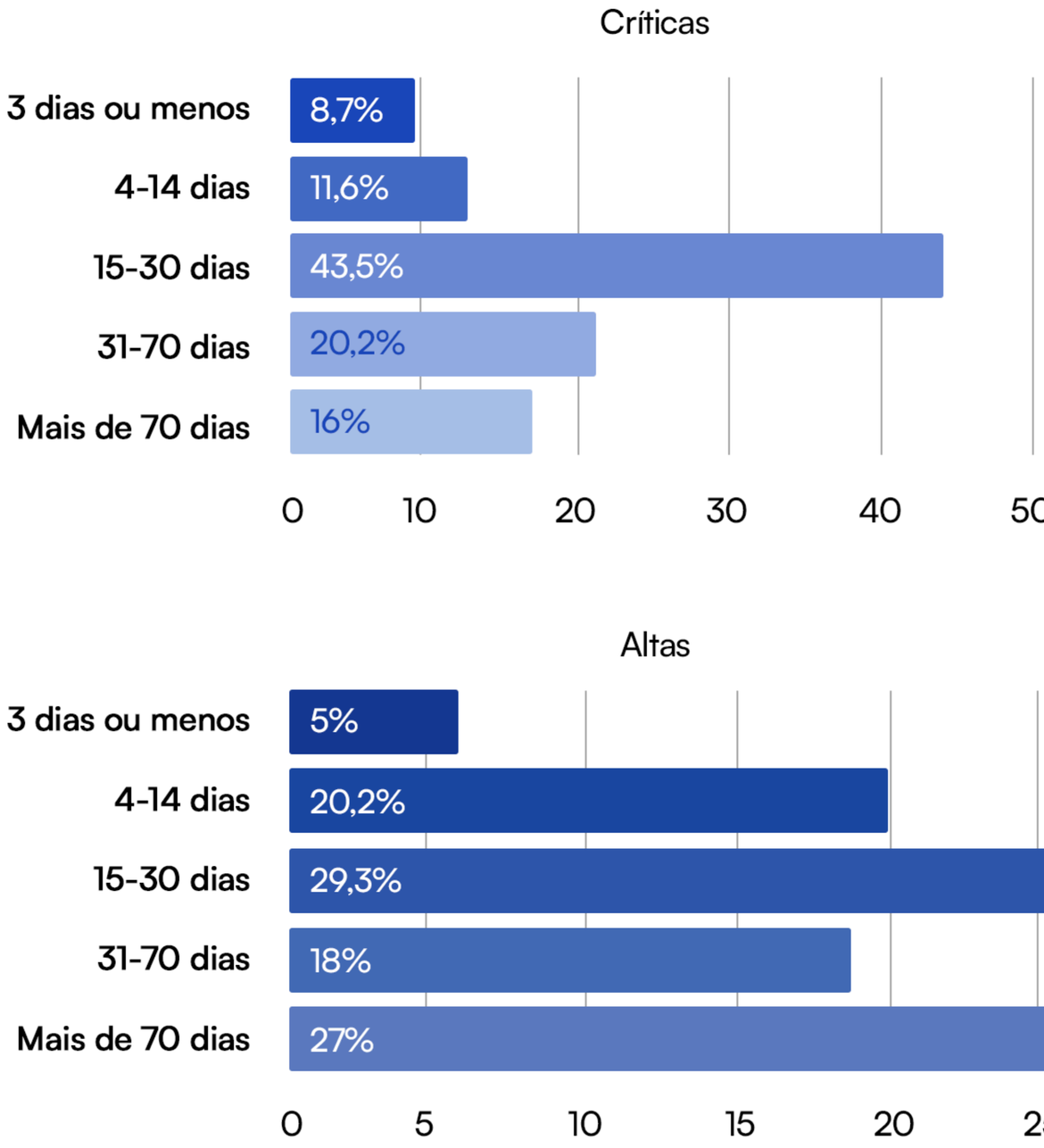


**Note que houve uma mudança na categorização das vulnerabilidades em relação às edições anteriores deste e-book, em que usávamos o padrão da Bugcrowd. A partir da edição atual (2026), estamos adotando o padrão do mercado, ou seja, a classificação da OWASP[1].

Severidade das vulnerabilidades encontradas



SLA para correção de vulnerabilidades

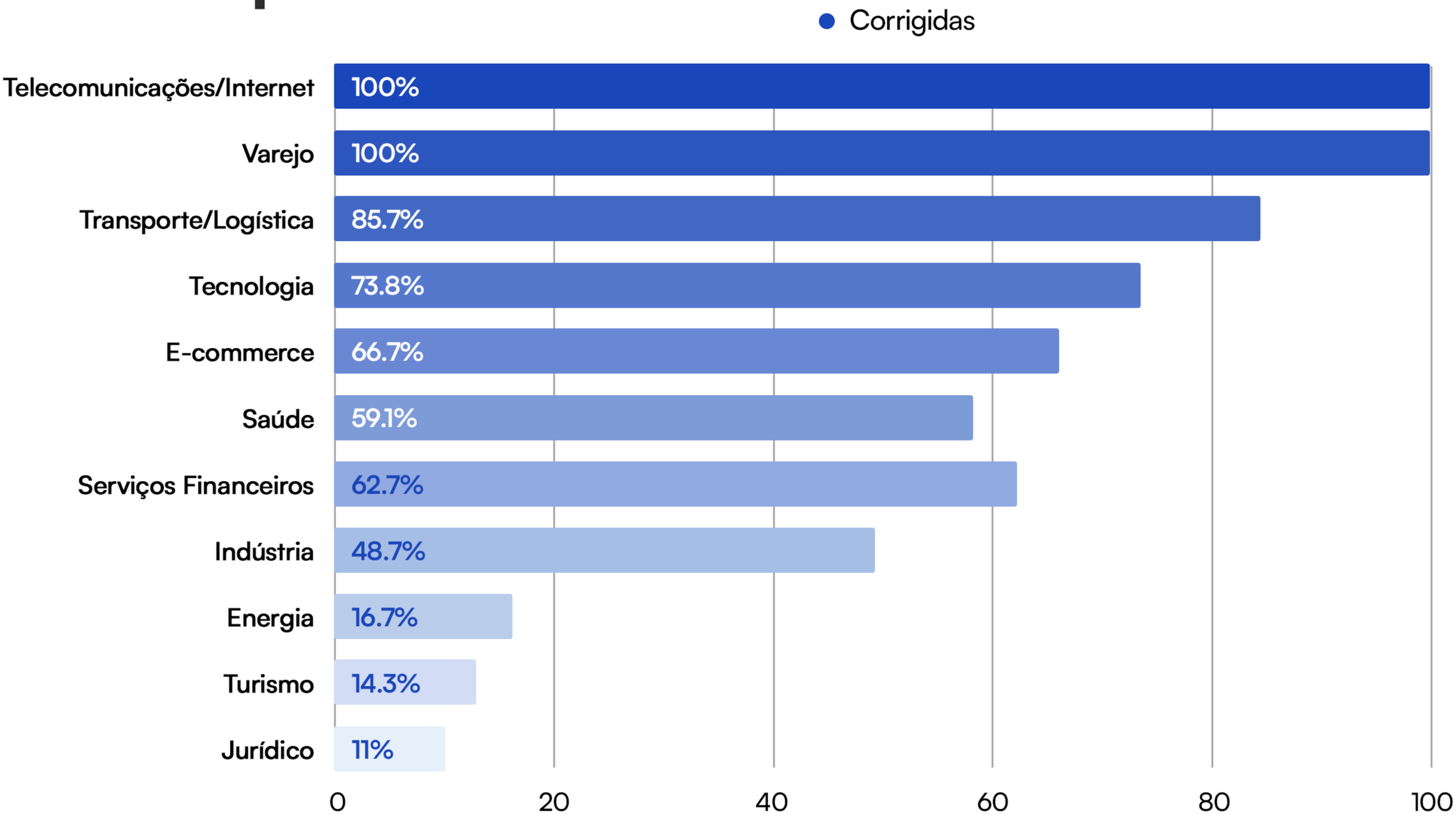


Embora a maioria das vulnerabilidades críticas e de alta severidade seja corrigida em até um mês, há uma parcela considerável cuja remediação ocorre posteriormente.

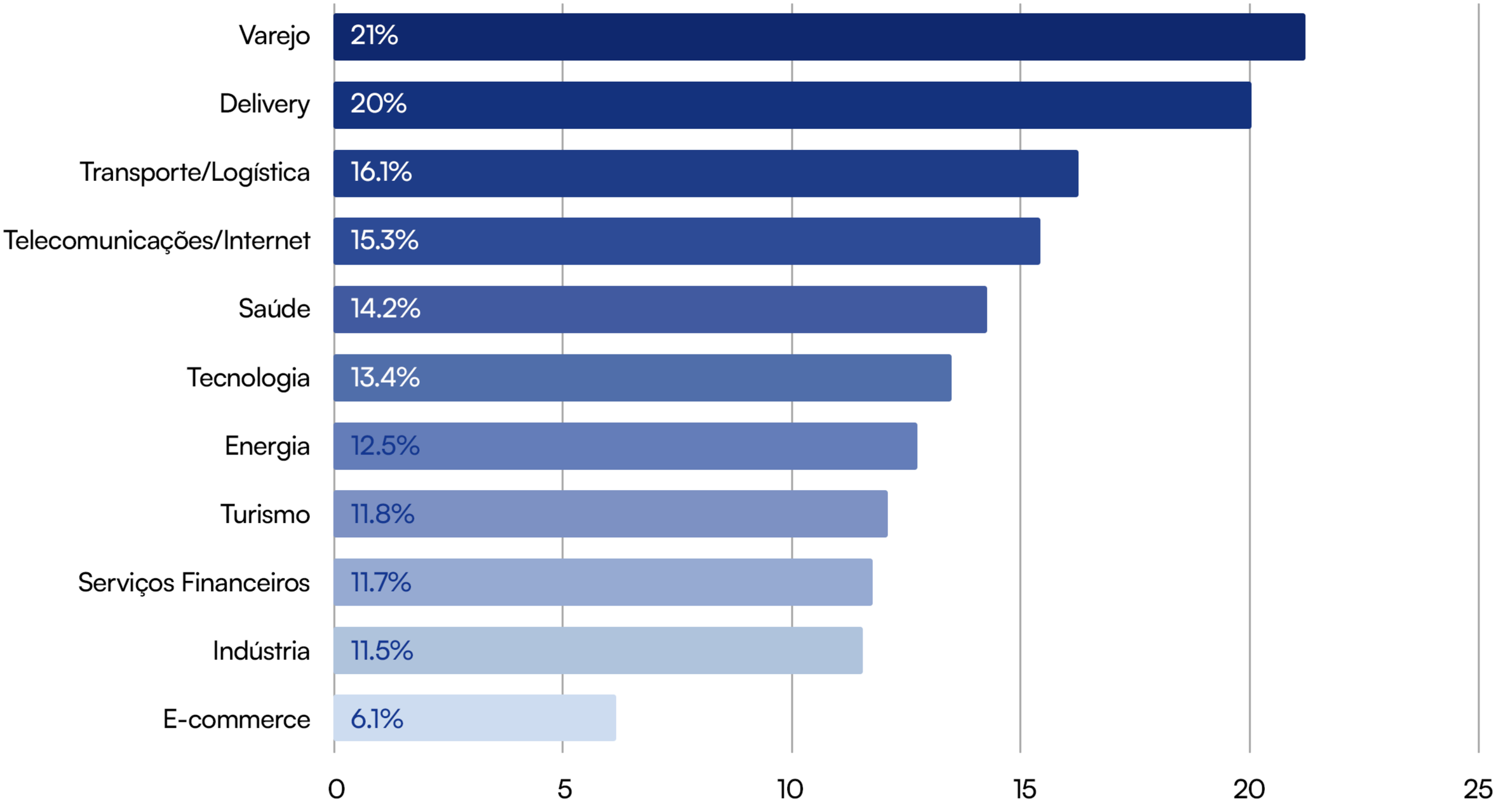
Esse atraso costuma refletir duas falhas recorrentes: a **incapacidade de integrar correções ao cotidiano operacional e a dificuldade de priorizar as correções de forma prática,** mesmo quando os relatórios já trazem classificação por impacto e probabilidade de exploração.

Como consequência, os achados podem permanecer expostos por mais tempo, aumentando os riscos de serem explorados.

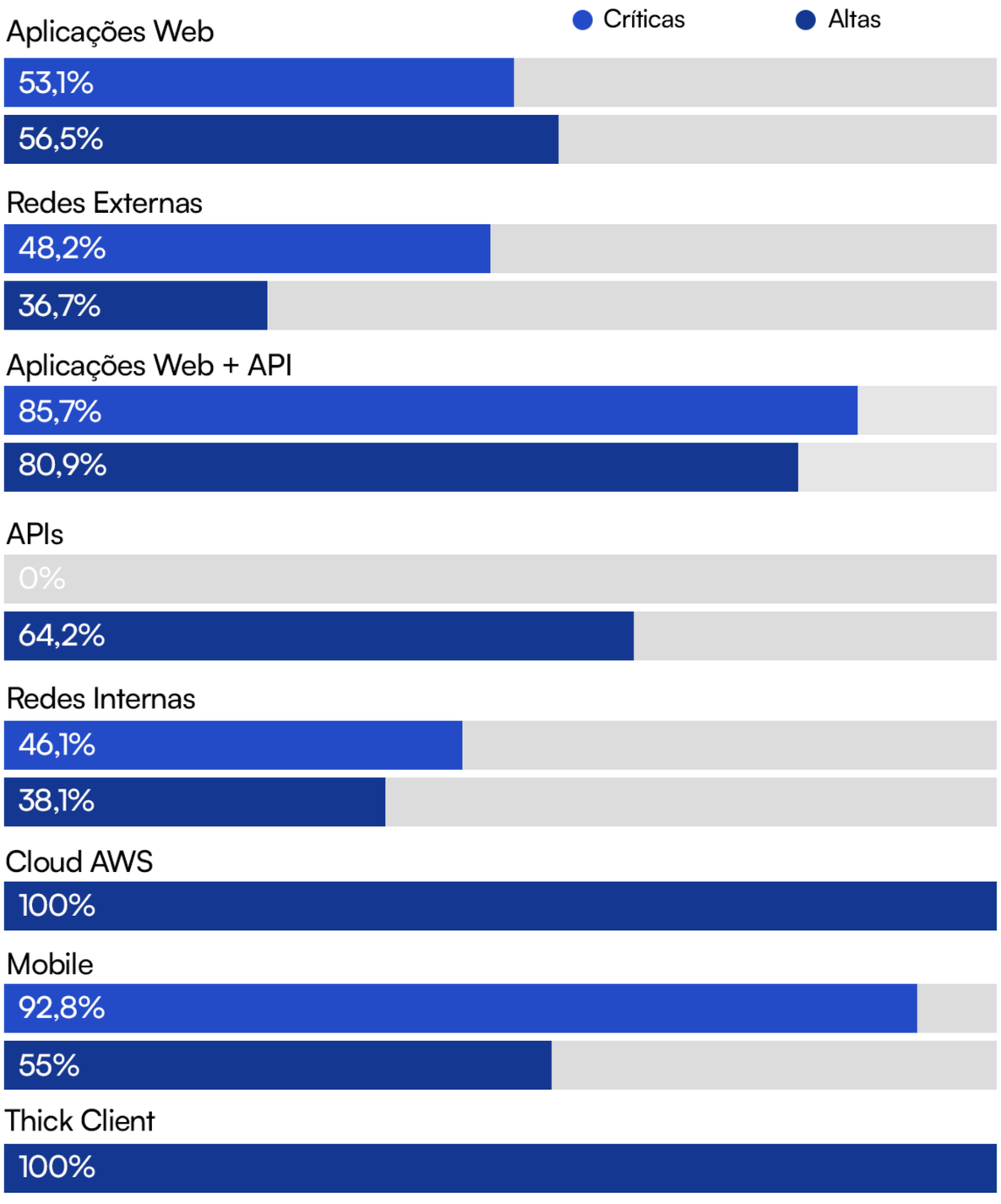
Correção de vulnerabilidades críticas e altas por setor



Prevalência de vulnerabilidades críticas e altas por setor



Correção baseada no tipo de pentest



Pentests executados em aplicações web + APIs, cloud AWS, thick client, e mobile, apresentam as maiores taxas de correção para vulnerabilidades altas e críticas, enquanto redes internas e externas têm desempenho pior nesse indicador.

Essa assimetria pode sugerir dois aspectos operacionais: as aplicações normalmente possuem donos claros e fluxos de deploy que permitem correções rápidas, já as correções de rede frequentemente exigem planejamento, janelas de mudança e intervenção em hardware ou provedores terceirizados.

Como consequência, isso pode gerar uma **falsa sensação de segurança,** com a organização se sentindo protegida pelas vulnerabilidades corrigidas em aplicações, sendo que continua vulnerável devido a **falhas de infraestrutura** que oferecem caminhos para movimentação lateral.

Tempo médio de correção de vulnerabilidades graves (críticas e altas) por tamanho da organização

Pequenas empresas

Pequenas empresas costumam apresentar processos mais simples e menos burocracia, o que, em tese, facilita correções rápidas.

Por outro lado, a falta de equipe técnica dedicada, a ausência de pipelines automatizados para deploy, a dependência de um pequeno grupo de pessoas e orçamento limitado podem impactar negativamente em alguns casos.processos de governança podem aumentar o tempo até a correção da vulnerabilidade.

Médias empresas

Essas organizações estão numa linha tênue entre estruturação e necessidade de agilidade.

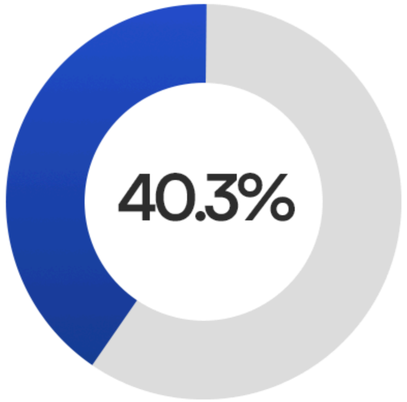
Elas podem ter equipes de desenvolvimento maiores e processos bem definidos, porém a dificuldade de aprovação, as janelas de manutenção e os testes adicionais podem elevar o tempo até a correção.

Grandes empresas | Enterprise

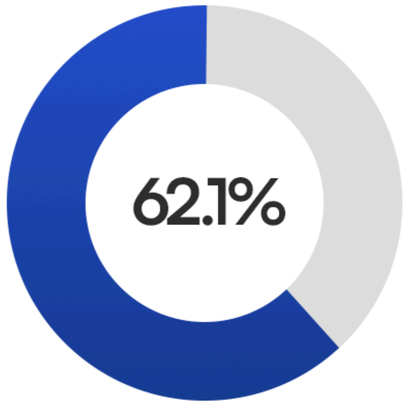
Organizações maiores têm desafios complexos: múltiplos ambientes, dependência de terceiros, políticas de compliance rigorosas, janelas de manutenção restritas e processos de aprovação multilayer.

Algumas correções podem ter complexidade técnica maior, e os processos de governança podem aumentar o tempo até a correção da vulnerabilidade.

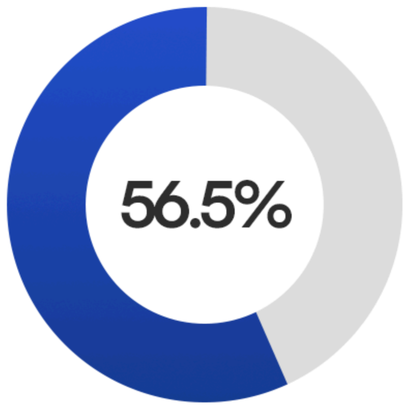
Vulnerabilidades corrigidas



de todas as vulnerabilidades encontradas foram corrigidas



das vulnerabilidades críticas foram corrigidas



das vulnerabilidades altas foram corrigidas

Em um pentest, a execução do teste é a parte fácil. Afinal, o fornecedor faz a maior parte do trabalho. O verdadeiro desafio vem depois, quando o relatório e é preciso planejar, priorizar e executar correções.

Segundo nossos dados, somente cerca de 40% de todas as vulnerabilidades encontradas nos testes são corrigidas.

Quando consideramos os achados críticos e de alta severidade, o número pelo menos ultrapassa a metade, indicando que as falhas graves são priorizadas pelas organizações.

Mesmo assim, ainda estamos falando de um **alto número de ameaças não corrigidas,** que continuam (e continuarão) representando sérios riscos para a segurança da empresa.

Na rotina de um time de segurança, a correção de vulnerabilidades precisa ganhar espaço para que a proteção seja eficiente.

5 principais vulnerabilidades críticas e altas

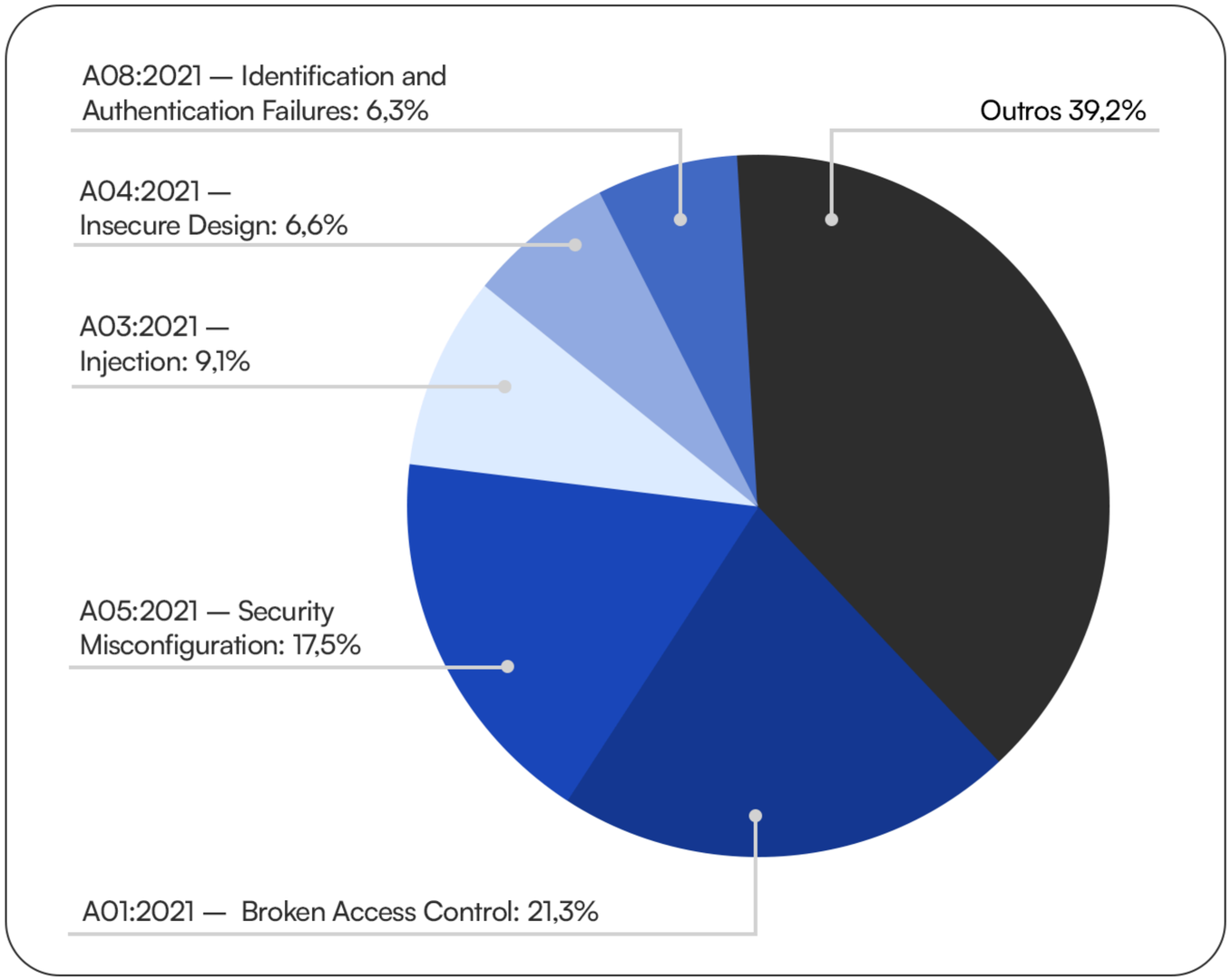
1. A01:2021
   Broken Access Control (21.3%)

2. A05:2021
   Security Misconfiguration (17.5%)

3. A03:2021
   Injection (9.1%)

4. A04:2021
   Insecure Design (6.6%)

5. A07:2021
   Identification and Authentication Failures (6.3%)



**Note que houve uma mudança na categorização das vulnerabilidades em relação às edições anteriores deste e-book, em que usávamos o padrão da Bugcrowd. A partir da edição atual (2026), estamos adotando o padrão do mercado, ou seja, a classificação da OWASP[1].

A01:2021 - Broken Access Control

O que é?

O controle de acesso garante que cada usuário acesse e modifique somente o que está dentro de suas permissões. A falha desses controles dá ao usuário poder de agir além desses limites.

Causas:

- Violação do princípio do privilégio mínimo ou negação por padrão.
- API acessível sem controles de acesso para POST, PUT e DELETE.
- Ausência de validação de permissões.
- Entre outros.

Algumas CWE associadas:

- CWE-284: Improper Access Control
- CWE-200 Exposure of Sensitive Information to an Unauthorized Actor
- CWE-201 Exposure of Sensitive Information Through Sent Data

A05:2021 - Security Misconfiguration

O que é?

Quando o sistema, aplicação ou serviço na nuvem é configurado indevidamente, ocasionando inúmeras brechas de segurança.

Causas:

- Falta de práticas de segurança que reforçam a segurança da aplicação (hardening).
- Permissões configuradas incorretamente em serviços na nuvem.
- Funcionalidades desnecessárias, como ports, páginas ou privilégios.
- Credenciais de fábrica (by default).
- Entre outros.

Algumas CWE associadas:

- CWE-16: Configuration.
- CWE-260: Password in Configuration File.

A03:2021 - Injection

O que é?

Falha na aplicação que permite uma entrada maliciosa interpretada como código ou comando.

Causas:

- Falta de validação de dados enviados pelo usuário.
- Dados não validados são usados nos parâmetros de pesquisa de mapeamento objeto-relacional (ORM) para extrair registros adicionais e sensíveis.
- Concatenação de comandos ou queries.
- Entre outros.

Algumas CWE associadas:

- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting').
- CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection').
- CWE-77 Improper Neutralization of Special Elements used in a Command ('Command Injection')
- CWE-80 Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)CWE-80 Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)
- CWE-94 Improper Control of Generation of Code ('Code Injection')

A04:2021 - Insecure Design

O que é?

Fragilidades que nascem na arquitetura e nas decisões de design, como ausência de requisitos de segurança, falta de threat modeling, entre outros.

Causas:

- Segurança tratada tardiamente (afterthought).
- Falta de integração entre arquitetos e segurança
- Ausência de critérios de aceitação de segurança.
- Entre outros.

Algumas CWE associadas:

- CWE-256: Unprotected Storage of Credentials.
- CWE-269: Improper Privilege Management.
- CWE-434: Unrestricted Upload of File with Dangerous Type.

A07:2021 - Identification and Authentication Failures

O que é?

Falhas que levam ao comprometimento de identidade, como problemas em login, recuperação de senha, tokens de sessão e políticas fracas de credenciais.

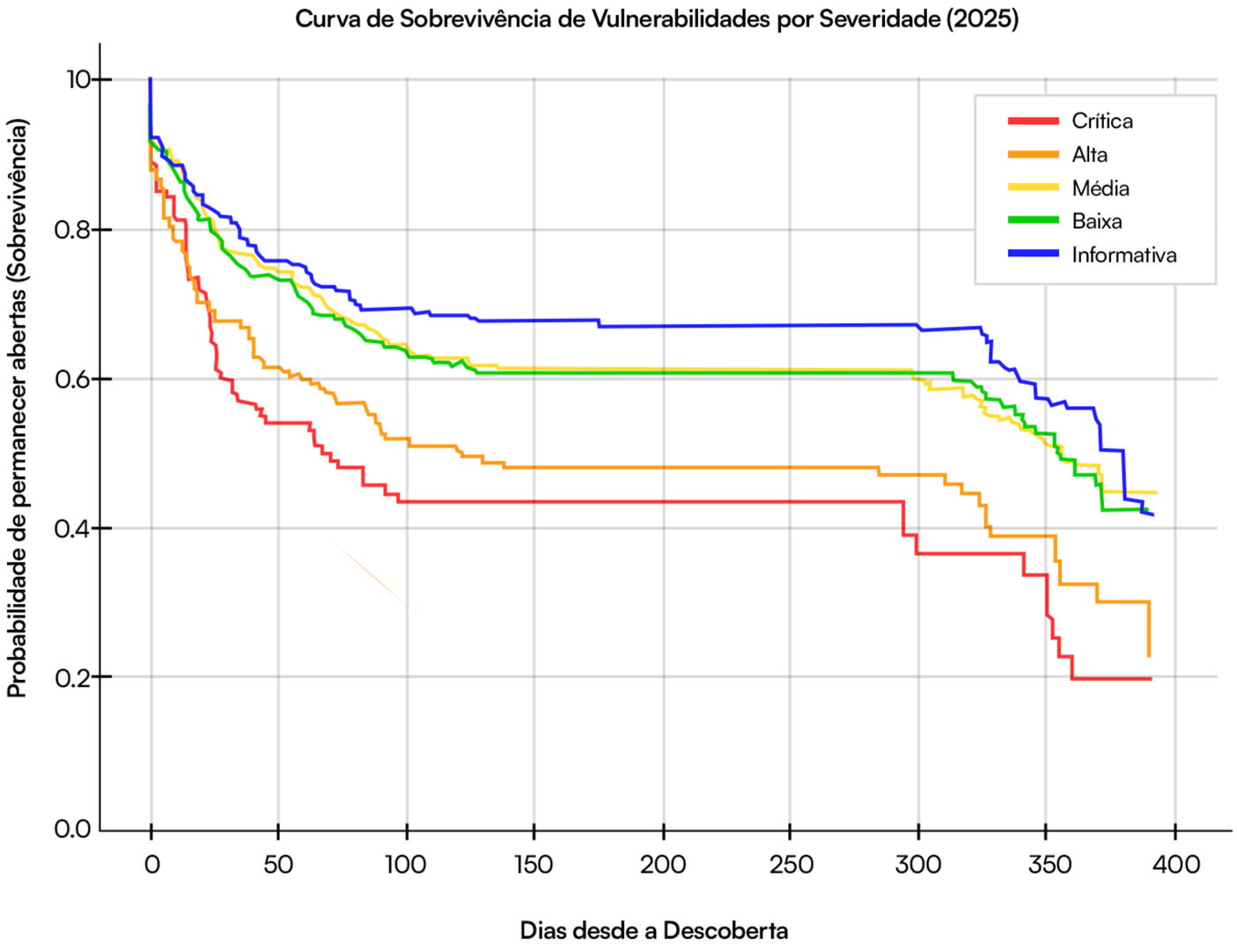
Causas:

- Políticas fracas de senhas.
- Ausência ou ineficácia de autenticação multifator.
- Força bruta.
- Entre outros.

Algumas CWE associadas:

- CWE-297: Improper Validation of Certificate with Host Mismatch.
- CWE-287: Improper Authentication.
- CWE-384: Session Fixation.

Taxa de sobrevivência das vulnerabilidades ao longo do ano

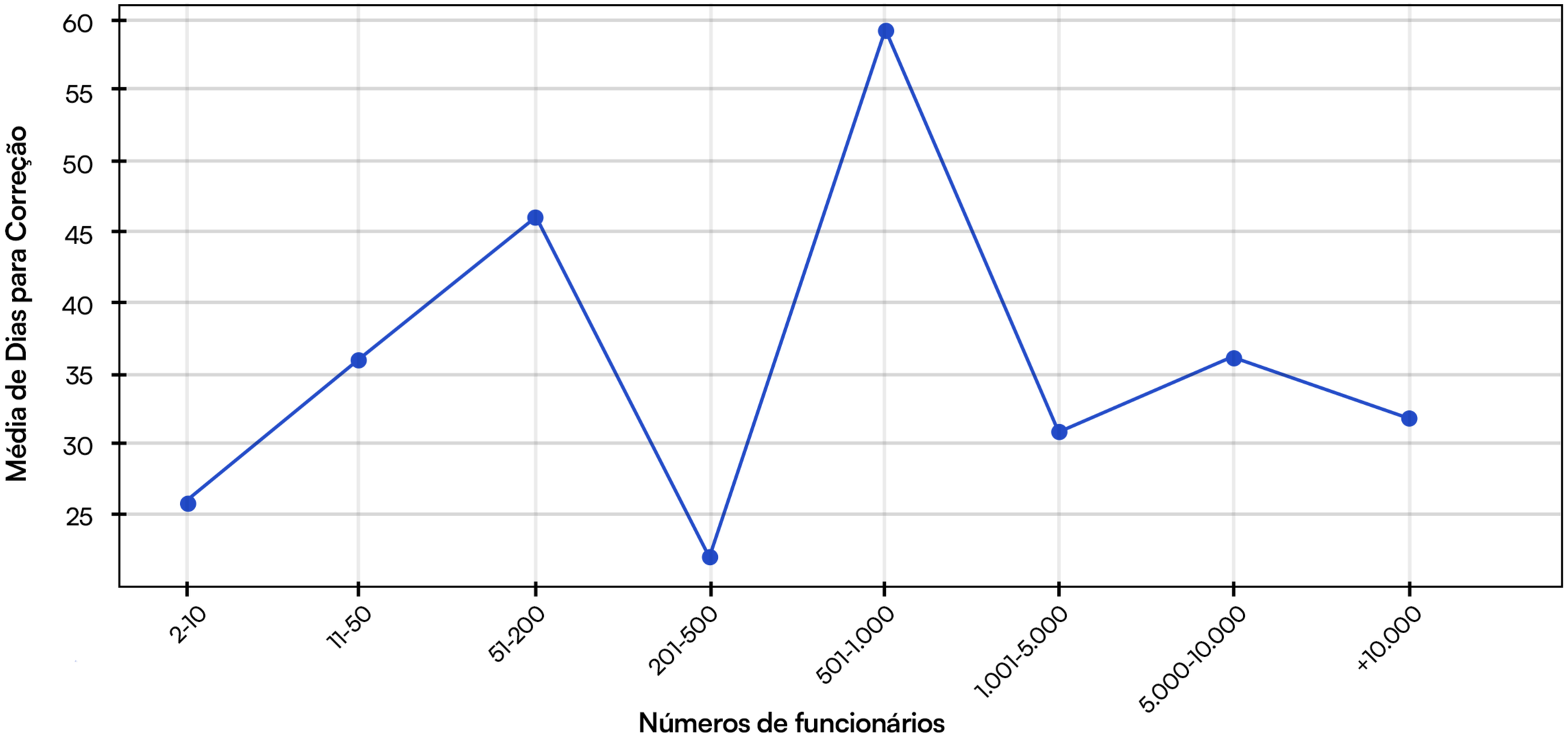


Neste gráfico, que mostra a probabilidade de uma vulnerabilidade permanecer aberta, podemos ver que as falhas críticas são corrigidas com maior agilidade. Isso indica que, embora o **tempo médio de correção seja de 65 dias,** são elas as que têm maior taxa de resolução final.

É possível notar também que, **entre os dias 150 e 250, as curvas ficam quase planas,** evidenciando poucas correções realizadas neste período. Isso pode sugerir um represamento de demandas ou foco em outros projetos.

Cerca de 20% das falhas críticas e quase 45% das falhas informativas/médias sobreviveram ao ciclo de um ano sem correção.

Tempo médio de correção de vulnerabilidades graves (críticas e altas) por tamanho da organização



A janela de exposição de uma organização varia conforme alguns fatores.

Por que o Pentest foi relevante em 2025?

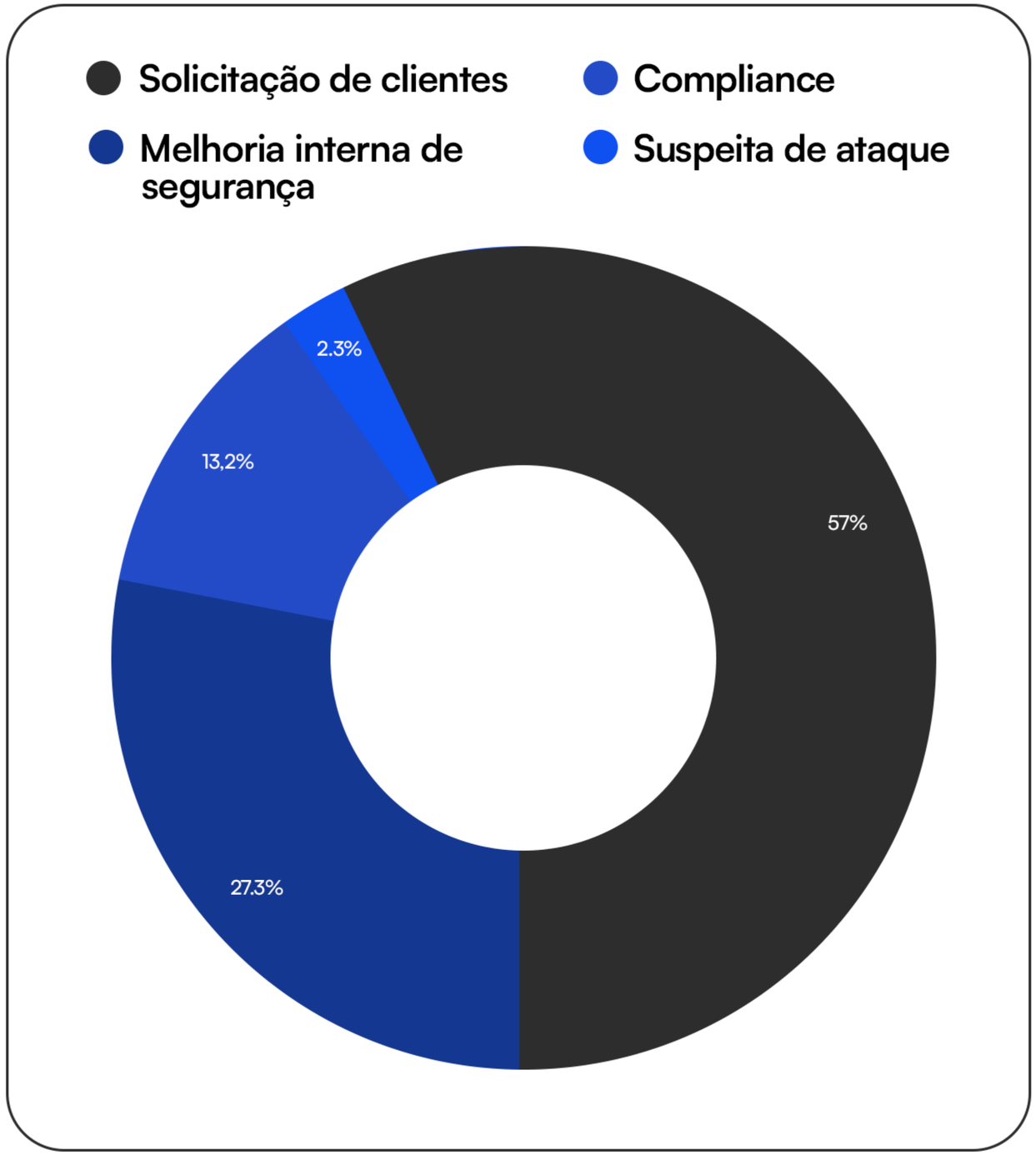
A solicitação de clientes (57%) segue sendo a principal motivação por trás de muitos Pentests.

Em grandes organizações, é frequente que o pentest seja um pré-requisito para fechar negócios ou manter contratos.

A presença desse requisito no ciclo comercial é benéfica porque impulsiona avaliações técnicas e remediação.

Ainda assim, há um risco: quando a motivação principal é externa, as ações tendem a ser reativas e pontuais.

Isso reforça que, **para muitas empresas, a preocupação com segurança ainda é uma exigência do mercado, não um interesse próprio.**



Análise de segurança por setor

Saúde
US$7.42 mi

foi o custo médio de uma violação de dados em 2025.[2]

93% das instituições de saúde enfrentaram um ataque cibernético em 2024.[3]

Estima-se que **40% das organizações** do setor irão enfrentar algum tipo de ataque de ransomware em 2026.[4]

Financeiro
US$5.56 mi

foi o custo médio de uma violação de dados em 2025.[2]

97% dos bancos estadunidenses sofreram vazamentos devido a terceiros e à cadeia de fornecedores em 2024.[5]

O **Comprometimento de E-mail Comercial (BEC)** é uma das ameaças de maior impacto financeiro do setor, tendo gerado US$2.7 bilhões em prejuízo em 2024.[6]

Industria
US$5 mi

foi o custo médio de uma violação de dados em 2025.[2]

Foi o **setor mais atingido** pelo quarto ano consecutivo, sofrendo 26% de todos os ataques.[7]

Intrusão em sistemas, engenharia social e ataques simples a aplicações web representam **85% das violações de segurança.[8]**

Energia
US$4.83 mi

foi o custo médio de uma violação de dados em 2025.[2]

Conforme a crise climática se intensifica, o setor energético se torna um alvo cada vez mais atrativo para os atacantes.[9]

A exploração de vulnerabilidades neste setor tem um enorme potencial de impacto, podendo **atingir a sociedade e afetar a economia.[9]**

Tecnologia
US$4.79 mi

foi o custo médio de uma violação de dados em 2025.[2]

Note que o setor de tecnologia envolve, majoritariamente, produtos SaaS, que também estão ligados a outros segmentos de mercado.

Entre os **setores mais atingidos por ataques de supply chain** em 2025 estão os serviços de TI e as empresas de tecnologia.[10]
São alvos extremamente visados, pois **comprometer um ativo pode levar ao acesso de dados de milhares (até milhões) de clientes.**

Custo de uma violação de dados

US$ 4.44 milhões

custo médio de uma violação de dados em 2025

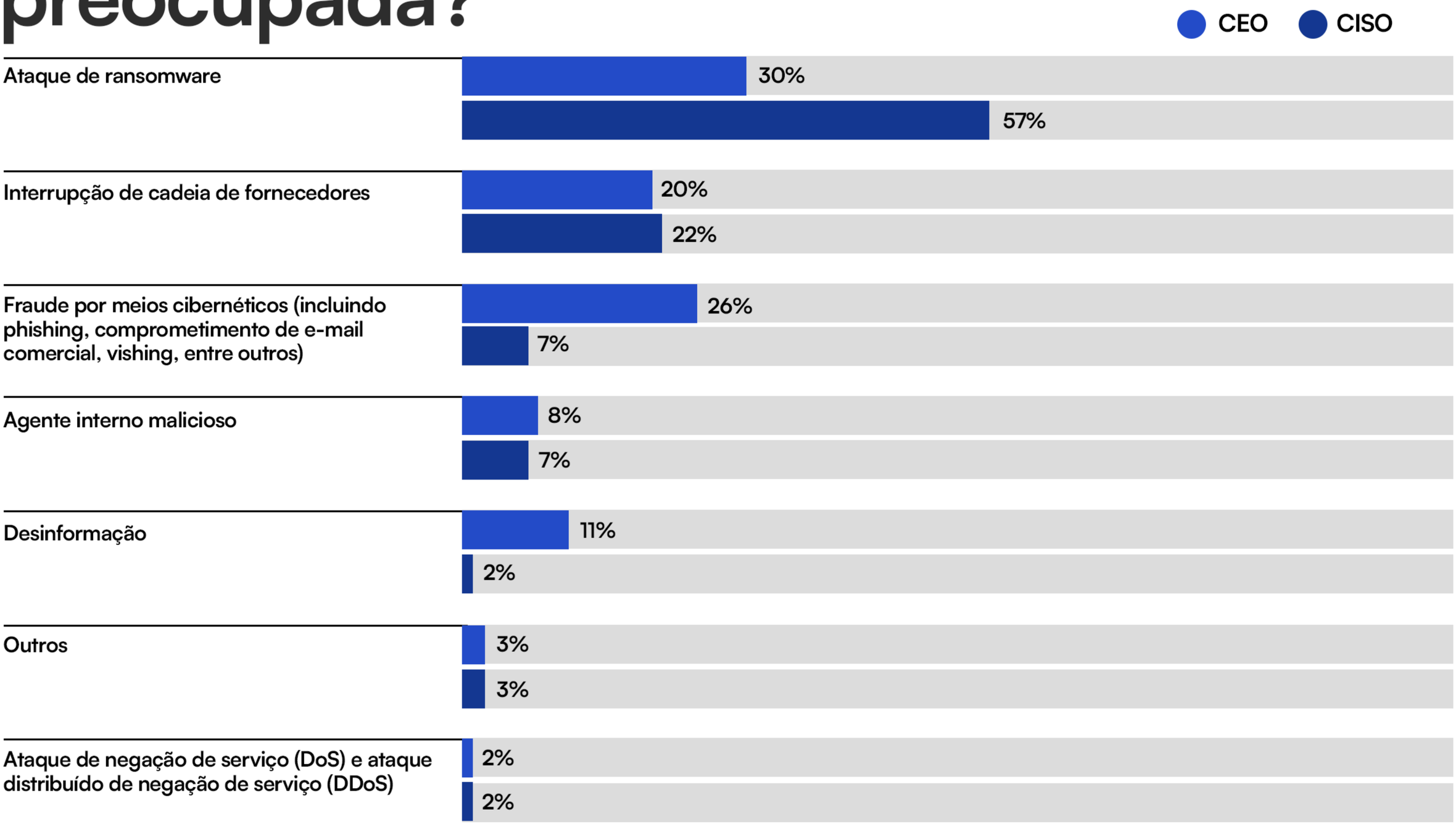
US$1.22 milhões

custo médio de uma violação de dados no Brasil em 2025

Houve uma redução no impacto financeiro das violações de dados, tanto no Brasil quanto na média global, que retornou aos níveis de 2023 após ter batido o recorde no ano passado.

Além disso, a IBM também afirma que as organizações que investiram extensamente em IA em 2025 tiveram uma economia de US$1.9 milhões em segurança.

Com quais riscos a sua organização está preocupada?



Fonte: World Economic Forum, 2025.[9]

Cibersegurança em 2025

1 Phishing/Engenharia social

O Phishing foi um dos principais vetores de ataque de 2025.

Esse dado representa dois fatores importantes, que irão influenciar o ano de 2026:

O fator humano como importante ponto de entrada para atacantes

No ano passado, 60% dos vazamentos de dados envolveram algum elemento humano.[8] Isso posiciona a **nossa conduta como um dos principais facilitadores para a concretização de um ataque.**

E, mesmo com treinamentos tradicionais, a complexidade e sofisticação dos ataques gerados por IA tornam a identificação da ameaça ainda mais difícil.

A influência da IA na criação de ataques mais sofisticados.

As campanhas de phishing geradas com IA cresceram 1.265%, o que demonstra uma escalada na capacidade operacional dos atacantes.[7]

Além disso, em 2025, 16% das violações de dados envolveram o uso de IA por parte dos invasores, sendo 37% para gerar phishing e 35% para o uso de deepfakes[2].

As ferramentas de Inteligência Artificial **estão escalando a velocidade que os ataques ocorrem, tornando-os altamente personalizados e ainda mais difíceis de identificar.**

Ferramentas como proteção avançada de e-mail e validação em vários canais (no caso de operações sensíveis) se tornaram indispensáveis. Treinar cenários de detecção e resposta específicas para esse cenário também se consolida como uma prática essencial.

2 Compliance ≠ Segurança

Segurança real vai muito além do compliance.

2025 foi o ano em que isso ficou escancarado, com tantos ataques devastadores em diversos setores e empresas que exibiam suas certificações com muito orgulho.

O problema nunca foi o compliance em si. Frameworks como PCI DSS e ISO 27001 são relevantes e contribuem para a implementação de práticas seguras.

Porém, essas práticas precisam ser **mantidas continuamente.** Ter um papel não significa nada sem políticas de segurança, testes frequentes e treinamentos.

---

3 Supply Chain de alto impacto

2025 deixou claro que nenhuma empresa vive isolada, e o comprometimento de um único fornecedor pode prejudicar, e até interromper, as operações de milhares de organizações.

Em relação a 2024, o risco de incidentes envolvendo terceiros praticamente dobrou no ano passado, chegando a 30%[11].

Com a expansão do uso de SaaS, isso se torna um ponto ainda mais crítico.
Fica cada vez mais claro que **uma empresa não depende somente de suas medidas de proteção,** mas também das estratégias de segurança adotadas por sua cadeia de fornecedores.
Um exemplo de grande destaque aconteceu aqui no Brasil, quando um incidente a um software de banking as a service (BaaS) permitiu que hackers roubasse bilhões de diferentes instituições bancárias.[12]

4 Uso descontrolado de IA

A IA tem auxiliado as organizações a otimizarem suas estratégias defensivas e a identificar comportamentos suspeitos com maior rapidez.

Porém, o rápido crescimento dessa ferramenta fez com que muitas empresas a adotassem sem processos de governança bem definidos. Segundo a IBM, esse número chega a 63%[2].

Isso significa que muitas IAs foram implementadas sem aprovação prévia, sem controles básicos, sem revisão de arquitetura e com o envio/armazenamento de dados sensíveis sem critério.

O custo de uma violação de dados que envolvia o uso de IAs não autorizados ou shadow AI chegou a US$4.63 milhões. Esse número exorbitante se deve à alta porcentagem de empresas que não realizam auditorias em seus modelos e não testam com frequência[2].

---

5 O desgaste emocional dos profissionais de segurança

O cenário da segurança é cada vez mais complexo e volátil, e isso tem um alto custo para osprofissionais da área.

Eles enfrentam pressão severa de seus líderes para promover um ambiente seguro e estarem à altura das ameaças, mesmo lidando com falta de pessoal e orçamento limitado.

Um relatório da Proofpoint mostrou que 69% desses profissionais enfrentam expectativas excessivas e 76% vivenciaram ou testemunharam um esgotamento mental no ano anterior.

Esses números representam um desafio humano e operacional cuja gravidade impacta diretamente a eficácia das defesas e a resiliência das empresas.

Tendências para 2026

1 Fator humano + IA potencializam a segurança

Para 2026, podemos esperar uma consolidação da combinação entre julgamento humano e capacidade de escala da IA.

As defesas devem evoluir para um modelo em que **a IA faz o trabalho pesado,** como correlação massiva de dados, triagem de sinais e geração de hipóteses, enquanto **o profissional assume o papel de estrategista e validador.**

Por outro lado, isso aumenta a necessidade de governança e supervisão, para evitar o uso não autorizado e riscos de segurança.

Delegue tarefas operacionais para os agentes de IA, mas mantenha decisões críticas sempre sob responsabilidade de pessoas qualificadas. Além disso, implemente políticas claras de uso e promova treinamentos frequentes.

2 A ascensão da Gestão de Identidades

Com a **explosão das identidades de máquina e o aumento exponencial de ameaças de engenharia social,** a gestão das identidades se torna um aspecto fundamental da estratégia de segurança.

Intrusões ocasionadas por replay de token de sessão, falsificação de identidades roubo de identidade de máquinas e uso indevido de contas de serviço devem se tornar mais e mais frequentes.[13]

A adoção de Zero Trust ou Zero Standing Privilege, além de outras medidas, deve estar no topo dos objetivos daqueles que ainda não os implementaram. Outras medidas de governança e proteção, como implementação de MFA, também devem estar entre as prioridades.

Para quem já se preocupa com identidade: testar, testar e testar. Vulnerabilidades podem estar muito bem escondidas ou surgirem conforme novas atualizações são feitas. Mantenha os controles funcionando e os testes em dia para garantir proteção contínua.

3 Resiliência no centro da estratégia

Com o aprimoramento dos ataques, não basta apenas se proteger contra possíveis ataques. Torna-se fundamental, também, **estar preparado para se identidade, conter e se recuperar após uma investida.**

Ou seja, a resiliência cibernética passa a estar no centro da estratégia de segurança, permitindo que a organização retome suas operações com prejuízo mínimo após incidentes.
E fica o alerta: resiliência ≠ compliance.

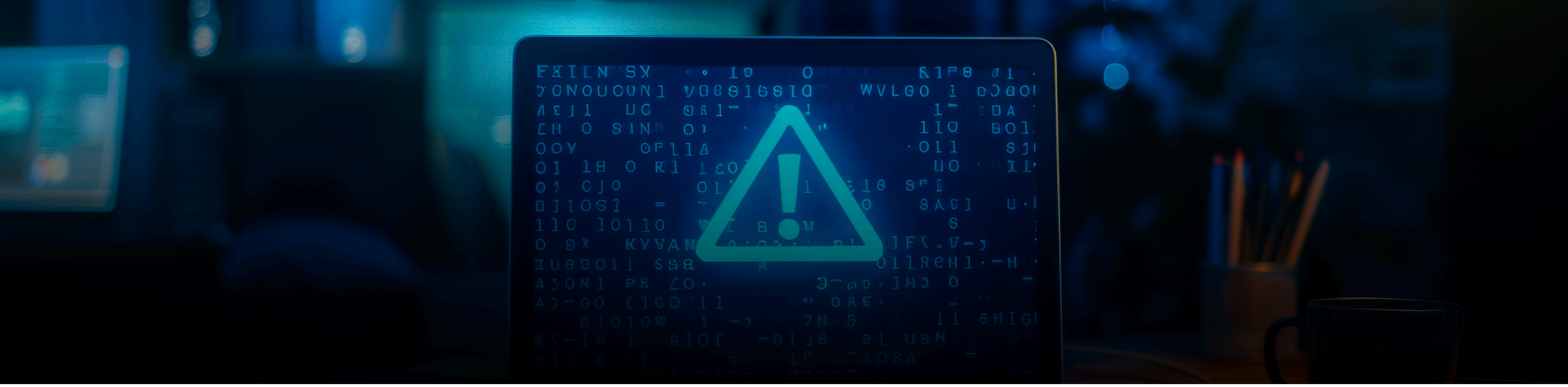
As certificações são necessárias e importantes. Mas elas, por si só, não garantem proteção eficiente ou capacidade de recuperação.

4 Riscos de Supply Chain se acentuam

Os ataques de supply chain já provaram seu potencial devastador. O problema é que, justamente por isso, eles devem apenas se identificar no próximo ano.

Plataformas SaaS, provedores de nuvem e outros fornecedores se tornam alvos extremamente valiosos.

A segurança dos seus fornecedores é a sua segurança. Isso significa que as organizações devem enrijecer suas estratégias de controle de fornecedores, tornando-se cada vez mais exigentes neste quesito.



5 Ransomware

A escalada do ransomware também é uma realidade.

Segundo o Google[14], **a combinação de ransomware, roubo de dados e extorsão deve permanecer como um dos crimes cibernéticos de maior impacto financeiro.**

Inserindo esse vetor de ataque na cadeia de fornecedores, o resultado é ainda mais devastador.
Com os agentes de IA, os atacantes conseguem escalar esses ataques com o mínimo de supervisão humana.[13]

Invista na implementação de autenticação robusta, proteção contra técnicas de engenharia social, uso de firewalls e proteção de endpoint.

Próximos passos

Este e-book trouxe dados e insights para orientar as suas decisões de segurança em 2026. Com a aceleração de vetores como o uso da IA em ataques, riscos associados à supply chain e engenharia social cada vez mais sofisticada, agir com base em evidências deixou de ser um diferencial e se tornou uma obrigação.

Agora, recomendamos que você:

- Revise sua postura de segurança atual e mapeie os gaps críticos existentes.
- Formalize ou atualize sua política de segurança ofensiva, incluindo os testes contínuos.
- Priorize os investimentos com base em riscos reais, avaliando as ameaças com base em impacto no negócio e na facilidade de exploração.

Com a Vantico, você tem um parceiro que te acompanha em todas as etapas dos testes de segurança.

Conte conosco em 2026!

Somos especialistas em Segurança Ofensiva

A Vantico oferece identificação eficiente de riscos, postura proativa e escopo personalizado em cada um de seus serviços:

Complexidade

Pen Test	Code Assisted Pen Test	Assumed Breach Testing	Red Team
Cloud Security Review	Code Review	Social Engineering	Adversary Emulation
Attack Surface Management	Spear Phishing	AD Security Review	
Para iniciar a jornada em testes de segurança e evoluir a maturidade	Aplicar boas práticas de código, utilizar referências reconhecidas e ampliar os cenários de ameaça	Estruturar defesas mais robustas, ampliar a frequência dos testes e capacitar pessoas, testando também o fator humano	Operar em nível avançado com Red Team e Emulação Realista de Adversários

Maturidade

Descubra como a Vantico transforma esses insights em ação:

↗ vantico.com.br

Vantico

Referências

- [1]OWASP Top 10 2025.
- [2]Cost of a Data Breach Report 2025 | IBM
- [3]2025 Ponemon Healthcare Cybersecurity Report | Proofpoint
- [4]Cyber Attacks on Healthcare to Affect Almost Half of Health Systems, Threaten Patient Treatment, and Drive Up Breach Costs. Unless? | Science Soft
- [5]SecurityScorecard Threat Intel Report: 97% of Leading U.S. Banks Impacted by Third-Party Data Breaches in 2024 | SecurityScorecard
- [6]The State of Cybersecurity in the Finance Sector | Darktrace
- [7]Top Industries Hackers Hit in 2025 | DeepStrike
- [8]2025 Data Breach Investigations Report | Verizon
- [9]Global Cybersecurity Outlook 2025 | World Economic Forum
- [10]Software Supply Chain Attacks Surge to Record High in October 2025 | Cyble
- [11]Cybersecurity Statistics 2025: Breach Costs, Ransomware & AI Threats | DeepStrike
- [12]Roubo bilionário em supply chain financeiro do Brasil | CISO Advisor
- [13]10 Cybersecurity Predictions That Will Define 2026 | Forbes