Crescimento acelerado, regulação mais robusta e soluções avançadas mostram que o mercado está pronto para atender riscos digitais cada vez mais severos

Ataques cibernéticos e vazamento de dados aparecem entre os três principais riscos atuais e já despontam como o risco número 1 no horizonte até 2028, segundo a Pesquisa Global de Gestão de Riscos 2025 da Aon para a América Latina. De olho nesta tendência, empresas ao redor do mundo têm buscado no mercado segurador a proteção necessária — e o Brasil tem se destacado nesse cenário.

Dados da Confederação Nacional das Seguradoras (CNseg) apontam alta na demanda pelo Seguro Cibernético. Entre janeiro e setembro deste ano, foram mais de R$ 173 milhões arrecadados, avanço de 5% em comparação com 2024. As indenizações somaram R$ 28 milhões no período, em linha com o montante pago no ano anterior, evidenciando um mercado em franca consolidação, com subscrição mais refinada e crescente maturidade técnica na gestão desses riscos.

A série histórica recente confirma a expansão contínua desse seguro no país. Considerando o mesmo período de janeiro a setembro, em 2021, o ramo arrecadou cerca de R$ 70,5 milhões; em 2022, o volume subiu para R$ 123,1 milhões, chegando a R$ 152,9 milhões em 2023 e a R$ 165,6 milhões em 2024. Comparando os primeiros nove meses de 2021 com os de 2025, o salto foi de 145%.

“Trata-se de um crescimento consistente, que mostra como a proteção ante ataques digitais deixou de ser um produto de nicho para se tornar parte estruturante do planejamento de risco das empresas brasileiras. Hoje, o mercado nacional dispõe de soluções avançadas, equipes altamente qualificadas e capacidade de acompanhar a sofisticação dos ataques”, afirma Victor Perego, membro da Subcomissão de Linhas Financeiras da Federação Nacional de Seguros Gerais (FenSeg). Segundo ele, as coberturas têm se mostrado estratégicas para a sustentabilidade operacional das grandes empresas e já fazem parte do portfólio de mitigação de riscos de organizações de todos os setores.

O avanço da demanda no Brasil ocorre em um ambiente regional de risco crescente. A Aon mostra que, na América Latina, ataques cibernéticos e vazamento de dados figuram entre os três principais riscos atuais e aparecem em primeiro lugar na lista de riscos futuros esperados até 2028 — à frente de temas como aumento da concorrência e mudanças climáticas.

Interrupção de negócios permanece no topo do ranking de riscos presentes, reforçando o papel do seguro cibernético como ferramenta essencial de proteção financeira diante de incidentes que paralisam operações, impactam cadeias de suprimentos e afetam a reputação corporativa.

No sistema financeiro, a relevância desse tipo de cobertura ganhou novo impulso com a Resolução BCB nº 498/2025, do Banco Central do Brasil, que tornou obrigatória a contratação de seguro de responsabilidade civil e de riscos operacionais — incluindo incidentes de fraude e segurança cibernética — para prestadores de serviços de tecnologia da informação que atuam no âmbito do Sistema de Pagamentos Brasileiro.

Para Perego, essa exigência chega em um momento oportuno. “Hoje, o mercado brasileiro está preparado. Temos oferta diversificada, maior padronização de processos, ferramentas de modelagem de risco mais robustas e uma cadeia de resposta a incidentes muito mais integrada. Essa maturidade permite atender desde empresas altamente reguladas até organizações que estão iniciando sua jornada de gestão de riscos digitais”, destaca.

Apesar dos avanços, o relatório da Aon indica que muitas organizações ainda subestimam o impacto financeiro de um ataque digital. Embora o cyber esteja entre as principais preocupações dos executivos, ainda são poucas as empresas que quantificam de forma estruturada sua exposição ao risco — o que limita a adoção de estratégias integradas de prevenção, resposta a incidentes e transferência de risco via seguro.

“O seguro cibernético não substitui investimentos em segurança, mas potencializa essa jornada ao oferecer recursos especializados de resposta, cobrir custos de investigação, notificação e recuperação de sistemas e proteger o caixa da empresa em momentos críticos. Ao mesmo tempo, funciona como um indutor de boas práticas de governança, estimulando as organizações a aprimorar políticas internas, mapear vulnerabilidades e estruturar planos de contingência mais sólidos. É uma camada estratégica dentro de um ecossistema de proteção cibernética muito mais amplo”, conclui Perego.

Fonte: CNseg, em 19.12.2025.