RELATÓRIO FINAL

GRUPO DE TRABALHO

Seguros & Segurança Cibernética

SUSEP

Superintendência de Seguros Privados

Relatório Final[1]

Grupo de Trabalho sobre Segurança Cibernética e Novos Seguros da Economia Digital

[1] As atas de reunião, apresentações e referências utilizadas podem ser encontradas no processo SEI nº 15414.631676/2024-31.

Dezembro/2024

Introdução

O Grupo de Trabalho (GT) Seguros & Segurança Cibernética foi constituído pela Portaria Susep nº 8.323, de 26 de agosto de 2024 e prorrogado pela Portaria Susep nº 8348, de 11 de novembro de 2024, com o propósito de discutir e elaborar estudos técnicos sobre a segurança cibernética do setor supervisionado pela Autarquia[2] e os desafios e oportunidades que o desenvolvimento da economia digital traz para o setor segurador brasileiro. A iniciativa decorre da prioridade conferida pela Susep, no Planejamento Estratégico Institucional 2024-2027, à segurança, integridade e transparência dos dados e informações dentro do seu perímetro de atuação.

Tabela 1 – Participantes externos do Grupo de Trabalho Seguros & Segurança Cibernética

I. Ministério da Fazenda (MF);	XIII. Câmara Brasileira da Economia Digital (Câmara e-net);
II. Ministério do Desenvolvimento, Indústria, Comércio e Serviços (MDICS);	XIV. Associação Brasileira de Fintechs (ABFintechs);
III. Ministério da Gestão e Inovação (MGI);	XV. Associação Brasileira de Insurtechs (ABI);
IV. Serviço Federal de Processamento de Dados (Serpro);	XVI. Escola de Negócios e Seguros (ENS);
V. Confederação Nacional das Empresas de Seguros Gerais, Previdência Privada e Vida, Saúde Suplementar e Capitalização (CNseg);	XVII. Associação Nacional de Certficação Digital (ANCD);
VI. Federação Nacional de Seguros Gerais (Fenseg);	XVIII. Instituto de Inovação em Seguros e Resseguros (IISR- FGV);
VII. Federação Nacional de Capitalização (FenaCap);	XIX. Associação Nacional de Certificação Digital (ANCD);
VIII. Federação Nacional dos Corretores de Seguros Privados e de Resseguros, de Capitalização, de Previdência Privada, das Empresas Corretoras de Seguros e de Resseguros (Fenacor);	XX. Instituto Brasileiro de Direito do Seguro (IBDS);
IX. Federação Nacional de Previdência Privada e Vida (Fenaprevi);	XXI. Associação Internacional do Direito do Seguro;
X. Federação Nacional das Empresas de Resseguros (Fenaber);	XXII. Federação Brasileira de Bancos (FEBRABAN);
XI. Associação Nacional das Resseguradoras Locais (ANre);	XXIII. Cássio Gomes Amaral;
XII. Confederação Nacional do Comércio de Bens, Serviços e Turismo (CNC);	XXIV. Rodrigo Ventura.

Fonte: Portaria Susep nº 8.323, Anexo I.

[2] Resumidamente, seguros, previdência complementar aberta, capitalização e resseguros.

O Diretor da Diretoria de Regulação Prudencial e Estudos Econômicos (DIRPE) da Susep foi responsável por coordenar as atividades do Grupo. Os demais integrantes eram servidores da Autarquia, bem como representantes dos órgãos e entidades, de direito público ou privado, e especialistas individualmente nomeados acima (Portaria Susep nº 8.323, Anexo I).

O GT foi composto por dois subgrupos, voltados aos seguintes eixos temáticos (Portaria Susep nº 8.323, art. 3º):

I. Adequação do sistema de cibersegurança do mercado supervisionado à Política Nacional de Cibersegurança; e
II. Novos Seguros para Economia Digital: para além do risco cibernético.

As atividades de ambos os subgrupos ocorreram em paralelo, com reuniões semanais de cada um deles, resultando em um total de 10 encontros entre setembro e outubro de 2024. As reuniões, com duração de até três horas, consistiram em painéis ou sequências de apresentações sobre temas selecionados, feitas pelos participantes ou eventuais indicados por eles, acompanhadas de debates entre os presentes para aprofundar as discussões.

A segunda etapa do trabalho foi a elaboração deste relatório, entre novembro e dezembro de 2024[3], para documentar as principais conclusões alcançadas pelo Grupo de Trabalho. Dessa forma, é importante destacar que **as sugestões aqui veiculadas não representam necessariamente a opinião da Susep**, configurando um registro do diálogo entre representantes dos setores público e privado sobre os tópicos em questão.

O restante do documento está estruturado da seguinte forma: a próxima seção aborda os seguros e segurança cibernética em contexto internacional, destacando padrões de boas práticas encontrados em outras jurisdições; a seção posterior apresenta o contexto nacional, com um levantamento das normas relevantes para a discussão em tela e uma apresentação dos principais indicadores sobre o mercado de seguros cibernéticos no país; depois, são registradas as principais considerações de cada subgrupo. As conclusões, ao final, sintetizam os principais resultados.

Contexto internacional

A insegurança cibernética é percebida como um dos principais riscos globais de curto prazo, figurando entre as três preocupações mais relevantes para os representantes de governos e do setor privado recentemente consultados pelo Fórum Econômico Mundial (WEF, 2024). O mesmo organismo aponta em outra pesquisa que: (i) há uma crescente iniquidade entre as organizações em termos de resiliência cibernética; (ii) as tecnologias emergentes, como a inteligência artificial generativa, exacerbarão os desafios relacionados à resiliência cibernética; e (iii) os riscos cibernéticos dos ecossistemas (isto é, considerando os parceiros, fornecedores e prestadores de serviço de uma firma) estão se tornando mais problemáticos – com uma crescente percepção de que as regulações sobre cibersegurança e proteção de dados podem atenuar esses desafios (WEF; ACCENTURE, 2024).

[3] O Grupo de Trabalho precisava concluir as suas atividades em até 60 (sessenta) dias, prorrogados por igual período, a partir de 28 de agosto de 2024 (Portarias Susep nº 8.323 e 8348).

Um levantamento feito com executivos de diferentes jurisdições traz resultados igualmente alarmantes: (a) os custos das violações de dados e o número das violações de alto valor estão em expansão; (b) os ataques a provedores de serviço em nuvem foram apontados como a principal preocupação cibernética, mas cerca de um terço das empresas consultadas afirma não ter um plano para gestão desses riscos; e (c) cerca de um terço das empresas consultadas afirma não seguir consistentemente algumas práticas convencionais de segurança cibernética (PWC, 2024). Os mesmos executivos apontam as seguintes regulamentações como as mais importantes para o futuro das suas organizações: (i) inteligência artificial, (ii) harmonização das leis de proteção de dados; (iii) relatórios para gestão, estratégia e governança dos riscos cibernéticos; e (iv) resiliência operacional (idem).

Grosso modo, esses resultados apontam para quatro constatações gerais. Primeiro, os riscos cibernéticos são importantes e resultam em perdas cada vez mais frequentes e expressivas, com grande potencial de gerar perdas catastróficas[4]. Segundo, a capacidade de gerenciar esses riscos varia entre organizações, em parte associado ao tamanho, escopo e local das suas operações. Terceiro, grandes transformações nas tecnologias de informação – incluindo aquelas associadas à computação em nuvem e à inteligência artificial generativa, mesmo que cada uma tenha atingido graus de maturidade diferentes – são capazes de alterar a superfície de riscos cibernéticos. Quarto, a regulação tem um papel relevante a desempenhar, estabelecendo condições mínimas para o tratamento dos riscos em questão.

Existem diferentes respostas para lidar com esses desafios, com esforços internacionais para definição de boas práticas. Com efeito, os padrões internacionais desempenham um papel particularmente relevante para definição de boas práticas de segurança cibernética, sejam eles desenvolvidas no âmbito dos setores públicos ou privados.

Os integrantes do Grupo de Trabalho identificaram a Cybersecurity Framework (CSF), do National Institute of Standards and Technology (NIST), órgão público dos EUA, como um exemplo importante. Esse conjunto de padrões, diretrizes e práticas foi desenhado para ser flexível e, com isso, poder ser adotado independentemente do tamanho, maturidade e sofisticação de uma organização. O seu núcleo, que está disponível em português, fornece uma taxonomia dos resultados que uma organização pode aspirar a alcançar, em termos de segurança cibernética, com base em seis funções essenciais – governar, identificar, proteger, detectar, responder e recuperar (NIST, 2024).

Os padrões divulgados pela International Organization for Standardization (ISO) e pela International Electrotechnical Commission (IEC), para sistemas de gestão de segurança da

[4] Em julho de 2024, um incidente cibernético sem precedentes paralisou diversas operações globais, especialmente no setor aéreo. A causa do caos foi um erro operacional durante uma atualização de software da empresa de segurança cibernética *CrowdStrike*. Essa falha em cascata afetou sistemas de companhias aéreas, bancos, hospitais e outras instituições em diversos países (BBC, 2024). A interrupção nos serviços aéreos, por exemplo, resultou no cancelamento de milhares de voos, causando transtornos a milhões de passageiros e gerando prejuízos bilionários para as companhias aéreas (CNN Brasil, 2024). Embora a *CrowdStrike* tenha rapidamente corrigido o problema, os efeitos colaterais do apagão cibernético foram sentidos por dias, evidenciando a fragilidade da infraestrutura global diante de falhas em sistemas críticos.
(Exame, 2024).
As estimativas de perdas financeiras exatas decorrentes desse incidente ainda estão sendo calculadas e podem variar de acordo com as diferentes fontes. No entanto, é consenso entre os especialistas que o impacto econômico foi significativo, afetando tanto as empresas diretamente envolvidas quanto a economia global como um todo.

informação, também foram mencionados no GT. Conhecidos como a família de padrões ISO/IEC 27.000, esses documentos tratam das políticas, processos e orientações, bem como dos recursos e atividades relacionadas, que são gerenciados por uma organização para proteger seus ativos de informação. As principais referências são o ISO/IEC 27.001, que descreve os requerimentos gerais; o ISO/IEC 27.006, que aborda os requerimentos para órgãos certificadores; e o ISO/IEC 27.009, que trata dos requerimentos específicos para diferentes setores (ISO; IEC, 2018).

Ambos os conjuntos de padrões identificados buscam ser flexíveis, com alguma sobreposição entre os temas que abordam, mas é notável como a família ISO/IEC 27.000 oferece recomendações mais granulares, quando comparadas com aquelas publicadas pelo NIST. A diferença estaria, em parte, associada aos padrões ISO/IEC contemplarem processos de certificação e auditoria por terceiros.

Sem a pretensão de exaurir os exemplos cabíveis, pode-se registrar ainda duas outras referências mencionadas pelos integrantes do Grupo de Trabalho. Uma delas é o Critical Security Controls do Center for Internet Security (CIS), que é descrito como um conjunto de boas práticas prescritivo, priorizado e simplificado para fortalecimento segurança cibernética (CIS, 2024); e o outro é a estrutura COBIT da Information Systems Audit and Control Association (ISACA), para governança e gestão da informação e tecnologia de corporações (ISACA, 2019).

Em suma, existe uma multiplicidade de padrões internacionais relacionados à segurança cibernética, que não necessariamente competem entre si e podem até mesmo ser complementares. Cada organização, seja ela pública ou privada, pode avaliar esses diferentes modelos e, com base em características como tamanho, setor e locais de atuação, escolher aqueles que considera mais adequados para as suas atividades.

Há ainda uma série de padrões, recomendações e orientações divulgadas específicas para os sistemas financeiros. Por exemplo, o G7 definiu os elementos fundamentais da segurança cibernética para entidades do setor financeiro, que são: (i) estratégia e estrutura de cibersegurança; (ii) governança; (iii) avaliação de riscos e controles; (iv) monitoramento; (v) resposta; (vi) recuperação; (vii) compartilhamento de informação; e (viii) aprendizado contínuo (G7, 2016).

O mesmo organismo definiu alguns anos depois os elementos fundamentais das avaliações sobre cibersegurança no sistema financeiro. Esses elementos incluem tanto os resultados desejáveis, quanto os componentes das avaliações realizadas pelas próprias entidades, seus supervisores e avaliadores independentes (G7, 2023).

A *International Association of Insurance Supervisors* (IAIS) é o organismo multilateral responsável pela definição de princípios, padrões e outros materiais de referência para a supervisão do setor de seguros. A sua atuação em matérias relacionadas à segurança cibernética se insere nos trabalhos sobre resiliência operacional, iniciados ainda na década passada (IAIS, 2016; 2018; 2023; 2024).

O seu ponto de partida foi a identificação da resiliência operacional como uma matéria conectada aos *Insurance Core Principles* (ICP), que constituem a principal referência entre os demais trabalhos da IAIS e oferecem uma base global para a supervisão do setor de seguros. Nesse contexto, a resiliência operacional passou a ser entendida como um resultado que se conecta, entre outros temas, com a resiliência cibernética, a terceirização de serviços de tecnologia da informação e a gestão da continuidade de negócios (IAIS, 2023).

Mais recentemente, a IAIS desenvolveu uma proposta de objetivos para resiliência operacional, com o intuito de apoiar os supervisores a desenvolver e fortalecer as suas abordagens frente ao tema (IAIS, 2024). Esses objetivos foram reproduzidos na tabela 2, para referência.

Tabela 2 – Objetivos para resiliência operacional do setor de seguros

Relação entre resiliência operacional, governança e gestão de risco operacional
A seguradora implementa e monitora uma abordagem eficaz para resiliência operacional que é apoiada por sua estrutura de governança
A abordagem da seguradora para resiliência operacional alavanca e é integrada com sua estrutura de gestão de risco operacional de forma consistente, abrangente e robusta
Elementos chave de uma abordagem sólida para resiliência operacional
A seguradora identifica e mantém um inventário atualizado de seus serviços críticos e interdependências
A seguradora define tolerâncias de impacto para interrupção de seus serviços críticos
A seguradora autoavalia e testa sua capacidade de suportar e se recuperar de cenários de interrupção operacional grave e garante que ações sejam tomadas para melhorar a resiliência operacional com base nas lições aprendidas
A seguradora gerencia efetivamente incidentes operacionais, incluindo, mas não se limitando a incidentes cibernéticos, afetando serviços críticos
A seguradora gerencia e mitiga o impacto do risco de tecnologia para serviços críticos implementando uma abordagem eficaz para resiliência operacional que aborda as fases de proteção, detecção, resposta e recuperação
A seguradora planeja, testa e implementa mudanças de forma controlada
A seguradora desenvolve, implementa, testa e atualiza seu Plano de Continuidade de Negócios e Plano de Recuperação de Desastres para garantir que possa responder, recuperar, retomar e restaurar a um nível pré-definido de operação após uma interrupção em tempo hábil
A seguradora gerencia efetivamente relacionamentos com provedores de serviços terceirizados, incluindo relacionamentos intragrupo e n-ésimas partes
Objetivos para supervisores de seguros
Ao avaliar a resiliência operacional da seguradora, os supervisores coordenam dentro da autoridade supervisora para capturar todas as áreas potenciais de vulnerabilidade
Os supervisores compartilham informações e cooperam com outros supervisores com o objetivo de minimizar riscos
Os supervisores cooperam e se comunicam de forma transparente com as partes interessadas
Os supervisores apoiam uma cultura de aprendizado e melhoria contínuos com relação à resiliência operacional dentro da autoridade supervisora

Fonte: IAIS (2024).

A indústria de seguros privados se situa em uma posição particular em qualquer discussão sobre segurança cibernética porque, ao mesmo tempo em que esse setor precisa se mostrar resiliente, ele também oferece proteção financeira e pode auxiliar na difusão de boas práticas

para os demais segmentos de uma economia. Uma estimativa recente aponta para a existência de uma lacuna de proteção para riscos cibernéticos[5] de aproximadamente US$ 944 bilhões por ano, em escala global, evidenciando amplas oportunidades para redução do nível de perdas e crescimento da cobertura securitária (GFIA, 2023).

Com base nessa avaliação, a redução da lacuna de proteção cibernética passa por: (i) promover a conscientização sobre e incentivar a prevenção de riscos cibernéticos; (ii) promover um ambiente com melhor resiliência cibernética, especialmente entre empresas e ativos de infraestrutura crítica; (iii) criar uma estrutura harmonizada de relatórios de incidentes cibernéticos para obter uma visão melhor da frequência e gravidade de incidentes importantes; e (iv) não proibir pagamentos de *ransomware*[6, 7] (GFIA, 2023).

Feitas essas breves considerações sobre o contexto internacional, cabe agora descrever os aspectos associados à realidade brasileira.

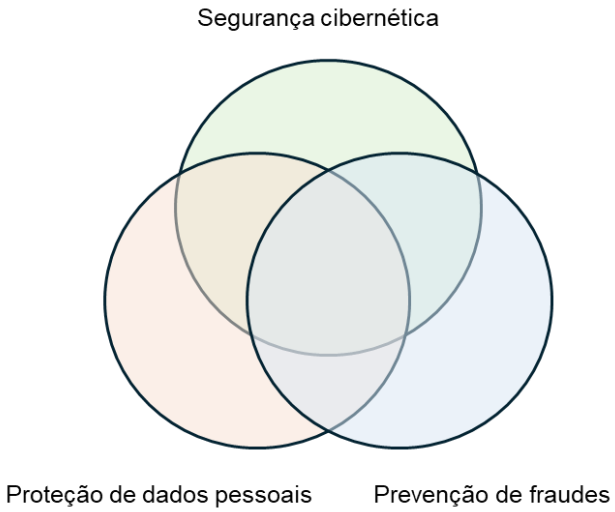
Contexto nacional

O cenário brasileiro pode não ser tão diferente daquele observado em outras jurisdições, quando se considera que os riscos cibernéticos resultam em perdas cada vez mais frequentes e expressivas, porém é necessário ressaltar os esforços para mitigação desses riscos no país. O custo médio das violações de dados – pessoais ou corporativos – no Brasil chegou a US$ 1,36 milhão em 2024, ante US$ 1,22 milhão em 2023, valor que permanece consideravelmente abaixo da média mundial (US$ 4,88 milhões) e da América Latina (US$ 4,16 milhões) (IBM, 2024).

Os integrantes do Grupo de Trabalho apontaram, desde o início, a importância das discussões sobre segurança cibernética no Brasil contemplarem aspectos de proteção de dados pessoais, bem como de prevenção de fraudes. A figura 1 ilustra essa percepção de que existe uma sobreposição ao menos parcial entre os assuntos mencionados, que levou à necessidade de abordá-los, mesmo que tentativamente, ao longo das atividades que resultaram neste relatório.

Figura 1 - Representação da conexão entre os temas abordados

[5] A lacuna de proteção para riscos cibernéticos é definida, nesse caso, como a diferença entre as perdas econômicas de primeira ordem devido a ataques cibernéticos (i.e., exclui perdas de segunda ordem, como danos reputacionais) e as perdas cobertas por seguros (GFIA, 2023).
[6] Programa malicioso que bloqueia acessos a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido (ANBIMA, 2021). O Departamento do Tesouro dos EUA emitiu orientação informando que as companhias que facilitarem o pagamento de resgates para ransomware, incluindo seguradoras, seriam passíveis de sanções (DEPARTMENT OF TREASURY, 2020; 2021).
[7] Há uma tendência global em que os países podem criar regulamentações para proibir o pagamento de resgastes de ransomware, de modo a coibir o avanço, financiamento de grupos organizados criminosos e lavagem de dinheiro (GAFI, 2023).



Fonte: Elaboração própria a partir das discussões do Grupo de Trabalho.

Dessa forma, uma pesquisa estima que, em 2023, ocorreram 3,7 milhões de tentativas de fraude no comércio digital no Brasil, representando cerca de R$ 3,5 bilhões no total e uma média de R$ 944 mil por tentativa (CLEARSALE, 2024). No setor de seguros privados, outro levantamento afirma que os avisos de sinistros comprovadamente fraudulentos alcançaram a marca de R$ 1 bilhão, quando somados o segundo semestre de 2023 e o primeiro semestre de 2024 (CNSEG, 2024).

As grandezas mencionadas não são comparáveis entre si, nem mesmo representam todos os danos e prejuízos associados aos temas em questão. Ainda assim, elas evidenciam conjuntamente a importância da segurança cibernética, proteção de dados pessoais e prevenção de fraudes para a economia brasileira.

Panorama jurídico

Uma das contribuições do Grupo de Trabalho ora descrito foi identificar o conjunto de normas relevantes para os temas em questão. Esses diplomas, que estão reunidos na tabela 3, envolvem desde referências legais mais abrangentes até normas específicas para os setores supervisionados pela Susep.

O primeiro marco abordado foi a Lei nº 13.709/2018, também conhecida como Lei Geral de Proteção de Dados (LGPD), que disciplina o tratamento de dados pessoais, inclusive por meios digitais, por pessoa natural ou jurídica de direito público ou privado. Destacadamente, a norma criou a Agência Nacional de Proteção de Dados (ANPD) para, entre outras competências, zelar pela proteção de dados pessoais e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação.

O Grupo de Trabalho teve a oportunidade de dialogar com uma representante da ANPD logo no início das atividades, para explorar a conexão entre proteção de dados pessoais, segurança cibernética e seguros. Algumas publicações da referida Autoridade foram indicadas como referências nessa discussão, incluindo os Guias Orientativos para Segurança da Informação para Agentes de Tratamento de Pequeno Porte (ANPD, 2021), para Definições dos Agentes de

Tratamento de Dados Pessoais e do Encarregado (ANPD, 2022) e para Tratamento de Dados Pessoais pelo Poder Público (ANPD, 2023).

Tabela 3 – Normas identificadas pelo Grupo de Trabalho

Norma	Tema	Ano
Lei nº 13.709	Lei Geral de Proteção de Dados Pessoais (LGPD)	2018
Lei nº 13.874	Declaração de Direitos de Liberdade Econômica	2019
Lei nº 14.063	Assinaturas eletrônicas	2020
MP nº 2.200-2	Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil)	2002
Decreto nº 11.856	Política Nacional de Cibersegurança (PNCiber)	2023
Decreto nº 11.200	Plano Nacional de Segurança de Infraestruturas Críticas (Plansic)	2022
Decreto nº 9.573	Política Nacional de Segurança de Infraestruturas Críticas (PNSIC)	2018
Resolução CNSP Nº 453	Letra de Risco de Seguro (LRS)	2022
Resolução CNSP nº 416	Sistema de Controles Internos, a Estrutura de Gestão de Riscos e a atividade de Auditoria Interna	2021
Resolução CNSP nº 415	Sistema de Seguros Aberto (Open Insurance)	2021
Resolução CNSP nº 413	Emissão de bilhete por meios remotos	2021
Resolução CNSP nº 408	Meios remotos nas operações de seguros	2021
Resolução CNSP nº 383	Sistema de Registro de Operações (SRO)	2020
Circular Susep nº 700	Instrução de processos de autorização da Susep	2024
Circular Susep nº 638	Requisitos de segurança cibernética para as entidades supervisionadas pela Susep	2021
Circular Susep nº 637	Seguros do grupo responsabilidades	2021
Circular Susep nº 619	Política de segurança e sigilo de dados e informações das registradoras	2020

Fonte: Elaboração própria.

O Decreto nº 11.856/2023, que institui a Política Nacional de Cibersegurança (PNCiber), o Decreto nº 11.200/2022, que aprova o Plano Nacional de Segurança de Infraestruturas Críticas

(Plansic), e o Decreto nº 9.573/2018, que aprova a Política Nacional de Segurança de Infraestruturas Críticas (PNSIC), representam outras três referências essenciais. Esses decretos foram abordados pelo Grupo de Trabalho em um diálogo com representante do Gabinete de Segurança Institucional (GSI), que permitiu explorar (i) a conexão entre as atividades da Susep e os princípios e objetivos da PNCiber; e (ii) a criticidade do setor de seguros privados para a economia brasileira.

Ademais, a Lei nº 14.063/2020 e a Medida Provisória nº 2.200-2/2001 foram citadas recorrentemente nas discussões, como referências sobre as assinaturas eletrônicas e seus possíveis usos para autenticação dos segurados em sistemas disponibilizados pelas seguradoras. A esse respeito, cabe notar que a legislação brasileira classifica as assinaturas eletrônicas em simples, avançada ou qualificada, estando essa última categoria reservada para aquelas que utilizam os certificados digitais emitidos pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) (BRASIL, 2020).[8]

Com relação às normas emanadas pelo Conselho Nacional de Seguros Privados (CNSP), a Resolução CNSP nº 294 de 2013 (atual 408 de 2021) foi identificada como uma primeira referência importante, por disciplinar a utilização de meios remotos na contratação dos produtos que especifica. A revisão, em 2017, foi um marco importante, diante do rápido avanço das inovações tecnológicas, tendo a Susep promovido flexibilização ao normativo com o objetivo de "colocar o setor de seguros alinhado com outros setores supervisionados, como bancos e mercado de capitais, no tocante ao uso de mecanismos reconhecidos envolvendo tecnologias digitais". (Susep, 2017).

---

[8] A esse respeito, os representantes da CNseg no GT entendem que: "*o entendimento de que a Lei nº 14.063 flexibilizou o uso do ICP-Brasil para interação entre pessoas e instituições privadas com os entes públicos e entre os próprios órgãos e entidades públicas ao estabelecer a assinatura eletrônica simples; assinatura eletrônica avançada; e assinatura eletrônica qualificada e reconhecer que os 3 (três) tipos de assinatura caracterizam o nível de confiança sobre a identidade e a manifestação de vontade de seu titular. Segundo exposição de motivos da Medida Provisória nº 983/2020, que deu origem à Lei nº 14.063, "A aplicação de tecnologias digitais por meio do uso de assinaturas eletrônicas e da digitalização de registros e documentos irá simplificar, desburocratizar, dar celeridade e evitar contato presencial em grande variedade de transações". Em 2023, Lei n.º 14.620/2023 inseriu novo parágrafo ao artigo 784, do Código de Processo Civil, para admitir que, nos títulos executivos constituídos ou atestados por meio eletrônico, é admitida qualquer modalidade de assinatura eletrônica prevista em lei. Dito de outra forma, ao acrescentar o § 4º ao art. 784 do CPC, a legislação passou a admitir - na constituição e no ato de atestar de títulos executivos extrajudiciais em meio eletrônico - qualquer modalidade de assinatura eletrônica desde que sua integridade seja conferida pela entidade provedora desse serviço, evidenciando mais uma vez a ausência de exclusividade da certificação digital do sistema ICP-Brasil. Qualquer medida diferente conflitaria com a Lei de Liberdade Econômica, na medida em que a obrigação de utilização de determinado tipo de assinatura pode representar uma ingerência indevida na atividade econômica, em especial a violação ao art. 4º da Lei nº 13.874/2019, que veda uma série de comportamentos da administração pública no exercício de regulamentação de norma pública, com visitas a evitar o abuso de poder regulatório, inclusive de maneira a, indevidamente, criar demanda artificial ou compulsória de produto, serviço ou atividade profissional, inclusive de uso de cartórios, registros ou cadastros. Além disso, a obrigatoriedade de utilização de determinado tipo de assinatura poderia promover aumento de custo para o consumidor, conflitando também com a iniciativa da Susep sobre a Política Nacional de Acesso ao Seguro. E por fim, o judiciário já se manifestou a esse respeito, declarando que A Lei 14620/2023, ao acrescentar o § 4º ao art. 784 do CPC, passou a admitir - na constituição e ateste de títulos executivos extrajudiciais em meio eletrônico - qualquer modalidade de assinatura eletrônica desde que sua integridade seja conferida pela entidade provedora desse serviço, evidenciando a ausência de exclusividade da certificação digital do sistema ICP-Brasil, vide RESP 2159442 – PR*"

Depois, a Resolução nº 415, do CNSP, que dispõe sobre a implementação do Sistema de Seguros Aberto (Open Insurance), foi tratada pontualmente, permitindo a identificação de padrões de segurança, equivalentes aos existentes em *Open Finance* que são usados como referência para as interfaces de programação de aplicação (APIs, na sigla em inglês) que caracterizam esse ambiente[9].

A Resolução nº 383, do CNSP, dispõe sobre o registro das operações de seguros, previdência complementar aberta, capitalização e resseguros e, dessa forma, constitui referência para o Sistema de Registro de Operações (SRO) - outra matéria abordada durante as reuniões do Grupo. Nesse contexto, a Circular nº 619, da Susep, dispõe sobre a política de segurança e sigilo de dados e informações das entidades registradoras credenciadas a prestarem o serviço de registro de operações de seguros, previdência complementar aberta e resseguros.

A Resolução nº 416, do CNSP, trata do Sistema de Controles Internos (SCI), da Estrutura de Gestão de Riscos (EGR) e a atividade de Auditoria Interna. Dessa forma, ela oferece o contexto necessário para definição dos requisitos de segurança cibernética que devem ser observados, dentro da categoria de risco operacional, pelas sociedades seguradoras, entidades abertas de previdência complementar, sociedades de capitalização e resseguradores locais.

A Circular nº 638, da Susep, estabelece essas exigências, contemplando, entre outros aspectos: (i) as políticas de segurança cibernética e seus requisitos mínimos; (ii) os processos procedimentos e controles efetivos para identificar e reduzir vulnerabilidades de forma proativa, bem como para detectar, responder e recuperar-se de incidentes; e (iii) a terceirização de serviços de processamento e armazenamento de dados. Os requisitos informacionais, como aqueles relacionados à comunicação às partes afetadas e à Susep no caso de incidentes, estão incluídos entre esses elementos.

De modo relacionado, a Circular nº 700, da Susep, estabelece que as entidades supervisionadas devem elaborar ou atualizar seus planos de negócio recorrentemente. Esses planos precisam conter, entre outros elementos, a política relativa à segurança cibernética e à proteção de dados, evidenciando o caráter essencial desses instrumentos para atuação no perímetro supervisionado.

Por fim, além dessas referências afeitas aos riscos operacionais das entidades supervisionadas, a Circular nº 637, da Susep, dispõe sobre os seguros do grupo responsabilidades. Estão incluídos nesse conjunto o ramo de seguro de Responsabilidade Civil Compreensivo Riscos Cibernéticos (RC Riscos Cibernéticos), cuja evolução é apresentada a seguir.

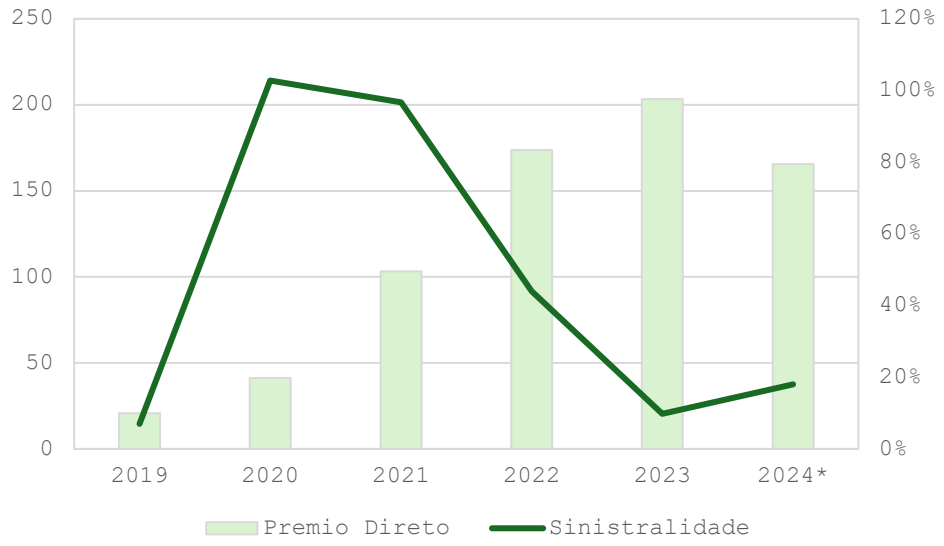
Evolução do mercado

[9] Como referência, ver os manuais de segurança disponibilizados pela Estrutura de Governança do Open Insurance em sua página na internet: https://opinbrasil.com.br/.

O ramo 327 (Compreensivo Riscos Cibernéticos) foi introduzido ao final de 2018 pela Circular nº 579, da Susep. O gráfico 1, abaixo, demonstra como a subscrição desse instrumento cresceu desde então, superando em 2023 a marca de R$ 200 milhões em prêmios diretos (último ano com informações completas, até a elaboração deste relatório).

Além do rápido crescimento, os primeiros anos desse produto registraram elevadas taxa de sinistralidade (medida como a razão entre prêmios ganhos e sinistros ocorridos). Como o gráfico 1 evidencia, a sinistralidade chegou a aproximadamente 103% em 2020 e 97% em 2021 – dois anos marcados pelos efeitos econômicos da pandemia da Covid-19, inclusive pelo aumento no número de incidentes cibernéticos.

Gráfico 1 – Responsabilidade Civil Compreensivo Riscos Cibernéticos
(R$ milhões; e % prêmios ganhos)



Fonte: Susep (2024). Nota: *Valores de 2024 apenas até setembro.

A sinistralidade caiu substancialmente desde então. Para ilustrar esse ponto, basta notar que, em 2021, os prêmios diretos alcançaram R$ 103 milhões e os sinistros ocorridos, R$ 75 milhões; enquanto dois anos depois, em 2023, os prêmios diretos quase duplicaram, chegando a R$ 203 milhões, e os sinistros ocorridos caíram para menos de um quarto, com R$ 18 milhões (Susep, 2024).

Essa ampla variação da taxa de sinistralidade é representativa dos eventos exógenos mencionados, mas pode indicar também adaptações nos processos de subscrição pelas seguradoras locais, à medida que o segmento de mercado em questão venha se amadurecendo. A esse respeito, nota-se também uma ampliação do número de empresas que operam nesse segmento – começando com 6 em 2019 e chegando a 11 em meados de 2024[10] (Susep, 2024).

[10] Dados para 2024 referem-se apenas até setembro, última informação publicada até a elaboração deste relatório.

Ainda assim, o ramo RC Risco Cibernético continua representando uma parcela muito pequena dos seguros de danos no geral. Em 2023, o ramo em questão recebeu menos de 0,2% dos prêmios para seguros de danos, evidenciando amplo espaço para seu crescimento.

Vale dizer também que a distribuição do ramo 327 é bastante concentrada em termos espaciais. Entre 2019 e 2023, os prêmios registrados na região sudeste representaram quase 90% do total nacional para o ramo em questão, sendo 70% desse mesmo montante contabilizado apenas em São Paulo (Susep, 2024).

Resumindo as observações apresentadas até o momento, o ramo RC Risco Cibernético cresceu rapidamente nos últimos anos, superando eventos exógenos que impactaram adversamente a sua sinistralidade. Contudo, o ramo em questão ainda representa uma parcela pequena do mercado de seguros de danos no país, particularmente concentrada no sudeste e, mais especificamente, no estado de São Paulo.

Principais Coberturas Ofertadas no mercado brasileiro

Como visto, o mercado de seguros cibernéticos no Brasil tem experimentado um crescimento exponencial nos últimos anos, impulsionado pela crescente digitalização das empresas e pelo aumento da frequência e complexidade dos incidentes cibernéticos. O Instituto de Inovação em Seguros e Resseguros da Fundação Getúlio Vargas (IISR/FGV) elaborou um estudo aprofundado sobre o tema, destacando a importância de compreender as coberturas disponíveis e suas limitações (FGV, 2023).

As coberturas oferecidas pelo ramo de responsabilidade civil de segurança cibernética são diversificadas e abrangentes, podendo ser divididas em três grandes grupos: resposta a incidentes, perdas do segurado e responsabilidade civil.

- Resposta a Incidentes: As coberturas de resposta a incidentes visam auxiliar as empresas na gestão de crises cibernéticas, desde a detecção até a resolução do problema. Incluem custos com especialistas em segurança, notificação de clientes, recuperação de dados, e até mesmo a contratação de serviços de relações públicas para gerenciar a reputação da empresa após um incidente.
- Perdas do Segurado: Essas coberturas protegem a empresa contra as perdas financeiras diretas decorrentes de um incidente cibernético, como a perda de receita, os custos com restauração de sistemas e os pagamentos de resgate em casos de *ransomware*. É importante destacar a cobertura de lucros cessantes, que indeniza a empresa pelos lucros que deixaria de obter em decorrência da interrupção de suas atividades.
- Responsabilidade Civil: As coberturas de responsabilidade civil protegem a empresa contra as responsabilidades legais decorrentes de um incidente cibernético que cause danos a terceiros. Incluem custos com defesa jurídica, indenizações por danos morais e materiais, e podem cobrir a responsabilidade por violação de dados pessoais, em conformidade com a LGPD.

Apesar da abrangência das coberturas, é importante destacar as exclusões, que são cláusulas contratuais que limitam a responsabilidade da seguradora. As principais exclusões incluem atos intencionais, guerras, catástrofes naturais, danos físicos e morais, perdas em instrumentos financeiros e eventos anteriores. Algumas exclusões podem ser consideradas ineficientes,

como a exclusão de danos físicos a hardware. Essa exclusão pode limitar a proteção das empresas em casos de ataques que danifiquem fisicamente seus equipamentos (FGV, 2023).

As exclusões existem nas coberturas por diversas razões, dentre as quais a incapacidade de mensuração atuarial e a natureza inseguravel do risco[11].Em que pesem muitas das exclusões serem relativamente comuns, como guerras e catástrofes naturais, no rol de exclusões frequentes trazidas pelos representantes do GT há algumas que poderiam, dadas algumas iniciativas, passarem a integrar o rol de eventos cobertos. Em particular, os integrantes do GT discutiram essa possibilidade para as coberturas de danos físicos a hardware.

É importante ressaltar que o mercado de seguros cibernéticos está em constante evolução, com novas coberturas e produtos sendo lançados regularmente.

Coberturas Não-Afirmativas

A cobertura não-afirmativa, ou *silent cyber coverage*, refere-se a situações em que apólices de seguro tradicionais não mencionam explicitamente a inclusão ou exclusão de riscos cibernéticos. Isso significa que o segurado e a seguradora podem ter diferentes interpretações sobre se uma apólice cobre ou não danos decorrentes de incidentes cibernéticos (IAIS, 2020). De acordo com a IAIS, do ponto de vista da supervisão de seguros, o crescimento do seguro cibernético gera preocupações, incluindo questões sobre a cobertura não-afirmativa e a acumulação de riscos, com potencial de perda catastrófica em diversos setores.

Algumas jurisdições de membros da OCDE também demonstraram preocupações com o tema e sugeriram ações para uma melhor clareza das coberturas inclusas e excluídas (OECD, 2017).

Coberturas disponíveis no exterior, mas ainda não oferecidas amplamente no Brasil

O mercado de seguros cibernéticos no Brasil, embora em constante crescimento, ainda apresenta algumas lacunas em relação aos países mais desenvolvidos. Algumas coberturas específicas, comuns em outros mercados, ainda não são amplamente oferecidas pelas seguradoras brasileiras.

Essa diferença pode ser decorrente de uma assimetria no estágio de maturidade dos mercados, da complexidade da mensuração dos riscos cibernéticos, ou mesmo da necessidade de aprimoramentos na regulamentação do setor no Brasil.

Algumas destas coberturas, incluem:

- Cobertura para perdas reputacionais: Essa cobertura indeniza o segurado pelas perdas financeiras decorrentes da deterioração da sua reputação após um incidente cibernético, como a diminuição do valor da marca.[12]

[11] **risco inseguravel** é aquele que, por suas características intrínsecas, não pode ser coberto por um seguro. Isso significa que as seguradoras não oferecem proteção contra esse tipo de evento, pois ele apresenta um grau de incerteza e potencial de perda que foge dos parâmetros tradicionais de avaliação de riscos.

[12] De certa forma outras perdas reputacionais já estão disponíveis no Brasil, como na cobertura de "lucros cessantes por perda reputacional", que cobre a perda de clientes por danos reputacionais em

- Cobertura para extorsão cibernética: Essa cobertura indeniza o segurado pelos pagamentos de resgate exigidos por hackers em casos de *ransomware*. Embora algumas seguradoras já ofereçam essa cobertura no Brasil, ela ainda não é tão comum quanto em outros países.
- Cobertura para fraudes financeiras com origem em ataques cibernéticos: Essa cobertura protege o segurado contra perdas financeiras causadas por fraudes cibernéticas.
- Cobertura para riscos emergentes: Essa cobertura é mais ampla e abrange uma variedade de riscos cibernéticos emergentes, como ataques de *deepfake*, ataques a IoT (internet das coisas) e ataques a redes 5G.

O oferecimento dessas coberturas no Brasil seria importante para um melhor alinhamento com as melhores práticas internacionais, uma proteção mais completa para as empresas, em particular micro, pequenas e médias, incluindo pessoas físicas, além de impulsionar o crescimento do mercado de seguros cibernéticos no Brasil, atraindo novos clientes e aumentando a competitividade entre as seguradoras.

É importante ressaltar que a oferta dessas coberturas depende de diversos fatores, que podem passar pela evolução da regulamentação, pela demanda do mercado e pela capacidade das seguradoras de avaliar e precificar esses riscos.

Classificação de Grupos e ramos

A norma da Susep que define os ramos e grupos de ramos de seguros é a Circular Susep nº 535/2016, alterada posteriormente por outras circulares, como a Circular Susep nº 579/2018, que introduziu formalmente o ramo de seguros cibernéticos no segmento de Responsabilidade Civil. Esse ramo é classificado no código 0327, conforme a tabela de codificação da Susep, que organiza os produtos de seguros para fins de controle e padronização regulatória.

Dada a diversidade de coberturas elencadas e suas naturezas, poderia ser conveniente estudar a conveniência e oportunidade de incluir novos códigos para os diferentes tipos de cobertura.

O papel regulatório do seguro

O seguro cibernético desempenha papel importante na mitigação das perdas decorrentes dos eventos cobertos, por meio da pulverização de riscos no sistema de seguros e resseguros global.

Contudo, há ainda um outro papel importante a ser desempenhado pelo seguro cibernético: o de instrumento de regulação, promovendo diretamente, através de serviços de gerenciamento de risco, medidas de aprimoramento da segurança cibernética de seus segurados (FGV, 2023).

As seguradoras desempenham um papel crucial na prevenção de riscos cibernéticos ao oferecer serviços como *cyber health checks*, análises de vulnerabilidades, consultorias e treinamentos em melhores práticas de cibersegurança. Além disso, elas fornecem serviços de

decorrência de uma ampla divulgação na mídia de um ataque cibernético ocorrido contra a empresa. A reparação do valor da marca, por não ser um bem tangível, de difícil mensuração e passível de ser contestada, não costuma ser coberta.

mitigação de danos após incidentes, incluindo assessoria jurídica. Dessa forma, contribuem para a melhoria da segurança dos segurados e a redução dos danos em caso de sinistros.

Da mesma forma, é possível promover essas boas práticas, por meio da criação de incentivos financeiros, como a redução de prêmios para empresas que implementam medidas de segurança adequadas, ou exigindo a adoção de padrões de segurança como condição para a contratação do seguro. Esta última opção, no entanto, tem grande potencial exclusivo, dificultando a eliminação das lacunas de proteção e reduzindo a eficiência do sistema.

Durante as reuniões do GT foi discutida a particular importância desse papel regulatório do seguro cibernético, uma vez que houve consenso quanto ao baixo nível de maturidade e conhecimento das empresas e dos altos custos de implantação e manutenção dos padrões exigidos, principalmente para micro, pequenas e médias empresas.

Compartilhamento de Dados de Incidentes Cibernéticos

Uma das melhores práticas na mitigação da frequência e severidade dos riscos cibernéticos é uma eficiente troca de dados entre os diversos participantes do ecossistema de segurança e resiliência cibernética. Algumas iniciativas já implantadas no Brasil valem ser citadas.

a. A CNseg possui um serviço específico para o compartilhamento de informações sobre incidentes cibernéticos, chamado de **Sistema de Compartilhamento de Incidentes Cibernéticos (CIC)**. Ele foi desenvolvido para permitir que as seguradoras associadas troquem informações sobre incidentes cibernéticos de maneira estruturada. O objetivo é aumentar a resiliência do mercado e facilitar a conformidade com regulamentações, como a **Circular Susep nº 638/2021**, que estabelece diretrizes sobre segurança cibernética. O sistema promove alertas e relatórios sobre incidentes, auxiliando as seguradoras na prevenção e resposta a ataques (CNSeg, 2024)

b. **CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil)**: Mantido pelo Comitê Gestor da Internet no Brasil (CGI.br), o CERT.br é uma referência no tratamento de incidentes cibernéticos e na conscientização sobre boas práticas de segurança. Ele fornece suporte técnico e promove a troca de informações entre diversas organizações.

c. **FEBRABAN (Federação Brasileira de Bancos)**: Possui iniciativas como o **Centro de Cibersegurança FEBRABAN**, que trabalha na proteção do setor bancário por meio da colaboração entre instituições financeiras.

d. **ABINC (Associação Brasileira de Internet das Coisas)**: Apesar de focada na Internet das Coisas, também aborda questões de segurança cibernética e promove fóruns para troca de informações.

e. **NIC.br (Núcleo de Informação e Coordenação do Ponto BR)**: Além de gerenciar o CERT.br, o NIC.br realiza projetos relacionados à segurança cibernética, incluindo estatísticas sobre ataques e eventos de segurança.

Taxonomias e padronizações para categorizar incidentes e perdas

A IAIS recomenda que supervisores e reguladores considerem, além das iniciativas de compartilhamento de dados, a padronização de taxonomias para aprimorar a análise e o entendimento dos riscos cibernéticos (IAIS, 2020). O relatório conclui que o fortalecimento das práticas de supervisão, aliado à capacitação técnica e à colaboração entre partes interessadas é fundamental para viabilizar o crescimento sustentável desse mercado e para reduzir a lacuna de proteção existente.

Educação Financeira

A educação securitário-financeira no contexto dos seguros cibernéticos também desempenha um papel essencial para aumentar a conscientização e a resiliência das empresas, especialmente pequenas e médias empresas (PMEs), frente aos riscos cibernéticos. Muitas associações de seguros internacionais têm desenvolvido materiais educacionais específicos para auxiliar empresários na compreensão dos riscos digitais e na escolha de opções adequadas de seguros.

Iniciativas como o guia francês "*Anticiper et minimiser l'impact d'un cyber risque sur votre entreprise: TPE, PME, vous êtes concernées!*"[13], o material britânico "*Making Sense of Cyber Insurance: A Guide for SMEs*", e recursos online no Canadá e nos Estados Unidos ilustram a importância de adaptar a comunicação às necessidades de públicos distintos. Esses materiais enfatizam como práticas preventivas e a contratação de seguros podem mitigar os impactos financeiros e operacionais de ataques cibernéticos, além de orientar sobre a cobertura mais adequada para cada tipo de negócio (OECD, 2017).

No Brasil, onde a cultura de seguros ainda enfrenta barreiras de entendimento e penetração, iniciativas similares podem ser fundamentais para educar empresários sobre os benefícios e limitações do seguro cibernético. A inclusão de tópicos como a importância da prevenção, o papel das apólices afirmativas e os desafios das coberturas não-afirmativas ajudariam a preparar melhor as empresas para lidar com os crescentes riscos digitais. Além disso, programas educativos podem fomentar maior confiança no mercado de seguros e contribuir para a redução da lacuna de proteção existente.

Iniciativas de educação financeira, portanto, não só fortalecem a capacidade de resposta das empresas aos riscos cibernéticos, como também promovem uma relação mais transparente e eficaz entre segurados e seguradoras, beneficiando todo o ecossistema.

Inovação nos canais de distribuição

Os canais de distribuição também podem desempenhar um papel relevante no suprimento de lacunas de conhecimento e especialização, complementando consideravelmente o papel da educação securitário-financeira. Isso fica demonstrado em pesquisas que constataram que a grande maioria dos corretores (próximo de 90%) desempenha um papel ativo na educação de seus clientes sobre os riscos cibernéticos (OECD, 2017).

[13] "Antecipar e minimizar o impacto de um risco cibernético na sua empresa: micros, pequenas e médias empresas, vocês estão abrangidos!" (tradução livre)

Durante as discussões do GT, dois canais de distribuição em particular foram discutidos como possuindo grande potencial de estimular a penetração dos seguros cibernéticos e suprir de alguma forma a lacuna de expertise das micro, pequenas e médias empresas (MPME):

- Seguros Embutidos (ou embarcados, ou integrados, ou incorporados): seguros que integram um pacote de produtos ou serviços, além da proteção securitária, como seguros cibernéticos embutidos em prestação de serviços se suporte técnico ou legal.
- *Managing General Agents* (MGA's): intermediários de seguros independentes com funções de subscrição, emissão de apólices e gerenciamento de sinistros e de apólices, com especialização em alguns tipos de seguros, em particular, os seguros cibernéticos.

Considerações do Grupo de Trabalho

As principais considerações do Grupo de Trabalho Segurança Cibernética & Seguros são apresentadas a seguir. Seguindo a organização das atividades, essas mesmas observações são distribuídas entre segurança cibernética e novos seguros para economia digital.

Segurança cibernética

1) A atuação da Susep em relação a segurança cibernética observa princípios e objetivos da Política Nacional de Cibersegurança. A PNCiber estabelece ao menos quatro princípios relevantes para as iniciativas da Superintendência nessa área (Decreto nº 11.856, art. 2º, I, III, IV e VI):

- a soberania nacional e a priorização dos interesses nacionais;
- a prevenção de incidentes e de ataques cibernéticos, em particular aqueles dirigidos a infraestruturas críticas nacionais e a serviços essenciais prestados à sociedade;
- a resiliência das organizações públicas e privadas a incidentes e ataques cibernéticos;
- a cooperação entre órgãos e entidades, públicas e privadas, em matéria de segurança cibernética;

As ações regulatórias da Susep identificadas na seção anterior mostram-se aderentes aos três primeiros princípios, estando esses conectados também com as medidas de segurança cibernética promovidas dentro da própria autarquia (por exemplo, pela observância do Programa de Privacidade e Segurança da Informação – PPSI da administração pública federal). Com relação ao quarto item, as atividades do Grupo de Trabalho ora descritas refletem a importância conferida pela Superintendência para o diálogo entre entidades públicas e privadas.

Em relação aos objetivos da PNCiber, ao menos três podem ser apontados como mais diretamente relacionados à atuação da Susep (Decreto nº 11.856, art 3º, V, VI e X):

- estimular a adoção de medidas de proteção cibernética e de gestão de riscos para prevenir, evitar, mitigar, diminuir e neutralizar vulnerabilidades, incidentes e ataques cibernéticos, e seus impactos;
- incrementar a resiliência das organizações públicas e privadas a incidentes e ataques cibernéticos;

- desenvolver mecanismos de regulação, fiscalização e controle destinados a aprimorar a segurança e a resiliência cibernéticas nacionais.

Novamente, as medidas normativas e supervisórias da Superintendência, bem como as ações para promover a sua própria segurança cibernética, permitem uma conexão com os objetivos da PNCiber. A Circular nº 638, da Susep, que disciplina os requisitos de segurança cibernética para as entidades supervisionadas, pode ser identificada como principal instrumento para promover a adoção de medidas de proteção cibernética e gestão dos riscos relacionados, bem como para incrementar a resiliência cibernética das seguradoras, entidades de previdência complementar aberta, sociedades de capitalização e resseguradoras.

2) A resiliência operacional do setor de seguros privados é crítica para a economia brasileira. A interrupção dos serviços desse setor, em um cenário de incidente cibernético de grande escala, poderia resultar em perdas econômicas e descontinuidades nos processos de contratação, regulação de sinistros e demais eventos da vida útil de um contrato de seguro.

As infraestruturas críticas foram definidas pelo Governo Federal como “instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provoque sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade” (Decreto nº 9.573, Anexo, art. 2º, I). Ademais, o Plano Nacional se Segurança das Infraestruturas Críticas identifica as finanças como uma das suas áreas prioritárias, que demandam planos setoriais próprios (Decreto nº 11.200, Anexo).

No perímetro supervisionado pela Susep, as registradoras credenciadas pela Autarquia, que conjuntamente integram o projeto denominado de Sistema de Registro de Operações (SRO), são as entidades passíveis de enquadramento como infraestruturas de mercado financeiro[14]. O SRO ainda se encontra em estágio de implementação, mas, a partir do momento em que estiver operando em plena capacidade, pode se mostrar pertinente realizar uma avaliação sobre o seu eventual enquadramento como uma infraestrutura crítica para o Estado brasileiro.

3) A gestão de mudanças nas tecnologias de informação é relevante para segurança cibernética. Três atividades ou tecnologias mereceram atenção particular nesse momento: autenticação de clientes, computação em nuvem e inteligência artificial.

Os processos para **autenticação dos clientes** nos ambientes desenvolvidos pelas entidades supervisionadas são cruciais para o adequado funcionamento dos meios remotos (Resolução CNSP nº 408, arts. 3º e 5º). As soluções adotadas variam caso-a-caso, de acordo as respectivas avaliações de risco e medidas para minimizar os seus impactos (como exemplo, ver NIST, 2023).Ressalta-se que nas discussões do GT não foram apresentadas evidências que justificassem, nesse momento, recomendações de alterações normativas da forma de atuação das supervisionadas.

Existem diferentes tipos de autenticadores, desde senhas decoradas, até dispositivos e programas, com ou sem uso de criptografia, que podem ser combinados para alcançar maiores níveis de segurança. O ICP-Brasil se apresenta como mais um exemplo, uma vez que viabiliza a emissão de certificados digitais com base em um modelo de raiz única, vinculada ao Instituto

[14] Como referência sobre o conceito, ver os Princípios para Infraestruturas de Mercado Financeiro (CPMI; IOSCO, 2012).

Nacional de Tecnologia da Informação (ITI), que constitui uma opção particular do caso brasileiro.

Os certificados digitais constituem-se em uma alternativa que pode ser considerada pelas entidades supervisionadas pela Susep ao desenvolverem seus respectivos sistemas para a autenticação dos usuários externos[15]. Como exemplo, o Governo Federal oferece a possibilidade dos cidadãos usarem certificados digitais para acessarem serviços na plataforma gov.br, sendo essa uma entre outras formas disponíveis para aumentar os níveis de segurança e acesso a serviços das contas individuais.

A **computação em nuvem**[16] vem sendo adotada amplamente, não apenas no Brasil, como forma de se alcançar benefícios como escalabilidade, flexibilidade e alto desempenho com menores custos. As soluções baseadas em nuvem podem ser empregadas por firmas de diferentes setores, portes e níveis de maturidade, para acessarem servidores, serviços e programas de modo compatível com as suas necessidades; mas a computação em nuvem oferece riscos próprios, que podem ser diferentes daqueles associados aos arranjos de terceirização mais tradicionais (A2II; IAIS, 2019).

A regulação da Susep estabelece requisitos específicos para a terceirização de serviços de processamento e armazenamento de dados, inclusive de computação em nuvem. Desse modo, entidades supervisionadas precisam, *inter alia*: (i) dispor de recursos, competências e práticas de governança necessários; (ii) certificar-se de que os potenciais prestadores de serviço cumprem determinadas exigências; e (iii) informar tempestivamente ao supervisor sobre a formalização de contratos de serviços relevantes de processamento e armazenamento de dados (Circular Susep nº 638, art. 10; ver também arts. 11 a 14).

Os usos de **inteligência artificial** (IA) – particularmente, de inteligência artificial generativa – encontram-se em estágios de maturidade diferentes, quando comparados com a computação em nuvem, de modo que podem se beneficiar de avaliações posteriores, buscando identificar em que medida eles apresentam riscos próprios, que se beneficiariam de mudanças normativas. As discussões do Grupo de Trabalho apontaram que a IA é uma ferramenta capaz de alterar substancialmente a superfície de riscos cibernéticos e, ao mesmo tempo, pode ser utilizada pelas entidades supervisionadas para aprimorar os seus sistemas de segurança.

Novos seguros para economia digital

[15] Os procedimentos de autenticação devem ser compatíveis com os canais eletrônicos oferecidos por cada supervisionada, considerando o nível de risco, o tipo de dado ou serviço compartilhado e o canal. A compatibilidade inclui fatores de autenticação, quantidade de etapas e duração do procedimento. As supervisionadas devem implementar mecanismos para garantir confiabilidade, integridade, segurança e sigilo, assegurando que outras partes envolvidas no compartilhamento não tenham acesso às credenciais do cliente. Os procedimentos devem estar alinhados à política de segurança cibernética ou gestão de riscos da empresa. A contratação de serviços para esses controles deve seguir a regulamentação de segurança cibernética vigente.

[16] Computação em nuvem é "serviço que permite acesso por demanda, e independentemente da localização, a um conjunto compartilhado de recursos configuráveis de computação, provisionados com esforços mínimos de gestão ou de interação com o prestador de serviços" (Circular Susep nº 638, art. 2º, VII).

- Objetivando uma maior disseminação de outras coberturas comuns em mercados mais maduros, é possível investigar oportunidades de aprimoramento regulatório e de fomento à inovação no mercado local. Assim, há de serem estudados estímulos para o desenvolvimento de produtos específicos para MPME's e pessoas físicas.
- O compartilhamento de dados de incidentes cibernéticos e a padronização de taxonomias se mostram essenciais para melhorar a análise e a gestão de riscos, o que deve ensejar um olhar mais atento do supervisor.
- Um ponto crucial para desdobramentos futuros é a análise mais aprofundada do potencial catastrófico dos incidentes cibernéticos. Esses eventos têm capacidade de gerar perdas simultâneas em múltiplos setores e regiões, o que exige soluções robustas para sua segurabilidade, em particular no que se refere à alta concentração de serviços em nuvem, cada vez mais comuns na economia[17].
- Essa análise deve passar, desejavelmente, pela avaliação da adequação da capacidade atual do mercado ressegurador para absorver grandes perdas, além de uma maior utilização de instrumentos inovadores, como Letras de Risco de Seguros (LRS), que integram o mercado de capitais e o setor securitário. Essas letras poderiam oferecer maior liquidez e diversificação de recursos para cobrir riscos cibernéticos catastróficos. (CNSP, 2024)
- Outros mecanismos de proteção contra eventos cibernéticos catastróficos, como fundos específicos, também poderiam ser estudados com maior aprofundamento como desdobramento dos achados do GT.
- Outro desdobramento importante é o estudo da regulação setorial para identificar barreiras e oportunidades de incentivo a novos modelos de distribuição de seguros cibernéticos. A regulamentação dos *Managing General Agents* (MGAs) e o uso de seguros embutidos apresentam grande potencial para ampliar a penetração desse tipo de seguro, reduzir as lacunas de proteção e promover a inclusão de pequenas e médias empresas. Essas abordagens podem melhorar a acessibilidade e a personalização das coberturas, mantendo a segurabilidade dos riscos cibernéticos ao exigir padrões mínimos de segurança dos segurados.
- Por fim, a abertura de novos códigos de ramos relacionados aos seguros cibernéticos é uma iniciativa que merece análise detalhada quanto à sua conveniência e oportunidade. Atualmente, as coberturas cibernéticas no Brasil estão majoritariamente concentradas no ramo de responsabilidade civil, mas a diversidade de riscos e necessidades identificadas no mercado — como perdas reputacionais, fraudes cibernéticas, interrupção de negócios, crises de relações públicas e danos físicos — sugere a possibilidade de segmentação mais granular. Essa expansão de códigos permitiria uma categorização mais precisa, promovendo maior clareza

[17] Conforme ressaltado pelos representantes da Câmara Brasileira de Economia Digital, as soluções em nuvem disponibilizam ferramentas que auxiliam as seguradoras e seus clientes na mitigação de riscos cibernéticos, por exemplo, pela facilidade na recuperação e/ou reconstrução de ambientes. Ademais, os riscos de concentração podem se relacionar à prestação de serviços diversos para os sistemas financeiros, não somente de computação em nuvem, conforme observa PIFS (2023).
Por fim, o Departamento do Tesouro dos Estados Unidos (2023, p. 57; tradução livre) observa que: "a mera presença de grandes provedores de serviços em nuvem não é necessariamente um problema para a resiliência operacional do setor financeiro. Avaliar os riscos operacionais que poderiam resultar da concentração nos serviços de nuvem depende de como as empresas usam e desenham esses serviços". A autoridade estrangeira ainda menciona que: "As limitações de dados impedem que o Tesouro e o [Comitê sobre Infraestrutura da Informação Bancária e Financeira] avaliem completamente a importância da concentração nos serviços de nuvem em todo o setor. Por exemplo, atualmente não há uma abordagem comum no setor financeiro para medir os usos críticos dos serviços de nuvem pelas instituições financeiras, o que dificulta que os reguladores financeiros agreguem os dados." (idem, p. 7; tradução livre)

regulatória, facilitando a subscrição de riscos e incentivando o desenvolvimento de produtos mais especializados. Além disso, a criação de novos códigos poderia estimular a inovação, ao oferecer flexibilidade para atender riscos emergentes como ataques a IoT e redes 5G, além de integrar melhores práticas internacionais. A implementação de tais mudanças depende de diálogo entre reguladores e o mercado, para assegurar que as novas categorias reflitam as demandas reais e ampliem a segurabilidade desses riscos, sem trazer custos regulatórios desnecessários.

Conclui-se que, para um crescimento sustentável do mercado de seguros cibernéticos no Brasil, é necessário um esforço conjunto de reguladores, seguradoras, resseguradoras e demais *stakeholders*, tanto do setor público quanto da sociedade civil. Iniciativas como o fortalecimento da supervisão, a ampliação das capacidades de resseguro, o incentivo à inovação nos canais de distribuição e a integração com o mercado de capitais serão fundamentais. Essas ações não apenas aumentarão a resiliência frente aos riscos cibernéticos, mas também consolidarão o papel do seguro cibernético como instrumento de mitigação e regulação dos riscos digitais no Brasil.

Conclusões

A segurança cibernética é um imperativo estratégico em um mundo cada vez mais digital e interconectado. A análise apresentada neste relatório evidencia que, independentemente dos avanços recentes no setor de seguros, o tema merece atenção contínua, dadas as constantes transformações no perfil dos riscos e incidentes.

A crescente sofisticação dos ataques cibernéticos e a complexidade das infraestruturas digitais exigem que as empresas do setor invistam de forma contínua em medidas de segurança robustas. Ao adotar as soluções mais adequadas às respectivas realidades, as firmas protegem seus ativos e a privacidade de seus clientes, mitigando os riscos operacionais associados.

Por outro lado, se torna a evidente a necessidade de maior investimento em inovação no setor securitário, para fazer frente aos mesmos desafios e oferecer soluções que permitam o desenvolvimento saudável e sustentável da economia brasileira, cada vez mais digital.

Encerrados os estudos no prazo assinalado, cabe registrar os agradecimentos da Susep aos participantes do Grupo de Trabalho Seguros & Segurança Cibernética. As considerações elencadas acima serão encaminhadas para apreciação do Conselho Diretor da Susep, como alternativas de próximos passos, sem prejuízo de outros encaminhamentos que o colegiado entender cabíveis.

Referências

A2ii; IAIS. *Cloud Computing: Regulatory and Supervisory Approaches Report of the A2ii – IAIS Consultation Call*. 2019.

ANPD. *Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado*. 2022. Disponível em: https://www.gov.br/anpd/pt-

br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf. Acesso em: 18/9/24.

ANPD. *Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte*. 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-orientativo-sobre-seguranca-da-informacao-para-agentes-de-tratamento-de-pequeno-porte. Acesso em: 18/9/24.

ANPD. T*ratamento de dados pessoais pelo Poder Público*. V. 2.0. 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 18/9/24.

BBC NEWS BRASIL. Crise cibernética global prejudica voos, mídia, finanças e telecomunicações. *BBC News Brasil*, [s.l.], 2023. Disponível em: https://www.bbc.com/portuguese/articles/c3gwzqe3287o. Acesso em: 20 set. 2024.

BRASIL. *Decreto nº 11.856*, de 26 de dezembro de 2023. Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-11.856-de-26-de-dezembro-de-2023-533845289. Acesso em: 18/9/24.

BRASIL. *Decreto nº 11.200*, de 15 de setembro de 2022. Aprova o Plano Nacional de Infraestruturas Críticas. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/decreto/D11200.htm. Acesso em: 23/12/24.

BRASIL. *Decreto nº 9.573*, de 22 de novembro de 2018. Aprova a Política Nacional de Segurança de Infraestruturas Críticas. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9573.htm. Acesso em: 23/12/24.

BRASIL. *Lei nº 13.874*, de 20 de setembro de 2019. Institui a Declaração de Direitos de Liberdade Econômica. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13874.htm. Acesso em: 23/12/24.

BRASIL. *Lei nº 13.709*, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 18/9/24.

BRASIL. *Medida Provisória nº 2.200-2*, de 24 de agosto de 2001. Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/MPV/Antigas_2001/2200-2.htm. Acesso em: 23/12/24.

CIS. *Critical Security Controls*. V. 8.1. 2024. Disponível em: https://www.cisecurity.org/controls. Acesso em: 19/9/24.

CNN BRASIL. Crise cibernética global prejudica voos, mídia, finanças e telecomunicações. *CNN Brasil*, [s.l.], 2023. Disponível em: https://www.cnnbrasil.com.br/internacional/crise-cibernetica-global-prejudica-voos-midia-financas-e-telecomunicacoes/. Acesso em: 20 set. 2024.

CNSeg. *Quantificação da fraude no mercado de seguros brasileiro*. 1º semestre de 2024. 2024.

CNSeg**.** *Sistema da CNseg identificou e reportou 228 incidentes cibernéticos nos últimos 12 meses*. 2024. Disponível em: https://cnseg.org.br/noticias/sistema-da-cnseg-identificou-e-reportou-228-incidentes-ciberneticos-nos-ultimos-12-meses-1. Acesso em: 04 dez. 2024.

CNSP. *Resolução nº 453*, de 19 de dezembro de 2022. Dispõe sobre a emissão de Letra de Risco de Seguro por meio de Sociedade Seguradora de Propósito Específico e dá outras providencias. Disponível em: https://www2.susep.gov.br/safe/scripts/bnweb/bnmapi.exe?router=upload/26914 . Acesso em: 06/12/24.

CNSP. *Resolução nº 416*, de 20 de julho de 2021. Dispõe sobre o Sistema de Controles Internos, a Estrutura de Gestão de Riscos e a atividade de Auditoria Interna. Disponível em: https://www2.susep.gov.br/safe/scripts/bnweb/bnmapi.exe?router=upload/28526. Acesso em: 23/9/24.

CNSP. Resolução nº 415, de 20 de julho de 2021. Dispõe sobre a implementação do Sistema de Seguros Abertos (Open Insurance). Disponível em: https://www2.susep.gov.br/safe/scripts/bnweb/bnmapi.exe?router=upload/29386. Acesso em: 23/12/24.

CNSP. *Resolução nº 413*, de 30 de junho de 2021. Dispõe sobre a contratação de seguros por meio de bilhete. Disponível em: https://www2.susep.gov.br/safe/scripts/bnweb/bnmapi.exe?router=upload/24966. Acesso em: 23/12/24.

CNSP. *Resolução nº 408*, de 30 de junho de 2021. Dispõe sobre a utilização de meios remotos nas operações de seguro, previdência complementar aberta e capitalização. Disponível em: https://www2.susep.gov.br/safe/scripts/bnweb/bnmapi.exe?router=upload/24962. Acesso em: 23/9/24.

CNSP. *Resolução nº 383*, de 20 de março de 2020. Dispõe sobre o registro das operações de seguros, previdência complementar aberta, capitalização e resseguro. Disponível em: https://www2.susep.gov.br/safe/scripts/bnweb/bnmapi.exe?router=upload/27981. Acesso em: 23/12/24.

CPMI; IOSCO. *Principles for Financial Market Infrastructures*. 2012. https://www.bis.org/cpmi/publ/d101a.pdf

EXAME. Apagão cibernético já gerou cancelamento de quase 1,4 milhão de voos pelo mundo; veja situação por país. *Exame*, [s.l.], 2023. Disponível em: https://exame.com/mundo/apagao-cibernetico-ja-gerou-cancelamento-de-quase-1-400-mil-voos-pelo-mundo-veja-situacao-por-pais/. Acesso em: 20 set. 2024.

FGV. Instituto de Inovação em Seguros e Resseguros. *Nota Técnica 10*: Seguro e Segurança Cibernética. Dez. 2023. Disponível em: https://fgviisr.fgv.br/sites/default/files/2022-12/Relatorio%20FGV%20-%20Regulacao%20e%20Governanca%20rev2.pdf. Acesso em: 25 dez. 2023.

FSB. *Cyber lexicon*. 2018. Disponível em: https://www.fsb.org/2018/11/cyber-lexicon/. Acesso em: 23/9/24.

G7. *Fundamental elements for effective assessment of cybersecurity in the financial sector*. 2023. Disponível em: https://home.treasury.gov/system/files/206/PRA_BCV_4728453_v_1_G7-Fundamental-Elements-for-Effective-Assessment.pdf. Acesso em: 23/9/24.

G7. Fundamental elements of cybersecurity in the financial sector. (2016). Disponível em: https://finance.ec.europa.eu/publications/g7-fundamental-elements-cybersecurity-financial-sector_en. Acesso em: 23/9/24.

GAFI. *Combate ao Financiamento de Ransomware*. 2023. Disponível em: https://www.fatf-gafi.org/content/dam/fatf-gafi/translations/reports/Portuguese_Combate%20ao%20Financiamento%20de%20Ransomware.pdf.coredownload.inline.pdf. Acesso em: 23/12/24.

GARTNER. Ransomware. In: GLOSSÁRIO DE TECNOLOGIA DA INFORMAÇÃO. Disponível em: https://www.gartner.com/en/information-technology/glossary/ransomware. Acesso em: 12/11/2024.

IAIS. Draft Application Paper: Operational Resilience Objectives [and Toolkit]. 2024. Disponível em: https://www.iaisweb.org/uploads/2024/08/Draft-Application-Paper-on-Operational-Resilience-Objectives-and-Toolkit.pdf. Acesso em: 23/9/24.

IAIS. Issues Paper on Insurance Sector Operational Resilience. 2023. Disponível em: https://www.iaisweb.org/uploads/2023/05/Issues-Paper-on-Insurance-Sector-Operational-Resilience.pdf. Acesso em: 23/9/24.

IAIS. *Cyber Risk Underwriting: Identified Challenges and Supervisory Considerations for Sustainable Market Development*. 2020. Disponível em: https://www.iaisweb.org/uploads/2022/01/201229-Cyber-Risk-Underwriting_-Identified-Challenges-and-Supervisory-Considerations-for-Sustainable-Market-Development.pdf. Acesso em: 23/9/24.

IAIS. *Application Paper: Supervision of Insurer Cybersecurity* 2018. Disponível em: https://www.iaisweb.org/uploads/2022/01/181108-Application-Paper-on-Supervision-of-Insurer-Cybersecurity.pdf. Acesso em: 23/9/24.

IAIS. Issues Paper: Cyber Risk to the Insurance Sector. 2016. Disponível em: https://www.iaisweb.org/uploads/2022/01/160812-Issues-Paper-on-Cyber-Risk-to-the-Insurance-Sector_final.pdf. Acesso em: 23/9/24.

IBM. *Relatório do custo das violações de dados 2024*. 2024. Disponível em: https://www.ibm.com/reports/data-breach. Acesso em: 22/11/24.

ISACA. *COBIT 2019 Framework: Introduction and Methodology*. 2019. Disponível em: https://www.isaca.org/resources/cobit#2. Acesso em: 18/9/24.

ISO/IEC. *27000:2018*: *Information technology — Security techniques — Information security management systems — Overview and vocabulary*. Ed. 5. 2018. Disponível em: https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html. Acesso em: 18/9/24.

NIST. *Estrutura de Segurança Cibernética (CSF) 2.0 do NIST*. 2024. Disponível em: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.por.pdf. Acesso em: 18/9/24.

NIST. "Digital Identity Guidelines". *NIST Special Publication,* n. 800-63, rev. 3. 2023. Disponível em: https://pages.nist.gov/800-63-3/sp800-63-3.html. Acesso em: 23/12/24.

OECD. *Enhancing the role of insurance in cyber risk management*. Paris: OECD Publishing, 2017. Disponível em: https://doi.org/10.1787/9789264282148-en. Acesso em: 04 dez. 24.

PIFS. *Cloud adoption in the Financial Sector and Concentration Risk*. 2023. Disponível em: https://www.pifsinternational.org/wp-content/uploads/2023/04/PIFS-Cloud-Adoption-in-the-Financial-Sector-and-Concentration-Risk-04.19.2023.pdf. Acesso em 23/12/24.

PWC. *Pesquisa Global Digital Trust Insights de 2024*. 2024. Disponível em: https://www.pwc.com.br/pt/estudos/servicos/consultoria-negocios/2024/global-digital-trust-insights-survey-2024.html. Acesso em: 3/12/24.

Susep. *Painel de Inteligência de Mercado*. 2024. Disponível em: https://www2.susep.gov.br/safe/menuestatistica/pims.html. Acesso em: 3/12/24.

Susep. *Circular nº 700*, de 4 de abril de 2024. Estabelece procedimentos relacionados com a instrução de processos de autorização da Susep para funcionamento, início das operações no país, exercício de cargos em órgãos estatutários ou contratuais, integralização de capital, conversão da autorização temporária das sociedades participantes do Sandbox Regulatório e sobre condições de estrutura de controle societário das supervisionadas, corretoras de resseguro, resseguradores estrangeiros

e escritórios de representação dos resseguradores admitidos. Disponível em: https://www2.susep.gov.br/safe/scripts/bnweb/bnmapi.exe?router=upload/28306. Acesso em: 23/12/24.

Susep. *Circular nº 638*, de 27 de julho de 2021. Dispõe sobre requisitos de segurança cibernética a serem observados pelas sociedades seguradoras, entidades abertas de previdência complementar (EAPCs), sociedades de capitalização e resseguradores locais. Disponível em: https://www2.susep.gov.br/safe/scripts/bnweb/bnmapi.exe?router=upload/25121. Acesso em: 18/9/24.

Susep. Circular nº 637, de 27 de julho de 2021. Dispõe sobre os seguros do grupo responsabilidades. Disponível em: https://www2.susep.gov.br/safe/scripts/bnweb/bnmapi.exe?router=upload/25074. Acesso em: 23/12/24.

Susep. *Circular nº 619*, de 4 de dezembro de 2020. Dispõe sobre a política de segurança e sigilo de dados e informações das entidades registradoras credenciadas a prestarem o serviço de registro de operações de seguros, previdência complementar aberta e resseguros. https://www2.susep.gov.br/safe/scripts/bnweb/bnmapi.exe?router=upload/23958. Acesso em: 18/9/24.

U.S. DEPARTMENT OF TREASURY. *The Financial Services Sector's Adoption of Cloud Services*. 2023. Disponível em: https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf. Acesso em: 23/12/24.

U.S. DEPARTMENT OF TREASURY. *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*. 2020. Disponível em: https://ofac.treasury.gov/media/48301/download?inline. Acesso em: 3/12/24.

U.S. DEPARTMENT OF TREASURY. *Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*. 2021. Disponível em: https://ofac.treasury.gov/media/912981/download?inline. Acesso em: 3/12/24.

WORLD ECONOMIC FORUM. *The Global Risks Report 2024*. 2024. Disponível em: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf. Acesso em: 3/12/24.

WORLD ECONOMIC FORUM; ACCENTURE. *Global Cybersecurity Outlook 2024* 2024. Disponível em: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf. Acesso em: 3/12/24.