A era digital potencializou avanços inéditos, mas também impôs uma nova camada de vulnerabilidade. Somente no primeiro semestre deste ano, 253 alertas de incidentes foram emitidos pela plataforma de Compartilhamento de Incidentes Cibernéticos (CIC), da Confederação Nacional das Seguradoras (CNseg). Uma média mensal de 42 eventos.

Dos incidentes, o Alerta de Vulnerabilidade se destaca como o tipo mais comum de comunicação, com 43% do total, somando 108. Notícias sobre incidentes, Curiosidades e Fatos de cyber estão em segundo com 17%; e Campanhas de Phishing ou Fraudes em terceiro, com 16%.

Tipo de Evento	Volume	% do Total
Alerta de Vulnerabilidade	108	43%
Diversos (Notícias sobre incidentes, Curiosidades e Fatos de cyber)	43	17%
Campanhas de Phishing ou Fraudes	40	16%
Atualizações Críticas	37	15%
Regulamentação e Política	19	7%
Notícia de Incidentes	6	2%

O CIC promove a troca de informações sobre ataques entre empresas com confidencialidade garantida, visando reduzir o tempo de resposta e aumentar a resiliência do setor. A notificação das vulnerabilidades, com agilidade, ajuda as organizações a tomarem ações preventivas, como o isolamento de sistemas em risco ou a aplicação imediata de correções.

No ano passado, o Brasil registrou 356 bilhões de tentativas de ataques cibernéticos, movimentando cerca de R$ 17 bilhões em investimentos em segurança digital. Ainda assim, os prejuízos estimados chegaram a mais de R$ 2,3 trilhões, afetando cerca de 40 milhões de brasileiros.

No contexto corporativo, o aumento da superfície de exposição, impulsionado pela transformação digital, uso de serviços em nuvem e terceirização de processos, exige mais do que ferramentas tecnológicas: requer uma abordagem estratégica de gestão de riscos. Nesse cenário, o seguro de riscos cibernéticos vem ganhando protagonismo. Voltado exclusivamente para empresas, o produto oferece proteção contra danos causados por ataques virtuais, como vazamento de dados, interrupção de serviços, perdas financeiras e até ações judiciais por uso indevido de informações.

Essa necessidade não se limita às grandes corporações. As médias empresas, embora em crescimento e cada vez mais digitalizadas, enfrentam desafios ainda maiores diante da falta de estrutura para mitigar incidentes cibernéticos. Estudo da AON mostra que 55% delas ainda não buscam nenhuma proteção contra riscos digitais.
Para Victor Perego, membro da subcomissão de Linhas Financeiras da FenSeg, o seguro precisa estar alinhado à estratégia de gerenciamento de risco da empresa: “A interrupção do negócio, por exemplo, é uma das coberturas mais sensíveis. Mas é preciso entender qual o tempo de paralisação que a empresa consegue suportar antes de sofrer perdas irreversíveis. Essa análise define o melhor desenho de apólice e o período de carência de lucros cessantes.”

A legislação brasileira também evoluiu. A Circular SUSEP 638/2021 inseriu a cibersegurança no centro do sistema de controle interno das seguradoras, exigindo que todas as supervisionadas tenham políticas compatíveis com seu porte, grau de exposição e complexidade operacional. A norma também impõe o registro e comunicação de incidentes, capacitação contínua e monitoramento de terceiros com acesso a dados sensíveis.

>> Saiba mais sobre o CIC e as demais soluções oferecidas pela CNseg clicando aqui.

Fonte: CNseg, em 23.09.2025