Bolsas — Na sexta-feira: 0,73% São Paulo; 1,9% Nova York

Pontuação B3 — Ibovespa nos últimos dias: 141.356 / 140.680 (7/10, 8/10, 9/10, 10/10)

Dólar — Na sexta-feira: R$ 5,503 (+ 2,39 %)

Últimos	
6/outubro	5,310
7/outubro	5,350
8/outubro	5,344
9/outubro	5,375

Salário mínimo — R$ 1.518

Euro — Comercial, venda na sexta-feira: R$ 6,392

CDI — Ao ano: 14,90%

CDB — Prefixado 30 dias (ao ano): 14,91%

Inflação — IPCA do IBGE (em %)

Abril/2025	0,43
Maio/2025	0,26
junho/2025	0,24
Julho/2025	0,26
Agosto/2025	-0,11

TECNOLOGIA

Pesquisa mostra que, mesmo com os riscos, investimento em tecnologia para impedir cibercrimes não é prioridade no país

IA aumenta necessidade de segurança para empresas

» RAPHAEL PATI

A inteligência artificial trouxe uma gama de facilidades para os usuários de tecnologia, principalmente nos últimos anos. No entanto, com as mudanças cada vez mais constantes nos sistemas tecnológicos, a segurança de dados em nuvem pode ficar cada vez mais comprometida. Dados levantados pela pesquisa *O Estado da Segurança de IA e Nuvem 2025*, elaborado pela empresa Tenable — que gerencia riscos cibernéticos —, em parceria com a Cloud Security Alliance (CSA), mostram que uma grande parcela das empresas no país não prioriza a segurança no ambiente virtual.

Além da segurança não ser uma prioridade, as empresas reconhecem que há falta de conhecimento especializado em segurança da nuvem. Um em cada três participantes da pesquisa apontou essa carência como o principal desafio à segurança nesse tipo de infraestrutura. Além disso, 31% apontaram que a causa maior é a ignorância dos chefes a respeito dos riscos nesse ambiente, enquanto que 20% sinalizaram crença em ferramentas "boas o suficiente" do provedor para evitar danos.

Quando questionados a respeito das barreiras para a implementação de novos recursos de segurança da nuvem, os entrevistados apontaram estratégia pouco clara (39%), orçamento insuficiente (35%) e desvios de recursos para outras prioridades (31%). Ao todo, a pesquisa consultou 1.025 profissionais de TI e segurança que atuam em empresas de diversos setores, como financeiro, telecomunicações e educação.

Com a possibilidade de armazenar dados de maneira remota, o uso da nuvem revolucionou a forma com que os usuários guardam arquivos, mas ao mesmo tempo aumentou as potencialidades de criminosos neste mundo. Mais recentemente, empresas passaram a adotar o sistema MultCloud, que permite a interação de duas ou mais nuvens ao mesmo tempo, como Google Cloud, Dropbox e Microsoft Azure, por exemplo. A ideia é otimizar os chamados workloads, ou cargas de trabalho, que são códigos e recursos que agregam valor para a empresa, como uma aplicação voltada para o cliente.

O MultCloud, ou multinuvem, amplia ainda mais a superfície de ataque de criminosos, além de aumentar a complexidade da segurança. Para o diretor de Engenharia de Segurança da Tenable para América Latina, Alejandro Dutto, as empresas devem adotar estratégias para minimizar esses riscos, como unificar a visibilidade, automatizar políticas de identidade e alinhar a liderança com uma estratégia de segurança proativa e orientada à redução de riscos do negócio.

"De acordo com o estudo, a principal dificuldade é a falta de visibilidade e controle unificado. Cada provedor de nuvem utiliza ferramentas, estruturas e padrões diferentes, o que torna mais difícil criar uma visão consolidada da postura de segurança e aplicar políticas de forma consistente", avalia o diretor. A complexidade do modelo multinuvem também faz com que muitas empresas ainda atuem de maneira reativa, como acrescenta Dutto. "O relatório mostra que 43% das organizações medem o sucesso pela quantidade de incidentes, e não pela redução real de riscos, o que indica falta de maturidade e padronização nas métricas de segurança."

O estudo ainda mostra que, apesar de as organizações agirem rapidamente para implementar a inteligência artificial, a compreensão dos riscos e de como mitigá-los ainda parece imatura. As causas mais frequentes de violações relacionadas à IA, segundo a pesquisa, incluem ameaças conhecidas, como vulnerabilidades de software exploradas (21%), falhas no modelo da IA (19%), ameaças internas (18%) e configurações incorretas da nuvem (16%).

Além disso, 34% das organizações com workloads de inteligência artificial já sofreram violações relacionadas à tecnologia e 14% não têm certeza. Para o diretor da Tenable, o fato de um terço das organizações com workloads de IA já ter sofrido violações indica que a tecnologia está sendo explorada sem a devida proteção. "Seria como construir uma casa sem fechaduras adequadas e colocar alguém para morar lá", compara.

Dutto questiona ainda que as empresas não dominam totalmente os riscos específicos da tecnologia. O fato de 14% não terem certeza também revela um problema grave de monitoramento e governança, na avaliação do executivo. "Se a empresa não sabe se foi violada, significa que não há controles eficazes de detecção ou resposta a incidentes", comenta.

Estar preparado

A adaptabilidade às novas funcionalidades de inteligência artificial passa por reconhecer os perigos extras que essas novas tecnologias podem gerar à segurança interna na empresa. O vice-presidente da Progress Software — empresa que cria aplicações a empresas — para América Latina e Caribe, Francisco Larez, considera que o fato da IA ser utilizada para acelerar processos, e torná-los mais robustos e eficientes também significa que ela pode ser usada com intenções ruins.

"Como toda ferramenta poderosa, a IA tem uma dualidade. Como todas as coisas, pode ser usada para fins muito bons, mas esse mesmo poder também pode ser usado para coisas não tão boas", afirma o executivo, que acredita em uma regulação equilibrada para evitar a atuação de criminosos. "Atualmente, a posição é que precisamos ser responsáveis, tentar usar (a tecnologia) com consciência e estar preparados — mais bem capacitados — para proteger nossas estruturas, nossas empresas e nosso software contra todos os hackers", acrescenta.

Além de proteger os sistemas por meio de programas mais avançados e conhecimento prático, as empresas também devem buscar minimizar os danos que envolvem falhas ou corruptibilidades humanas. Um caso mais recente ocorreu do âmbito da Operação Carbono Oculto, a maior contra o crime organizado da história do país, e que apontou que um funcionário da empresa C&M foi cooptado por criminosos a fornecer as senhas para entrar no sistema da empresa e praticar as ilicitudes.

Na visão do advogado especialista em cibercrimes e direito digital pelo Ibmec-SP Luiz Augusto D'Urso, há, atualmente, dois grandes desafios com relação às grandes fraudes que envolvem milhões, ou até bilhões, como no caso das fintechs. "A primeira situação é realmente o risco cibernético e isso é tratado das mais variadas formas, desde treinamento, desde compliance, desde investimento, até em programas de recompensa de vulnerabilidade, nos chamados bug bounties. Então, é sempre possível evoluir a tecnologia em si", acredita.

Em segundo plano, o especialista afirma que há também a situação de lidar com sistemas seguros usados por usuários. Ele explica que muitos colaboradores não têm a cautela, a malícia e o treinamento necessário, o que facilita a atuação de criminosos em cooptar esses funcionários. "Então, a própria empresa, ao liberar determinados acessos ou a terceirizar serviços, precisa ter cautela para que se tenha gestão de liberação de acesso, de validação de chaves e etc.", alerta o advogado.

"Falando das empresas brasileiras em geral, com certeza. Ainda no Brasil não existe essa cultura máxima de segurança, de proteção dos dados, de proteção dos sistemas, de pensar que hoje, por exemplo, investir em cibersegurança é melhor do que investir em marketing, porque uma empresa que sofre um vazamento tem um desgaste enorme com relação à sua imagem", conclui D'Urso.

Multinuvem

Sobre a adoção do sistema MultCloud, a especialista em direito digital Elaine Keller destaca que a utilização desses recursos deve ocorrer sem que se perca de vista a segurança da informação e o rigor no cumprimento das legislações, em especial da Lei Geral de Proteção de Dados (LGPD). Ela explica que muitas organizações adotam a multinuvem de forma "acidental", seja por deficiências na governança tecnológica, por processos de fusão e aquisição ou por decisões operacionais desarticuladas, e não como resultado de uma estratégia corporativa consciente e estruturada.

"Sob a ótica jurídica, esse cenário é particularmente delicado. A adoção de uma arquitetura multicloud demanda uma governança sólida das políticas de privacidade e de compartilhamento de dados, bem como a definição clara das responsabilidades entre as empresas contratantes e os provedores de serviços em nuvem", esclarece.

A ausência de critérios contratuais precisos e de mecanismos de controle efetivos pode gerar riscos significativos de conformidade, além da exposição indevida de dados e passivos legais relevantes, como explica Keller. "Portanto, a realidade é que muitas companhias migram para o modelo multicloud sem o devido planejamento estratégico, sem políticas robustas de gestão de riscos e sem um plano consistente de segurança da informação. Essa tendência pode comprometer não apenas a integridade dos dados corporativos, mas também a conformidade regulatória e a própria reputação institucional das organizações", finaliza a advogada.

Além dos dados já mencionados, a pesquisa mostra que há um caminho de maturidade para as empresas que deve ser trilhado enquanto os avanços em inteligência artificial ocorrem em uma velocidade cada vez mais rápida. Embora a infraestrutura e a inovação tenham evoluído rapidamente, a estratégia de segurança não acompanhou esse ritmo.

Diante disso, os responsáveis pelo estudo afirmam que, para fortalecer os programas de segurança da nuvem e IA, as organizações precisam passar de respostas reativas a estratégias proativas e embasadas em riscos. "Em outras palavras, a tecnologia evolui mais rápido que o investimento e a mentalidade das organizações. É preciso mudar o foco: sair da reação para a prevenção, com visibilidade integrada, governança de identidade e cultura de segurança em todos os níveis da empresa", complementa o diretor da Tenable, Alejandro Dutto.

Desafios em cibersegurança

O levantamento da Tenable e Cloud Security Alliance revela os gargalos que ainda impedem um investimento ainda maior na segurança de dados entre as empresas

34% Falta de conhecimento especializado

31% Liderança sem conhecimento suficiente dos riscos de nuvem

20% Crença em ferramentas "boas o suficiente" do provedor de nuvem

Principais barreiras para implementação de segurança

- Estratégia pouco clara para segurança da nuvem – **39%**
- Verba insuficiente – **35%**
- Recursos desviados para outras prioridades – **31%**
- Falta de conhecimento especializado – **30%**

Caminho para a maturidade

1. **Priorizar a visibilidade unificada** — Aplicação consistente de políticas em ambientes híbridos e multinuvem.
2. **Investir em governança de identidade** — Incluindo controles para identidades com privilégios mínimos e não humanas (IA).
3. **Expandir os KPIs (Indicadores-Chave de Desempenho)** — Para refletir a prevenção e a resiliência, não apenas a resposta a incidentes.
4. **Alinhar o entendimento da liderança** — Com as realidades operacionais para apoiar um planejamento e alocação de recursos mais inteligentes.
5. **Ir além da conformidade** — Como o limite máximo da segurança de IA, usando-a como ponto de partida para salvaguardas técnicas mais profundas.

Novo modelo de maturidade em cibersegurança deve possuir

1. **Visibilidade unificada da superfície de ataque** — Integrar a observabilidade e o controle sobre todos os ativos em nuvem, local e ambientes híbridos é fundamental.
2. **Governança de identidade fortalecida** — O relatório aponta que 59% das violações estão ligadas a problemas de identidade, como permissões excessivas e falhas de autenticação. Implementar privilégios mínimos, Zero Trust e autenticação multifator são medidas prioritárias.
3. **KPIs voltados à prevenção e resiliência** — A maioria das empresas ainda mede o sucesso pela frequência de incidentes, não pela redução real de riscos. É preciso redefinir métricas para refletir prevenção, tempo de resposta, maturidade e impacto mitigado.
4. **Alinhamento entre liderança e equipes técnicas** — Um dos maiores desafios é a lacuna de conhecimento executivo sobre segurança da nuvem e IA. É necessário educar a alta gestão e incluir a cibersegurança como pilar estratégico de negócio, e não apenas como custo operacional.
5. **Superar a "segurança de conformidade"** — Muitas empresas limitam sua segurança ao atendimento regulatório (como NIST (Instituto Nacional de Padrões e Tecnologia dos EUA) ou ISSO (Organização Internacional para Padronização). A recomendação é ir além da conformidade, aplicando práticas técnicas mais profundas, como testes de segurança específicos para IA, MLOps (operações de Aprendizado de Máquina) seguro e governança de dados.

Valdo Virgo/CB/D.A Press

Fontes: O Estado da Segurança de IA e Nuvem 2025, Tenable e Cloud Security Alliance, e Alejandro Dutto, diretor de Engenharia de Segurança da Tenable para América Latina

Divulgação/Tenable

Alejandro Dutto, da Tenable, acredita que é preciso sair da reação para a prevenção

> **A adoção de uma arquitetura multicloud demanda uma governança sólida das políticas de privacidade e de compartilhamento de dados, bem como a definição clara das responsabilidades"**
>
> ***Elaine Keller,*** *especialista em direito digital*