Bolsas — Na sexta-feira: 0,03% São Paulo; 0,14% Nova York

Pontuação B3 — IBovespa nos últimos dias: 169.649 / 168.333 (16/6, 17/6, 18/6, 19/6)

Dólar — Na sexta-feira: R$ 5,164 (-0,2%)

Dólar — Últimos	
15/junho	5,066
16/junho	5,086
17/junho	5,107
18/junho	5,175

Salário mínimo — R$ 1.621

Euro — Comercial, venda na sexta-feira: R$ 5,928

CDI — Ao ano: 14,15%

CDB — Prefixado 30 dias (ao ano): 14,15%

Inflação — IPCA do IBGE (em %)

Dezembro/2025	0,33
Janeiro/2026	0,33
Fevereiro/2026	0,70
Março/2026	0,88
Abril/2026	0,67

CIBERSEGURANÇA

Empresas gastam para remediar ataques

Pesquisa mostra que sete em cada 10 companhias desembolsaram mais para recuperar estragos causados por invasões

» RAPHAEL PATI

O aumento do número de ataques cibernéticos tem causado mais dor de cabeça para os empresários brasileiros. Sem planejamento, ou, muitas vezes, sem recursos para tal, as empresas preferem gastar mais em remediar esses ataques depois que eles ocorrem do que investir em prevenção, apesar de, geralmente, a segunda opção ser mais barata do que a primeira. Com modelos cada vez mais sofisticados de invasões, a cibersegurança ainda não é um assunto popular no mercado nacional.

Dados do CIO Report 2026 — pesquisa promovida pela Logicalis, uma empresa global de soluções e serviços de tecnologia da informação e comunicação, em parceria com a Vanson Bourne — mostram que 72% das companhias brasileiras aumentaram o orçamento para remediar ataques após os incidentes, enquanto 28% não observaram essa elevação. A nível global, o movimento é parecido, com 68% confirmando o aumento do orçamento para remediação. Isso sinaliza, na visão dos pesquisadores, que os investimentos deveriam ser mais focados em estratégias preventivas mais robustas.

Outro dado que merece destaque no levantamento é a parcela de organizações que afirmam que seus orçamentos são suficientes para atender às necessidades críticas de cibersegurança. A pesquisa mostra que elas representam 66% do total. Além disso, 58% realizam testes de penetração de maneira regular. Eles funcionam como uma espécie de simulação para identificar as fraquezas operacionais nos sistemas dessas instituições. Por outro lado, 40% afirmaram que não fazem esses testes regularmente.

Na avaliação do CEO da Logicalis, Fabio Hashimoto, existe uma percepção entre as empresas de que elas podem estar "investindo demais", de forma desnecessária, em cibersegurança. "Porque, se você quiser comprar produtos, por exemplo, tem produto infinito, para todos os tipos de disciplinas e minúcias que existem, e isso leva a essa dicotomia. Às vezes, ele (o empresário) não aguenta mais gastar dinheiro com segurança. 'Parece que quanto mais eu faço, mais eu estou desprotegido', ele pode pensar", destaca.

Hashimoto explica que a maioria dos empresários acredita que o orçamento de segurança já é suficiente para combater ataques, embora a pesquisa revele um aumento de gastos com remediação. "Isso quer dizer que você foi invadido. Ou seja, no fim do dia, eu acho que é a mesma tendência. Talvez a gente tenha uma dificuldade de justificar o crescimento do investimento e fazer isso pelos meios corretos", avalia o CEO.

Falta talento

A escassez de profissionais especializados também segue como um dos principais gargalos. Segundo a CIO Report, 94% das organizações no Brasil já adotaram medidas para mitigar o problema, priorizando contratação baseada em habilidades, treinamentos e certificações. O dado indica uma mudança estrutural no mercado, e que a cibersegurança tornou-se uma disputa por capital humano qualificado.

Mesmo diante dos desafios, a percepção geral entre os empresários é positiva. Do total de entrevistados, 66% discordam de que não extraem valor das soluções, 63% discordam de que os sistemas de aplicação de patches de segurança (atualizações de sistemas feitas para corrigir vulnerabilidades) são complexos demais para serem gerenciados de forma eficaz, e 58% rejeitam a ideia de que há um investimento exagerado em soluções subutilizadas.

Falta prioridade

Não há dúvidas de que a prevenção é muito menos custosa do que o trabalho posterior a um ataque cibernético, como afirma o advogado especialista em cibercrimes e direito digital pelo Ibmec-SP, Luiz Augusto D'Urso. Segundo ele, há uma avaliação entre especialistas na área de que o investimento, quando feito de maneira prévia, deve representar 10% do valor do prejuízo que ocorreria em caso de invasão dos sistemas. "Então, você precisa investir 10% sobre aquele eventual prejuízo", conclui.

"Nós estamos falando de, principalmente, ataques que atrapalham a empresa do ponto de vista de produção. Que, por exemplo, sequestram dados, que tiram do ar muitos canais de venda, ou até afetam o seu financeiro. E aí, o prejuízo é gigantesco, fora em eventual vazamento de dados ou de desgaste à marca", reforça o advogado.

D'Urso acredita que a maioria das empresas do Brasil ainda não está preparada para o avanço cada vez maior da inteligência artificial no campo dos ataques cibernéticos. "A grande maioria das empresas no Brasil é de pequeno ou médio porte. Não são megaempresas, que estão muito seguras, nem microempresas, que sequer têm alguma coisa para perder", explica o advogado. Ele ainda completa: "Por conta disso, é difícil justificar a retirada dessas margens para investir previamente, por exemplo, em cibersegurança", reconhece o especialista.

A baixa maturidade das empresas que possuem mais condições financeiras, em governança, também é um entrave para os investimentos, na avaliação do especialista em proteção de dados e gestão de riscos Bruno Souza Pinto. Segundo ele, o mercado já trata esse assunto como "resiliência operacional", e não apenas como segurança da informação, no sentido restrito ou puramente técnico. "A discussão deixou de ser apenas sobre proteger sistemas e passou a envolver a capacidade da empresa de prevenir, detectar, responder e se recuperar de incidentes, preservando a continuidade do negócio", comenta.

Segundo ele, empresas líderes de mercado já tendem a inserir esse tema na agenda estratégica, de forma integrada à gestão de riscos, à governança corporativa, à proteção de dados, à gestão de fornecedores e à continuidade do negócio. "Nas organizações com menor maturidade, porém, o assunto ainda costuma permanecer concentrado na área de tecnologia, o que faz com que a prevenção avance de forma fragmentada e pouco conectada às decisões mais relevantes da empresa", complementa o especialista.

Um dos principais erros, no entanto, é acreditar que o sistema não será invadido de forma alguma, independentemente do tamanho do investimento, como explica o CEO da Logicalis, responsável pela pesquisa. Esse é um dilema que acompanha o empresário na hora de decidir investir em cibersegurança. "Por mais que eu invista em prevenção, eventualmente eu vou ser invadido. Porque eu vou esquecer de atualizar alguma coisa, porque vai ter algum funcionário que vai fazer uma besteira, vai ter um criminoso que vai fazer um acordo com alguém vislumbrado. Existe um 'mercado negro' de senhas por aí, e aí você não está pronto para lidar com isso", avalia Hashimoto.

> **Às vezes, ele (o empresário) não aguenta mais gastar dinheiro com segurança"**
>
> ***Fabio Hashimoto,*** *CEO da Logicalis*

Risco para prevenir

Pesquisa feita pela Logicalis mostra que ainda há falta de empenho das empresas brasileiras em investir na prevenção, enquanto gastam para remediar problemas

Valdo Virgo/CB/D.A Press

PRINCIPAIS CONCLUSÕES

- As empresas brasileiras estão aumentando os investimentos em cibersegurança, mas ainda adotam uma postura predominantemente reativa diante das ameaças.
- O crescimento dos gastos com remediação pós-incidente sugere que muitos recursos continuam sendo direcionados para corrigir problemas após ataques, e não para preveni-los.

INVESTIMENTOS E ORÇAMENTO

- 72% das empresas brasileiras aumentaram o orçamento destinado à remediação de incidentes ou pagamentos relacionados a ataques cibernéticos.
- No cenário global, esse percentual é de 68%.
- Apesar disso, 66% das organizações brasileiras afirmam que seus orçamentos atuais são suficientes para atender às necessidades críticas de cibersegurança.

CULTURA DE PREVENÇÃO

- 58% das empresas realizam testes de intrusão (pentests) regularmente.
- 40% ainda não fazem esses testes de forma consistente.
- 2% não souberam informar se realizam ou não esse tipo de avaliação.
- O dado indica avanços, mas também revela lacunas importantes na prevenção.

FALTA DE PROFISSIONAIS ESPECIALIZADOS

- 94% das organizações já adotaram medidas para enfrentar a escassez de profissionais de cibersegurança.

As principais estratégias incluem:

- Contratação baseada em habilidades práticas.
- Programas de treinamento e certificação.
- Ampliação do recrutamento para novos perfis profissionais.

ESTRATÉGIAS PARA ATRAÇÃO E RETENÇÃO DE TALENTOS

- 58% investem em programas de reentrada profissional e segunda carreira em cibersegurança.
- 56% oferecem incentivos financeiros para funcionários que identificam ou evitam ataques cibernéticos.
- Apenas 6% não possuem planos estruturados para lidar com a falta de profissionais.

PREPARAÇÃO PARA A COMPUTAÇÃO QUÂNTICA

- 47% das empresas possuem estratégias mais maduras para enfrentar os desafios da computação quântica.
- 44% estão em estágio intermediário de preparação.
- 9% ainda não abordaram o tema.
- Na prática, 52% das organizações não estão totalmente preparadas para os impactos da computação quântica na segurança digital.

PERCEPÇÃO SOBRE O RETORNO DOS INVESTIMENTOS

- 66% discordam que não estejam obtendo valor das soluções contratadas.
- 63% discordam que os sistemas de atualização de segurança (patches) sejam complexos demais para serem gerenciados.
- 58% discordam que haja excesso de investimento em ferramentas pouco utilizadas.

Fonte: CIO Report 2026, Logicalis

Na indústria, invasões digitais elevam preço

» EDUARDA ESPOSITO

Os ataques virtuais estão entre as principais ameaças também para o setor industrial, junto com crimes patrimoniais, como furtos e roubos. Entre empresários, a preocupação é crescente, já que invasões do tipo podem paralisar as operações por horas, ou mesmo dias, com grande prejuízo para a produção.

Segundo a pesquisa Segurança Patrimonial, realizada pela Confederação Nacional da Indústria (CNI) em parceria com a Nexus, 17% das fábricas registraram incidentes de segurança cibernética, 20% sofreram com roubo de cargas nas rodovias, e 16% foram alvo de crimes patrimoniais.

De acordo com o levantamento, 30% das vítimas cibernéticas tiveram perdas financeiras diretas. "O que acontece, muitas vezes, a partir de invasão de hackers, é a paralisação do próprio sistema de produção. A cada minuto, hora ou dia de produção paralisada, a empresa está experimentando prejuízo", explicou o assessor especial da CNI Cassio Borges.

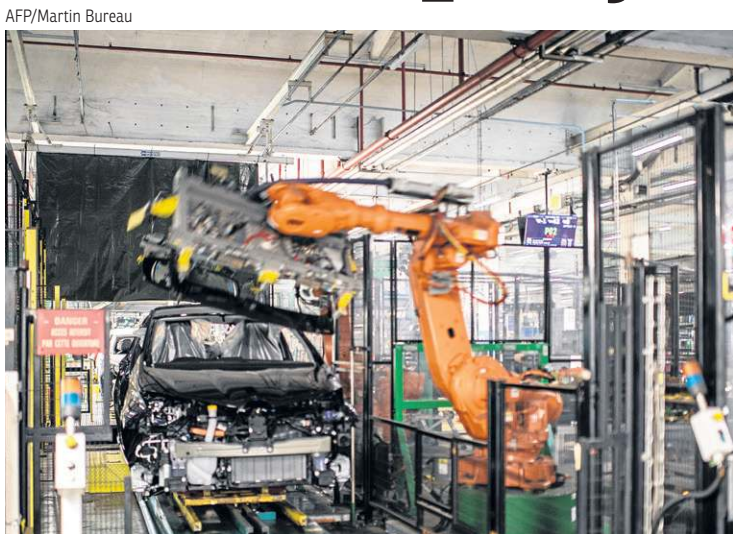
Além desse tipo de insegurança, há também um outro problema no que tange a roubo de dados. Borges alerta que, dependendo das informações sequestradas em invasões, as empresas podem sofrer prejuízo reputacional. Contudo, a pesquisa mostra que mais da metade das empresas ainda gastam pouco com segurança digital: 59% investe menos de 0,5% do faturamento com essa proteção. Como alternativa, as indústrias têm usado táticas de defesas como backups de informações (75%) e softwares de segurança (67%).

Roubo

Mesmo com o avanço da digitalização, crimes mais tradicionais ainda causam grande parte da preocupação do setor. Uma em cada cinco indústrias já sofreu roubo de mercadorias, e 68% dos entrevistados no estudo afirmam que as subtrações acontecem nas rodovias. Outro grande problema citado é o furto de cabos.

Para se proteger, as companhias acabam investindo em soluções que elevam o preço do produto final, como a contratação de seguro de carga, câmeras e equipes de monitoramento. "Isso tudo só faz com que haja um encarecimento da produção industrial, e , consequentemente, do produto brasileiro. Então, se comparar o mercado interno com o externo, isso inviabiliza a competição das empresas brasileiras. Esse é um problema econômico seríssimo", enfatizou Cassio.

AFP/Martin Bureau



Linhas de produção podem ficar alguns dias paradas após ataques