# Relatório de Mercado: Cibersegurança e Inteligência Artificial no Brasil e no Mundo

## Sumário Executivo

O mercado de Tecnologia da Informação (TI) global e, em particular, o brasileiro, encontra-se em um ponto de inflexão, impulsionado por duas forças transformadoras e intrinsecamente ligadas: a Cibersegurança e a Inteligência Artificial (IA). Este relatório detalha a dinâmica paradoxal desses mercados, onde o crescimento exponencial das ameaças coexiste com o avanço da defesa tecnológica e onde a escassez de talentos é uma crise tanto quantitativa quanto qualitativa.

A análise revela que o cenário de ameaças cibernéticas está mais intenso do que nunca, com o Brasil emergindo como um dos alvos mais frequentes no mundo. No entanto, o custo médio global de uma violação de dados apresentou uma leve queda em 2025, uma aparente contradição que se explica pelo uso estratégico de soluções de segurança baseadas em IA, que permitem uma identificação e contenção mais rápidas dos incidentes. Este avanço, contudo, é obscurecido pelo aumento recorde de custos em mercados mais maduros, como os Estados Unidos, e pelo impacto persistente de interrupções operacionais.

No domínio da IA, a situação se desdobra em outro paradoxo: a alta adoção individual por brasileiros, que superam a média global no uso de IA generativa, contrasta nitidamente com a adoção corporativa embrionária. Essa lacuna reflete desafios como custo e capacitação, mas, mais criticamente, aponta para a proliferação da "IA invisível" (*shadow AI*), que cria um vetor de risco de segurança significativo para as organizações.

A raiz comum desses desafios é a crise de talentos. O Brasil enfrenta um déficit crônico e um desalinhamento educacional, onde as formações acadêmicas falham em preparar profissionais com as competências práticas mais demandadas pelo mercado, como segurança em nuvem e IA/Machine Learning. Esta escassez é agravada pelo fenômeno da "fuga de cérebros" (*brain drain*), impulsionado por salários significativamente mais altos em mercados internacionais, que se tornam acessíveis com o trabalho remoto.

Para mitigar esses riscos e aproveitar as oportunidades, o relatório conclui com recomendações estratégicas que enfatizam a necessidade de um esforço coordenado entre o setor privado, a academia e o governo. A superação dos desafios identificados — desde a implementação de governança de IA até a reforma curricular — é fundamental para que o Brasil não apenas adote tecnologias, mas se posicione como um ator global em inovação e segurança digital.

## 1. O Cenário Macro do Mercado de Tecnologia da Informação

O mercado de TI tem se consolidado como o principal motor da transformação econômica e social em escala global. No epicentro dessa evolução, a Cibersegurança e a Inteligência Artificial se destacam não como campos isolados, mas como forças interdependentes que moldam o futuro da tecnologia. A IA, em particular, tem se mostrado um fator dual: é tanto a maior ameaça a ser enfrentada pelas organizações quanto a ferramenta mais poderosa para defender ativos digitais. A sinergia entre esses dois domínios é um tema central deste relatório, que busca desvendar as complexidades e os paradoxos que definem o mercado atual, tanto no cenário global quanto no contexto específico do Brasil.

O investimento e a inovação em TI são cruciais para a competitividade das nações e empresas, e a capacidade de gerenciar os riscos digitais e alavancar novas tecnologias determinará quem prosperará na economia do futuro. A ascensão da cibersegurança como uma prioridade estratégica, e não apenas um custo operacional, reflete a crescente conscientização sobre a importância de proteger dados e infraestruturas críticas. Paralelamente, a IA evolui de uma tecnologia promissora para um recurso essencial que automatiza processos, gera valor e, crucialmente, fortalece as capacidades de defesa cibernética, criando um novo paradigma de resiliência digital.

## 2. Dinâmica do Mercado de Cibersegurança: A Crise do Risco Digital

### 2.1. O Aumento Exponencial das Ameaças Cibernéticas

O panorama das ameaças cibernéticas é marcado por um crescimento alarmante em volume e sofisticação. O Brasil, em particular, enfrenta um cenário de alta vulnerabilidade. Um estudo recente apontou que o país é o segundo no mundo com mais ataques cibernéticos, registrando mais de 700 milhões de incidentes em um período de 12 meses, o que se traduz em aproximadamente 1.379 golpes por minuto.1 Em uma perspectiva regional, outro levantamento posiciona o Brasil como o 4º país na América Latina com o maior número de ameaças digitais detectadas no primeiro semestre de 2024, com 201 mil ocorrências.2 Essa discrepância de rankings, que o coloca em posições elevadas em ambas as escalas, ressalta a magnitude do problema no país.

A sofisticação dos ataques está em constante evolução, impulsionada em grande parte pelos avanços da inteligência artificial. A tecnologia permite aos cibercriminosos a criação de ameaças mais complexas e difíceis de detectar. Exemplos incluem o uso de IA para otimizar a engenharia social e o *vishing*—uma modalidade de ataque que utiliza recursos de voz para enganar as vítimas.1 A capacidade de emular vozes e estilos de escrita pessoais torna esses golpes mais convincentes e eleva a necessidade de defesas igualmente sofisticadas. Diante desse cenário, a especialista em cibersegurança Chelsea Jarvie enfatiza que a resiliência cibernética não pode depender apenas de tecnologias modernas, mas também da capacitação e conscientização dos colaboradores para evitar as armadilhas otimizadas pela IA.1

### 2.2. A Economia da Cibersegurança: Custos e Investimentos

Apesar do aumento das ameaças, a análise dos custos de violação de dados apresenta um quadro intrigante. O custo médio global de uma violação de dados, que era de USD 4,45 milhões em 2023 [User Query], caiu ligeiramente para USD 4,44 milhões em 2025, marcando o primeiro declínio em cinco anos.3 No entanto, esta estatística não deve ser interpretada como uma diminuição da ameaça. Pelo contrário, ela é uma evidência de uma melhoria na capacidade de resposta das organizações. A IBM atribuiu essa queda à identificação e contenção mais rápidas dos incidentes, um avanço diretamente relacionado ao uso extensivo de soluções de segurança baseadas em IA.4 A automação e a análise em tempo real proporcionadas pela IA geraram uma economia de até USD 1,9 milhão para as organizações que as implementaram.4

No entanto, o impacto da ameaça permanece alto. O custo médio de uma violação nos Estados Unidos atingiu um recorde de USD 10,22 milhões em 2025, indicando que em mercados mais maduros, a complexidade e as interrupções operacionais ainda geram prejuízos massivos.3 A "cauda longa" de uma violação de dados, que se manifesta em interrupções operacionais que podem levar mais de 100 dias para serem recuperadas, continua a ser um desafio significativo para quase todas as organizações.3

No Brasil, o investimento no setor acompanha a crescente preocupação. O mercado de cibersegurança movimentou cerca de R$ 17 bilhões em 2024, o que corresponde a quase USD 3 bilhões.5 Este valor difere dos R$ 21 bilhões mencionados para 2023 [User Query], o que pode ser atribuído a diferentes metodologias de pesquisa e fontes. A Peers Consulting + Technology, fonte da informação de 2024, projeta um crescimento de 9% para 2025, com o setor atingindo USD 4,5 bilhões até 2029.5 Em média, as empresas brasileiras dedicam entre 4% e 7% de seus orçamentos de TI à cibersegurança.5

A seguir, a Tabela 1 consolida os principais dados financeiros do setor:

**Tabela 1: Evolução dos Custos de Violação de Dados e Investimento em Cibersegurança**

| Indicador | 2023 | 2024 | 2025 (Projeção) |
| --- | --- | --- | --- |
| Custo Médio Global de Violação de Dados | USD 4,45 milhões | Não disponível | USD 4,44 milhões (queda) |
| Custo Médio de Violação de Dados (EUA) | Não disponível | Não disponível | USD 10,22 milhões (recorde) |
| Investimento em Cibersegurança no Brasil | R$ 21 bilhões | R$ 17 bilhões | 9% de crescimento |
| % do Orçamento de TI no Brasil para Cibersegurança | Não disponível | 4-7% | Não disponível |

## 3. A Escassez de Talentos em Cibersegurança: Uma Crise Qualitativa

### 3.1. O Déficit Quantitativo e Qualitativo

Apesar da demanda aquecida, o mercado de cibersegurança enfrenta uma crise de talentos que é, ao mesmo tempo, quantitativa e qualitativa. Globalmente, o déficit de profissionais é massivo, com a necessidade de 3,4 milhões de especialistas para proteger ativos digitais de forma eficaz.6 No Brasil, a situação é particularmente grave. A demanda anual por profissionais de TI é estimada em 159 mil, enquanto a oferta de formandos é de apenas 53 mil, o que significa que apenas uma em cada três vagas criadas consegue ser preenchida.7 Essa lacuna numérica cria um ambiente de intensa competição por profissionais qualificados.

O problema, no entanto, vai além dos números. A escassez de profissionais é também um problema de qualificação.8 Uma pesquisa com 208 gestores de TI no Brasil revelou que metade deles acredita que as universidades não preparam os profissionais adequadamente para o setor, e outros 30% consideram a preparação "mínima".9 Este desalinhamento educacional é um dos principais motores do déficit, criando um ciclo vicioso onde as empresas precisam de profissionais com um conjunto de habilidades práticas que o sistema de formação tradicional não está produzindo.

### 3.2. O Desalinhamento Crítico com o Mercado

O desalinhamento entre a formação acadêmica e as necessidades do mercado é evidente. As empresas buscam desesperadamente por especialistas que "não sejam apenas rodadores de ferramentas", mas que possuam um entendimento profundo das ameaças e a capacidade de atuar de forma proativa em cenários de ataques reais.8 As competências de maior demanda citadas pelos gestores de TI incluem segurança na nuvem, inteligência artificial,

*machine learning* e arquitetura "zero trust".9 A falta de alinhamento com essas áreas críticas agrava a dificuldade de contratação e pode impedir o avanço do país em maturidade cibernética.8

A percepção de que as formações acadêmicas carecem de alinhamento prático destaca a necessidade de um repensar sistêmico na educação. A crise de talentos é um problema sistêmico que não pode ser resolvido apenas com o aumento do número de vagas. O foco deve estar em garantir que os profissionais formados possuam as habilidades práticas e estratégicas necessárias para gerenciar as complexidades da segurança moderna, um desafio que exige uma colaboração mais estreita entre a academia, o setor privado e as políticas públicas.

## 4. Inteligência Artificial e Machine Learning: O Catalisador da Transformação

### 4.1. O Brasil no Epicentro da Adoção Pessoal

O Brasil se destaca globalmente no que diz respeito ao uso e ao otimismo em relação à IA. Pesquisas realizadas pela Ipsos e pelo Google em 2024 mostram que 54% dos brasileiros utilizaram IA generativa, um percentual que supera a média global de 48%.10 Esse alto índice de adoção é acompanhado por um notável otimismo: 65% dos brasileiros veem a IA como uma tecnologia promissora, em comparação com 57% da média mundial.11 Uma pesquisa da Thoughtworks também corrobora essa tendência, indicando que o Brasil é o segundo país mais entusiasmado com a IA generativa, atrás apenas da Índia.14 Esse entusiasmo é alimentado pela crença de que a IA pode aumentar a expectativa de ganhos e o número de empregos, uma visão compartilhada por 60% dos brasileiros, superando a média global de 49%.11

### 4.2. O Paradoxo da Adoção Corporativa

A alta adoção individual de IA no Brasil contrasta de forma significativa com a adoção corporativa. Segundo a pesquisa TIC Empresas de 2024, apenas 13% das empresas brasileiras utilizaram IA nos últimos dois anos.15 Os principais desafios para a adoção incluem o alto custo da tecnologia, a incompatibilidade com os modelos de negócio e a falta de capacitação de colaboradores.15 Esse atraso na adoção formal por parte das empresas cria um risco de segurança considerável. Se 78% dos brasileiros já utilizam IA no ambiente de trabalho 10, mas apenas uma pequena fração das empresas implementou a tecnologia de forma estruturada, isso aponta para a proliferação da "IA invisível" (

*shadow AI*).4

A ausência de políticas de governança e controles de acesso adequados para gerenciar o uso não autorizado de IA é um problema grave, já que 97% das organizações que relataram incidentes de segurança relacionados à IA não possuíam os controles necessários.4 A pesquisa da IBM aponta que sistemas de IA sem governança são mais propensos a sofrer violações e geram custos mais elevados quando isso ocorre.4 Essa lacuna entre a adoção individual e a corporativa é um reflexo da imaturidade do ecossistema e exige uma atenção urgente à governança e à segurança.

### 4.3. Setores e Profissões em Crescimento

Apesar da adoção corporativa ainda incipiente, a IA já está transformando diversos setores da economia brasileira. A tecnologia é vista como uma força transformadora na ciência (80%), medicina (77%), agricultura (74%) e segurança cibernética (67%).10 A aplicação prática já é evidente em áreas como finanças, com a detecção de fraudes e análise de risco; agricultura, com a otimização de recursos e previsão de safras; e varejo, com a personalização da experiência do cliente.16

O avanço da IA tem gerado uma demanda por profissionais altamente especializados. O Fórum Econômico Mundial identificou especialistas em IA e *Machine Learning* como alguns dos cargos com maior demanda em 2024.17 Vagas para Engenheiros de

*Machine Learning* e Cientistas de Dados estão em alta 17, reforçando a necessidade de uma qualificação que combine conhecimentos de ciência da computação, algoritmos, estatística e implementação em ambientes de produção.18

## 5. A Convergência de IA e Cibersegurança: A Nova Fronteira

A relação entre IA e cibersegurança é uma corrida armamentista digital, onde a tecnologia é usada tanto como uma arma de ataque quanto um escudo de defesa.

### 5.1. A IA como Arma de Ataque

Os cibercriminosos estão rapidamente alavancando a IA para escalar e otimizar seus ataques. Ferramentas de IA generativa facilitam a criação de *malware* e campanhas de *phishing* mais convincentes e em maior volume.19 O FBI emitiu um alerta especial sobre o aumento dessas ameaças.19 A engenharia social, uma das principais táticas de ataque, é otimizada pela IA através da imitação de estilos de escrita pessoais e da criação de

*deepfakes*, tornando os golpes mais difíceis de serem identificados pelas vítimas.19 O Centro Nacional de Cibersegurança do Reino Unido (NCSC) prevê que esses usos maliciosos agravarão o impacto de ameaças como o

*ransomware* e aumentarão o volume de ciberataques nos próximos dois anos.19 A capacidade da IA de automatizar a coleta de dados públicos para fins maliciosos também amplifica o vetor de ameaças.19

### 5.2. A IA como Escudo de Defesa

Em contrapartida, a IA e o *Machine Learning* são ferramentas vitais para a proteção digital. A IA permite a análise de grandes volumes de dados em tempo real, identificando ameaças, detectando comportamentos suspeitos e priorizando alertas de segurança.19 Sistemas impulsionados por IA conseguem automatizar respostas a incidentes, como o bloqueio de IPs maliciosos e o isolamento de seções de rede, tornando a reação a incidentes mais eficiente.19 A automação de análises reduz os falsos positivos, aliviando a carga de trabalho dos Centros de Operações de Segurança (SOCs) e aumentando a produtividade das equipes.19

O valor da IA como ferramenta de defesa é demonstrado pelos dados. A economia de custos de USD 1,9 milhão para organizações que utilizam a IA em segurança, comparado a aquelas que não a usam 4, é uma prova tangível do retorno sobre o investimento. Esse dado é crucial para justificar a priorização de investimentos em tecnologia e talentos, posicionando a segurança como um habilitador de negócios em vez de apenas um centro de custo.

## 6. Análise de Remuneração e o Fenômeno do "Brain Drain"

### 6.1. O Salário como Indicador de Escassez

A escassez de talentos qualificados é refletida diretamente na remuneração. No Brasil, os salários para profissionais de cibersegurança são altamente valorizados, com cargos estratégicos podendo superar R$ 40 mil mensais.6 Especialistas em nichos de alta demanda, como segurança na nuvem, podem receber até R$ 25 mil.9 Essa valorização indica a intensa competição por profissionais com as habilidades certas.

### 6.2. O Desafio da Globalização e do Trabalho Remoto

Apesar da alta remuneração no Brasil, o mercado enfrenta o desafio do "brain drain", onde talentos altamente qualificados são atraídos por oportunidades no exterior. A disparidade salarial entre o Brasil e mercados mais maduros, como os Estados Unidos e a Europa, é massiva e o advento do trabalho remoto exacerba esse problema.

A Tabela 2 apresenta um comparativo salarial para ilustrar a magnitude da diferença:

**Tabela 2: Comparativo Salarial (Brasil vs. EUA/Europa) para Cargos de TI e Cibersegurança**

| Cargo | Salário Médio Anual (Brasil) | Salário Médio Anual (EUA) | Salário Médio Anual (Alemanha/Reino Unido) |
| --- | --- | --- | --- |
| CISO | Não disponível | USD 584.000 (US) 21 | £ 318.000 (UK) 21 |
| Pentester | Não disponível | USD 127.718 (US) 22 | €63.000 (DE) 22 |
| Cientista de Dados | Não disponível | USD 108.000 (US) 23 | €48.484 (DE), £29.619 (UK) 24 |
| Engenheiro de Machine Learning | Não disponível | Não disponível | Não disponível |

A capacidade de profissionais brasileiros trabalharem remotamente para empresas estrangeiras por salários em moeda forte cria uma pressão salarial insustentável para as empresas nacionais e agrava a escassez de talentos no mercado interno. A falta de profissionais qualificados, somada à atratividade do mercado internacional, impede que o Brasil desenvolva e retenha o capital humano necessário para inovar e construir um ecossistema digital robusto e seguro.

## 7. Conclusão e Recomendações Estratégicas para o Ecossistema

O mercado de TI no Brasil e no mundo é definido pela interconexão de Cibersegurança e Inteligência Artificial. A análise deste relatório revela que, para navegar com sucesso neste cenário, o ecossistema brasileiro deve adotar uma abordagem coordenada e estratégica.

### 7.1. Para as Empresas

Para construir resiliência digital, as empresas devem ir além da simples compra de ferramentas.

* **Investimento em Formação Interna:** Diante da crise de talentos, é fundamental focar na capacitação e requalificação de colaboradores existentes para suprir a lacuna de habilidades técnicas e estratégicas.8
* **Priorização da Cultura e Metodologia:** A adoção de metodologias como o *DevSecOps* é crucial para integrar a segurança desde o início do ciclo de desenvolvimento de software, evitando que seja tratada como um elemento de última hora.25
* **Governança de IA:** É imperativo que as empresas superem a adoção tímida e implementem políticas de governança para mitigar o risco da "IA invisível". A falta de controle sobre o uso de IA pelos colaboradores representa uma ameaça de segurança significativa.4

### 7.2. Para o Setor Acadêmico

A academia desempenha um papel fundamental na resolução da crise de talentos.

* **Reforma Curricular:** Os currículos precisam ser rapidamente atualizados para incluir competências práticas de alta demanda, como segurança em nuvem, IA e arquitetura "zero trust".9
* **Parcerias com a Indústria:** É essencial fomentar a colaboração com o setor privado para garantir que a formação reflita as necessidades reais do mercado e prepare os alunos para os desafios e oportunidades do mundo real.

A superação dos desafios identificados, como a crise de talentos e a adoção corporativa de IA, não é apenas uma questão de crescimento, mas de soberania e segurança digital. Um esforço coordenado entre empresas, academia e governo é crucial para que o Brasil desenvolva uma base sólida de talentos qualificados, capaz de enfrentar os desafios complexos e interligados de Cibersegurança e Inteligência Artificial e se posicione como um líder global em inovação e segurança digital.

#### Referências citadas

1. Brasil é vice-campeão em ataques cibernéticos, com 1.379 golpes ..., acessado em agosto 19, 2025, <https://www.cnnbrasil.com.br/economia/negocios/brasil-e-vice-campeao-em-ataques-ciberneticos-com-1-379-golpes-por-minuto-aponta-estudo/>
2. Brasil é o 4º país da América Latina com mais ameaças digitais no 1º semestre de 2024, diz pesquisa, acessado em agosto 19, 2025, <https://www.cnnbrasil.com.br/economia/macroeconomia/brasil-e-o-4o-pais-da-america-latina-com-mais-ameacas-digitais-no-primeiro-semestre-de-2024-diz-pesquisa/>
3. Custo de uma violação de dados teve primeira queda em cinco ..., acessado em agosto 19, 2025, <https://inforchannel.com.br/2025/07/30/custo-de-uma-violacao-de-dados-teve-primeira-queda-em-cinco-anos-afirma-ibm/>
4. Custo das violações de dados de 2025 | IBM, acessado em agosto 19, 2025, <https://www.ibm.com/br-pt/reports/data-breach>
5. Cibersegurança no Brasil deve movimentar R$ 17 bilhões em 2024 ..., acessado em agosto 19, 2025, <https://www.portaltela.com/entretenimento/tecnologia/2025/05/24/ciberseguranca-no-brasil-deve-movimentar-r-17-bilhoes-em-2024-com-crescimento-previsto>
6. Salário de profissional de segurança pode superar R$ 40 mil - CISO Advisor, acessado em agosto 19, 2025, <https://www.cisoadvisor.com.br/salario-de-profissional-de-ciberseguranca-pode-superar-r-40-mil/>
7. Escassez de profissionais de TI no mercado brasileiro e os desafios da qualificação, acessado em agosto 19, 2025, <https://www.youtube.com/watch?v=ndInuUvoBlA&pp=0gcJCfwAo7VqN5tD>
8. Déficit de profissionais de cibersegurança: mercado brasileiro precisa de especialistas, acessado em agosto 19, 2025, <https://boletimsec.com.br/deficit-de-profissionais-de-ciberseguranca-mercado-brasileiro-precisa-de-especialistas/>
9. Formação acadêmica falha na preparação de profissionais de ..., acessado em agosto 19, 2025, <https://fenati.org.br/formacao-academica-falha-na-preparacao-de-profissionais-de-ciberseguranca-diz-pesquisa/>
10. Brasil está entre os países que mais utilizaram Inteligência Artificial ..., acessado em agosto 19, 2025, <https://conselhodigital.org.br/2025/01/brasil-esta-entre-os-paises-que-mais-utilizaram-inteligencia-artificial-generativa-em-2024/>
11. 54% dos brasileiros usaram IA generativa em 2024, mostra pesquisa - Poder360, acessado em agosto 19, 2025, <https://www.poder360.com.br/poder-tech/54-dos-brasileiros-usaram-ia-generativa-em-2024-mostra-pesquisa/>
12. Brasil está entre os países que mais usam inteligência artificial, acessado em agosto 19, 2025, <https://agenciabrasil.ebc.com.br/geral/noticia/2025-01/brasil-esta-entre-os-paises-que-mais-usam-inteligencia-artificial>
13. IA Generativa: Brasil entre os Países mais Receptivos à Tecnologia - :upd8, acessado em agosto 19, 2025, <https://upd8.com.br/ia-generativa-brasil-entre-os-paises-mais-receptivos-a-tecnologia/>
14. O Brasil é o segundo país do mundo mais entusiasmado com IA, aponta pesquisa - Softex, acessado em agosto 19, 2025, <https://softex.br/o-brasil-e-o-segundo-pais-do-mundo-mais-entusiasmado-com-ia-aponta-pesquisa/>
15. Apenas 13% das Empresas Utilizaram IA em 2024; O que o Número ..., acessado em agosto 19, 2025, <https://forbes.com.br/forbes-tech/2025/05/apenas-13-das-empresas-utilizaram-ia-em-2024-o-que-o-numero-diz-sobre-o-brasil/>
16. Inteligência Artificial No Brasil: Quais Setores Estão Em Expansão - Prelúdio Digital, acessado em agosto 19, 2025, <https://preludiodigital.com.br/inteligencia-artificial-setores-em-expansao/>
17. Conheça 10 profissões com IA em alta para 2024 - AIoT Brasil, acessado em agosto 19, 2025, <https://aiotbrasil.com.br/noticias/conheca-10-profissoes-com-ia-em-alta-para-2024>
18. 100+ Vagas Machine Learning | Vagas para brasileiros - Turing, acessado em agosto 19, 2025, <https://www.turing.com/pt/jobs/engenheiro-machine-learning-remoto>
19. O impacto da inteligência artificial na cibersegurança - WeLiveSecurity, acessado em agosto 19, 2025, <https://www.welivesecurity.com/pt/antimalware-day/o-impacto-da-inteligencia-artificial-na-ciberseguranca/>
20. El impacto de la inteligencia artificial en la ciberseguridad - WeLiveSecurity, acessado em agosto 19, 2025, <https://www.welivesecurity.com/es/antimalware-day/impacto-inteligencia-artificial-en-ciberseguridad/>
21. Quanto ganha um CISO nos EUA e no Reino Unido - CISO Advisor, acessado em agosto 19, 2025, <https://www.cisoadvisor.com.br/quanto-ganham-hoje-os-cisos-nos-eua-e-no-reino-unido/>
22. Qual é o salário de um profissional de TI / Cibersegurança no Exterior? - ibsec, acessado em agosto 19, 2025, <https://ibsec.com.br/qual-e-o-salario-de-um-profissional-de-ti-ciberseguranca-no-exterior/>
23. Quanto ganha um cientista de dados nos EUA e como trabalhar - TuttiHub, acessado em agosto 19, 2025, <https://tuttihub.com/pt/imigracao/vollare/noticias/quanto-ganha-um-cientista-de-dados-nos-eua/>
24. Salários de analistas de dados em todo o mundo: Quanto ganham os analistas de dados?, acessado em agosto 19, 2025, <https://www.datacamp.com/pt/blog/data-analyst-salaries-worldwide>
25. A ascensão do DevSecOps - Check Point Software, acessado em agosto 19, 2025, <https://www.checkpoint.com/pt/cyber-hub/cloud-security/devsecops/the-rise-of-devsecops/>
26. DevSecOps: segurança e crescimento do seu negócio na Nuvem - Cloud Target, acessado em agosto 19, 2025, <https://www.cloudtarget.com.br/recursos/blog/devsecops-seguranca-e-crescimento-do-seu-negocio-na-nuvem>