



Apoio:  **ABRASECI** ASSOCIAÇÃO BRASILEIRA DE SEGURANÇA CIBERNÉTICA  **HACKERS DO BEM**

Relatório de Cibersegurança

2026



A Brasscom autoriza a exploração e uso do conteúdo contido nesta apresentação desde que os devidos créditos sejam concedidos.



1

Resumo executivo

2

3

4





Investimento, ameaças, talentos, IA e regulação: a maturidade cibernética do Brasil em uma visão integrada

O BRASIL NA JORNADA DE MATURIDADE CIBERNÉTICA

+49%

Crescimento do mercado de cibersegurança até 2029, alcançando **R\$ 126,9 bilhões**.

141 organizações

Brasileiras atingidas por **ransomware³** em 2025.

6,4%

Do orçamento vai para cibersegurança — **36% abaixo da referência global**.

50 mil

Certificados emitidos pelo **programa Hackers do Bem** e 1,8 mil novos concluintes em Segurança da Informação.

+41%

Avanço do NCSI¹ em dois anos: de **50,65 para 71,67 pontos**.

18,6% ao ano

Crescimento do emprego em cibersegurança (**2019-2025**).

Mercado, capacidade institucional e talentos avançam juntos; investir em segurança é o que separa quem absorve o risco de quem o transforma em vantagem competitiva.

EMPRESAS: DA GOVERNANÇA AO RETORNO DO INVESTIMENTO



Mundo



Brasil

Custo médio de uma violação de dados

US\$ 4,4 Mi

US\$ 1,3 Mi

Impacto adicional na violação por IA oculta

**+ \$ 200 mil
+5%**

**+ \$ 109 mil
+8%**

Redução do custo de violação comparando **organizações sem uso e com uso amplo de IA²**

**- US\$ 3,6 Mi
-34%**

**- US\$ 1,2 Mi
-26%**

% das organizações relatam **não possuir políticas de governança de IA**

63%

87%

Investir em **talentos** reduz até **US\$ 1,6 milhão** no custo das violações

A IA agrava as ameaças, mas também é a solução: combinada a governança e talentos, ela transforma risco em retorno mensurável.

Notas: ¹ National Cyber Security Index (NCSI); ² Refere-se ao uso de IA e automação em atividades de prevenção, detecção, investigação e resposta a incidentes de segurança;

³ Ransomware é um tipo de ataque cibernético que bloqueia o acesso a sistemas ou dados e exige pagamento de resgate para sua liberação.

Fonte: Brasscom; IDC Black Book; National Cyber Security Index (NCSI); ISH; Gartner; IBM, Cost of a Data Breach 2025, resultados do Brasil · IBM e Ponemon Institute, Cost of a Data Breach Report 2025.

1

2

3

4

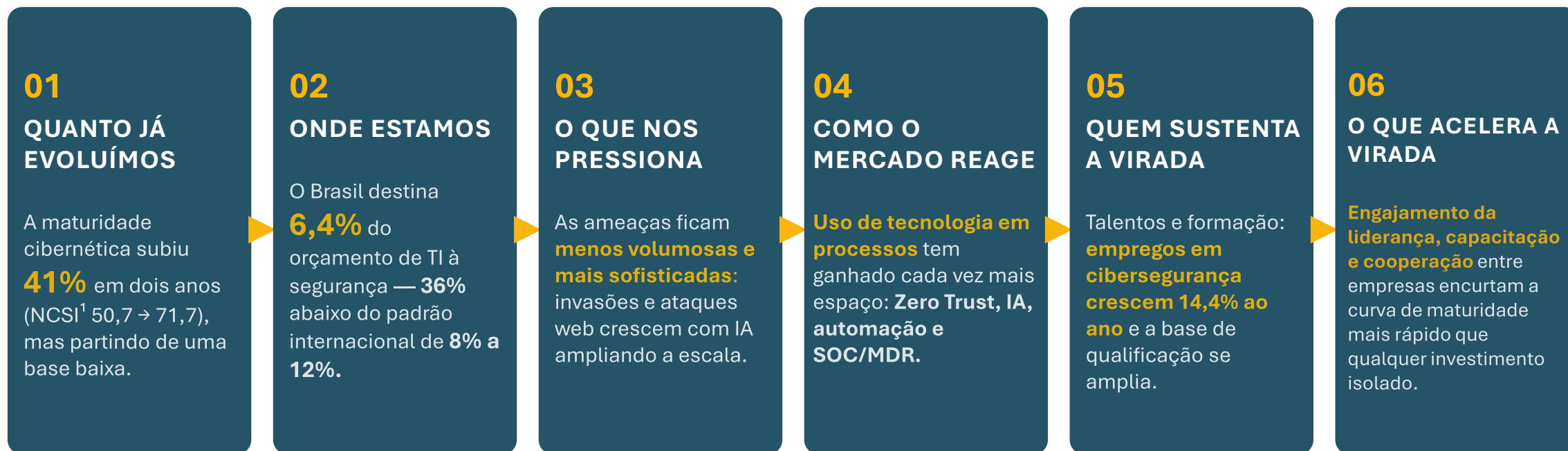
Onde o Brasil está
no cenário de
cibersegurança?





Fio condutor: a trajetória da cibersegurança no Brasil

Da lacuna de investimento que ainda nos separa do padrão global à mobilização que já está em curso.



Para onde isso leva: **a lacuna de investimento é real, mas o Brasil já entrou em rota de amadurecimento.**
Acelerar essa transição significa tratar a cibersegurança não como custo, mas como investimento essencial para a continuidade dos negócios e a confiança digital.

Notas: ¹ National Cyber Security Index (NCSI): : índice que mede a capacidade nacional de prevenir, detectar e responder a incidentes cibernéticos;

Zero Trust: modelo de segurança baseado em validação contínua de acessos. SOC/MDR: estruturas e serviços especializados em monitoramento, detecção e resposta a ameaças cibernéticas.

Fonte: Brasscom; IDC Black Book; ISG; CERT.br; National Cyber Security Index (NCSI); ISH; Gartner.



O investimento no Brasil subiu 66% e a maturidade 41%, mas diferentes índices mostram que ainda há oportunidades para transformar estrutura em capacidade

Diferentes lentes sobre a cibersegurança nacional: NCSI e GCI se complementam, mas não são diretamente comparáveis.

Investimento +66%:

De 2023 a 2025, o investimento saltou de R\$ 13,4 bi para R\$ 22,2 bi.

NCSI — National Cyber Security Index

Avalia capacidades nacionais de cibersegurança, considerando aspectos como políticas, proteção de serviços, resposta a incidentes, gestão de crises e combate ao cibercrime.

Apesar da posição no **National Cyber Security Index** ter se mantido praticamente estável, o **Brasil aumentou seu índice em 41%**, saindo de 50,65 para 71,67 entre 2023 e 2025.

2023			2025		
Posição	País	NCSI Index	Posição	País	NCSI Index
1º	 Bélgica	94,81	1º	 República Tcheca	98,33
2º	 Lituânia	93,51	2º	 Canadá	96,67
3º	 Estônia	93,51	3º	 Estônia	96,67
4º	 República Tcheca	90,91	4º	 Finlândia	95,83
5º	 Alemanha	90,91	5º	 Lituânia	95,01
6º	 Romênia	89,61	6º	 Moldávia	94,17
7º	 Grécia	89,61	7º	 Bélgica	94,17
8º	 Portugal	89,61	8º	 Jordânia	93,33
9º	 Reino Unido	89,61	9º	 Hungria	93,33
10º	 Espanha	88,31	10º	 Romênia	92,50
...			...		
54º	 Brasil	50,65	55º	 Brasil	71,67

GCI — Global Cybersecurity Index

Avalia o compromisso e a estrutura nacional de cibersegurança em cinco dimensões: medidas legais, técnicas, organizacionais, desenvolvimento de capacidades e cooperação.

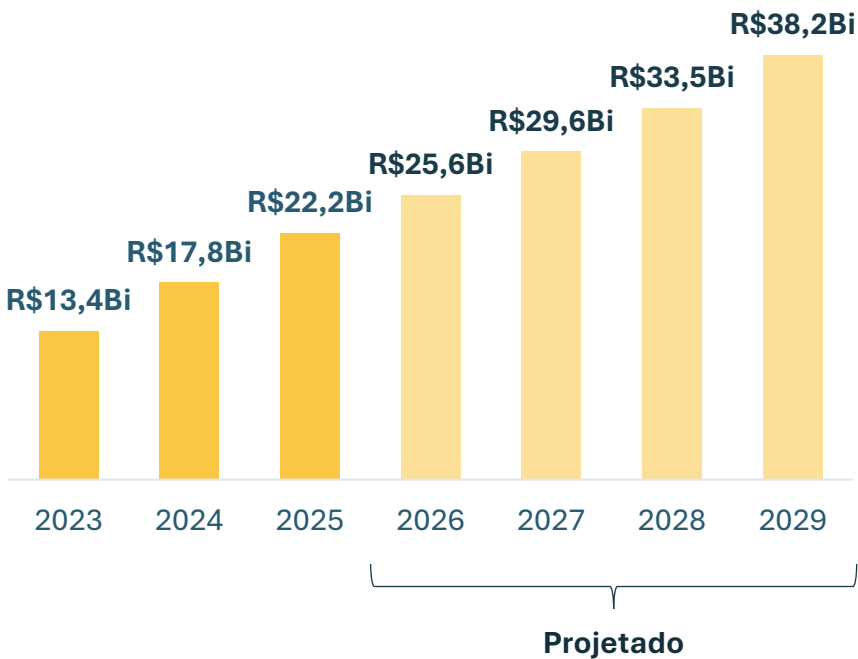
O GCI mostra elevada estruturação institucional

Em 2024, o Brasil foi classificado no **Tier 1 – Role-modelling** (referência global), **com 96,4 pontos**, indicando forte estruturação nacional nos cinco pilares avaliados.

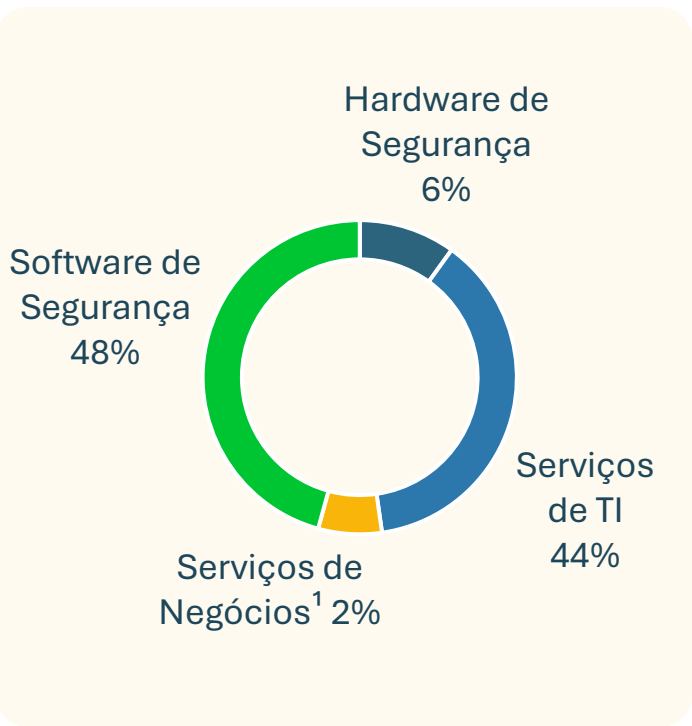


Crescimento de 49% nos investimentos em cibersegurança no Brasil, entre 2026 e 2029

Mesmo assim o investimento ainda é 36% abaixo do padrão médio internacional de 8% a 12%



Projeção de Gastos de **R\$126,9 Bi** entre **2026 e 2029** em **Cibersegurança** no Brasil, com o gasto anual saindo de R\$ 25,6 bi para R\$ 38,2, alta de **49%**



Brasil investe 6,4% do seu orçamento de TI em cibersegurança, **36% menos** que o **padrão médio adotado internacionalmente**.

O Gartner projeta que os gastos globais com cibersegurança alcançarão US\$ 240 bilhões em 2026, um aumento de 12,5% em relação a 2025. Estudos internacionais observam investimentos em cibersegurança equivalentes a **aproximadamente 8% a 12% do orçamento de TI**, podendo atingir **percentuais mais elevados** em setores de maior exposição ao risco, como saúde e serviços financeiros.

Fonte: [Cybersecurity Budget 2026: Benchmarks & Spending Trends](#)

Cibersegurança não é uma fatia fixa do orçamento: a vulnerabilidade e a perda potencial são os fatores que elevam esse investimento.

Fonte: [Gordon e Loeb, The economics of information security investment, ACM TISSEC 5\(4\), 2002](#)

Notas: ¹Serviços de Negócios correspondem às atividades de consultoria empresarial (Business Consulting) e terceirização de processos de negócio (BPO), conforme a taxonomia da IDC.

Fonte: Brasscom; IDC Black Book Live Edition, 2025V4.



A profissionalização do cibercrime transforma o Brasil em alvo e laboratório de operações digitais



O cibercrime no Brasil é industrializado, cada vez mais escalável e além de assertivo, lucrativo



Automação em larga escala

Ataques automatizados tornam as operações mais rápidas e sofisticadas.



Exploração em horas ou dias

O tempo entre descoberta e exploração de vulnerabilidades diminui drasticamente.



Reuso de credenciais e acessos

Credenciais, acessos e vulnerabilidades são comercializados e reutilizados em larga escala.



Ataques contínuos e persistentes

Ataques passam a operar continuamente, com foco em impacto e retorno financeiro.



O crime digital tornou-se uma indústria.



O Brasil ocupa posição relevante no ecossistema global de crime digital e concentra infraestrutura comprometida em larga escala



Principais Dados de 2025

141

Organizações brasileiras afetadas por ransomware

Maior número na América Latina¹



Alta presença de botnets

Brasil entre os países com maior concentração de infraestrutura comprometida na LATAM².



Infraestrutura comprometida ativa

LATAM registrou 2,09 bilhões de detecções de botnet em 2025, crescimento de 12% em relação ao ano anterior.



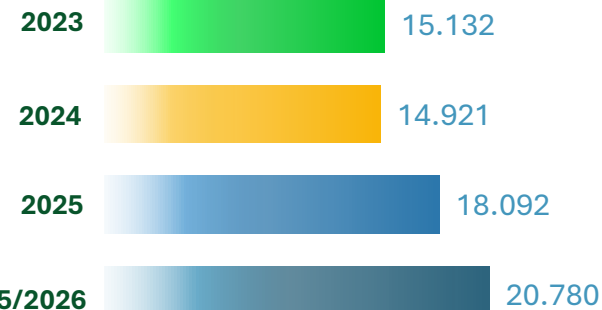
O Brasil ocupa uma posição relevante dentro desse ecossistema.



Os registros nacionais mostram aceleração consistente da atividade maliciosa a partir de 2025 pela Vultus¹

Total de Notificações

Incidentes + Vulnerabilidade



Crescimento mai/2025 – mai/ 2026

▲ 175%



Os indicadores nacionais mostram essa atividade crescendo.



A ameaça deixa de ser apenas volume a passa a ser eficiência: **menos tentativas dispersas e mais ataques direcionados, rápidos e economicamente estruturados.**

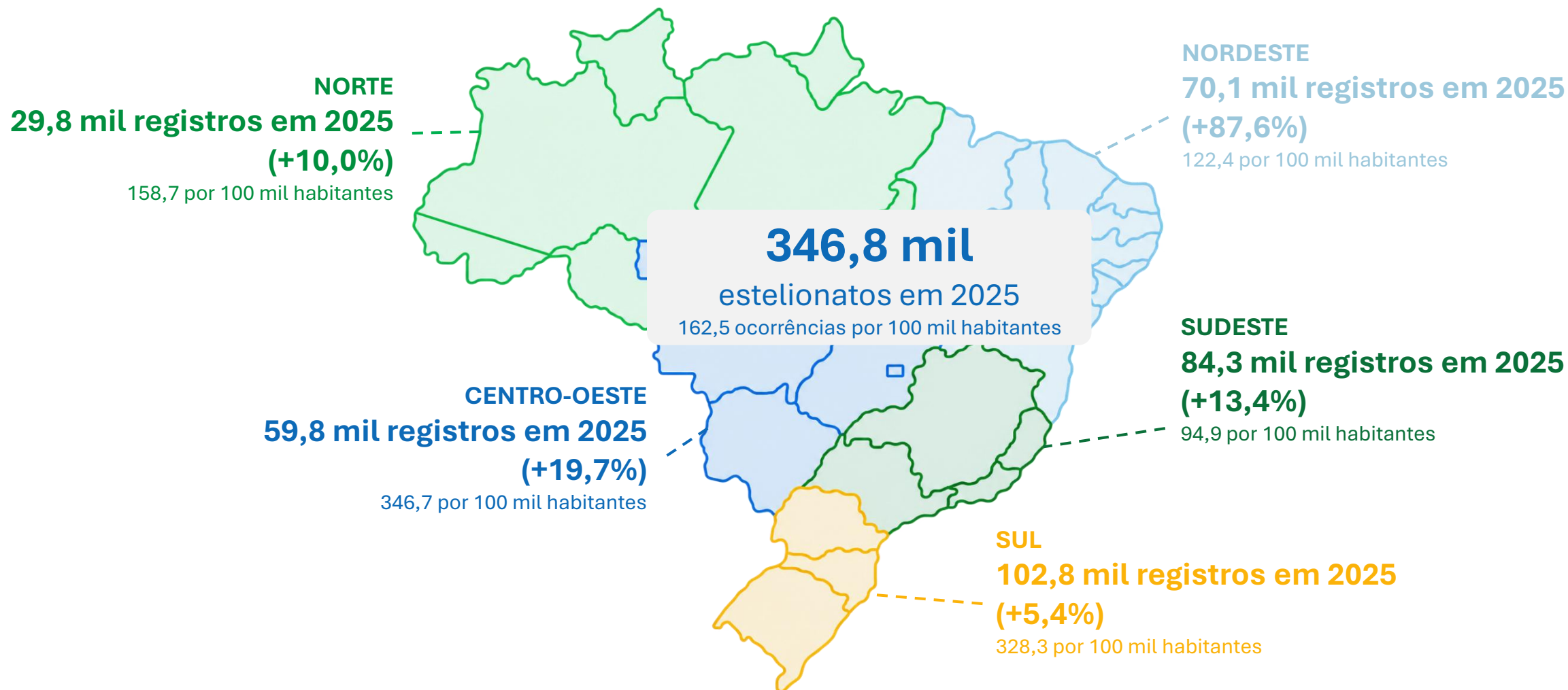
Notas: ¹ Vultus é uma consultoria especializada em gestão de riscos cibernéticos; Botnets: redes de dispositivos comprometidos e controlados remotamente para execução de ataques cibernéticos.

Fonte: Brasscom; VULTUS Cybersecurity Ecosystem; CrowdStrike Threat Intelligence Report.



Golpes digitais são um problema alastrado por todo o país

O Brasil registrou 346,8 mil ocorrências em 2025, alta de 21,1% frente a 2024 (+60,5 mil casos), impulsionada pelo avanço de 87,6% no Nordeste; o Sul lidera em volume e o Centro-Oeste em incidência por habitante.



Nota: Registros de estelionato eletrônico refere-se a golpes praticados em ambiente digital, como fraudes realizadas pela internet, aplicativos de mensagens, redes sociais ou outros meios eletrônicos; UFs com informação indisponível não foram consideradas no cálculo regional.

Fonte: Brasscom; Dados do Anuário Brasileiro de Segurança Pública 2026.



Aplicações web e invasões ampliam a exposição ao risco digital

Invasões passaram de **527 para 3.729 registros** entre 2019 e 2025, enquanto os incidentes em aplicações web saltaram de **7.937 para 19.965 em apenas um ano (2024 a 2025)**, evidenciando a ampliação da superfície de ataque e o uso crescente de automação por agentes maliciosos.

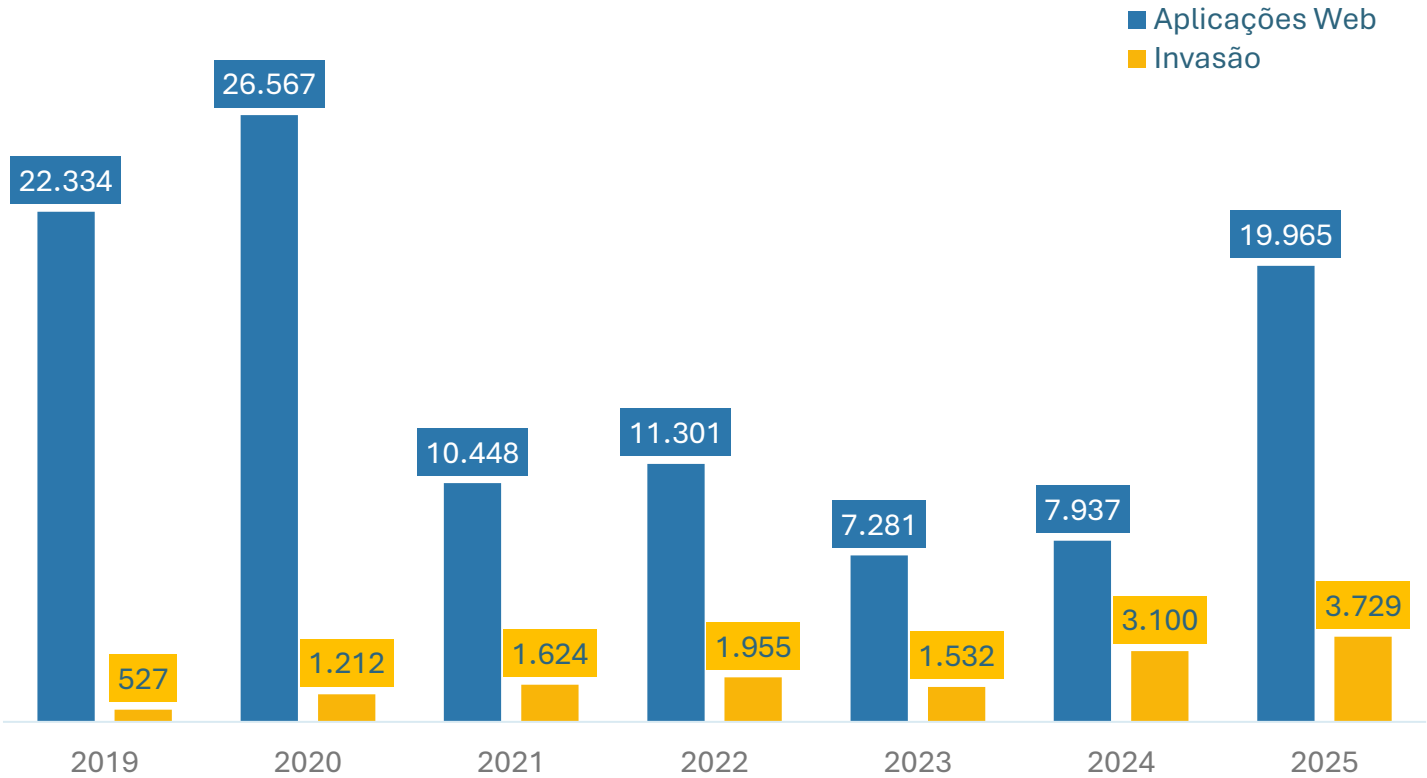
Incidentes cibernéticos por tipo no Brasil
(2019 – 2025)

Aplicações web

Os registros de ataques a aplicações web e invasões cresceram nos últimos anos, indicando maior exploração de vulnerabilidades em sistemas, aplicações e serviços expostos à internet.

IA Generativa

A IA amplia a escala e a eficiência dos ataques, automatizando a identificação de vulnerabilidades e tornando campanhas maliciosas mais sofisticadas.



Notas: Invasão: acesso não autorizado a sistemas, redes ou dispositivos. Aplicações Web: exploração de vulnerabilidades em sites, aplicações e serviços expostos à internet. Os dados refletem incidentes reportados voluntariamente ao CERT.br e podem estar sujeitos à subnotificação. Os resultados indicam tendências observadas nos registros recebidos pela entidade, não representando necessariamente a totalidade dos incidentes cibernéticos ocorridos no Brasil.

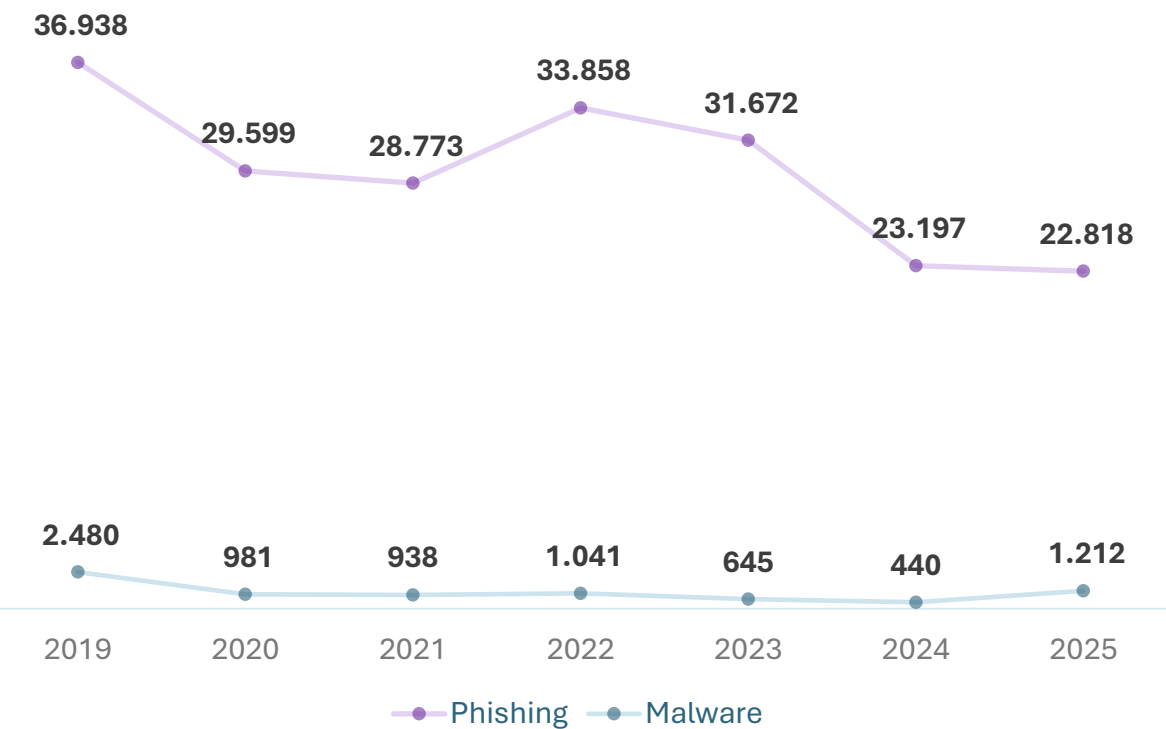
Fonte: Brasscom; CERT.br (entidade responsável pelo recebimento e tratamento de notificações de incidentes cibernéticos no Brasil) - Incidentes Notificados.



O fator humano continua sendo um dos principais alvos dos cibercriminosos

Mesmo considerando apenas os incidentes reportados ao CERT.br, as notificações de phishing permanecem muito superiores às de softwares maliciosos, evidenciando a persistência dos ataques baseados em engenharia social.

Notificações anuais de phishing e malware ao CERT.br
(2019 – 2025)



2025
22.818
Notificações de phishing

19x mais
Que as notificações relacionadas a malware



O fator humano continua no centro do risco

As notificações de phishing permanecem em patamares significativamente superiores aos demais vetores analisados, refletindo a eficácia de golpes que exploram confiança, urgência e engenharia social.

IA amplia a escala dos golpes

Ferramentas de IA tornam golpes baseados em engenharia social mais convincentes e escaláveis, ampliando o alcance dos ataques e reduzindo barreiras para sua execução.

Notas: Phishing é um golpe digital em que criminosos se passam por empresas legítimas para roubar seus dados; Malware é um termo genérico para softwares maliciosos criados para invadir e danificar seus dispositivos. Os dados refletem incidentes reportados voluntariamente ao CERT.br e podem estar sujeitos à subnotificação. Os resultados indicam tendências observadas nos registros recebidos pela entidade, não representando necessariamente a totalidade dos incidentes cibernéticos ocorridos no Brasil.

Fonte: Brasscom; CERT.br (entidade responsável pelo recebimento e tratamento de notificações de incidentes cibernéticos no Brasil) - Incidentes Notificados.



Mesmo após se reestabelecerem, as empresas sofrem efeitos das violações

A maior parte das organizações que concluíram sua recuperação reportou períodos superiores a 100 dias, deslocando a prioridade da prevenção para a neutralização do impacto econômico.

A recuperação completa ainda leva meses para a maioria das organizações

76% das empresas levam mais de 100 dias para se reestabelecer; e dessas, **65%** seguem sofrendo impactos após a recuperação, prejuízos operacionais prolongados que podem levar as organizações a avaliar, entre suas alternativas de gestão de riscos, mecanismos de transferência de risco como o Seguro Ciber.

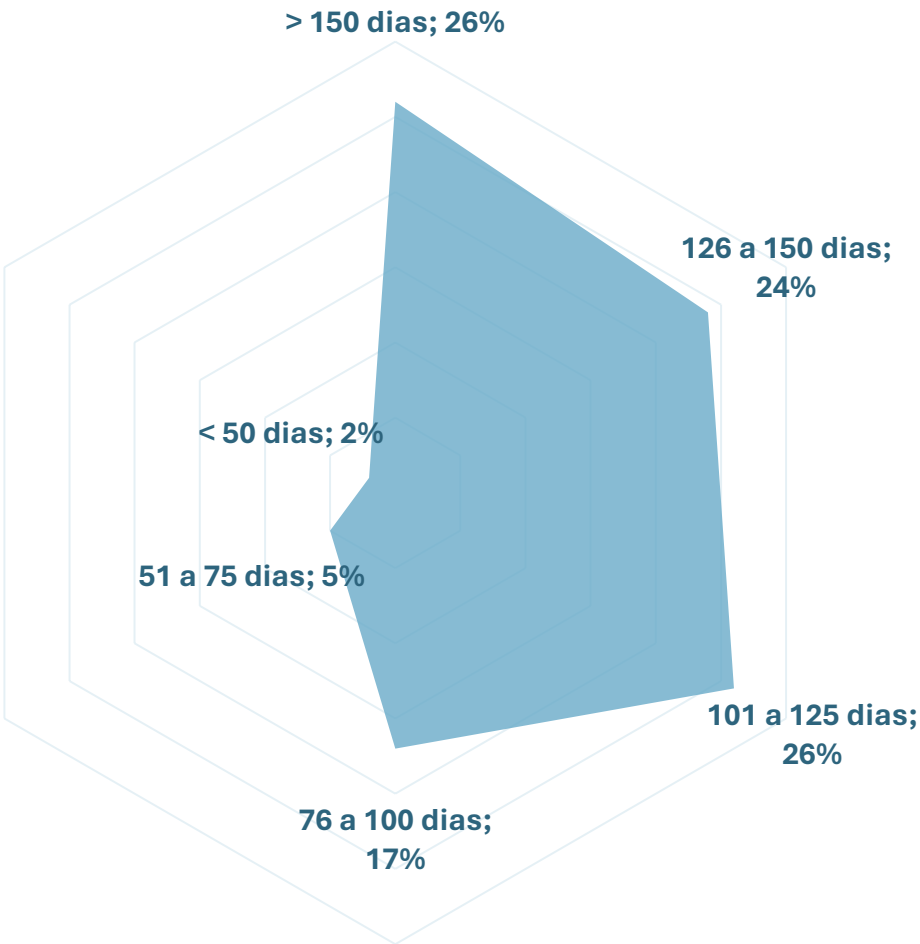
Aceleração do mercado de Seguro Ciber

A CNseg divulgou que, no 1º semestre de 2024, o Seguro Cibernético arrecadou R\$ 110,6 milhões, o melhor resultado para um primeiro semestre nos cinco anos anteriores. O valor foi 12,7% maior que no mesmo período de 2023.

Alta sinistralidade e indenizações

O volume de indenizações pagas por incidentes digitais aumentou 258% no primeiro bimestre de 2024 em comparação ao mesmo período do ano anterior, refletindo o avanço dos impactos operacionais e financeiros sobre as organizações brasileiras.

A expansão das violações trazem uma necessidade para o setor de tecnologia em desenvolver soluções de prevenção, detecção e resposta aos incidentes. O seguro cibernético complementa essas medidas ao contribuir para a transferência dos impactos financeiros e a continuidade dos negócios.





Da reação à resiliência: como diferentes setores enfrentam o risco cibernético

O gap de maturidade atual do mercado abre uma janela única de oportunidade para liderar a transformação em cibersegurança com espaço para valorização, conformidade e captura de mercado.

Índice de Maturidade em Cibersegurança (Metodologia VULTUS, baseada nos princípios do NIST CSF).

0 – 1: Inicial/Improvisada;
2: Processos básicos implementados;
3: Processos definidos e gerenciados;
4: Processos medidos e monitorados;
5: Otimização contínua e resiliência avançada.



Ações Práticas de Mitigação por Setor

EDUCAÇÃO: 0,99



Microsegmentação de rede:

Isolamento de redes de alunos, gestão e pesquisa.

Criptografia de dados:

Armazenamento seguro e restrito de pesquisas e patentes sensíveis.

Revogação automática de

acessos: Desativação de credenciais ao fim de semestres/projetos.

GOVERNO: 1,05



Eliminação de credenciais

estáticas: Substituição de senhas por chaves de curta duração.

Adoção de Zero Trust (ZTNA):

Validação contínua de identidade e dispositivos.

Auditoria diária de identidade:

Varredura diária contra alterações suspeitas de acessos.

TECNOLOGIA: 1,71



Proteção contra ransomware:

Backups isolados e planos de recuperação para minimizar impactos de ataques.

Gestão contínua de

vulnerabilidades: Correção acelerada de falhas exploradas por agentes maliciosos.

Segurança em nuvem e

aplicações: Monitoramento permanente de ambientes críticos e acessos privilegiados.

TELECOM: 2,23



Monitoramento avançado de

rede: Detecção contínua de atividades suspeitas em infraestruturas críticas.

Segmentação de ambientes:

Isolamento de sistemas estratégicos para reduzir movimentação lateral.

Proteção contra espionagem

cibernética: Fortalecimento dos controles de acesso e da gestão de identidades.

Nota: As notas apresentadas seguem metodologia VULTUS baseada no NIST CSF (framework de cibersegurança); não correspondem a uma pontuação oficial do framework NIST CSF 2.0.

Fonte: Brasscom; VULTUS Cybersecurity Ecosystem; CrowdStrike Threat Intelligence Report 2026.



As organizações deixam de reagir a incidentes para antecipar ameaças

Apesar do aumento da sofisticação dos ataques, o mercado brasileiro está avançando para uma postura mais proativa, integrando governança, automação, inteligência artificial e monitoramento contínuo para fortalecer a resiliência cibernética.



Governança e segurança mais estratégicas

Cibersegurança deixa de ser um custo operacional e passa a ser tratada como **pilar de confiança, resiliência e continuidade dos negócios**.

Ampliação de iniciativas de **governança, gestão de riscos, Zero Trust e governança de IA**.

Esses modelos se baseiam em "não confiar automaticamente em ninguém ou em nenhum dispositivo", mesmo dentro da rede corporativa. Todo acesso deve ser continuamente verificado e autorizado.



Uso crescente de IA e automação na defesa

Empresas estão incorporando **IA, automação e análise preditiva** para antecipar ameaças e acelerar respostas.

Adoção de ferramentas de **SOAR (Security Orchestration, Automation and Response), triagem automatizada e resposta em velocidade de máquina**.

Essas soluções reduzem as atividades manuais e aceleram a reação a ataques.



Monitoramento contínuo e resposta 24/7

Crescimento da contratação de serviços de **SOC (Centros de Operações de Segurança) e MDR (Managed Detection and Response) de nova geração**, com monitoramento contínuo, inteligência de ameaças e resposta automatizada a incidentes.

Evolução de modelos reativos para modelos de **detecção proativa e caça a ameaças**.



Gestão contínua de vulnerabilidades

Substituição das avaliações pontuais por modelos de **Continuous Threat Exposure Management (CTEM)** e gestão contínua de exposição, substitui auditorias pontuais por um processo permanente de identificação, priorização e correção de vulnerabilidades com base no impacto para o negócio.

Priorização de vulnerabilidades com base no impacto para o negócio e probabilidade real de exploração.



Fortalecimento do ecossistema de fornecedores

Fornecedores ampliam investimentos em centros de excelência, automação, inteligência de ameaças e soluções personalizadas para o contexto brasileiro.

Mercado caminha para **operações mais preditivas e integradas**.

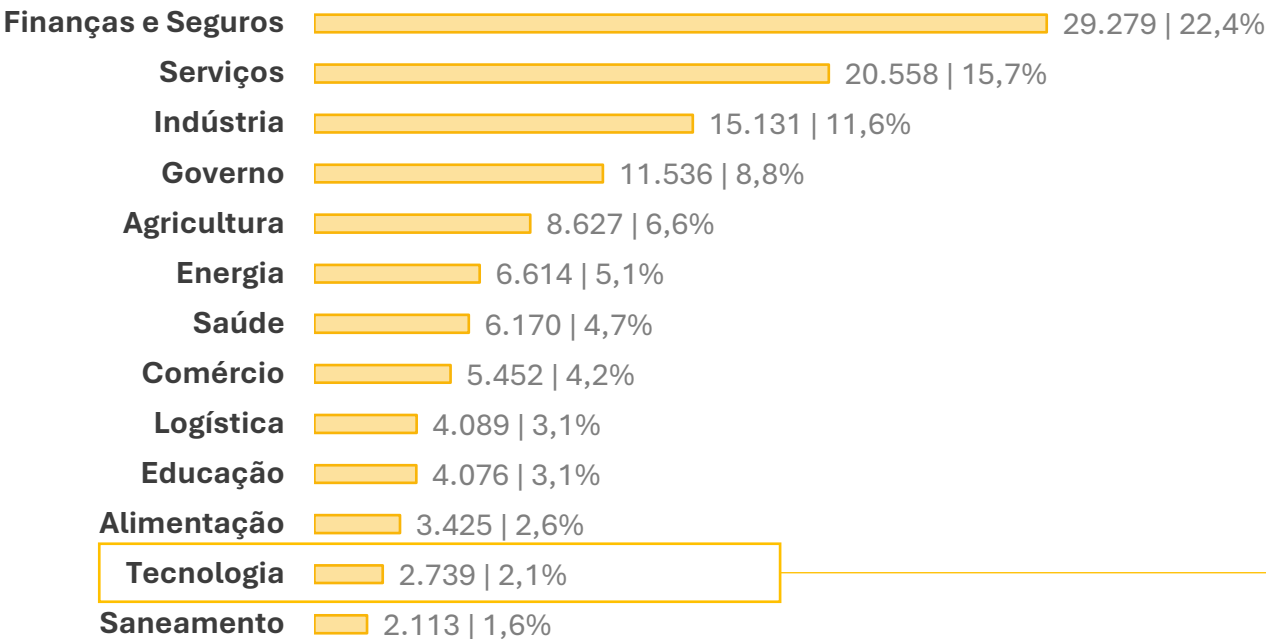


Tecnologia sustenta a resiliência da economia digital

O setor de Tecnologia atua desenvolvendo soluções, serviços e capacidades que protegem sistemas, dados e infraestruturas utilizados por todos os demais segmentos econômicos.

Volume de violações por setor no 2º trimestre de 2025

Percentual sobre o universo monitorado pela ISH (empresa de cibersegurança)



**MAIS DO QUE UM SETOR
ECONÔMICO, A TECNOLOGIA É A
INFRAESTRUTURA DE DEFESA DA
ECONOMIA DIGITAL:**

enquanto os ataques se sofisticam, o
setor amplia investimentos, talentos e
capacidades para fortalecer a
resiliência de todo o ecossistema.

**Representa apenas 2,1%
das violações observadas.**

Nota: Percentuais calculados sobre o total de violações mapeadas pela ISH; os setores exibidos não necessariamente representam a totalidade das categorias monitoradas.

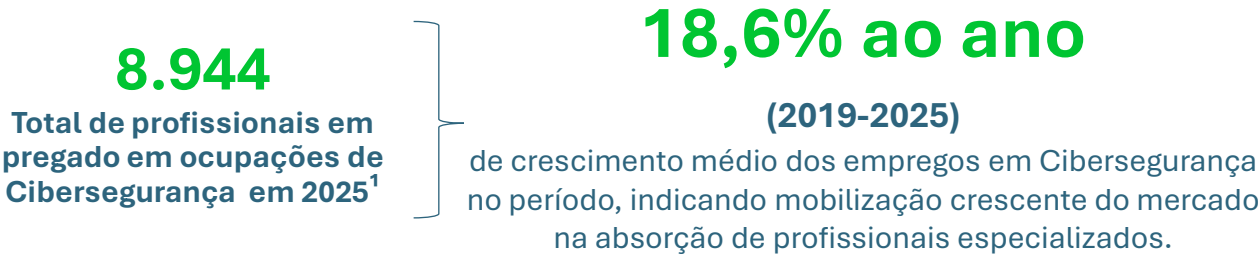
Fonte: Brasscom; Relatório Semestral ISH de Cibersegurança.



Esforço consistente de desenvolvimento de capacidades e talentos

O avanço da cibersegurança impulsiona a formação e a absorção de profissionais em diversos segmentos da economia.

EMPREGABILIDADE



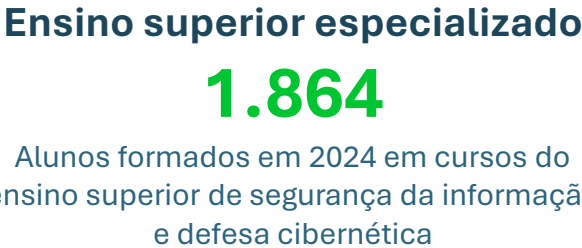
Participação dos profissionais de
Cibersegurança sobre os profissionais
que atuam em tecnologia em 2025

TIC e TELECOM
0,8%

TI IN HOUSE
1,1%

Tecnologia ultrapassa fronteiras, e amplia o papel da cibersegurança, sua presença nas áreas de tecnologia de diferentes setores reforça que a proteção digital já é uma competência essencial da transformação tecnológica.

FORMAÇÃO



Nota: ¹A análise considera duas ocupações específicas da Classificação Brasileira de Ocupações (CBO): Gerente de Segurança de TI e Administrador em Segurança da Informação. No entanto, profissionais da área podem estar classificados em outras CBOs, como Analista de Sistemas ou Engenheiro da Computação, o que pode levar à subrepresentação do total de empregos em segurança da informação.

Fonte: Brasscom; RAIS; CAGED: Dados de 07/2026; RNP (Hackers do Bem)

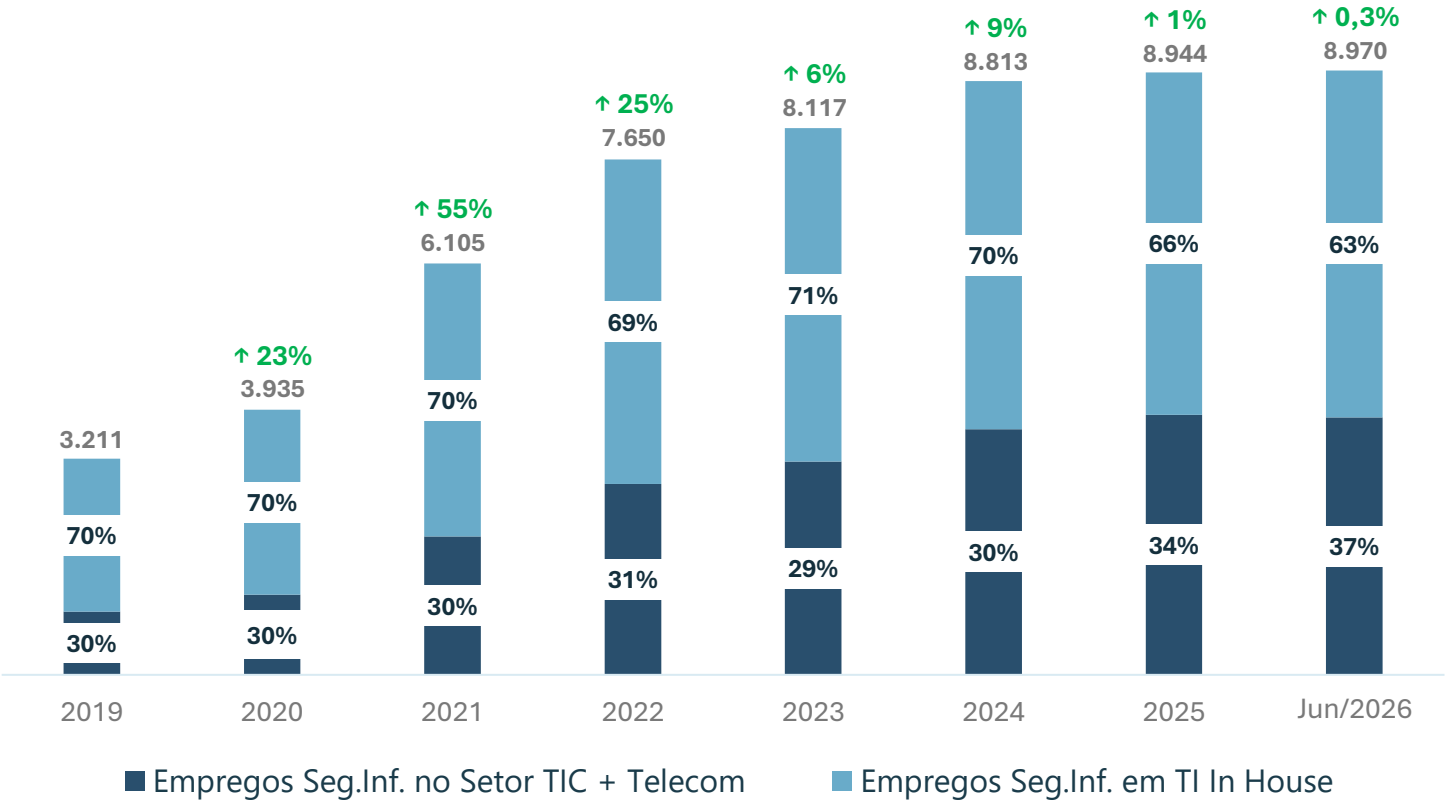


A demanda por cibersegurança se espalha por todos os setores

O desenvolvimento de competências de Segurança da Informação por empresas de diversos setores reforçam a demanda por capacidades especializadas de proteção digital.

Empregados em Segurança da Informação

% Crescimento de Empregos | Total de Empregos | % de Participação



Com 79% das empresas percebendo maior exposição a ataques e 66,5% tratando Ciber como risco corporativo (CNN Brasil), a resposta aparece no emprego:

Crescimento médio do emprego em cibersegurança (2019-2025)

- 26,6% a.a. em TIC e Telecom
- 14,4% a.a. em TI In House

As empresas estruturam times próprios de proteção e, ao mesmo tempo, ampliam a contratação de serviços especializados, sustentando um mercado em expansão para tecnologias e serviços de proteção digital.

Nota: A análise considera duas ocupações específicas da Classificação Brasileira de Ocupações (CBO): Gerente de Segurança de TI e Administrador em Segurança da Informação. No entanto, profissionais da área podem estar classificados em outras CBOs, como Analista de Sistemas ou Engenheiro da Computação, o que pode levar à subrepresentação do total de empregos em segurança da informação.

Fonte: Brasscom; RAIS; CAGED: Dados de 07/2026.

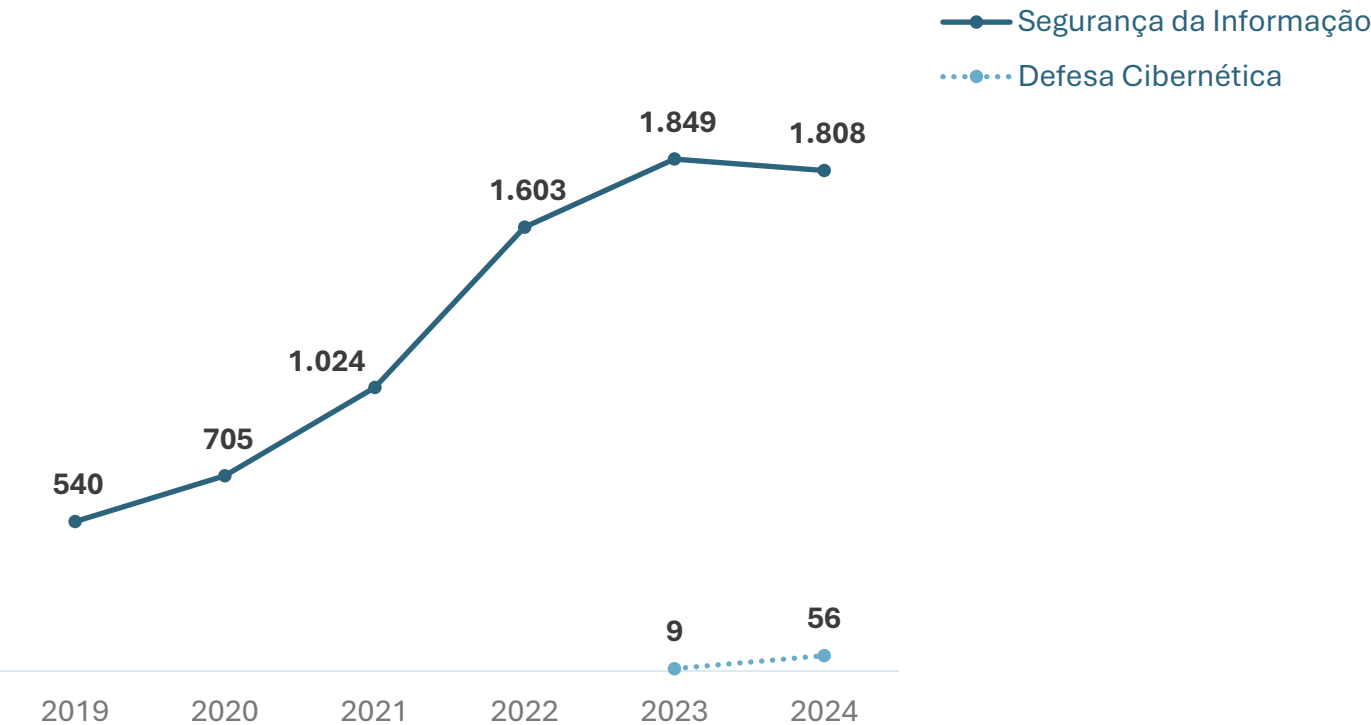


Formação em cibersegurança amplia a capacidade nacional de proteção

O número de concluintes em cursos de Segurança da Informação mais que triplicou entre 2019 e 2024, fortalecendo a formação de profissionais para atender à crescente demanda por competências em proteção digital.

Formação superior em cibersegurança no Brasil

Total de concluintes



Embora o número de graduados em Segurança da Informação tenha registrado uma **redução de 2,2% em 2024**, a formação de profissionais em cibersegurança vai além dos cursos superiores específicos. A natureza multidisciplinar da área permite a absorção de talentos oriundos de diferentes formações em tecnologia, enquanto certificações, programas de capacitação e iniciativas de requalificação ampliam os caminhos de ingresso e especialização profissional.

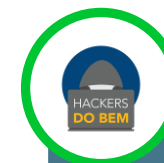
Nota: A formação em “Defesa Cibernética” é recente e passa a aparecer a partir de 2023. Em períodos anteriores, cursos similares estavam classificados em Segurança da Informação ou áreas correlatas.

Fonte: Brasscom; INEP (Censo da Educação Superior 2024).



Iniciativas demonstram o potencial de ampliar a formação de talentos

O **Hackers do Bem** forma talentos em cibersegurança com ampla escala, qualidade e competências alinhadas às demandas pelo mercado, além de despertar o interesse para a área.



ETAPAS DO PROGRAMA HACKERS DO BEM

O programa Hackers do Bem estrutura uma jornada de qualificação que combina formação progressiva, especialização técnica e experiência prática. A trilha contempla desde o desenvolvimento de competências fundamentais até etapas avançadas de aprofundamento e aplicação em ambientes reais, contribuindo para ampliar a formação de profissionais em cibersegurança. Ao integrar capacitação, especialização e aproximação com o mercado, a iniciativa fortalece o desenvolvimento de talentos e a ampliação das capacidades nacionais em proteção digital.



Governo também demonstra preocupação com elaboração de estratégias

O avanço da Inteligência Artificial ampliará a demanda por cibersegurança no Brasil. O próprio Plano Brasileiro de Inteligência Artificial (PBIA) posiciona a segurança, a privacidade e a proteção das infraestruturas digitais como condições para o desenvolvimento de uma IA confiável e segura.

Cibersegurança é um eixo estruturante da estratégia nacional de IA

O PBIA prevê investimentos para fortalecer a infraestrutura digital, desenvolver modelos nacionais de IA e ampliar a capacidade tecnológica brasileira, associado à proteção de dados, à governança e à segurança digital.

Oportunidades para o mercado de cibersegurança

A expansão da IA em governo, saúde, finanças, indústria e serviços digitais tende a elevar a demanda por especialistas em segurança de IA, proteção de dados, gestão de riscos, segurança em nuvem, resposta a incidentes e monitoramento de infraestruturas críticas.

IA amplia a superfície de ataque e cria novos desafios de segurança

A proteção dos dados de treinamento, dos modelos de IA e da infraestrutura computacional passa a ser requisito estratégico para garantir confiabilidade, integridade e resiliência dos sistemas.

No Brasil, a cibersegurança deixa de ser apenas uma função de proteção e passa a ser uma **capacidade estratégica para viabilizar a inteligência artificial** e garantir a confiança no ambiente digital.



O Brasil tem potencial para transformar desafios em vantagem competitiva

A combinação de digitalização intensa, demanda crescente por proteção digital, amadurecimento regulatório e desenvolvimento de talentos pode posicionar o país como referência regional em resiliência cibernética e inovação em segurança digital

Embora a sofisticação das ameaças continue crescendo, o mercado brasileiro de cibersegurança vem respondendo com aumento dos **investimentos**, expansão da **força de trabalho especializada**, adoção de **tecnologias avançadas** e fortalecimento das capacidades de **prevenção, detecção e resposta**, consolidando a segurança digital como um vetor de competitividade e confiança para a economia.

Crescimento do mercado de cibersegurança no Brasil



Impulsionado por:



As empresas estão migrando de uma postura reativa para uma **abordagem estratégica**: a cibersegurança deixou de ser vista apenas como custo de proteção e passa a ser tratada como fator de confiança, inovação, continuidade operacional e crescimento sustentável dos negócios.

O ecossistema brasileiro apresenta **elevada capacidade de adaptação e inovação**. Fornecedores e empresas estão incorporando IA, automação, monitoramento contínuo, gestão contínua de vulnerabilidades e novas arquiteturas de segurança para responder às ameaças mais sofisticadas.

1

2

3

4

Onde as empresas
estão no cenário de
cibersegurança?





Fio condutor: da governança de IA ao retorno do investimento

A evolução da IA desloca o foco da adoção para a governança, a supervisão contínua e a geração de valor mensurável em cibersegurança.



Para onde isso leva: **governança, tecnologia e talentos formam um único pacote de investimento**. Ampliar a supervisão sobre os modelos de IA é o que converte gasto em retorno mensurável e prepara o terreno para as recomendações a seguir.



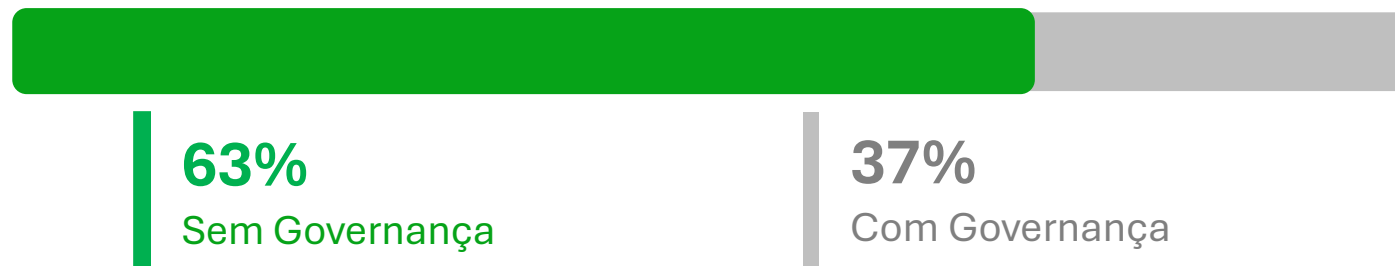
O ritmo da adoção de IA abre espaço para uma nova oferta de segurança

Cada ponto de defasagem entre adoção de IA e governança é demanda endereçável: controles de acesso, monitoramento de modelos e políticas formais são hoje a fronteira de expansão do setor.



MAPEAMENTO DA POLÍTICA FORMAL DE GOVERNANÇA DE IA

A velocidade com que os times adotam IA avançou de forma desproporcional à capacidade da área de TI de supervisioná-la, gerando uma perigosa lacuna de governança nas organizações.



Brasil

87%

não possuem governança

13%

das empresas possuem governança

CONSEQUÊNCIAS DO DESCONTROLE:

Sem mecanismos de detecção de IA oculta (Shadow AI), as equipes de TI não tem visibilidade de quais ferramentas os colaboradores estão alimentando com dados corporativos sensíveis, gerando mais investimento em remediação do que prevenção.

FALSA SEGURANÇA:

Mesmo entre os 37% que declaram ter governança, menos da metade exige aprovações e validações rigorosas antes da implementação dos algoritmos de produção.

CUSTO FINANCEIRO E REPUTACIONAL:

Organizações sem governança paga um preço significativamente mais alto ao sofrerem incidentes e vazamentos envolvendo modelos vulneráveis.



Governança de IA vira componente da estratégia de segurança

A adoção de práticas de governança de IA avança em ritmos distintos: a aprovação formal já é prática consolidada, enquanto monitoramento contínuo e auditoria de modelos seguem em estágio de expansão.

Entre as organizações que já possuem políticas de governança de IA, quais práticas são adotadas?

Quanto mais operacional o controle, menor a proporção de organizações que já o implementaram.



Quem Vigia a Inteligência Artificial?

50%

das **organizações com governança de IA** utilizam equipes internas para avaliação de riscos de evasão de modelos.

- **Validação independente:** 34% das organizações realizam auditorias com parceiros externos neutros.
- **Gargalo humano:** Em 62% das empresas, a ausência de ferramentas automatizadas de risco aumenta a carga operacional dos analistas e reduz a eficácia do monitoramento e da mitigação de riscos em tempo real.

Nota: Os indicadores apresentados medem aspectos distintos da governança de IA e, portanto, não devem ser somados ou interpretados como partes de um mesmo total.

Fonte: Brasscom; IBM, Cost of a Data Breach Report 2025 (dados globais); IBM, Cost of a Data Breach Brazil 2025 (dados Brasil).



No Brasil, IA oculta e cadeia de fornecedores pesam mais no custo das violações que na média global

Violações envolvendo Shadow AI e dependências da cadeia de fornecedores geram custos adicionais.



IA Oculta (Shadow AI)

O uso não supervisionado e não autorizado de ferramentas públicas de inteligência artificial pelos funcionários gera vulnerabilidades críticas de vazamento de dados confidenciais.



Cadeia de Fornecedores

Subestimar a segurança dos parceiros comerciais e integradores da sua cadeia de suprimentos abre portas para ataques indiretos devastadores.

Notas: * Percentual de acréscimo em relação ao custo médio da violação de dados;
¹ Valores convertidos para dólares pela taxa média de câmbio de 2025. Os valores originais divulgados pela IBM para o Brasil foram apresentados em reais.
Fonte: Brasscom; IBM, Cost of a Data Breach Report 2025 (dados globais); IBM, Cost of a Data Breach Brazil 2025 (dados Brasil).



Tecnologias de maior maturidade reduzem o impacto financeiro das violações

Capacidades maduras de segurança estão associadas a menores custos de violação; os maiores ganhos aparecem na detecção, resposta e contenção dos incidentes.



Quando a defesa digital amadurece, a organização deixa de apenas reagir a incidentes e passa a reduzir perdas de forma mensurável.

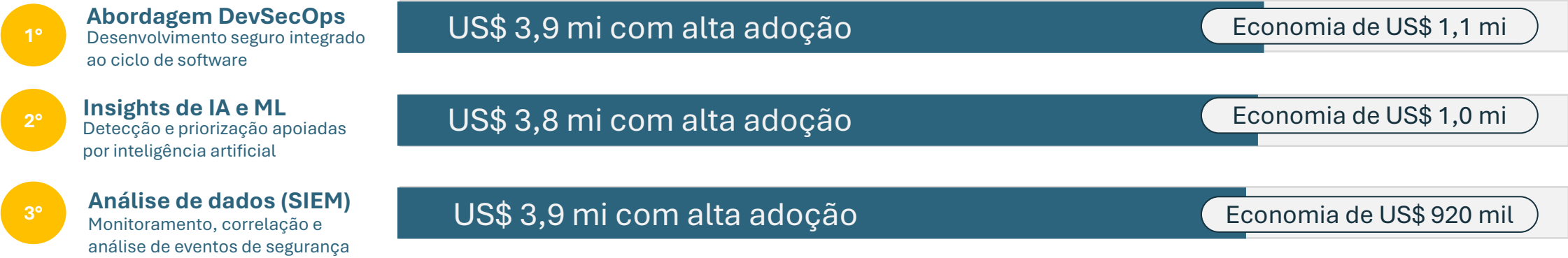
Maior diferença observada

US\$ 1,1 mi

Por violação

O retorno aparece na queda do custo médio dos incidentes, não apenas na prevenção absoluta de ataques.

DIFERENÇA DE CUSTO ASSOCIADA À ALTA ADOÇÃO DE CAPACIDADES DE SEGURANÇA



Brasil

Inteligência de ameaças
US\$ 121 mil¹
de redução média por violação
(R\$ 655 mil)

Tecnologia de governança de IA
US\$ 116 mil¹
de redução média por violação
(R\$ 630 mil)

Notas: ¹ Valores convertidos para dólares pela taxa média de câmbio de 2025. Os valores originais divulgados pela IBM para o Brasil foram apresentados em reais.
Fonte: Brasscom; IBM, Cost of a Data Breach Report 2025 (dados globais); IBM, Cost of a Data Breach Brazil 2025 (dados Brasil).



Investir em talentos reduz até US\$ 1,6 milhão por incidente

A maturidade das defesas não é definida apenas pela tecnologia, mas pela capacidade de operá-la. Análises mundiais mostram que contratação e capacitação reduzem perdas financeiras e ampliam a capacidade de resposta aos incidentes.



Talentos também são investimento

A falta de especialistas qualificados reduz a capacidade operacional de prevenção, detecção e respostas a incidentes.

Custo médio do incidente

(com e sem foco em talentos)

Sem foco
US\$ 5,2 mi

Com foco
US\$ 3,6 mi

Custo menor de

US\$ 1,6 mi

com contratação e capacitação de talentos

TOP INVESTIMENTOS

		Sem investimento adequado	Com investimento adequado	Economia
1º	IA & Machine Learning	US\$ 4,9 mi	US\$ 3,8 mi	US\$ 1,0 mi
2º	DevSecOps	US\$ 5,0 mi	US\$ 3,9 mi	US\$ 1,1 mi
3º	Contratação e Capacitação de Talentos	US\$ 5,2 mi	US\$ 3,6 mi	US\$ 1,6 mi
4º	Gestão de IA Oculta (Shadow AI)	US\$ 4,7 mi	US\$ 4,1 mi	US\$ 0,7 mi



- Alta escassez de talentos
- Baixa ou nenhuma escassez de talentos



Uso amplo de IA reduz o custo das violações em 26% no Brasil e 34% no mundo

Organizações com uso amplo de IA apresentam menor custo médio de violação de dados, evidenciando o potencial da tecnologia para acelerar a detecção, a resposta e a mitigação de riscos.

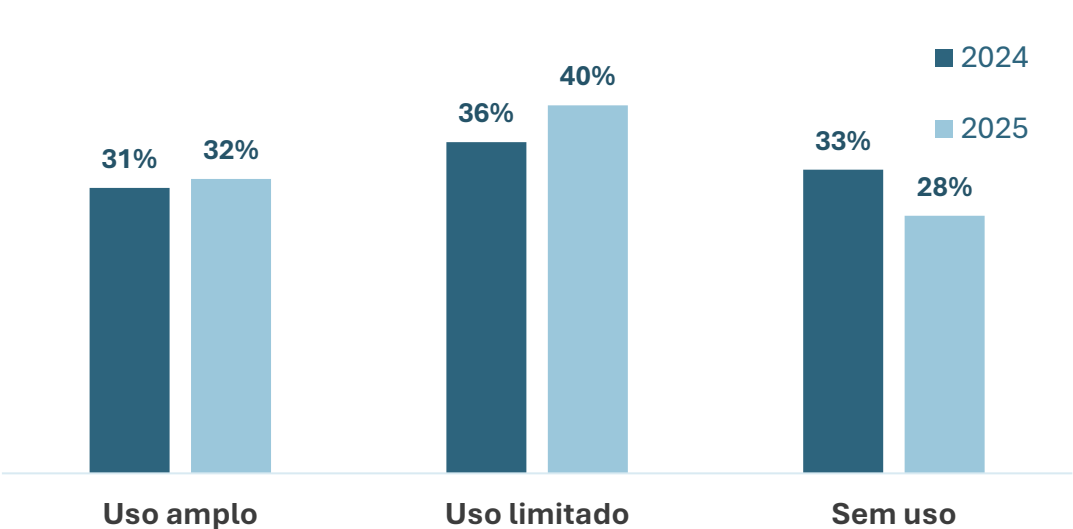
USO AMPLO DE IA:

Refere-se ao uso de IA e automação em atividades de prevenção, detecção, investigação e resposta a incidentes de segurança

Ou seja:

- IA para identificar ameaças
- IA para detectar comportamentos anômalos
- IA para investigação de incidentes
- IA para resposta e contenção de ataques

32% das empresas utilizando amplamente a IA em 2025.



Brasil | ↓ 26% no custo da violação com uso amplo de IA

US\$ 1,6 mi¹
(R\$ 8,8 milhões)
Sem IA

US\$ 1,2 mi¹
(R\$ 6,5 milhões)
Uso amplo de IA

↓ **US\$ 0,4 mi**



Mundo | ↓ 34% no custo da violação com uso amplo de IA

US\$ 5,5 mi
Sem IA

US\$ 3,6 mi
Uso Amplo da IA

↓ **US\$ 1,9 mi**

Notas: ¹ Valores convertidos para dólares pela taxa média de câmbio de 2025. Os valores originais divulgados pela IBM para o Brasil foram apresentados em reais.

Fonte: Brasscom; IBM, Cost of a Data Breach Report 2025 (dados globais); IBM, Cost of a Data Breach Brazil 2025 (dados Brasil).



A IA acelera a resposta e reduz a exposição ao risco

A adoção limitada de IA reduz ganhos de velocidade, eficiência e mitigação de perdas já observados nas organizações mais maduras.

+80 dias

Organizações sem IA permanecem, em média, mais de 80 dias adicionais com invasores em seus ambientes antes da contenção do incidente.

28% menos tempo de exposição

A adoção madura de IA acelera a resposta aos incidentes, reduzindo o tempo de exposição e os impactos associados às violações.

ARMADILHA DO INVESTIMENTO TÍMIDO

- Uso limitado:** A adoção superficial de IA deixa invasores nos sistemas por até **243 dias**, aumentando a exposição aos riscos.
- Uso maduro:** A IA acelera a identificação e a resposta aos incidentes, reduzindo o tempo de exposição e os impactos financeiros.

Maturidade do Uso de IA no Ciclo de Segurança

A maioria das organizações ainda utiliza IA de forma pontual ou nula na gestão de riscos.

Fase do Fluxo	Uso Extensivo	Uso Limitado	Nenhum Uso
Prevenção	30%	43%	27%
Deteção	29%	44%	27%
Investigação	26%	46%	28%
Resposta	45%	28%	

Participação da IA em cada etapa do ciclo de segurança (%)

O PARADOXO DA PARIDADE ORGANIZACIONAL

77%

Embora 77% dos times de segurança achem que acompanham o ritmo das demais áreas da empresa, comparar-se a setores de menor risco digital gera uma falsa percepção de evolução.

1

2

3

4

Recomendações e
Conclusões





Recomendações para empresas

As recomendações representam referências de boas práticas observadas no mercado. Sua adoção deve considerar o perfil de risco, os requisitos regulatórios aplicáveis, o nível de maturidade da organização e as particularidades de cada setor.

1

Segurança de Inteligência Artificial (IA):

Tratar modelos de IA, APIs e repositórios de dados como recursos estratégicos de operação, inventariando acessos e aplicando o princípio do menor privilégio para evitar envenenamento de dados, uso indevido de LLMs e roubo de credenciais de dev/GPU.

2

Identidade e SaaS como Primeira Linha de Defesa:

Adotar autenticação multifator (MFA) resistente a phishing (FIDO2/Passkeys), já que invasores priorizam vishing, abuso de OAuth e sequestro de tokens de sessão para invadir sistemas/aplicações sem disparar alarmes tradicionais.

3

Eliminação de Pontos Cegos Interdominiais:

Unificar a visibilidade entre endpoints, nuvem, SaaS e sistemas de identidade utilizando plataformas de XDR e SIEM de próxima geração, correlacionando dados em tempo real para interromper o encadeamento do ataque.

4

Blindagem da Cadeia de Suprimentos de Software:

Proteger ambientes de desenvolvedores (CI/CD pipelines), assinar códigos digitalmente e validar dependências open-source para evitar que softwares corporativos confiáveis virem vetores de invasão.

5

Threat Hunting e Inteligência Proativa:

Migrar da defesa passiva/reativa para a busca ativa de ameaças (Threat Hunting) suportada por IA, identificando movimentações imperceptíveis de atacantes antes do impacto real.

6

Cultura de Treinamento Baseada em Ataques Reais:

Treinamentos anuais, por si só, podem ser insuficiente. Recomenda-se simulações contínuas baseadas em táticas de ponta, como Adversary-in-the-Middle (AiTM) e clonagem de voz por IA (deepfake vishing), medindo a taxa de reporte do usuário e não apenas a de clique.

7

Proteção Contra "Pretexting" e Falsificação de TI:

Estabelecer mecanismos claros para que colaboradores confirmem a identidade do suporte de TI antes de aceitarem chamadas de voz, compartilhem credenciais ou concederem acesso remoto aos seus dispositivos.

8

Exercícios de Crise Executiva (Tabletop Exercises):

Testar a tomada de decisão da alta liderança diante de extorsões, vazamento de dados corporativos e fraudes financeiras sob pressão real, garantindo clareza sobre papéis, comitês de crise e protocolos de comunicação interna/externa.



9

Letramento Digital em cibersegurança

Cibersegurança robusta não se sustenta apenas com softwares modernos: ela depende de uma cultura corporativa com letramento digital elevado, capaz de identificar riscos e adotar práticas seguras como padrão.

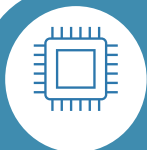


Nota: ¹Passphrases são sequências de quatro ou mais palavras usadas no lugar de senhas tradicionais
Fonte: Brasscom; Secure Our World - CISA (Cybersecurity and Infrastructure Security Agency — EUA); CrowdStrike Global Threat Report (2026).



O futuro da IA segura depende de governança, tecnologia e talentos, com monitoramento contínuo

As empresas de tecnologia vêm desenvolvendo mecanismos robustos de governança, segurança e uso responsável da Inteligência Artificial por compromisso com a inovação confiável, a proteção dos usuários e a confiança digital. A evolução da IA exige não apenas tecnologia, mas também supervisão contínua, qualificação profissional e monitoramento permanente dos potenciais riscos.



IA RESPONSÁVEL É COMPROMISSO CONTÍNUO

- Desenvolvimento baseado em princípios éticos, transparência, segurança e gestão de riscos.
- Processos de validação, testes, auditoria e controles internos já fazem parte da estratégia de diversas organizações.
- A confiança na IA é construída com base na inovação responsável.



NOVOS RISCOS EXIGEM SUPERVISÃO PERMANENTE

- Casos recentes demonstram que modelos podem ser alvo de manipulação, uso indevido ou exploração por agentes maliciosos.
- O acompanhamento de modelos, dados, APIs e cadeias de fornecedores é uma premissa estruturante da estratégia de cibersegurança.



PESSOAS PERMANECEM NO CENTRO DA SEGURANÇA

- A IA não substitui a supervisão humana. Quanto mais avançados os sistemas, maior a importância da **supervisão, da capacitação e do monitoramento** contínuo para garantir segurança, confiança e benefício social.
- A combinação entre **talentos, governança e tecnologia** é o principal fator para ampliar a resiliência digital.

BD 30+ 



Infraestrutura para a Transformação Digital



Tecnologias Estratégicas



Pesquisa, Desenvolvimento e Inovação



Educação e Capacitação Digital



Inclusão Social e Digital



Ambiente de Negócios

A **cibersegurança** integra o eixo de tecnologias estratégicas, ao lado de inteligência artificial, data centers e economia de dados. A leitura é de interdependência: sem infraestrutura digital robusta, segura e acessível, não há competitividade produtiva nem inserção plena do Brasil na economia global de dados e IA.

2FA (Two-Factor Authentication): Método de autenticação que exige dois fatores distintos para confirmar a identidade do usuário.

AiTM (Adversary-in-the-Middle): Ataque em que o criminoso intercepta a comunicação entre o usuário e um serviço legítimo para capturar informações ou credenciais.

API (Application Programming Interface): Conjunto de regras que permite a comunicação e troca de dados entre sistemas e aplicações.

Botnet: Rede de dispositivos comprometidos e controlados remotamente para execução de ataques cibernéticos.

CI/CD (Continuous Integration / Continuous Delivery): Práticas de automação utilizadas para integrar, testar e distribuir softwares de forma contínua.

Deepfake: Conteúdo de áudio, imagem ou vídeo manipulado por inteligência artificial para simular pessoas ou situações reais.

Endpoint: Dispositivo conectado a uma rede, como computadores, celulares ou servidores.

Estelionato eletrônico: Golpe praticado em ambiente digital, como fraudes realizadas pela internet, aplicativos de mensagens, redes sociais ou outros meios eletrônico

FIDO2 (Fast Identity Online 2): Padrão de autenticação baseado em criptografia, projetado para reduzir a dependência de senhas e aumentar a segurança contra phishing.

GPU (Graphics Processing Unit): Unidade de processamento utilizada para executar tarefas computacionais intensivas, incluindo aplicações de inteligência artificial.

LLM (Large Language Model): Modelo de inteligência artificial treinado com grandes volumes de texto para compreender e gerar linguagem natural.

Malware: Termo genérico para softwares maliciosos criados para invadir, comprometer ou danificar sistemas e dispositivos.

MDR (Managed Detection and Response): Serviço especializado de monitoramento contínuo, detecção e resposta a ameaças cibernéticas.

MFA (Multi-Factor Authentication): Método de autenticação que exige dois ou mais fatores de validação para confirmar a identidade do usuário.

NCSI (National Cyber Security Index): Índice que mede a capacidade nacional de prevenir, detectar e responder a incidentes cibernéticos.

NIST CSF (NIST Cybersecurity Framework): Framework de referência para gestão de riscos de cibersegurança desenvolvido pelo National Institute of Standards and Technology (NIST).

OAuth (Open Authorization): Protocolo de autorização que permite que aplicações acessem recursos de outras aplicações sem compartilhar diretamente a senha do usuário.

Passkey: Credencial digital baseada em criptografia que permite autenticação sem necessidade de senha tradicional.

Passphrase: Sequência de quatro ou mais palavras utilizada no lugar de senhas tradicionais.

Phishing: Golpe digital em que criminosos se passam por empresas ou pessoas legítimas para induzir usuários a fornecer dados ou realizar ações indevidas.

Pretexting: Técnica de engenharia social em que o atacante utiliza uma história ou identidade falsa para convencer a vítima a fornecer informações ou acessos.

Ransomware: Tipo de ataque cibernético que bloqueia o acesso a sistemas ou dados e exige pagamento de resgate para sua liberação.

SaaS (Software as a Service): Modelo de software disponibilizado pela internet como serviço, geralmente acessado por assinatura.

Shadow AI (IA Oculta): Uso de ferramentas de inteligência artificial sem aprovação, supervisão ou controle da área de TI da organização.

SIEM (Security Information and Event Management): Solução que centraliza, correlaciona e analisa eventos de segurança para apoiar a identificação de ameaças.

SOC (Security Operations Center): Estrutura responsável pelo monitoramento, detecção e resposta a incidentes de segurança.

Threat Hunting: Busca proativa por ameaças e atividades suspeitas que não foram identificadas pelos mecanismos tradicionais de segurança.

Vishing (Voice Phishing): Golpe realizado por meio de chamadas telefônicas ou mensagens de voz para obter informações confidenciais ou credenciais.

XDR (Extended Detection and Response): Plataforma que integra dados de múltiplas fontes para ampliar a detecção e a resposta a ameaças cibernéticas.

Zero Trust: Modelo de segurança baseado na validação contínua de identidades, dispositivos e acessos, independentemente da origem da conexão



DECLARAÇÃO DE USO

O conteúdo com indicação de confidencialidade é de uso restrito da Brasscom e suas Associadas. A Brasscom não se responsabiliza por quaisquer usos realizados por terceiros, nem por suas consequências patrimoniais, pessoais ou de qualquer natureza.

SÃO CONCEDIDAS AS SEGUINTE PERMISSÕES:



Compartilhar: copiar e redistribuir o material em qualquer suporte ou formato.

Adaptar: recompor, transformar e inspirar a partir do material, desde que respeite os termos abaixo e assuma total responsabilidade pelas alterações.

DE ACORDO COM OS SEGUINTE TERMOS:



Atribuição: dar crédito à Brasscom de forma clara, incluir link para a fonte original e indicar se houve alterações. Não sugerir apoio ou aprovação sem autorização expressa.



Uso Comercial: permitido apenas para associados Brasscom e parceiros autorizados. Empresas não associadas devem solicitar autorização formal.



Proibições: não usar para fins ilegais, políticos, discriminatórios ou que prejudiquem a imagem da Brasscom. Não aplicar termos jurídicos ou barreiras tecnológicas que restrinjam usos permitidos.

Liderança



Affonso Nina
Presidente Executivo



Mariana Oliveira
Diretora de Operações



Helena Loiola Persona
Gerente de Inteligência

Gerência

Equipe



João Vitor Hidaka
Analista de Inteligência



Mateus Ortega Mendes
Analista de Inteligência



Luana Lucio de Jesus
Assistente de Inteligência



Juliana Reichardt
Assistente de Inteligência

Apoio



OBRIGADO!

Brasscom.org.br

Siga-nos nas redes sociais