Circular Susep nº 638, de 27/07/2021, que dispõe sobre os requisitos de segurança cibernética das seguradoras

CHALFIN
GOLDBERG
VAINBOIM
ADVOGADOS

Circular Susep nº 638, de 27/07/2021, que dispõe sobre os requisitos de segurança cibernética das seguradoras

Premente necessidade adequação das supervisionadas dos segmentos S1 a S4

Há pouco menos de um ano, foi publicada a Circular Susep nº 638, em vigor desde 1º de setembro de 2021, que dispõe sobre *requisitos de segurança cibernética a serem observados pelas sociedades seguradoras, entidades abertas de previdência complementar (EAPCs), sociedades de capitalização e resseguradores locais,* supervisionadas (art. 2º, inciso I).

Embora o normativo esteja próximo de completar seu primeiro aniversário, as normas começam agora a ter sua execução obrigatória para as supervisionadas: para as enquadradas nos segmentos S1 ou S2, assim definidas de acordo com a Resolução CNSP nº 388, de 08/09/2020[1] foi concedido prazo para adaptação até 30/06/2022; para as enquadradas nos segmentos nos S3 ou S4, o prazo vai até 01/09/2022. Portanto, a Circular Susep 638/2021 é assunto da ordem do dia: já a partir da última quinta-feira e até o começo de setembro, o mercado terá de estar em *compliance* regulatório.

Na exposição de motivos, pontuou-se que o normativo visa a instituir 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*". De princípios a diretrizes de proteção das informações pelas supervisionadas contra ameaças e ataques cibernéticos, preocupou-se com a melhoria da segurança da informação.

A se destacar, além de parâmetros de boas práticas a serem seguidos no tratamento e controle dos riscos cibernéticos, o normativo acerta ao determinar a promoção de ações voltadas à disseminação da cultura de segurança cibernética, incluindo programa de capacitação contínua de colaboradores, com base na sensibilidade das informações por eles manipuladas. O que se busca é aumentar a maturidade cibernética do mercado segurador.

Como se sabe, especialmente por aqueles que estão familiarizados com o seguro de responsabilidade civil de riscos cibernéticos, o maior vetor de entrada de elementos maliciosos e falhas de segurança é o componente humano das sociedades, sendo certo que nem mesmo a adoção do sistema mais rígido e seguro já criado é infalível diante de uma cultura de dados parca e desatualizada e uma má conduta cibernética.

Assim, inexiste para o ambiente cibernético o conceito de segurança plena, que, diante das ameaças constantes, internas e externa, impõe às sociedades a condição de permanente vigilância, tratada pela SUSEP na exigência de treinamentos.

Ademais, a norma em comento representa mais uma etapa no processo de aculturamento do mercado segurador à proteção de dados pessoais. Após o contato inicial com a LGPD (Lei nº 13.709/2018) e, espera-se, a adoção de providências necessárias à implementação dessa, é vital manter o monitoramento da edição de novas *guidelides* pelos órgãos reguladores sobre a temática, a exemplo da Circular Susep nº 638 ora examinada. Com efeito, o normativo insere obrigatoriamente a segurança cibernética nos controles internos e na gestão de riscos das supervisionadas, relacionando-a diretamente com a Resolução CNSP nº 416, de 20/07/2021, ao situá-la como política complementar na gestão dos riscos (art. 3, p.u., inc. II)[2].

[1] O inteiro teor da Resolução CNSP nº 388, de 2020, pode ser encontrado em: https://www2.susep.gov.br/safe/scripts/bnweb/bnmapi.exe?router=upload/23525

[2] O inteiro teor da Resolução CNSP nº 416, de 2021, pode ser encontrado em: https://www2.susep.gov.br/safe/scripts/bnweb/bnmapi.exe?router=upload/25061

Dentre as implementações obrigatórias, destaca-se a necessidade de que as supervisionadas possuam uma Política de Segurança Cibernética, com elementos mínimos dispostos no artigo 4º e cujos requisitos orientadores são o grau de exposição aos riscos cibernéticos e a compatibilidade da política com o porte, a natureza e a complexidade das operações da sociedade.

Desta forma, o normativo segue o movimento da SUSEP de impor ao mercado normas principiológicas e orientadoras, sem tutelar detalhadamente cada passo e conduta a ser tomada pelas supervisionadas. A norma também reforça outra tendência recente da autarquia, de transferir às supervisionadas o dever de cumprir as normas por si só, fiscalizadas por seus órgãos e controles internos, sem que a autarquia tenha que realizar aprovações e autorizações prévias [3].

Um dos temas que tem suscitado algum debate, por conta da vagueza de conceitos a causar insegurança no mercado, é a disciplina da *terceirização de serviços de processamento e armazenamento de dados*, tema abordado no Capítulo VI (artigos 10 ao 14).

Trata-se de louvável iniciativa da SUSEP, que, detentora de dados sobre o seguro de riscos cibernéticos, é ciente de que os ataques são realizados sempre no lado mais frágil da relação (prestadores de serviços) e o acesso a dados de clientes seria catastrófico. Como exemplo, basta citar o apetite de hackers pelos dados de segurados que tenham contratado o seguro de riscos cibernéticos, para serem mais assertivos ao exigirem o resgate decorrente de um ataque por *malware.*

Dentre as obrigações decorrentes da terceirização, está a de reportar à SUSEP, dentro do prazo de até 30 (trinta) dias após a formalização, de contratos que envolvam "*serviços relevantes de processamento e armazenamento de dados*" (art. 10, inciso III).

Nesse sentido, o artigo 2º, inc. V, determina que serviços relevantes de processamento e armazenamento de dados são aqueles "*inclusive de computação em nuvem, que: a) envolvam acesso ou manipulação de dados relevantes; ou b) suportem atividades que a supervisionada considere essenciais para a continuidade de seu negócio*". A definição, como se nota, não é dotada de absoluta precisão, mas de noções orientadoras e gerais.

Essa redação, no entanto, não era a inicialmente proposta na consulta pública [4] e foi alterada para destacar, nas palavras da SUSEP, "*aspectos relativos à criticidade do serviço para a continuidade do negócio, com base em parâmetros definidos pela supervisionada*" [5].

[3] Como exemplo, registre-se a paradigmática mudança que deixou de exigir das seguradoras a aprovação prévia das condições contratuais para os seguros de danos, o que funcionava como filtro para as condições inadequadas, passando a exigir, na atual Circular SUSEP nº 621, apenas o registro do produto, sem análise da autarquia. A mudança exige uma conduta muito mais ativa das supervisionadas, retirando obrigações da SUSEP.

[4] O inciso era assim redigido: "VI - serviços relevantes de processamento ou armazenamento de dados: serviços, inclusive de computação em nuvem, que envolvam processamento ou armazenamento de dados relevantes".

[5] A manifestação da SUSEP pode ser encontrada no quadro de sugestões feitas pelo mercado no âmbito da Consulta Pública nº 15/2021, que precedeu a publicação da Circular SUSEP nº 638, especificamente em relação ao inciso V do art. 2º.

De igual forma, foi inserido o § 2º no art. 11 para permitir que a política de segurança cibernética estabeleça, a critério da supervisionada, exceções para serviços de processamento e armazenamento de dados que não sejam classificados como relevantes, definindo expressamente os requisitos mínimos de segurança cibernética a serem observados e, para eles, não sendo exigida comunicação à SUSEP.

Assim, caberá à sociedade definir quais são os serviços, terceirizados ou não, cuja relevância é tamanha que um incidente poderia afetar a continuidade do negócio, dispondo-os na política de segurança cibernética.

Deve ser registrado, porém, que essa não é a primeira vez que a SUSEP deixa ao encargo da supervisionada determinar o que é atividade relevante para os negócios da companhia, tendo adotado postura semelhante ao fornecer ao mercado esclarecimentos a respeito do art. 9º, § 2º, da Resolução CNSP nº 416, de 2021, que trata da vedação ao diretor responsável pelos controles internos de exercer "direta ou indiretamente, o acúmulo de funções relativas à gestão, de caráter executivo ou operacional, ou que impliquem em assunção de riscos relevantes relativos ao negócio" [6].

Naquela oportunidade, a autarquia assim se manifestou:

> "• Considerando a redação da norma, que traz a previsão de riscos relevantes, e considerando seu caráter principiológico, entendemos que a questão passa primeiro pela definição, por parte da supervisionada, de quais riscos, entre os quais já assume ou pretende assumir, seriam relevantes. Isto feito, cabe então avaliar quais funções ou áreas da supervisionada assumiriam riscos considerados relevantes, as quais não poderiam estar sob a responsabilidade, direta ou indireta, do diretor responsável pelos controles internos.
> • Entretanto, ressalta-se que o processo descrito no item anterior é passível de avaliação por parte da supervisão da Susep, que pode questionar a supervisionada quanto à classificação de riscos relevantes e as funções ou áreas que os assumem. Caso tais questionamentos ocorram, cabe à supervisionada estar preparada para respondê-los, com base nas análises já mencionadas, tendo a supervisão da Susep a prerrogativa de não concordar com a classificação realizada." (Destacou-se)

Considerando que a inserção da segurança cibernética nos mecanismos de controles internos e gestão de riscos, objetos da referida Resolução CNSP nº 416, que gerou a orientação, a posição expressa da SUSEP é bastante bem-vinda para as sociedades que estão obrigadas a adotar o procedimento normativo e precisam de algum norte para seguir.

[6] O inteiro teor do documento pode ser encontrado em: http://www.susep.gov.br/setores-susep/cgsoa/cgrep/Manual%20de%20SCI%20EGR%20AI%20%20-%20versao%20fev22%20e%20vigencia%20jan22.pdf

Esta é, ainda, uma estrada que será longa. Conforme o artigo 16 do normativo, o prazo para adequação dos contratos de terceirização de serviços de processamento e armazenamento de dados firmados antes da vigência da Circular vai até 1º de setembro de 2024, ainda existindo um caminho a experimentar e percorrer.

O time estratégico do Chalfin, Goldberg & Vainboim Advogados destaca ainda outros pontos de atenção:

- a necessidade do envolvimento e do compromisso dos órgãos de administração com a segurança cibernética (art. 4);
- exigência de processos e controles efetivos para identificar e reduzir vulnerabilidades, de forma proativa, além de detectar, recuperar e responder a incidentes (art. 5);
- a existência de um plano de continuidade de negócios, para cenários de ataques e outros eventos que possam causar danos; acesso, modificação, exclusão ou divulgação de dados relevantes; ou interrupção de serviços relevantes de processamento e armazenamento (art. 7);
- prazo máximo de até 5 dias úteis contados do conhecimento de incidentes relevantes (outro conceito abstrato presente na norma) para informá-los à Susep (art. 8º);
- necessidade de elaboração de relatório anual sobre prevenção e tratamento de incidentes, nos termos do art. 9º; e
- a determinação de uma série de exigências a serem feitas aos prestadores de serviço envolvidos na terceirização de processamento e armazenamento de dados, inclusive com o não embaraço à atuação da SUSEP e exigência de acesso da autarquia a contratos e informações dos serviços (art. 11).

O Chalfin, Goldberg & Vainboim Advogados coloca-se inteiramente à disposição para esclarecer os pontos mencionados, bem como para assessorar na adequação de procedimentos em linha com o normativo.