OPINIÃO

Como o Brasil se compara a outros países na maturidade de cibersegurança

Fernando Dulinski (*)

A economia digital brasileira cresceu de forma acelerada nos últimos anos. E, com ela, a superfície de risco.

Hoje, o país se consolidou como um dos principais alvos de ataques cibernéticos no mundo, movimentando prejuízos bilionários que atingem os diversos níveis de negócios. Mas, embora o tema tenha avançado na agenda nacional, o Brasil ainda enfrenta um desafio fundamental: transformar capacidades técnicas em maturidade estratégica.

O cenário interno expõe uma assimetria significativa. Enquanto grandes empresas brasileiras já operam com estruturas de segurança que se aproximam das adotadas por mercados mais maduros, como Estados Unidos e Europa, a base de PMEs, maioria na economia brasileira, permanece dramaticamente vulnerável. Essa fragilidade não afeta apenas cada negócio isoladamente; ela compromete cadeias inteiras de valor, criando riscos sistêmicos que podem desestabilizar setores inteiros.

Estudos mostram que, embora tenhamos avançado em tecnologia e controles, ainda falta dar o passo mais difícil: transformar a cibersegurança em pauta de negócio, e não apenas de infraestrutura. Enquanto o tema continuar restrito às áreas técnicas, o Brasil seguirá vulnerável. Elevar a discussão ao nível decisório executivo é essencial para reduzir riscos sistêmicos e aproximar o país das economias mais maduras.

Quando comparamos o Brasil com mercados líderes, a distância se torna mais evidente. Países que historicamente priorizam segurança digital, como Reino Unido, Alemanha, Israel e Singapura, avançaram de forma agressiva na integração entre políticas públicas, incentivos regulatórios e cultura corporativa orientada ao risco. Esses ecossistemas estabelecem padrões mínimos claros, fortalecem mecanismos de resposta a incidentes e, sobretudo, têm conselhos e lideranças preparados para lidar com ameaças cada vez mais estratégicas. Globalmente, segundo a PwC, 76% dos conselhos já discutem cibersegurança de forma recorrente. No Brasil, apenas 54% fazem o mesmo, demonstrando uma lacuna de governança que ainda precisa ser resolvida.

A diferença também aparece no impacto econômico dos incidentes. Segundo o estudo de 2025 da IBM, o custo médio global de uma violação atingiu US$ 4,88 milhões, o maior já registrado. No Brasil, o prejuízo médio chegou a R$ 7,19 milhões, com aumento de 6,5% em relação ao ano anterior, colocando o país entre os mercados mais afetados da América Latina. Não é apenas um problema técnico, mas um risco direto à competitividade.

Essa transformação reforça que a cibersegurança deixou de ser um tema operacional para se tornar um indicador estratégico de liderança. É uma tendência que deve moldar o cenário global e que o Brasil precisa acompanhar para não perder competitividade.

Mas, já estamos diante de um ponto de virada. O ciberespaço deixou de ser apenas uma camada técnica da infraestrutura nacional para se tornar um componente essencial da soberania, da produtividade e da confiança na economia. À medida que tensões geopolíticas se intensificam e ataques se tornam mais sofisticados, o país precisa decidir se irá liderar a construção da nova cibereconomia ou se continuará assistindo à erosão gradual de sua segurança econômica.

A oportunidade está clara: fortalecer a governança, capacitar conselhos, reduzir a vulnerabilidade das PMEs, adotar métricas estratégicas e integrar esforços entre governo, empresas e academia. As nações que liderarem essa agenda serão também as que definirão os rumos da inovação, da competitividade e do crescimento nas próximas décadas. O Brasil tem potencial para estar entre elas, mas precisa acelerar.

(*) CEO da Cyber Economy Brasil, hub estratégico com foco em acelerar a maturidade cibernética no Brasil.

OpenAI lança ChatGPT Health mas recomenda não o usar para fins médicos

Embora os chatbots de Inteligência Artificial (IA) sejam muito populares, eles têm gerando uma enxurrada de desinformação que tem alarmado especialistas.

Vivaldo José Breternitz (*)

Corina_Ciocirlans_Images_CANVA

Uma investigação recente do jornal britânico *The Guardian* revelou que os "AI Overviews" do Google, que acompanham a maioria das páginas de resultados de busca forneceram diversas informações de saúde imprecisas que podem levar a riscos graves se seguidas.

Aparentemente indiferente aos repetidos avisos de que os conselhos médicos dados por IA não são confiáveis, a OpenAI está dobrando a aposta com o lançamento do **ChatGPT Health**. O novo recurso promete processar os registros médicos dos usuários para gerar respostas "mais relevantes e úteis".

Apesar de ser "projetado em estreita colaboração com médicos" e construído sob "fortes controles de privacidade, segurança e dados", a empresa ressalta que o recurso foi feito para "apoiar, e não substituir, o atendimento médico". Na verdade, a ferramenta chega ao mercado com uma ressalva contraditória: a de que este recurso de saúde personalizado "não se destina ao diagnóstico ou tratamento".

"O ChatGPT Health ajuda as pessoas a desempenharem um papel mais ativo na compreensão e gestão de sua saúde e bem-estar, ao mesmo tempo em que apoia, e não substitui, o cuidado de médicos", diz o site da empresa. Na prática, porém, é certo que os usuários utilizarão a ferramenta exatamente para o tipo de aconselhamento que a OpenAI desaconselha, o que pode gerar problemas sérios, inclusive mortes.

O problema apenas agrava dilemas já existentes. Como reportado pelo grupo de mídia americano, *Business Insider*, o ChatGPT está transformando pessoas em médicos amadores, gerando preocupações entre os profissionais da área.

Além dos riscos referentes ao uso equivocado de medicamentos, há ainda a questão da privacidade. Usuários parecem dispostos a entregar históricos médicos e informações altamente sensíveis, uma decisão agora incentivada pelo ChatGPT Health. De forma similar, Elon Musk incentivou usuários a enviar dados médicos para o Grok, ferramenta concorrente do concorrente do ChatGPT.

O resultado foi uma onda de confusão, com usuários recebendo diagnósticos alucinados após compartilharem exames de raio-X e tomografias (PET scans).

Especialistas alertam que, dado o histórico da indústria de IA com vazamentos de dados, os riscos são iminentes. "Os dados de saúde são algumas das informações mais sensíveis que as pessoas podem compartilhar e devem ser protegidos", afirmou Andrew Crawford, conselheiro sênior do *Center for Democracy and Technology*, à BBC.

Crawford destaca que, com a OpenAI explorando a publicidade como modelo de negócio, a separação entre dados de saúde e outras interações do ChatGPT precisa ser "estanque". Como não há leis específicas para esses casos, as empresas definem suas próprias regras e podem alterar os termos de serviço a qualquer momento.

Riscos Jurídicos e de Segurança

Por fim, há o temor de que dados sensíveis, como informações de saúde reprodutiva, sejam repassados à polícia sem o consentimento do usuário. "Como a OpenAI lida com solicitações de autoridades?", questiona Crawford. "Eles simplesmente entregam as informações? O usuário é informado de alguma forma? São muitas perguntas para as quais ainda não temos boas respostas."

(*) Doutor em Ciências pela Universidade de São Paulo, é professor, consultor e diretor do Fórum Brasileiro de Internet das Coisas – vjnitz@gmail.com.

A destruição criativa dos modelos obsoletos de tecnologia com IA autônoma

A inteligência artificial autônoma, especialmente aquela baseada em agentes, já é uma das forças mais disruptivas do século XXI. Longe de ser apenas uma promessa, ela representa a aceleração máxima do processo de "destruição criativa" descrito por Joseph Schumpeter, em 1942 — o mecanismo em que novas tecnologias substituem modelos obsoletos e impulsionam o crescimento econômico.

Recentemente, economistas laureados com o Prêmio Nobel expandiram essa teoria, formalizando como a inovação tecnológica se traduz em ciclos econômicos mensuráveis. A IA autônoma, nesse contexto, é o catalisador mais potente já visto: ela não apenas automatiza tarefas, mas toma decisões, aprende e adapta-se de forma independente, algo que reconfigura profundamente estruturas empresariais e profissionais.

A destruição criativa sempre foi o motor do progresso, mas a IA adiciona um componente inédito: velocidade e autonomia. E, com isso, já produz efeitos claros no mercado:

- Obsolescência de funções tradicionais — Processos rotineiros e manuais estão sendo substituídos por agentes digitais, reduzindo a necessidade de tarefas repetitivas.
- Disrupção setorial — Indústrias inteiras, como logística, finanças e saúde, passam por reconfiguração estrutural diante de práticas autônomas.
- Desvalorização de competências antigas — Habilidades baseadas em tarefas lineares perdem valor, enquanto cresce a demanda por profissionais de dados, ética e governança.

O impacto é transversal: não muda só "como" as empresas operam, mas "quem" está apto a trabalhar nelas, além de inaugurar novas profissões e indústrias. Funções emergentes incluem agora treinadores de IA, engenheiros de MLOps (Machine Learning Operations), cientistas de dados especializados em ética e explicabilidade, e gestores de governança digital.

Ao mesmo tempo, setores inteiros são revitalizados. Em finanças e seguros, por exemplo, a agilidade gera benefícios por meio de análise preditiva e da detecção autônoma de fraudes, reduzindo custos. Na área da saúde, a transformação chega por meio de diagnósticos assistidos e telemedicina inteligente. Em cadeias de suprimentos, novos níveis de eficiência são atingidos com logística adaptativa e previsão de demanda. E a cibersegurança se torna cada vez mais proativa, com agentes que monitoram, detectam e respondem em tempo real.

Toda essa evolução dá origem à chamada economia do "Faça Isso Por Mim" (Do It For Me - DIFM), um modelo em que agentes digitais não apenas executam, mas decidem em nome do usuário. Mas, apesar dos avanços, a autonomia plena ainda é exceção. A maioria das implementações depende de supervisão humana em decisões complexas ou críticas, e a ausência de explicabilidade e transparência em relação a como agem compromete a confiança.

Imagine um agente autônomo encarregado de ajustar itinerários aéreos com base em múltiplas fontes de informações. Se ele acessar dados divergentes sobre horários de voos, toda a malha logística poderá ser afetada e esse erro se multiplicará exponencialmente. Esse é o risco em ambientes interconectados. Para mitigar esse tipo de problema, as organizações precisam construir uma "fonte única da verdade", consolidando dados dispersos em estruturas interoperáveis, com rastreabilidade ponta a ponta. A qualidade e a governança de dados tornam-se, portanto, o alicerce técnico e ético da IA autônoma.

A esse desafio somam-se riscos como alucinações, com a geração de informações falsas, de interpretações equivocadas e de falhas sistêmicas quando os dados não são devidamente contextualizados. Por isso, a maturidade da IA autônoma depende da combinação de três fatores: dados confiáveis, algoritmos auditáveis e supervisão humana inteligente.

Para que a implementação da IA de forma bem-sucedida se concretize, é essencial adotar uma arquitetura robusta e multidisciplinar. Em resumo, ela envolve pipelines de dados confiáveis; governança e ética na criação de frameworks que assegurem rastreabilidade e responsabilidade sobre decisões automatizadas; além de capacitação e requalificação para formar profissionais capazes de interpretar e ajustar sistemas autônomos. Ainda, são necessários segurança cibernética para proteger agentes e dados contra vulnerabilidades, manipulações e ataques, e integração com legados para harmonizar sistemas antigos e APIs empresariais em ambientes híbridos ou multicloud.

Esses pilares sustentam a tecnologia e definem a sustentabilidade de todo o ecossistema digital. Empresas que implementarem a IA autônoma com base nesses princípios e compreenderem seu papel como agente de transformação estrutural, e não apenas tecnológica, estarão mais bem posicionadas para prosperar. As que permanecerem presas à inércia dos modelos legados correm o risco de ficarem para trás em um cenário de mudança acelerada. A era da IA autônoma já está em curso, e o desafio não é resistir à transformação, mas aprender a abraçá-la.

(Fonte: Jorge Moskovitz, Executivo de Contas Enterprise da Qlik)

News@TI

Unico conquista certificação internacional SOC 2 e reforça padrão global de segurança

@A Unico, rede líder em verificação de identidade na América Latina, acaba de conquistar a certificação SOC 2 Tipo II, um dos mais relevantes padrões internacionais de segurança da informação para empresas de tecnologia e soluções SaaS (Software as a Service). O relatório foi emitido pela KPMG, com base nos critérios definidos pelo Instituto Americano de Contadores Públicos Certificados (AICPA), referência global em auditoria e asseguração. A certificação SOC 2 Tipo II comprova, de forma independente, que os controles de segurança e disponibilidade da Unico não apenas foram corretamente desenhados, mas operam de maneira eficaz (ao longo de um período contínuo de avaliação anual). Esses fatores evidenciam a maturidade operacional e consistência nos processos da Empresa. O relatório avalia a descrição, o desenho e a efetividade operacional dos controles adotados pela Unico, considerando os princípios de Segurança e Disponibilidade, essenciais para empresas que operam dados sensíveis e infraestruturas críticas no ambiente digital.

Empresas & Negócios **José Hamilton Mancuso (1936/2017)** **Laurinda Machado Lobato (1941-2021)** Responsável: **Lilian Mancuso**

Editorias
Economia/Política: J. L. Lobato (lobato@netjen.com.br); *Ciência/Tecnologia:* Ricardo Souza (ricardosouza@netjen.com.br); *Livros:* Ralph Peter (ralphpeter@agenteliterarioralph.com.br);
Comercial: comercial@netjen.com.br
Publicidade Legal: lilian@netjen.com.br

Webmaster/TI: Fabio Nader; *Editoração Eletrônica:* Ricardo Souza.
Revisão: Maria Cecília Camargo; *Serviço informativo:* Agências Brasil, Senado, Câmara, EBC, ANSA.

Artigos e colunas são de inteira responsabilidade de seus autores, que não recebem remuneração direta do jornal.

Colaboradores: Claudia Lazzarotto, Eduardo Moisés, Geraldo Nunes e Heródoto Barbeiro.

ISSN 2595-8410

Jornal Empresas & Negócios Ltda
Administração, Publicidade e Redação: Rua Joel Jorge de Melo, 468, cj. 71 – Vila Mariana – São Paulo – SP – CEP.: 04128-080
Telefone: (11) 3106-4171 – E-mail: (netjen@netjen.com.br)
Site: (www.netjen.com.br). CNPJ: 05.687.343/0001-90
JUCESP, Nire 35218211731 (6/6/2003)
Matriculado no 3º Registro Civil de Pessoa Jurídica sob nº 103.