



A publicação do novo Manual de Orientações sobre Segurança Cibernética, da Superintendência de Seguros Privados (Susep), ocorre em um momento de avanço dos riscos digitais para empresas e do próprio mercado de seguros. Dados da Confederação Nacional das Seguradoras (CNseg) mostram que, entre janeiro e abril de 2026, as seguradoras desembolsaram quase R\$ 30 milhões em indenizações de Seguro Cibernético, alta de 253,1% em relação ao mesmo período do ano anterior. No mesmo intervalo, a arrecadação da modalidade cresceu 71,1%, alcançando R\$ 134,6 milhões em prêmios.

Os números indicam que os ataques cibernéticos passaram a produzir impactos financeiros mais frequentes para empresas de diferentes portes. Ao mesmo tempo em que aumentam as indenizações, cresce a procura por mecanismos capazes de reduzir os prejuízos decorrentes de paralisações operacionais, vazamento de dados e outros incidentes digitais.

Nesse cenário, o manual da Susep reúne orientações para auxiliar seguradoras, resseguradoras, entidades abertas de previdência complementar, sociedades de capitalização e cooperativas de seguros na adoção dos requisitos mínimos de segurança previstos na regulamentação. Embora tenha caráter orientativo, o documento reforça que a cibersegurança passou a integrar a estratégia de gestão de riscos das companhias, deixando de ser tratada apenas como uma obrigação regulatória.

Parte dessa evolução já vinha sendo construída pelo próprio mercado. Antes da publicação do manual, a Confederação Nacional das Seguradoras (CNseg) estruturou a plataforma de Compartilhamento de Incidentes Cibernéticos (CIC), que permite às empresas compartilhar, de forma confidencial, informações sobre ataques, vulnerabilidades e novas ameaças.

A iniciativa vem ganhando escala. Em 2025, o CIC registrou 527 alertas relacionados a incidentes cibernéticos. Apenas no primeiro trimestre de 2026, outros 123 eventos foram compartilhados entre as empresas participantes, demonstrando que a troca estruturada de inteligência passou a fazer parte da rotina operacional das seguradoras.

Entre os registros mais frequentes estão alertas sobre vulnerabilidades, notícias de incidentes, atualizações críticas de segurança, campanhas de phishing e informações regulatórias.

Para o diretor de Serviços às Associadas da CNseg, André Vasco, a centralização dessas informações acelera a resposta das empresas diante de novas ameaças e reduz custos associados ao cumprimento das exigências regulatórias.

"Além de dar celeridade para as seguradoras protegerem seus dados e evitarem danos aos seus negócios e aos seus clientes, o CIC estabelece uma redução de custos operacionais diante da necessidade de cumprir a legislação."

Na prática, o sistema funciona como uma rede de inteligência compartilhada. Ao identificar uma nova ameaça, uma seguradora consegue alertar rapidamente as demais participantes, permitindo a adoção antecipada de medidas de contenção, como o isolamento de sistemas comprometidos, a aplicação de correções e o reforço dos mecanismos de proteção.

O avanço das indenizações do Seguro Cibernético, o crescimento da demanda pela cobertura e a ampliação do compartilhamento de informações sobre incidentes apontam para a mesma direção: a gestão do risco cibernético passou a ocupar espaço permanente na estratégia das seguradoras. O manual da Susep reforça esse movimento ao reunir diretrizes que aproximam regulação e boas práticas adotadas pelo próprio mercado.

O que explica o avanço do Seguro Cibernético?

O aumento da contratação acompanha a maior exposição das empresas aos riscos digitais. Ao contrário do que se imagina, o Seguro Cibernético não se limita a cobrir ataques de hackers. Dependendo da apólice, a cobertura pode incluir investigação forense, recuperação de sistemas, gerenciamento de crises, comunicação com clientes e autoridades, despesas jurídicas, perdas decorrentes da interrupção das operações, responsabilidade por vazamento de dados e custos relacionados a ataques de ransomware e extorsão digital.

À medida que as empresas se tornam mais dependentes de sistemas e dados, cresce a importância de integrar prevenção tecnológica, capacidade de resposta e proteção financeira. Para Victor Perego, membro da Subcomissão de Linhas Financeiras da Federação Nacional de Seguros Gerais (FenSeg), é nessa combinação que o Seguro Cibernético amplia sua contribuição às organizações.

“O Seguro Cibernético não substitui os investimentos em segurança digital. Ele funciona como uma camada complementar dentro de uma estratégia mais ampla de gestão de riscos, oferecendo capacidade de resposta, suporte especializado e recuperação financeira quando, apesar dos controles adotados, um incidente acontece. Além da indenização, o produto pode incluir serviços de prevenção, monitoramento, resposta a incidentes e gestão de crise, contribuindo para a continuidade dos negócios e a resiliência operacional das empresas”, afirma.

Fonte: CNseg, em 30.07.2026.