

Especialistas defendem regulação equilibrada da inteligência artificial, prevenção e cooperação entre governos, seguradoras e empresas

Michelle Hughes, Aguinaldo Ribeiro, Adam Steeden, Vinicius Malacco e Chris Bose

Londres, 24 de junho de 2026 – A rápida evolução da inteligência artificial, o crescimento dos ataques cibernéticos e a necessidade de ampliar a proteção das pequenas e médias empresas dominaram os debates do painel "**Seguros, Cibersegurança e Riscos Digitais**", realizado na última terça-feira, 23, na sede da **Association of British Insurers (ABI)**, como parte do **2º Fórum Brasil-Reino Unido de Seguros**. Executivos do mercado segurador, especialistas em riscos cibernéticos e representantes do poder público defenderam maior cooperação entre governos, seguradoras, reguladores e empresas para fortalecer a resiliência digital.

Na abertura do encontro, o diretor de Seguros Gerais e Assuntos Internacionais da ABI, Chris Bose, destacou que os riscos cibernéticos estão entre as ameaças de crescimento mais acelerado no mundo, impulsionados pelo aumento da digitalização e pelo avanço da inteligência artificial.

Segundo ele, o seguro cibernético vai além da indenização financeira após um ataque, funcionando também como ferramenta de prevenção, gestão de riscos e disseminação de boas práticas de segurança digital.

Mercado brasileiro amadurece

Representando a Tokio Marine, Vinicius Malacco, gerente de linhas financeiras da Tokio Marine, afirmou que o mercado brasileiro de seguro cibernético evoluiu rapidamente nos últimos anos. Embora seja um produto relativamente recente no país — com expansão mais consistente a partir de 2019 —, as seguradoras já oferecem coberturas comparáveis às disponíveis nos mercados mais desenvolvidos.

O executivo destacou que, após um período de elevada sinistralidade entre 2021 e 2022, o segmento passou por ajustes técnicos e hoje apresenta resultados bastante equilibrados. Também chamou atenção para o aumento da capacidade de contratação de grandes riscos.

Como exemplo, citou que uma apólice contratada pela Petrobras passou de um limite de aproximadamente US\$ 100 milhões para US\$ 400 milhões em pouco tempo, refletindo a evolução do mercado brasileiro.

Apesar desse avanço, Malacco afirmou que o principal obstáculo continua sendo a falta de conhecimento das empresas sobre os riscos digitais.

"Não basta explicar o que é um seguro cibernético. Muitas empresas ainda precisam entender o que é cibersegurança e por que ela é fundamental para o negócio", observou.

Segundo ele, as seguradoras vêm ampliando sua atuação ao oferecer treinamentos, softwares de proteção, testes contra ataques de phishing e serviços especializados antes mesmo da contratação da apólice.

Inteligência artificial amplia riscos e exige adaptação

O subscritor sênior de responsabilidade cibernética da Zurich, Adam Steeden, afirmou que a inteligência artificial vem alterando profundamente o cenário de riscos enfrentado pelas empresas.

Além de aumentar a produtividade, a tecnologia também cria novas vulnerabilidades relacionadas à proteção de dados, ao uso de agentes de IA e à sofisticação dos ataques conduzidos por criminosos.

Para acompanhar essa evolução, explicou, as seguradoras passaram a incorporar o uso da inteligência artificial aos processos de subscrição, avaliando o grau de dependência tecnológica dos clientes e exigindo controles específicos de segurança.

Entre as medidas recomendadas estão o treinamento de funcionários, o bloqueio de ferramentas públicas de IA quando necessário, planos de continuidade de negócios e protocolos específicos para resposta a incidentes envolvendo inteligência artificial.

Steeden ressaltou ainda que as apólices vêm sendo adaptadas para oferecer cobertura explícita a riscos relacionados à IA, reduzindo incertezas para os segurados.

Seguro como ferramenta permanente de prevenção

A líder global de produtos de Linhas Financeiras da QBE, Michelle Hughes, reforçou que o seguro cibernético deve ser encarado como um processo contínuo de gestão de riscos, e não apenas como uma compensação financeira após um incidente.

Segundo ela, antes da emissão de uma apólice, as seguradoras verificam se as empresas adotam controles mínimos, como autenticação multifator, monitoramento de ameaças, proteção de dispositivos e treinamento dos colaboradores.

Para Hughes, esse processo contribui para elevar o nível geral de segurança digital das organizações. Ela comparou o seguro a um "acesso permanente a especialistas", especialmente importante para pequenas e médias empresas, que normalmente não possuem equipes próprias de segurança da informação, advogados especializados ou consultores em gerenciamento de crises.

"O relacionamento com a seguradora continua durante toda a vigência da apólice, acompanhando a evolução das ameaças e oferecendo suporte sempre que necessário", explicou.

Regulação busca equilíbrio entre inovação e proteção

O deputado federal Aguinaldo Ribeiro (PP-PB), relator do projeto que estabelece o marco regulatório da inteligência artificial na Câmara dos Deputados, afirmou que o principal desafio do Brasil é construir uma legislação que estimule a inovação sem comprometer a proteção dos direitos dos cidadãos.

Segundo ele, o texto atualmente em discussão foi profundamente revisado para incorporar os avanços da inteligência artificial generativa, que sequer existia quando a proposta foi aprovada inicialmente pelo Senado.

O parlamentar explicou que o modelo brasileiro vem sendo desenvolvido a partir da experiência internacional, incluindo Reino Unido e União Europeia, mas com adaptações à realidade nacional.

Para Ribeiro, o sucesso da regulação dependerá da construção de uma governança flexível, capaz de acompanhar a velocidade da inovação tecnológica.

Ele também defendeu o fortalecimento da Autoridade Nacional de Proteção de Dados (ANPD), ampliando sua capacidade de fiscalização e resposta rápida diante de incidentes envolvendo

inteligência artificial e proteção de dados.

Educação é prioridade para reduzir o gap de proteção

Na parte final do painel, os participantes discutiram como ampliar o acesso ao seguro cibernético entre pequenas e médias empresas, segmento considerado o mais vulnerável aos ataques digitais.

Houve consenso de que a principal barreira continua sendo a falta de conscientização dos empresários sobre a dimensão dos riscos. Adam Steeden observou que muitas empresas ainda acreditam estar fora do radar dos criminosos, quando, na prática, organizações de todos os portes são alvo de ataques cada vez mais sofisticados.

Michelle Hughes defendeu que a educação digital deve começar ainda na escola e envolver governos, reguladores, empresas e seguradoras.

Segundo ela, medidas simples, como a adoção da autenticação multifator e treinamentos periódicos, podem reduzir significativamente a exposição aos ataques.

Os especialistas também ressaltaram que o fortalecimento da cibersegurança passa por políticas públicas, investimentos em infraestrutura digital, compartilhamento de inteligência entre os setores público e privado e pelo desenvolvimento de mecanismos que ampliem o acesso das pequenas empresas ao seguro.

Ao final do painel, a principal mensagem foi de que, diante da rápida evolução das ameaças digitais, o seguro cibernético deixa de ser apenas um instrumento de transferência de riscos para se consolidar como um componente estratégico da resiliência digital das organizações e da economia.

Fonte: [CNseg](#), em 24.06.2026.