Por Rejane Rejo Tamoto

A proteção de dados pessoais, da privacidade e do acesso à informação ganham um reforço com o Decreto 11.856, publicado no final de 2023, que instituiu a Política Nacional de Cibersegurança. A norma traz os princípios que orientarão as ações do Estado brasileiro em relação à cibersegurança junto a empresas e instituições públicas, para garantir os direitos fundamentais dos cidadãos. Um dos objetivos principais da política é promover o desenvolvimento de produtos, serviços e tecnologias nacionais, assegurando a confidencialidade, integridade, autenticidade e disponibilidade das soluções e dados no ambiente digital. Além disso, visa fortalecer a atuação diligente no ciberespaço, reconhecendo a existência de vulnerabilidades, como a deep web, e busca medidas para mitigar riscos e neutralizar ataques cibernéticos.

Adriana Carvalho Vieira, Secretária Executiva do Colégio de Coordenadores de Governança e Riscos da Abrapp, avalia que é importante que as EFPC acompanhem a evolução dessas normas em suas políticas de cibersegurança. “A Política Nacional estimula a adoção de medidas de proteção cibernética e de gestão de riscos para prevenir, evitar, mitigar, diminuir ou neutralizar vulnerabilidades, incidentes e ataques cibernéticos. Ao detalhar que o objetivo é estimular a adoção de proteção e da gestão de riscos, isso está bem alinhado não só com a regulamentação do segmento das EFPC, mas com a do sistema financeiro, na qual a gestão de riscos é um item obrigatório e tem sido adotado pelos órgãos de fiscalização e supervisão dessas atividades”, explica.

Segundo ela, o Decreto reforça a importância da aferição dos riscos de vulnerabilidades e o quanto que isso pode impactar a atividade das entidades. “Embora seja uma atividade que se desenvolve em âmbito privado, ela tem uma dimensão de interesse público, porque congrega milhares de participantes, informações cadastrais e pagamentos de benefícios previdenciários. A política vem no sentido de ratificar o padrão de gestão de riscos do setor”, afirma.

O risco cibernético aparece entre os cinco mais relevantes para o sistema, segundo a mais recente edição da Pesquisa sobre Riscos do Sistema Fechado de Previdência Complementar. Com participação de 100 entidades fechadas, o levantamento mapeou que os riscos mais urgentes que atingiram o sistema, em 2022, foram os relativos aos seguintes temas: macroeconômico, regulamentação, taxas de juros, desempenho dos investimentos e cibernético.

A Secretária Executiva do Colégio de Coordenadores de Governança e Riscos da Abrapp diz que acompanhou situações de fundações que sofreram violação e ataques cibernéticos. “Nós temos tratado o tema com bastante preocupação e ênfase, inclusive junto aos nossos conselhos deliberativos, tendo em vista que este é estratégico e pode trazer ruptura ou suspensão de disponibilidade sistêmica com prejuízos graves, uma vez que lidamos com dados cadastrais e também com pagamentos de benefícios”, avalia.

Adriana destaca que é essencial que os profissionais que lidam com riscos no âmbito das entidades fortaleçam seus processos de segurança. “A criação do Conselho Nacional de Cibersegurança é uma iniciativa oportuna para coordenar esforços e envolver diversos atores, incluindo representantes da sociedade civil. O que nós temos visto é que tanto o Estado, por intermédio de órgãos públicos, quanto os particulares, por intermédio de empresas e pessoas físicas, têm tido inúmeros problemas, ataques e perdas financeiras importantes por violação de dados pessoais. Então é necessário um enfrentamento conjunto coletivo, no qual toda a sociedade civil esteja amparada e segura em participar desse processo. Certamente todo esse arcabouço vai fornecer uma base e pavimentar todas as ações que serão adotadas posteriormente”, concluiu.

Fonte: Abrapp em Foco, em 05.02.2024.