FGV | INSTITUTO DE INOVAÇÃO EM SEGUROS E RESSEGUROS

20

NOTA TÉCNICA

Seguro Cibernético; uma análise das coberturas oferecidas pelo mercado

DEZEMBRO 2024

As Notas Técnicas do Instituto de Inovação em Seguros e Resseguros da Fundação Getulio Vargas (FGV IISR) são textos para discussão a respeito de matérias relevantes para a regulação do mercado de seguros. Analisam temas atuais que procuram inovar na regulação do setor. Apresentam o resultado de pesquisas e estudos feitos no FGV IISR. As opiniões e colocações feitas nos textos são de responsabilidade de seus autores e não representam a posição da Fundação Getulio Vargas.

APRESENTAÇÃO

O mercado de Seguros e Resseguros no Brasil apresenta um grande potencial de crescimento e é um segmento de grande relevância para o desenvolvimento socioeconômico do país. A utilização dos produtos e serviços desta indústria pela população brasileira ainda é bastante limitada. O desenvolvimento de pesquisas e a realização de debates com a presença da academia, agentes do setor, reguladores, parlamentares e representantes da sociedade em geral são fatores importantes para a realização do potencial de crescimento deste setor.

Nesse sentido, em 2021, a Fundação Getulio Vargas (FGV), em conjunto com diversos agentes do mercado e reguladores que atuam no setor, decidiram criar o **Instituto de Inovação em Seguros e Resseguros (IISR)**. O Instituto possui o propósito de contribuir para a transformação da indústria de seguros e resseguros no Brasil e impulsionar o desenvolvimento do país, através do desenvolvimento de pesquisas, organização de debates e oferta de cursos para os profissionais do setor.

Além da FGV participam do **Conselho Consultivo do IISR** empresas, reguladores e organizações que atuam direta ou indiretamente nos segmentos de seguros, resseguros, tecnologia e infraestrutura. O Conselho se reúne mensalmente com o objetivo de identificar temas relevantes para o desenvolvimento de pesquisas e organização de debates. A estrutura e os procedimentos de funcionamento do Conselho garantem a total independência e isenção acadêmica da FGV.

São atividades principais do IISR:

- Produzir e difundir pesquisas e análises de alta qualidade relacionadas à inovação e tendências futuras na Industria de Seguros no Brasil;
- Acompanhar os movimentos mercadológicos, regulatórios e tecnológicos, em nível global que possam criar impacto na dinâmica da indústria de Seguros no Brasil;
- Detectar as primeiras ideias e debates emergentes sobre questões políticas, econômicas e sociais relativas à Industria de Seguros no Brasil;
- Promover uma conexão de qualidade entre a geração de conhecimento acadêmico e os gestores públicos e privados, decisores políticos, regulatórios e da iniciativa privada;
- Desenvolver e promover entendimento amplo sobre o papel e a importância da indústria de Seguros na economia e na sociedade por meio de pesquisa acadêmica, publicações, conferências e debate ativo com formuladores de políticas, reguladores, supervisores, acadêmicos e outros constituintes importantes.

MANTENEDORES

APOIO INSTITUCIONAL

FGV | INSTITUTO DE INOVAÇÃO EM SEGUROS E RESSEGUROS

FICHA TÉCNICA

Pesquisadores

Eugenio Augusto Franco Montoro
(FGV EAESP)

Luiz Guilherme Pessoa Cantarelli
(FGV DIREITO RIO)

20

NOTA TÉCNICA

Seguro Cibernético; uma análise das coberturas oferecidas pelo mercado

O seguro cibernético tem se consolidado como um instrumento indispensável em um mundo cada vez mais digitalizado e interconectado, em que os riscos cibernéticos representam uma ameaça crescente para empresas de todos os portes. No Brasil, apesar de ainda estar em estágio inicial de desenvolvimento, o mercado tem apresentado sinais claros de expansão, refletidos tanto no aumento da procura por apólices quanto na diversificação das coberturas oferecidas pelas seguradoras. Dados recentes destacam o impacto de eventos como ataques de ransomware, violações de dados e interrupções de serviços, que não apenas comprometem a continuidade dos negócios, mas também geram prejuízos financeiros e reputacionais consideráveis. Nesse contexto, o seguro cibernético desponta não apenas como uma ferramenta de proteção, mas também como um estímulo à adoção de boas práticas de segurança cibernética.

FGV | INSTITUTO DE INOVAÇÃO EM SEGUROS E RESSEGUROS

Embora os avanços sejam evidentes, o mercado brasileiro de seguros cibernéticos enfrenta desafios significativos. Entre eles, estão a dificuldade de precificação devido à escassez de dados históricos sobre sinistros e o desconhecimento do público-alvo sobre os benefícios e limitações desse tipo de produto. Tais questões foram amplamente discutidas em Mesa-redonda sobre Desafios da Cibersegurança e o Seguro Cibernético promovida pelo IISR-FGV, um evento que reuniu seguradoras, resseguradoras e prestadoras de serviços de tecnologia, promovendo um diálogo essencial para entender as lacunas existentes e os potenciais caminhos de evolução do setor. O encontro destacou, ainda, a importância de harmonizar regulamentações e alinhar práticas empresariais às exigências de proteção de dados estabelecidas pela Lei Geral de Proteção de Dados (LGPD) e por normas setoriais.

Neste artigo, busca-se complementar as reflexões geradas no debate com uma análise empírica das apólices de seguro cibernético atualmente oferecidas no mercado brasileiro. A partir de um estudo detalhado de contratos de seguradoras representativas — AIG, Zurich, Allianz, AXA, Tokio Marine, AKAD e Bradesco/Swiss Re —, o trabalho procura responder a questões fundamentais: quais riscos são cobertos? Como as coberturas variam entre as empresas? Existe convergência nas práticas contratuais ou predominam divergências significativas? Essas perguntas são especialmente relevantes para avaliar a capacidade do setor de oferecer soluções que atendam às crescentes demandas por proteção cibernética de maneira eficaz e acessível.

Ao integrar os insights do debate setorial com a análise das práticas de mercado, o artigo pretende oferecer uma visão abrangente sobre o estado atual do seguro cibernético no Brasil. Mais do que mapear os desafios e as tendências, a proposta é contribuir para um entendimento mais profundo das dinâmicas que moldam esse segmento e fomentar discussões sobre como aprimorar a proteção contra riscos cibernéticos no país. Assim, espera-se que o estudo sirva como base para reflexões futuras, tanto no campo acadêmico quanto na prática do mercado segurador.

Panorama da cibersegurança no Brasil

A cibersegurança tem ganhado destaque crescente no Brasil, impulsionada pela combinação de uma infraestrutura digital em expansão e um aumento expressivo nos ataques cibernéticos. Dados recentes mostram que o Brasil ocupa uma posição intermediária no *Cybersecurity Capacity Maturity Model for Nations* da Universidade de Oxford, refletindo avanços relevantes, mas ainda insuficientes para equiparar o país às nações mais maduras no tema. Ataques como ransomware, que cresceram 51% na América Latina, ilustram a vulnerabilidade do ambiente digital brasileiro, especialmente em setores críticos como saúde, finanças e varejo. Esses ataques frequentemente resultam em violações de dados

sensíveis, interrupções operacionais e prejuízos financeiros que, no Brasil, chegam a custos médios de US$ 5,17 milhões em casos envolvendo nuvens públicas.

Embora as ameaças sejam significativas, a resposta do Brasil ainda carece de uniformidade. Iniciativas como a Política Nacional de Cibersegurança (2023) e o fortalecimento do Comitê Nacional de Cibersegurança (CNCiber) buscam criar diretrizes e fomentar a cooperação internacional. Regulamentações setoriais, como a Resolução Conjunta nº 6/2023, que obriga instituições financeiras a compartilharem indícios de fraudes, também demonstram esforços para mitigar riscos cibernéticos. No entanto, a fragmentação de estratégias entre diferentes setores e a falta de conscientização sobre segurança da informação entre pequenas e médias empresas comprometem a eficácia dessas medidas.

A introdução da Lei Geral de Proteção de Dados (LGPD) representou um marco regulatório importante, ao estabelecer diretrizes claras para o tratamento de dados pessoais e incentivar práticas mais robustas de cibersegurança. No entanto, muitas organizações ainda enfrentam dificuldades para alcançar plena conformidade com a lei, seja pela ausência de recursos técnicos e financeiros, seja pela resistência cultural em priorizar investimentos preventivos. É comum que empresas enxerguem a segurança cibernética como um custo, e não como uma estratégia essencial para a continuidade dos negócios.

O seguro cibernético

O seguro cibernético é um instrumento criado para proteger empresas contra os impactos financeiros e operacionais de incidentes cibernéticos, que incluem desde ataques como ransomware até falhas na segurança de sistemas e vazamentos de dados. Sua característica mais notável é a abrangência das coberturas, que frequentemente combinam indenizações por perdas diretas do segurado, como lucros cessantes ou custos de extorsão, com responsabilidades por danos causados a terceiros, como violações de dados sensíveis. Essa dualidade, que abrange riscos de primeira e terceira partes, reflete uma tentativa de oferecer proteção integrada em um cenário em que a interdependência tecnológica torna as vulnerabilidades mais complexas e imprevisíveis. A nível regulamentar, esse tipo de seguro é enquadrado no ramo Responsabilidade Civil Compreensivo Riscos Cibernéticos, ou simplesmente (RC Riscos Cibernéticos)[1].

1 CARLINI, Angélica. Nova regulação dos seguros de responsabilidade civil no brasil e os seguros para riscos cibernéticos. Revista IBERC, vol. 5, n.2, p. 1-17, 2022.

Aspecto interessante dos seguros cibernéticos é o fato de que, além das indenizações propriamente ditas, há uma tendência de que a sua contratação acompanhe uma série de serviços técnicos ancilares. Mais do que um simples mecanismo de transferência de risco, o seguro cibernético inclui, em muitos casos, serviços como consultoria de segurança, suporte técnico emergencial e estratégias de mitigação de danos. Essa abordagem busca ajudar as empresas não apenas a recuperar-se de incidentes, mas também a reduzir a probabilidade de novos ataques, promovendo uma gestão mais proativa dos riscos cibernéticos. É nesse sentido, como já trabalhado em nota anterior deste instituto[2], que se pode dizer que o seguro cibernético tem o potencial funcionar como um instrumento regulatório da cibersegurança no Brasil.

Apesar de sua relevância no atual contexto de crescente exposição digital, o mercado de seguros cibernéticos no Brasil enfrenta desafios significativos. Um dos principais problemas é a baixa conscientização das empresas sobre os benefícios dessa modalidade de seguro. Muitas organizações, especialmente pequenas e médias empresas, enxergam o seguro cibernético como um custo adicional em vez de uma ferramenta estratégica de proteção. Essa percepção é agravada pela tendência de delegar a decisão sobre a contratação à área de TI, que frequentemente se concentra em aspectos técnicos e pode não considerar os impactos financeiros e operacionais mais amplos que um incidente cibernético pode causar.

Outro desafio significativo é a dificuldade de precificar os riscos cibernéticos devido à ausência de dados históricos consistentes e à natureza dinâmica das ameaças digitais. Essa falta de referências concretas torna complexo para as seguradoras avaliar a probabilidade e a gravidade dos incidentes, o que pode impactar tanto o valor das apólices quanto a clareza das condições contratuais.

Além disso, muitas empresas enfrentam dificuldades para compreender plenamente as apólices de seguro cibernético. A linguagem técnica e as exclusões

2 Ver Nota Técnica 10 – Seguro e Segurança Cibernética, disponível em: https://fgviisr.fgv.br/sites/default/files/2024-03/Nota%20Tecnica%2010%20 %20Seguro%20e%20Seguranc%CC%A7a%20Ciberne%CC%81tica%20.pdf

específicas podem gerar confusão, dificultando que os segurados tenham uma visão clara do que está efetivamente coberto. Esse desafio de comunicação reforça a importância de maior transparência e clareza na elaboração dos contratos, para que as empresas possam tomar decisões informadas sobre a contratação e uso de seguros cibernéticos.

O quais riscos são cobertos? As coberturas básicas

Que no plano teórico, o seguro cibernético se coloca como um instrumento de proteção contra riscos e de promoção de boa governança é algo estabelecido. Questão que se coloca é: como, na prática, são desenhados esses contratos? A presente nota técnica se propõe a iniciar uma resposta a essa pergunta. Embora não seja possível, dados os limites deste trabalho, respondê-la em sua completude, uma primeira análise que se pode fazer diz respeito às coberturas dos contratos de seguro cibernético. Afinal, que riscos são cobertos pelas apólices atualmente negociadas em mercado?

A fim de responder essa pergunta, foram coletadas e analisadas sete Condições Contratuais de seguros cibernéticos negociados por 7 companhias de seguros que operam no Brasil: AIG[3], Zurich[4], AKAD[5], Allianz[6], AXA[7], Tokio Marine[8] e Bradesco/ Swiss Re[9]. Esses documentos foram extraídos dos próprios sites institucionais das seguradoras. De antemão, observa-se que eles possuem níveis de complexidade diferenciados, que podem ser ilustrados a partir da mera comparação de tamanho dos documentos: enquanto alguns são mais pormenorizados e chegam a quase cem páginas, outros são mais sucintos e não chegam a trinta.

3 AIG. Cyber Edge: Condições Gerais, Seguro de proteção de dados e responsabilidade cibernética. Disponível em: https://www.aig.com.br/content/dam/aig/lac/brazil/documents/brochure/cg-seguro-protecao-de-dados-e-responsabilidade-cibernetica.pdf.coredownload.pdf. Acesso em: 20/11/2024.

4 Zurich. Zurich Cyber Solution: Apólice de Responsabilidade Civil por Violação de Segurança e Privacidade. Disponível em: https://edge.sitecorecloud.io/zurichinsurf8c0-zwpshared-prod-d824/media/project/zurich-headless/brazil/docs/protecao-digital/2023/cc---15414900493_2016-61--v20231214.pdf. Acesso em: 20/11/2024.

5 AKAD. CyberRisk Pro: Condições Gerais. Disponível em: https://akadseguros.com.br/content/uploads/2023/06/condicoes-gerais-seguro-de-cyber-akad.pdf. Acesso em: 20/11/2024.

6 Allianz. Condições Gerais: Responsabilidade Civil por Ataques Cibernéticos. Disponível em: https://www.allianz.com.br/content/dam/onemarketing/iberolatam/allianz-br/documents/outros-seguros/responsabilidade-civil/riscos-ciberneticos/Resp-Civil-por-Ataques-Ciberneticos_Agosto-2017.pdf. Acesso em: 20/11/2024.

7 AXA. Seguro de Responsabilidade Cibernética e Proteção de Dados A Base de Reclamações com Notificação – Condições Gerais. Disponível em: https://strgaccdataaxaprod.blob.core.windows.net/strapi-uploads/assets/AXA_Riscos%20Cibern%C3%A9ticos_15414.603184.2023-74_20220203_Vigente.pdf. Acesso em: 20/11/2024.

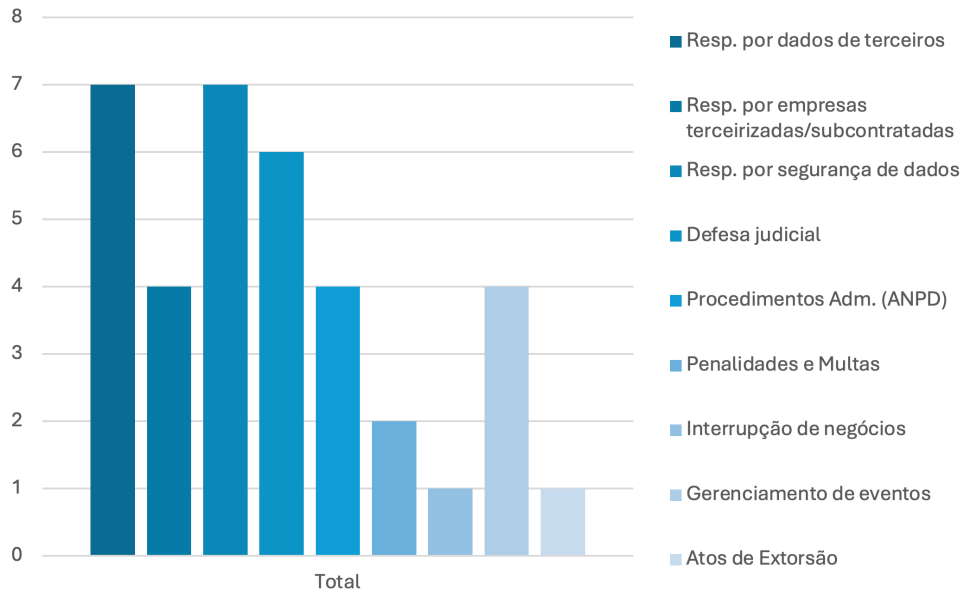
8 Tokio Marine. Seguro de Responsabilidade e proteção cibernética (apólice à base de reclamações com cláusula de notificações) – Condições Gerais. Disponível em: https://www.tokiomarine.com.br/wp-content/uploads/2024/09/tokio-marine-riscos-digitais-condicoes-gerais-092024v01.pdf. Acesso em: 20/11/2024.

9 Bradesco; Swiss Re. Condições Gerais. Disponível em: https://www.bradescoseguros.com.br/clientes/produtos/outros-seguros/riscos-ciberneticos-pme. Acesso em: 20/11/2024.

No que diz respeito às coberturas, é necessário separar aqui entre dois casos: as coberturas "básicas" e as "extensões" ou coberturas "adicionais". Embora nem todas as seguradoras analisadas operem dessa forma, é possível dizer que a maior parte delas realiza a separação entre essas condições. As coberturas ditas "básicas", normalmente, são aquelas mínimas que devem ser contratadas pelos segurados para fins de realização do negócio. Já as coberturas adicionais se somam às básicas para estender o campo dos riscos cobertos pelo seguro, não podendo em geral ser contratadas de maneira isolada.

Dada a especificidade e a dificuldade de comparação das coberturas adicionais, a presente seção se preocupa especificamente com as coberturas básicas. A seção seguinte descreve, qualitativamente, as coberturas adicionais oferecidas. Isso posto, pergunta-se: o que as seguradoras, minimamente, oferecem a seus clientes em matéria de proteção contra riscos cibernéticos? O gráfico abaixo oferece uma primeira ideia da situação do mercado:

Gráfico 1: Coberturas básicas - Seguro Cibernético



Fonte: Elaboração própria, 2024.

Como se pode observar, as coberturas foram classificadas em 9 categorias: responsabilidades por dados de terceiros; responsabilidade por empresas terceirizadas/subcontratadas; responsabilidade por segurança de dados; defesa judicial; procedimentos administrativos; penalidades e multas; interrupção de negócios; gerenciamento de eventos; e atos de extorsão. A construção dessas categorias buscou respeitar, dentro do possível, a forma com que as próprias seguradoras tendem a organizar.

Dentre as coberturas mais comuns está o que se optou por denominar de "responsabilidade por dados de terceiros". Compreende-se aqui eventuais situações de responsabilização dos segurados em decorrência da divulgação de informações pessoais e/ou corporativas que detiverem e tenham sido, de maneira indevida, divulgadas. A classificação (e sua separação de casos de responsabilidade de segurança de dados), segue em linhas gerais o desenho das apólices analisadas. Todas as apólices cubram esse tipo de evento, ainda que sob denominações diversas – o que é esperado em se tratando de um seguro de responsabilidade civil. Não se quer dizer, com isso, que as coberturas sejam idênticas, mas que são, em linhas gerais convergentes.

A mesma situação se verifica com os casos de responsabilidade por segurança de dados. Aqui, se enquadram os riscos referentes a perdas que possam decorrer do acesso indevido aos sistemas do segurado, da introdução de códigos maliciosos ou outros tipos de ataques cibernéticos que possam importar consequências como a perda ou destruição de dados, sua alteração e/ou sua divulgação indevida. Novamente, embora haja diferenças na forma com que as coberturas são redigidas, havendo redações mais detalhadas e redações mais genéricas acerca desses riscos, verifica-se que todas elas em alguma medida abrangem os chamados "riscos de segurança".

Também se mostraram comuns, embora não presentes em todos os casos, as coberturas referentes aos custos de defesa judicial dos segurados. A curiosidade, no entanto, é que uma das empresas não inclui os custos de defesa judicial na cobertura, porem o faz em cláusula própria referente à atuação do segurado em decorrência de processos judiciais. Na prática, portanto, os produtos de todas as seguradoras contemplam, cada um ao seu modo, custos judiciais.

Três tipos de coberturas foram encontrados por quatro vezes nas apólices analisadas. A primeira delas é o que se denominou de "responsabilidade por empresas terceirizadas/subcontratadas". O problema aqui reside na possibilidade de responsabilização

do segurado por violações de dados que ocorram através de empresas prestadoras de serviços, subcontratadas e/ou terceirizadas. Quatro das apólices identificadas mencionam expressamente essa possibilidade, enquanto outras três são silentes sobre o tema.

Igualmente recorrentes são as coberturas referentes a procedimentos administrativos, notadamente procedimentos no âmbito da Autoridade Nacional de Proteção de Dados (ANPD). Aqui faz-se referência aos custos decorrentes de investigações e da necessidade de apresentação de defesa perante a ANPD. Essas coberturas podem ou não vir acompanhadas de previsão de pagamento das multas em decorrência de eventos de violação de dados. É de se observar, no entanto, que a inclusão do pagamento de multas nas coberturas básicas ocorre em apenas duas das apólices encontradas.

O terceiro tipo de cobertura recorrente foi o que aqui se denominou de "gerenciamento de eventos". A denominação, propositadamente genérica, ser propõe a compreender todas as medidas voltadas para a mitigação dos danos causados pelo ataque cibernético, notificação de terceiros e órgãos governamentais, consultoria de imagem, criação de serviços de *call center* para atendimento dos interessados e outros serviços. É de se observar aqui que esse tipo de cobertura pode variar bastante em relação ao seu conteúdo, dado que compreende uma série de serviços. O mais comum é que as seguradoras forneçam coberturas referentes a alguns serviços de gerenciamento de eventos em detrimento de outros.

Por fim, as coberturas encontradas com menor frequência nas condições básicas foram as de "interrupção de negócios" e "atos de extorsão". No primeiro caso, cobre-se os prejuízos dos segurados em decorrência da interrupção dos seus negócios em razão de ataque ou falha dos sistemas cibernéticos. No segundo, faz-se referência a pagamentos realizados pelo segurado a fim de afastar uma ameaça de extorsão cibernética.

Dessa forma, o que se pode aprender com a análise das apólices? Em primeiro lugar, que o produto do seguro cibernético, embora jovem, é razoavelmente bem definido. Na sua base estão as coberturas de responsabilidade civil por dados de terceiros e em decorrência de problema de segurança cibernética do segurado, que se somam, no mais das vezes, à cobertura de custos de defesa. A essas coberturas, adicionam-se outras que cobrem uma ampla gama de

situações, desde lucros cessantes, responsabilidade violação de dados decorrente das atividades de terceiros e apoio em processos administrativos regulatórios. Embora convergentes no plano geral, parece haver significativo espaço para divergências no campo das condições contratuais, podendo cada uma focar em diferentes aspectos dos riscos de trabalho no ambiente virtual.

É de se observar, contudo, que a análise aqui realizada diz respeito somente às coberturas básicas. Os produtos oferecidos, na realidade, oferecem opções mais amplas ao segurado, com a possibilidade de que adquiram coberturas adicionais que complementam aquelas oferecidas como básicas. É sobre o que se discorre, brevemente, na seção seguinte.

As coberturas adicionais

A análise das coberturas básicas oferece alguma facilidade em termos de classificação e comparação entre diferentes condições contratuais de seguros negociados no mercado, tendo em vista se tratar de um campo mais reduzido de clausulas que, em alguma medida, guardam grande similaridade entre diferentes seguradoras. Diferente é o caso das coberturas adicionais, que se apresentam como mais numerosas e contextualmente específicas. Não se procurará aqui quantificar, mas apenas mencionar algumas das coberturas adicionais comuns.

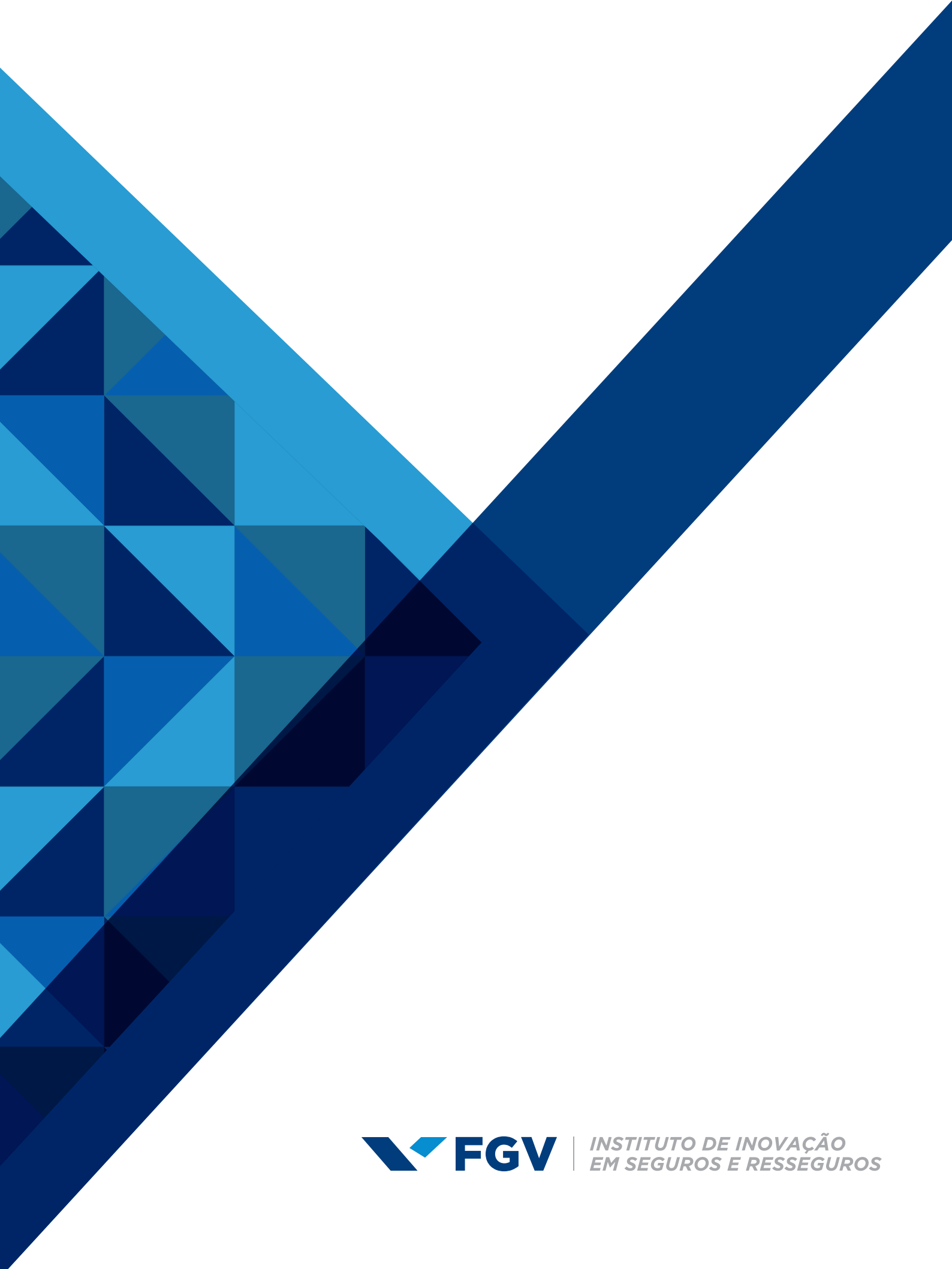
A possibilidade de que as coberturas adicionais sejam contratadas para a complementação do produto remediam, em grande medida, eventuais diferenças que foram mencionadas na seção anterior. Tome-se como ilustração aqui as condições contratuais do seguro cibernético oferecido por uma das seguradoras. Ela oferece, como coberturas básicas, coberturas de responsabilidade civil pela privacidade e pela segurança dos dados, abrangendo nisso também os custos de defesa e eventos causados por terceiros subcontratados. Não obstante, verifica-se que as condições permitem a contratação de coberturas muito mais amplas, que abrangem, dentre outras: gerenciamento de eventos, despesas emergenciais para a proteção contra danos ainda não ocorridos, perdas do segurado decorrentes da interrupção de negócios, despesas com extorsão, despesas com procedimentos administrativos regulatórios (incluindo multas), além do que especificam como danos de publicação eletrônica que tenha sido realizada pelo próprio segurado e que possa gerar alguma situação de responsabilização.

Como se pode ver, boa parte dessas coberturas adicionais corresponde às categorias descritas na seção anterior. Se, na sua modalidade mínima, o seguro garantia da companhia limita as coberturas a apenas alguns dos sinistros normalmente contemplados pelo seguro cibernético, na prática é dado os clientes a possibilidade de expandir essas coberturas de acordo com o que entenda ser mais aderentes aos seus negócios.

Uma grande parte das coberturas adicionais oferecidas dizem respeito aos serviços que aqui foram denominados de "gerenciamento de eventos". Como observado na seção anterior, se procurou reunir uma série de serviços nessa categoria e se considerou que as coberturas básicas compreendem "gerenciamento de eventos" quando alguns desses serviços são contemplados. No entanto, é possível tanto que as coberturas básicas não contemplem qualquer serviço de gerenciamento de eventos quanto que, contemplando alguns desses serviços, deixem de contemplar outros que possam ser de interesse do contratante. As coberturas adicionais oferecem, nesse sentido, a oportunidade de complementação do produto. Dentre as despesas com "gerenciamento de eventos" para que se disponibiliza cobertura adicional encontram-se desde os custos com gestão de imagem e comunicação ao consumidor até perícias e despesas de salvamento e recuperação de sistemas.

Se consideradas as coberturas básicas juntamente às coberturas adicionais, diferentes produtos de seguro, pelo menos no que diz respeito às suas condições contratuais, tornam-se significativamente próximos. Não se quer dizer aqui que eles sejam iguais na extensão dos riscos cobertos, mas que eles ofereçam coberturas que, em grande medida se sobrepõem – com diferenças na forma de organizá-las, discriminá-las e de definir aquilo que consta como cobertura básica e como adicional. Isso permite algum grau de customização do produto pelo cliente, de acordo com as suas necessidades. Eventuais diferenças encontradas, possivelmente, decorrem de esforços de diferenciação competitiva dos produtos e dos públicos-alvo diversos para quem são dirigidas as respectivas apólices.

A dificuldade que se coloca, seguindo o apontamento anteriormente realizado, é: como comunicar ao cliente exatamente o que é oferecido por cada um desses produtos. Além já serem naturalmente complexos, a possibilidade de que se adicionem elementos dentre as coberturas oferecidas adiciona um novo nível de complexidade ao processo de contratação – isso sem nem considerar as clausulas de exclusão de risco presentes nesses contratos. Esse é um desafio que se coloca para o mercado e para os reguladores de seguros.


FGV
INSTITUTO DE INOVAÇÃO
EM SEGUROS E RESSEGUROS