

As tentativas de ataque contra empresas no Brasil não param de crescer

Em agosto, cada organização no país recebeu em média 4.174 tentativas de ataque por semana. É quase o dobro da média mundial e 48% a mais do que um ano antes. Nesta edição, explicamos o que está por trás dessa alta e trazemos [seis recomendações práticas para aplicar nos próximos 30 dias](#) (página 3).

Equipe de Segurança da Informação e Privacidade, Protiviti Brasil

Os relatórios mensais da Check Point Research¹ mostram uma tendência que já não pode ser tratada como pico isolado. Desde agosto de 2025, a média semanal de tentativas de ataque contra cada organização brasileira passou de 2.822 para 4.174. No mesmo intervalo, a média global subiu bem menos, de 1.994 para 2.422 (gráfico 1).

A Fortinet² chegou a uma conclusão parecida por outro caminho. Entre janeiro e julho de 2026, o país somou cerca de 249 bilhões de tentativas de ataque, volume maior do que o registrado em todo o ano passado.

Em agosto, Governo, Utilities e Serviços Empresariais foram os setores mais visados no Brasil. O e-mail continua sendo a principal porta de entrada: uma em cada 112 mensagens analisadas era phishing, na maioria das vezes com link malicioso, e não com anexo.

O ransomware também voltou a acelerar. Foram 1.042 vítimas divulgadas no mundo no mês, quase o dobro de agosto de 2025. Para as empresas, isso significa mais risco de parada de operação e de exposição pública de dados.

EM NÚMEROS

249 bi

tentativas de ataque no Brasil de janeiro a julho, mais que em todo o ano de 2025

1.042

vítimas de ransomware divulgadas no mundo em agosto

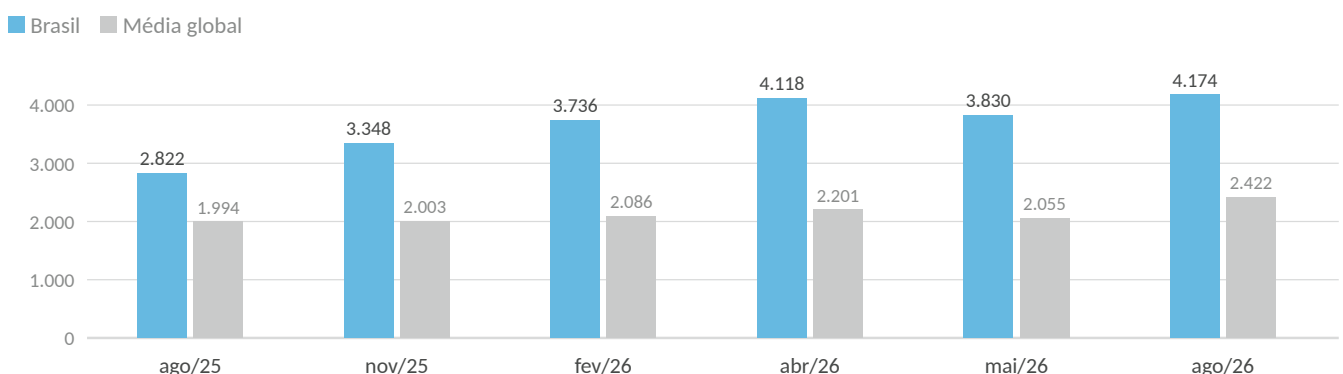
1 em 112

é a proporção de phishing entre os e-mails analisados em agosto

US\$ 4,99 mi

custo médio global de uma violação de dados em 2026, recorde da série

Gráfico 1. Tentativas de ataque por semana, por organização: Brasil e média global



Fonte: Check Point Research (meses selecionados). Os valores medem tentativas de ataque detectadas, e não incidentes confirmados.

Por que os números sobem

IA nas mãos dos atacantes. Ferramentas de IA deixaram o phishing mais convincente e reduziram o tempo para executar um ataque. Segundo a IBM³, uma em cada quatro violações maliciosas estudadas em 2026 envolveu IA, alta de 56% sobre o ano anterior.

Ransomware como serviço. Quem desenvolve o ransomware aluga ferramentas e infraestrutura para afiliados, o que permite multiplicar campanhas em pouco tempo. Em abril, três grupos (Qilin, The Gentlemen e DragonForce) responderam por 34% dos ataques publicados¹.

Fornecedores como porta de entrada. No Brasil, o comprometimento de terceiros e da cadeia de suprimentos aparece em 15% das violações e tem o maior custo médio entre os vetores analisados, R\$ 8,98 milhões⁴.

IA generativa sem regras de uso. Em abril, um em cada 28 prompts enviados a partir de redes corporativas tinha alto risco de vazamento de informação sensível¹.

Quanto custa um incidente

R\$ 7,19 mi

custo médio de uma violação de dados no Brasil⁴

O valor da edição 2025 do estudo da IBM ficou 6,5% acima do ano anterior, e o phishing aparece como vetor inicial mais comum no país, com 18% dos casos. Na edição 2026, com dados globais, detecção, escalonamento e perda de negócios somaram 63% do custo total de uma violação³. Na prática, o prejuízo maior vem da operação parada e da reação dos clientes.

A visão da Protiviti

1º

lugar para ameaças cibernéticas entre os riscos de curto prazo apontados por conselheiros e executivos⁵

43%

dos executivos colocam cibersegurança como principal prioridade de investimento⁵

2 em 3

empresas relatam uso de IA por funcionários sem a supervisão adequada⁶

Na pesquisa Top Risks 2026, conduzida pela Protiviti com a NC State University junto a 1.540 conselheiros e executivos no mundo, as ameaças cibernéticas aparecem como o principal risco de curto prazo, e os riscos de terceiros ficam logo atrás, em segundo⁵. Os dados de mercado desta edição mostram por que essa percepção faz sentido: os caminhos que mais crescem são justamente o e-mail, os fornecedores e o uso de IA sem regras claras.

Na nossa leitura, isso muda quem precisa estar na conversa. Segurança da informação deixou de ser um tema restrito à TI e passou a fazer parte da gestão de riscos do negócio, com dono na liderança, orçamento definido e acompanhamento periódico pela diretoria e pelo conselho. As empresas que já tratam o tema dessa forma costumam responder mais rápido quando um incidente acontece, e o custo de um incidente depende muito dessa velocidade.

O que recomendamos para os próximos 30 dias

- 1 Exigir autenticação em dois fatores (MFA).** Vale para o acesso ao e-mail, à VPN e aos sistemas em nuvem que a empresa já usa, começando pelas contas de administrador. Credenciais roubadas seguem entre as formas de entrada mais comuns, e o segundo fator bloqueia boa parte dessas tentativas.
- 2 Manter um backup desconectado e testar a restauração.** Ter backup não garante recuperação. É preciso manter ao menos uma cópia desconectada da rede (offline), fora do alcance de um ransomware que comprometa o ambiente, e confirmar, na prática, quanto tempo a restauração leva e se esse prazo atende ao negócio.
- 3 Encurtar o prazo de correção do que está exposto à internet.** Sistemas acessíveis de fora da rede são os primeiros a serem explorados quando surge uma vulnerabilidade nova, e merecem prioridade sobre o restante do ambiente.
- 4 Revisar os fornecedores críticos.** Liste quem tem acesso a dados ou sistemas importantes, verifique o que o contrato exige deles em segurança e defina uma avaliação periódica proporcional ao risco de cada um.
- 5 Atualizar a conscientização dos colaboradores.** Os treinamentos precisam incluir golpes feitos com IA, como áudios e vídeos falsos imitando executivos e pedidos urgentes de pagamento ou de troca de dados bancários.
- 6 Definir regras para o uso de IA generativa.** Estabeleça quais ferramentas podem ser usadas e que tipo de informação não pode ser inserido nelas, e comunique isso de forma simples para toda a empresa.

Para levar à próxima reunião de diretoria

- Se um ransomware parasse a operação amanhã, em quanto tempo voltaríamos a funcionar?
- Quando testamos pela última vez o plano de resposta a incidentes com as áreas de negócio?
- Quais fornecedores poderiam ser a porta de entrada para um ataque contra nós?

SOBRE ESTE BOLETIM

Publicação mensal da Protiviti Brasil sobre Cyber, Segurança da Informação e Privacidade, destinada a clientes e parceiros. A cada edição tratamos um tema, com dados recentes, a leitura da Protiviti e recomendações práticas.

CONTATOS

Rodrigo Oliveira

rodrigo.felipe@protiviti.com.br

Alexandre Tamura

alexandre.tamura@protiviti.com.br

Na próxima edição: ransomware e como se preparar antes do ataque.

1. Check Point Research, relatórios mensais de inteligência de ameaças, agosto de 2025 a agosto de 2026.
2. Fortinet, Cenário Global de Ameaças, 2026.
3. IBM e Ponemon Institute, Cost of a Data Breach Report 2026.
4. IBM e Ponemon Institute, Cost of a Data Breach Report 2025, recorte Brasil.
5. Protiviti e NC State University ERM Initiative, Executive Perspectives on Top Risks and Opportunities 2026.
6. Protiviti, AI Pulse Survey, vol. 4, 2026.