Com faturamento de R$ 228,8 milhões em 2025, produto amplia serviços de resposta a incidentes, recuperação de sistemas, suporte jurídico e comunicação, enquanto PMEs ainda enfrentam baixa maturidade em proteção de dados

O Seguro Cibernético está mudando de função no mercado brasileiro. Em vez de atuar apenas como um mecanismo de reembolso depois de um ataque, o produto passa a integrar a gestão de crise, a continuidade operacional e a governança das empresas, mobilizando especialistas desde a detecção do incidente até a recuperação dos sistemas e da confiança dos clientes.

Entre 2021 e 2025, o faturamento do ramo cresceu 121,7% e alcançou R$ 228,8 milhões, segundo dados da Confederação Nacional das Seguradoras (CNseg) reunidos no material que deu origem a esta análise. Em outro recorte, considerando o período de janeiro a setembro, a arrecadação avançou de aproximadamente R$ 70,5 milhões, em 2021, para R$ 173 milhões, em 2025, enquanto as indenizações ficaram em torno de R$ 28 milhões.

O crescimento dos prêmios em ritmo superior ao dos pagamentos não significa, por si só, menor risco. A leitura mais relevante é que parte crescente do valor do seguro está nos serviços agregados à apólice: equipes de resposta, perícia digital, recuperação de dados, suporte jurídico, comunicação de crise e orientação para a retomada dos negócios.

Por que o Seguro Cibernético está mudando?

A mudança acompanha a evolução dos ataques digitais e da dependência das empresas em relação à tecnologia. Um incidente pode interromper sistemas de vendas, meios de pagamento, emissão de notas fiscais, plataformas de atendimento, produção industrial, logística e acesso a dados de clientes.

Nesse contexto, esperar o fim da crise para calcular o prejuízo deixou de ser suficiente. O problema mais urgente passa a ser conter o ataque, entender o que aconteceu, restaurar a operação e cumprir as obrigações legais e regulatórias.

As apólices modernas de riscos cibernéticos costumam reunir dois grandes blocos de proteção. O primeiro cobre responsabilidades decorrentes do incidente, como danos a terceiros, custos de defesa e despesas relacionadas à proteção de dados. O segundo é voltado diretamente à resposta operacional, permitindo que a empresa acione os serviços contratados assim que identifica o ataque.

A Federação Nacional de Seguros Gerais (FenSeg) explica que as coberturas podem envolver investigação do incidente, recuperação do ambiente tecnológico, assistência especializada disponível durante a crise, responsabilidade civil, lucros cessantes e suporte de comunicação quando o caso se torna público.

O Seguro Cibernético, portanto, passa a funcionar como um plano de contingência previamente estruturado. Em vez de improvisar fornecedores e procedimentos no momento mais crítico, a organização aciona uma rede de profissionais já preparada para responder.

Como o seguro atua durante um ataque cibernético?

O Seguro Cibernético pode participar de três etapas da gestão do risco: preparação, resposta e recuperação. As coberturas e os serviços variam entre apólices, mas o desenho do produto tem convergido para esse ciclo.

Antes do incidente: prevenção e prontidão

A contratação costuma começar com questionários de risco e análise dos controles existentes. Esse

processo pode funcionar como um diagnóstico inicial da governança digital da empresa.

Entre as práticas avaliadas com frequência estão:

- autenticação multifator;
- controle de acessos;
- inventário de sistemas e dados;
- atualização de softwares;
- cópias de segurança;
- testes de restauração;
- plano de resposta a incidentes;
- treinamento de funcionários;
- avaliação de fornecedores.

Dependendo da apólice, a empresa também pode ter acesso a consultorias de segurança da informação, testes de vulnerabilidade e recomendações para reduzir a exposição.

A subscrição deixa, assim, de observar apenas o tamanho da empresa ou o volume de dados tratados. Ela passa a considerar a capacidade da organização de prevenir, identificar e responder a incidentes.

Durante o incidente: contenção e gestão da crise

Quando um ataque é detectado, podem ser mobilizados especialistas em resposta a incidentes e forense digital para identificar a origem, a extensão e os sistemas afetados.

A apólice pode prever despesas relacionadas a:

- investigação técnica;
- contenção do ataque;
- recuperação do ambiente digital;
- negociação em casos de extorsão, dentro dos limites legais e contratuais;
- suporte jurídico;
- comunicação com clientes e parceiros;
- relações públicas e assessoria de imprensa;
- notificação de titulares e autoridades, quando necessária.

Essa atuação integrada é especialmente importante porque um incidente cibernético raramente pertence a uma única área. Tecnologia, jurídico, comunicação, compliance, atendimento e direção executiva precisam tomar decisões coordenadas e, muitas vezes, sob forte pressão de tempo.

Depois do ataque: continuidade e recuperação

A retomada pode envolver reconstrução de bases de dados, reinstalação de aplicações, reforço dos controles de segurança e recuperação da receita perdida durante a paralisação.

Quando contratada, a cobertura de interrupção de negócios pode indenizar perdas decorrentes da indisponibilidade de sistemas essenciais, observados os limites, as franquias e os períodos definidos na apólice.

A recuperação também possui uma dimensão reputacional. Vazamentos de dados, indisponibilidade de serviços e invasões de canais oficiais podem reduzir a confiança de clientes, fornecedores e investidores. Por isso, o suporte de comunicação deixou de ser acessório e passou a integrar alguns programas de resposta.

Por que o seguro passou a fazer parte da governança?

O Seguro Cibernético é cada vez mais tratado como componente ativo da governança porque sua contratação exige que a empresa conheça os próprios ativos, dados, sistemas críticos e fornecedores.

Na prática, o processo de subscrição pode induzir a organização a:

- mapear informações e sistemas essenciais;
- documentar responsabilidades;
- formalizar políticas de segurança;
- testar planos de continuidade;
- estabelecer rotinas de backup;
- avaliar dependências tecnológicas;
- integrar o risco digital ao mapa corporativo de riscos.

Esse movimento aproxima o seguro das agendas de compliance, continuidade dos negócios e proteção de dados.

Em 2024, a Superintendência de Seguros Privados (Susep) criou o Grupo de Trabalho Seguros e Segurança Cibernética para estudar a segurança digital do setor supervisionado e os desafios e oportunidades trazidos pela economia digital. O grupo trabalhou em dois eixos: novos seguros para a economia digital e adequação do sistema de cibersegurança do mercado à Política Nacional de Cibersegurança. O trabalho já foi concluído e resultou em relatório final.

A iniciativa regulatória reforça que o tema não se limita à cobertura de vazamentos. Ele envolve resiliência operacional, novos riscos tecnológicos e a própria capacidade do mercado segurador de responder à digitalização da economia.

Qual é a relação entre Seguro Cibernético e LGPD?

A Lei Geral de Proteção de Dados Pessoais (LGPD) exige que agentes de tratamento adotem medidas técnicas e administrativas capazes de proteger dados pessoais contra acessos não autorizados, destruição, perda, alteração ou tratamento inadequado.

O seguro não substitui essas obrigações. Também não transforma uma empresa despreparada em organização automaticamente compatível com a legislação.

Sua função é complementar os controles de segurança e fornecer recursos financeiros, técnicos e jurídicos quando ocorre um incidente coberto.

Entre as despesas que podem aparecer nas apólices estão:

- avaliação do incidente;
- orientação sobre comunicação à Autoridade Nacional de Proteção de Dados (ANPD);
- notificação dos titulares;
- defesa em procedimentos administrativos e judiciais;
- investigação forense;
- atendimento às pessoas afetadas;
- gestão de crise.

A cobertura efetiva depende das cláusulas contratadas e da possibilidade jurídica de indenização de cada despesa. Multas punitivas, condutas intencionais e falhas conhecidas e não corrigidas podem receber tratamento restritivo ou ser excluídas.

A LGPD também vale para pequenas empresas?

Sim. Microempresas, empresas de pequeno porte, startups e outros agentes de tratamento de pequeno porte permanecem submetidos à LGPD, embora a ANPD tenha criado regras simplificadas

para algumas obrigações.

A Resolução CD/ANPD nº 2 permite, por exemplo, registros simplificados de operações e políticas de segurança adequadas à estrutura e ao volume de atividades do pequeno negócio. A norma, porém, determina que essas organizações adotem medidas administrativas e técnicas essenciais para proteger os dados pessoais.

Os pequenos agentes de tratamento não são obrigados, como regra geral, a indicar um encarregado pelo tratamento de dados. Quando não fazem essa indicação, precisam disponibilizar um canal de comunicação com os titulares. A própria resolução considera a nomeação do encarregado uma prática positiva de governança.

A ANPD também mantém um guia de segurança da informação e um checklist voltados especificamente a agentes de tratamento de pequeno porte. Os materiais abordam controles mínimos e oferecem modelos simplificados para apoiar a adequação.

Por que as PMEs estão especialmente expostas?

Pequenas e médias empresas costumam reunir três fatores de vulnerabilidade: forte dependência de tecnologia, menor estrutura de segurança e pouca capacidade financeira para contratar especialistas durante uma crise.

Uma loja virtual pode deixar de vender se o sistema sair do ar. Um escritório pode perder acesso aos documentos dos clientes. Uma clínica pode ter prontuários indisponíveis. Uma empresa de serviços pode ficar sem emitir notas fiscais ou processar pagamentos.

O material-base cita pesquisa segundo a qual 80% dos pequenos empreendedores já ouviram falar da LGPD, mas apenas 5% afirmam conhecer muito a legislação e 77% não adotaram providências concretas de adequação.

Embora esses percentuais precisem ser observados dentro do recorte e da metodologia da pesquisa original, eles ilustram uma situação recorrente: muitos pequenos negócios conhecem a lei pelo nome, mas ainda não incorporaram proteção de dados, segurança da informação e resposta a incidentes aos processos cotidianos.

O Sebrae destaca que a proteção de dados em pequenos negócios envolve políticas, procedimentos, prevenção de acessos não autorizados, backups e preparação para vazamentos, tanto para cumprir a legislação quanto para preservar a confiança de clientes e parceiros.

Nesse cenário, o seguro pode funcionar como acesso compartilhado a especialistas que uma PME dificilmente manteria de forma permanente.

Como o seguro pode ajudar uma pequena empresa?

Para uma PME, o principal valor do Seguro Cibernético pode estar menos na indenização final e mais na disponibilidade imediata de uma estrutura de resposta.

Uma apólice adequada pode oferecer, conforme as condições contratadas:

- central de atendimento para comunicar o ataque;
- especialistas em contenção e perícia;
- recuperação de dados;
- suporte jurídico;
- orientação para notificações;
- apoio de comunicação;
- cobertura de interrupção de negócios;
- recursos para retomada da operação.

A FenSeg informa que o serviço de resposta pode ser acionado antes mesmo de existir uma reclamação formal de terceiros. Essa antecipação é decisiva em ataques que se espalham rapidamente ou comprometem sistemas essenciais.

O seguro, entretanto, não elimina a necessidade de governança mínima. Uma empresa sem backups, com sistemas desatualizados e sem controle de acessos pode ter maior dificuldade de contratação, enfrentar prêmio mais elevado ou ficar sujeita a exclusões.

O que muda para as grandes empresas?

Nas grandes organizações, o Seguro Cibernético tende a integrar estruturas mais amplas de governança, continuidade operacional e risco de terceiros.

Essas empresas operam com redes complexas de fornecedores, ambientes em nuvem, sistemas legados, diferentes jurisdições e grande volume de dados pessoais e corporativos.

Por isso, a análise não se limita ao risco interno. Ela inclui a possibilidade de que um fornecedor, prestador de tecnologia ou parceiro comercial se torne a porta de entrada para o ataque.

O material-base cita levantamento internacional segundo o qual aproximadamente metade das violações analisadas ocorreu na cadeia de suprimentos. A informação reforça a importância de verificar controles de terceiros, cláusulas contratuais, planos de continuidade e responsabilidades em caso de incidente.

Para grandes empresas, o seguro pode apoiar:

- exercícios simulados de crise;
- revisão de planos de resposta;
- avaliação de fornecedores críticos;
- estruturação de programas multinacionais;
- definição de limites e camadas de cobertura;
- integração entre cyber, responsabilidade civil e seguro patrimonial.

O que é risco cyberfísico?

Risco cyberfísico é o incidente que começa em sistemas digitais e produz consequência física ou operacional.

Entre os exemplos estão:

- paralisação de uma fábrica;
- falha em sistema de energia;
- interrupção de serviço hospitalar;
- comprometimento de equipamentos conectados;
- impacto sobre infraestrutura crítica;
- danos a produtos ou instalações controladas digitalmente.

Esse tipo de evento desafia as fronteiras tradicionais entre coberturas. Um mesmo ataque pode produzir perda de dados, interrupção de negócios, dano material, responsabilidade civil e prejuízo a terceiros.

O relatório do grupo de trabalho criado pela Susep parte justamente da necessidade de estudar riscos da economia digital que ultrapassam a concepção mais restrita do Seguro Cibernético.

Para o mercado, o desafio é definir com clareza qual apólice responde por cada dano, como evitar lacunas entre diferentes contratos e como dimensionar perdas capazes de se espalhar simultaneamente por várias empresas.

O seguro cobre qualquer ataque?

Não. O Seguro Cibernético transfere parte do impacto financeiro e operacional, mas não cobre todo tipo de ocorrência.

As exclusões e limitações variam, mas podem envolver:

- atos dolosos de administradores ou sócios;
- falhas conhecidas e deliberadamente não corrigidas;
- ausência de controles declarados no questionário de risco;
- guerra cibernética e atos patrocinados por Estados;
- danos anteriores à vigência;
- descumprimento intencional de obrigações;
- perdas não mensuráveis de reputação;
- valores acima do limite contratado.

A empresa também precisa observar franquias, períodos de espera, sublimites e requisitos para acionamento dos serviços.

Por isso, TI, jurídico, comunicação, gestão de riscos e área financeira devem participar da contratação. Uma apólice tecnicamente sofisticada pode continuar inadequada quando não reflete os sistemas críticos, as dependências operacionais e os cenários reais de interrupção.

O Seguro Cibernético substitui investimentos em segurança?

Não. O seguro complementa os controles de segurança e a governança, mas não substitui prevenção, treinamento, atualização tecnológica, backups e planejamento.

Na prática, seguradoras e empresas possuem interesses convergentes: reduzir a probabilidade do incidente e limitar sua severidade.

Ao condicionar aceitação, preço e capacidade de cobertura à adoção de medidas básicas, o seguro também atua como indutor de boas práticas.

A empresa que conhece seus ativos, testa a restauração dos dados, controla acessos e simula crises tende a responder melhor ao ataque, reduzir perdas e apresentar um risco mais compreensível para a seguradora.

De indenização a infraestrutura de resiliência digital

O avanço do Seguro Cibernético no Brasil reflete uma transformação maior: os riscos digitais deixaram de ser exclusivamente técnicos e passaram a afetar receita, reputação, contratos, cadeias de fornecedores e serviços essenciais.

Nesse novo cenário, a pergunta não é apenas quanto a seguradora pagará depois do incidente. Também importa saber quem será acionado nas primeiras horas, como a operação continuará, quais autoridades deverão ser comunicadas e de que forma a confiança será reconstruída.

Para grandes empresas, o seguro se aproxima das agendas de governança, continuidade e gestão de riscos complexos. Para PMEs, pode representar acesso a uma estrutura especializada que dificilmente seria contratada de forma independente.

O produto não impede o ataque, mas pode reduzir o improviso, acelerar a recuperação e limitar os efeitos financeiros, jurídicos e reputacionais da crise. É essa combinação de proteção e capacidade de resposta que faz o Seguro Cibernético deixar de ser apenas um cheque de reembolso para se tornar parte da infraestrutura de resiliência digital das organizações.

Fonte: CNseg, em 20.07.2026