A Resolução CNSP nº 497/2026 e a Resolução SUSEP nº 99/2026, publicadas recentemente, reforçam as exigências aplicáveis ao mercado segurador em matéria de controles internos, gestão de riscos e prevenção à lavagem de dinheiro e ao financiamento do terrorismo.

Publicada em 24 de setembro, a Resolução CNSP nº 497/2026 altera pontualmente a Resolução CNSP nº 416/2021, que regula os sistemas de controles internos, a estrutura de gestão de riscos e a auditoria interna das entidades supervisionadas e das corretoras de seguros de maior porte.

Na prática, as principais mudanças são:

i. ampliação do conteúdo mínimo da estrutura de gestão de riscos, que deverá incluir, entre as diretrizes aplicáveis aos riscos mais relevantes ou prioritários, políticas de transferência de riscos, de segurança cibernética e, quando cabível, de tratamento de riscos específicos previstos na regulamentação setorial; e
ii. obrigatoriedade de declaração, na contratação ou substituição do auditor independente responsável pelas funções da Auditoria Interna, do cumprimento de determinadas restrições e autorizações.

No mesmo movimento de fortalecimento da governança e dos mecanismos de controle, a Resolução SUSEP nº 99/2026, publicada em 1º de outubro, revogará e substituirá integralmente a Circular SUSEP nº 612/2020 a partir de 1º de janeiro de 2027. A norma atualiza o regime de prevenção à lavagem de dinheiro (PLD) e ao financiamento do terrorismo (FT) e inclui expressamente a prevenção ao financiamento da proliferação de armas de destruição em massa (FPADM) entre os riscos que devem ser monitorados pelo setor de seguros.

Os principais pontos de atenção para as empresas são:

i. inclusão da FPADM no escopo da norma;
ii. inclusão de novos sujeitos obrigados: sociedades seguradoras de propósito específico (SSPEs), administradoras de operações de proteção patrimonial mutualista e sociedades processadoras de ordem do cliente (SPOCs);
iii. reforço da responsabilidade do diretor encarregado do cumprimento da Lei nº 9.613/1998 por orientar e supervisionar, em todas as áreas da entidade, a implementação e a operação das políticas, dos procedimentos e dos controles de PLD, FT e FPADM, sem afastar a responsabilidade dos demais diretores em suas respectivas áreas;
iv. aprimoramento da abordagem baseada em risco, com três níveis de devida diligência: reforçada para situações de alto risco, padrão e simplificada para situações de baixo risco. Serão admitidas subdivisões, desde que proporcionais ao risco identificado;
v. possibilidade de aproveitar procedimentos de conhecimento do cliente (KYC) realizados por empresas do mesmo conglomerado, desde que observadas as condições previstas na regulamentação;
vi. possibilidade de simplificar, mas não dispensar, a identificação e a qualificação de clientes no KYC, considerando o perfil de risco e a natureza do negócio, nos casos de devida diligência padrão ou simplificada;
vii. maior rigor na identificação do beneficiário final, com análise da estrutura de propriedade e controle, consulta a fontes independentes e adoção de procedimentos proporcionais ao risco;
viii. adoção de medidas específicas para relações de negócio envolvendo jurisdições classificadas pelo GAFI como de maior risco, incluindo restrições, condições adicionais, recusa ou limitação de operações, exigência de documentos complementares e encerramento do relacionamento quando o risco for considerado inaceitável;
ix. exigência de que o relatório anual de efetividade contenha indicadores quantitativos e qualitativos sobre os controles, além de métricas relativas ao monitoramento, à detecção, à seleção e à comunicação de operações suspeitas;
x. possibilidade de a SUSEP divulgar listas estruturadas de operações de maior e menor risco e

estabelecer controles obrigatórios para situações específicas.

Embora preserve a estrutura central da Circular SUSEP nº 612/2020, a nova resolução eleva o padrão de conformidade exigido das empresas, amplia o escopo para incluir a FPADM e consolida uma abordagem de controles efetivamente orientada por risco.

Como próximo passo, as entidades devem avaliar os impactos das novas normas e revisar políticas, procedimentos, sistemas e controles. A prioridade deve recair sobre a classificação de riscos, a incorporação da FPADM, os processos de KYC, o monitoramento de operações e a qualidade dos relatórios regulatórios, de modo a assegurar a adequação no prazo e reduzir riscos operacionais, regulatórios e reputacionais.

(26.10.2026)