SUPERINTENDÊNCIA DE SEGUROS PRIVADOS

EXPOSIÇÃO DE MOTIVOS

1. Trata-se de proposta de minuta de Circular que visa a estabelecer requisitos de segurança cibernética a serem observados pelas sociedades seguradoras, entidades abertas de previdência complementar (EAPC), sociedades de capitalização e resseguradores locais.

CONTEXTO

2. O mundo cada vez mais globalizado e digital vem acelerando o desenvolvimento dos mais diversos mercados, inclusive o de seguros e previdência. Entretanto, o que se percebe, é que as medidas de proteção cibernética não se desenvolvem na mesma velocidade. Recentemente, tem sido noticiado com frequência em veículos de comunicação a ocorrência de diversos ataques cibernéticos ao redor do mundo[1][2][3], impulsionados pelo mercado de monetização de dados pessoais. Em razão disso, é latente a preocupação dos órgãos reguladores com padrões de segurança cibernética necessários aos seus mercados regulados, com o objetivo de minimizar as vulnerabilidades dos sistemas empresariais e garantir maior segurança aos segurados. Neste cenário, a Susep deve estabelecer as diretrizes de proteção aplicáveis às supervisionadas, atentando-se para que, no exercício de elaboração normativa, não desestimule a inovação.

3. A presente proposta visa exatamente preencher esta lacuna, uma vez que institui requisitos para a mitigação dos riscos inerentes ao ambiente digital que contribuirão para uma maior resiliência cibernética do mercado segurador, buscando padrões adequados de segurança. A proposta prevê os princípios e diretrizes de proteção das informações detidas pelas supervisionadas contra ameaças e ataques cibernéticos, preocupando-se ainda com a melhoria contínua da segurança dos dados, além da manutenção da confidencialidade e da integridade das informações.

4. Vale destacar que a presente proposta normativa segue em linha com as melhores práticas internacionais e com as recomendações da *International Association of Insurance Supervisors* (IAIS), expostas nos seus Princípios Básicos de Seguros (ICPs, na sigla em inglês), em especial nos ICPs 7 e 8 (*Corporate Governance e Risk Management and Internal Controls*), além de buscar aproximar a Susep da abordagem adotada por outros supervisores do Sistema Financeiro Nacional, que já possuem regulamentações similares, como a Resolução CMN nº 4.893, de 26 de fevereiro de 2021 (que substituirá, a partir de 01/07/2021, em razão de consolidação normativa realizada no âmbito do Decreto nº 10.139, de 28 de novembro de 2019, a Resolução CMN nº 4.658, de 26 de abril de 2018, que dispõe sobre sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil), e a Instrução CVM nº 612, de 21 de agosto de 2019 (que aprimorou os controles internos e as práticas das instituições intermediárias quanto ao registro e arquivamento de ordens de forma a garantir a confidencialidade, autenticidade, integridade e disponibilidade das informações). A proposta complementa o arcabouço geral de controles internos e de gestão de riscos, cuja norma proposta, que trata da consolidação dos requisitos regulatórios relativos ao Sistema de Controles Internos (SCI) e à Estrutura de Gestão de Risco (EGR), também encontra-se submetida ao processo de consulta pública.

5. Além disso, é importante frisar que as boas práticas de segurança cibernética, uma vez definidas pela Susep, serão de importante utilidade neste momento em que o mercado supervisionado passa por um processo de inovação e digitalização de suas operações, em razão de iniciativas promovidas pela autarquia como a

implantação do *sandbox* regulatório e do *open insurance*, além da implementação do Sistema de Registro de Operações - SRO. O conjunto de conceitos, instrumentos e práticas estabelecidos na norma poderão ser referenciados para a definição de outros requisitos específicos de segurança cibernética, eventualmente necessários para os propósitos de inovação regulatória promovido pela Susep.

ANÁLISE DA PROPOSTA

6. A iniciativa da Susep visa estabelecer boas práticas de segurança cibernética a serem observadas pelo mercado supervisionado em suas operações. Para tanto, a gestão do risco cibernético, inserida no contexto do Sistema de Controles Internos e da Estrutura de Gestão de Risco, deve estar alinhada a uma política de segurança cibernética, criar procedimentos relativos à prevenção e resposta a incidentes e obedecer a critérios mínimos quando da terceirização de serviços de processamento e armazenamento de dados.

7. A política de segurança cibernética deve conter as diretrizes em relação ao tema, sendo de conhecimento de todos da organização. Assim, constitui-se uma cultura de segurança capaz de fornecer os subsídios para a implantação das boas práticas nacionais e internacionais. Neste cenário, a empresa consegue identificar e reduzir suas vulnerabilidades de forma proativa, além de detectar e recuperar-se de incidentes em um curto espaço de tempo, mitigando os efeitos adversos por eles causados e tornando mais robusto seu plano de continuidade de negócios.

8. Como já informado, a proposta normativa aproxima a regulação da Susep da abordagem adotada por outros supervisores do Sistema Financeiro Nacional, que já possuem regulamentações similares, além de seguir em linha com as melhores práticas e recomendações internacionais. Como principais aspectos relativos à presente proposta normativa, destacamos os seguintes:

I - **Política de segurança cibernética:**

a) Elaboração de uma política de segurança cibernética, aprovada pelo órgão de administração máximo da supervisionada (o Conselho de Administração ou, se inexistente, a Diretoria) e divulgada a seus colaboradores e clientes, que estabeleça diretrizes para classificação dos dados quanto a sua sensibilidade e para a implementação de processos, procedimentos e controles destinados à gestão do risco cibernético, em linha com boas práticas nacionais e internacionais.

b) Tal política poderá ainda ser única para supervisionadas pertencentes a um mesmo grupo prudencial, em linha com o "SCI/EGR unificado", instituído no arcabouço normativo geral de controles internos e gestão de riscos.

II - **Tratamento de incidentes:**

a) Implementação de processos, procedimentos e controles relativos a prevenção e resposta a incidentes, que incluam um trabalho proativo de identificação e redução de vulnerabilidades, além de ações efetivas para responder a eventuais incidentes. No tocante à resposta a incidentes, busca-se ainda estabelecer de uma relação com o plano de continuidade de negócios previsto no arcabouço geral de controles internos e gestão de riscos, especialmente quanto à contenção de efeitos e restabelecimento do funcionamento normal.

b) Previsão de ações complementares relativas ao registro do incidente, compartilhamento de informações com outras supervisionadas, comunicação com clientes e outras partes potencialmente afetadas e, no caso de incidentes relevantes (que envolvem dados pessoais, de clientes ou relativos a processos críticos de negócio), comunicação de sua ocorrência à Susep.

c) Elaboração de um relatório anual sobre prevenção e tratamento de incidentes, que deverá ser disponibilizado a diversas instâncias internas da empresa visando subsidiar avaliações independentes da efetividade de todo processo.

d) Vale ressaltar que tanto a comunicação à Susep, como o relatório sobre incidentes, poderão servir como instrumentos para uma melhor supervisão por parte da Autarquia.

III - **Terceirização de serviços de processamento e armazenamento de dados:**

a) Adoção de procedimentos específicos que incluem a verificação da capacidade interna para administrar a prestação do serviço e a análise de possíveis fornecedores quanto a uma série de requisitos. Dentre tais requisitos, destacam-se a necessidade de adoção de processos, procedimentos e controles de segurança cibernética não inferiores aos da própria supervisionada, e, no caso de serviços relevantes (que envolvem dados

pessoais, de clientes ou relativos a processos críticos de negócio), a exigência de certificação relativa ao tipo de serviço contratado.

b) No caso de terceirização de serviços relevantes exige-se ainda, visando evitar graves impactos operacionais em caso de descontinuidade na sua prestação, que sejam previstas estratégias para a execução própria do serviço ou para a substituição do respectivo prestador. A terceirização de tais serviços relevantes deverá ainda ser comunicada previamente à Susep, o que permitirá, por exemplo, mapear o acúmulo de exposições por fornecedor ou região, fortalecendo, assim, a supervisão da Autarquia.

c) Garantia de que a Susep poderá ter acesso aos dados objeto do contrato e a informações relativas à prestação do serviço independentemente do local onde ele seja prestado.

d) Vale destacar que as exigências descritas nos itens anteriores não se aplicam às entidades registradoras do Sistema de Registro de Operações, previsto na Circular Susep nº 599, de 30 de março de 2020. Para todos os demais casos de contratos de terceirização de serviços de processamento e armazenamento de dados, prevê-se um prazo de adaptação de 2 (dois) anos a contar do início de vigência da norma.

IV - **Disposições gerais:**

a) Exigência de designação, perante a Susep, de um diretor responsável pela implementação das medidas de segurança cibernética dispostas na norma. Visando evitar conflitos de interesse na avaliação da efetividade de tais ações, estabeleceu-se que o referido diretor não poderá ser o mesmo indicado como responsável pelos controles internos.

b) Necessidade de conservação de documentação que comprove o atendimento dos requisitos previstos na norma.

c) Estabeleceu-se a data de vigência da norma em 03 de janeiro de 2022, data compatível com o início esperado do projeto do *open insurance*. Contudo, foram previstos prazos de adaptação às novas regras, que, em linha com uma abordagem da regulação prudencial proporcional, são diferenciados por segmento (ref.: Resolução CNSP nº 388, de 8 de setembro de 2020).

DISPOSIÇÕES FINAIS

9. A Susep convida todos os interessados a participar da construção da presente proposta normativa por meio da Consulta Pública nº 15, que ficará aberta pelo prazo de 30 (trinta) dias, a contar de sua publicação, e pode ser acessada em hpttp://susep.gov.br/menu/atosnormavos/normas-em-consulta-publica.

---

[1] https://minutodaseguranca.blog.br/34-bilhoes-de-tentativas-de-ataques-ciberneticos-ja-atingiram-o-pais-em-2020/

[2] https://pt.wikipedia.org/wiki/Ataque_cibern%C3%A9tico_ao_Superior_Tribunal_de_Justi%C3%A7a

[3] https://pt.wikipedia.org/wiki/WannaCry

Referência: Processo nº 15414.600373/2021-23 SEI nº 1004640