Como as novas regras de PLD/FTP reforçam a necessidade de conectar riscos, dados e decisões no mercado segurador



Por Ricardo Saponara

A publicação da Resolução Susep nº 99/2026, com vigência a partir de 1º de janeiro de 2027, marca uma nova etapa na prevenção à lavagem de dinheiro, ao financiamento do terrorismo e da proliferação de armas de destruição em massa (PLD/FTP) no mercado supervisionado pela Susep. Ao substituir a Circular 612/2020, a norma preserva fundamentos anteriores, mas amplia seu alcance e reforça a aplicação proporcional de controles, como detalha a síntese oficial da Susep.

Mais do que uma atualização normativa, essa evolução convida a uma pergunta: estamos tratando PLD/FTP como parte integrante da gestão de riscos ou ainda operamos com informações, processos e decisões fragmentados? A resposta exige uma abordagem integrada, que combine áreas, qualidade dos dados, rastreabilidade, identidade digital e escolhas tecnológicas economicamente sustentáveis.

Da conformidade regulatória à inteligência de riscos

A nova regulamentação prevê expressamente três níveis de diligência: simplificada, padrão e reforçada, definidos a partir da Avaliação Interna de Riscos (AIR) e das situações de risco divulgadas pela Susep. A simplificação, quando cabível, não dispensa requisitos mínimos de identificação e monitoramento. A norma também atualiza práticas de identificação e qualificação de clientes, PEPs e beneficiários finais, e admite o aproveitamento condicionado de procedimentos

dentro de conglomerados e sistemas cooperativos, alcançando novas categorias de supervisionados, como cooperativas de seguros, administradoras de proteção patrimonial mutualista, SPOCs e SSPEs.

A lógica está alinhada a uma diretriz internacional: alocar controles e recursos conforme os riscos identificados. Em fevereiro de 2025, o GAFI/FATF reforçou a proporcionalidade de suas recomendações e o estímulo a medidas simplificadas em contextos de menor risco. O ponto sensível, contudo, é operacional: como transformar uma AIR periodicamente documentada em critérios efetivamente usados para orientar diligência, monitoramento e investigação?

Uma classificação de baixo risco pode ser adequada no início da relação, mas exige revisão diante de mudanças cadastrais, societárias ou comportamentais. A maturidade do programa depende, portanto, menos da quantidade de controles e mais da capacidade de conectar a avaliação de risco às decisões tomadas ao longo do relacionamento.

Essa conexão exige definir quais fatores elevam ou reduzem a exposição, quando reavaliar uma classificação, quem pode aprovar exceções e como registrar o fundamento de cada encaminhamento. Ou seja, não basta atribuir uma nota estática ao cliente: a instituição precisa incorporar sinais provenientes de produtos, canais, contrapartes e operações, sem produzir avaliações automáticas discriminatórias ou desvinculadas de evidências. A proporcionalidade deve orientar a profundidade da diligência e não justificar perda de visibilidade sobre riscos relevantes.

O custo das decisões desconectadas

Nas seguradoras, subscrição, sinistros, prevenção a fraudes, PLD/FTP, compliance e gestão de riscos frequentemente examinam dimensões distintas de um mesmo cliente ou operação. Cada análise pode estar correta isoladamente e, ainda assim, a instituição perder informações relevantes quando os resultados não são correlacionados. Alterações de beneficiários, vínculos societários, transações e eventos de sinistro podem parecer triviais em separado, mas merecer diligência adicional quando observados em conjunto – sem que isso constitua, por si só, indício conclusivo de irregularidade.

A integração não elimina a segregação de funções nem a independência da auditoria interna. Significa compartilhar inteligência com regras claras de acesso, finalidade e responsabilização. A Resolução CNSP nº 416/2021 já estabelece fundamentos para sistemas de controles internos, estrutura de gestão de riscos e auditoria interna; e a Resolução CNSP nº 471/2024 aproxima gestão de riscos e gestão de capital por meio do ORSA nas entidades por ela abrangidas.

Esses referenciais ilustram uma mesma preocupação: uma decisão boa para determinada área pode gerar custos, exposições ou perdas quando seus efeitos são considerados no conjunto da organização. Não se trata de unificar todas as decisões, mas de assegurar que cada uma delas utilize o contexto relevante.

Na prática, essa integração pode assumir a forma de uma camada de decisão capaz de consumir dados e sinais de diferentes processos, aplicar políticas de maneira consistente e devolver encaminhamentos adequados a cada área. Um alerta de fraude, por exemplo, não precisa se converter automaticamente em suspeita de lavagem de dinheiro, mas pode enriquecer a avaliação de risco e orientar verificações. O desenho deve respeitar a finalidade dos dados, a necessidade de compartilhamento e a autonomia decisória dos responsáveis.

Governança: decisões verificáveis anos depois

Com a crescente adoção de modelos analíticos e de IA, surge uma pergunta essencial: se uma classificação de risco for questionada anos após a sua emissão, a instituição conseguirá demonstrar quais dados, regras, versões de modelos e políticas sustentaram aquele resultado?

No setor bancário, a Resolução Conjunta nº 18/2025 dispõe sobre a qualidade das informações

prestadas na esfera de atuação do Banco Central e exige, entre outros elementos, governança e controles documentados.

Seu art. 11 fixa retenção mínima de cinco anos para a documentação da política de qualidade da informação e seus relatórios específicos; porém não determina a reprodução universal de toda decisão automatizada por esse período.

No setor de seguros, a Circular Susep nº 605/2020 estabelece regras próprias para o armazenamento de documentos operacionais, em geral, por cinco anos, com condições e marcos de contagem próprios. A Consulta Pública Susep nº 11/2026 propõe ampliar as obrigações das supervisionadas quanto à guarda de documentos que subsidiam auditorias independentes – proposta que não deve ser confundida com uma obrigação já vigente.

Convém distinguir rastreabilidade (identificar insumos, versões e responsáveis), de reprodutibilidade (recalcular um resultado sob condições equivalentes) e de auditabilidade (dispor de evidências verificáveis). Sistemas generativos nem sempre permitem repetir respostas de forma idêntica. Portanto, preservar entradas, saídas, versões, contexto, intervenções humanas e justificativas pode ser indispensável, conforme a finalidade e a legislação aplicável.

Para as instituições, isso sugere políticas de versionamento, registro de critérios, retenção de evidências e testes periódicos de recuperação. Uma trilha auditável deve permitir distinguir a sugestão de um modelo da decisão institucional efetivamente aprovada, além de registrar alterações de política e eventuais intervenções manuais. A resposta adequada não é armazenar indiscriminadamente toda informação, mas preservar o conjunto necessário de evidências pelo prazo aplicável, com proteção contra acesso indevido, alteração e exposição de dados pessoais.

No plano internacional, a Associação Internacional de Supervisores de Seguros (IAIS), em seu Application Paper de 2025, também destaca governança, responsabilização, robustez, transparência e explicabilidade na supervisão da IA em seguros. Portanto, uma decisão inteligente precisa continuar compreensível e verificável quando o modelo ou o processo já tiver mudado.

Analytics, IA e a próxima fronteira da identidade

Nesse cenário, regras de negócio, modelos estatísticos e de machine learning, detecção de anomalias e Network Analytics têm papéis complementares. A análise de redes permite correlacionar pessoas, empresas, beneficiários e intermediários; enquanto motores de decisão podem reunir políticas, modelos e fluxos operacionais. Já a IA generativa e os agentes podem apoiar na triagem, leitura de documentos, contextualização e preparação de investigações. O verdadeiro ganho vem da combinação de diferentes técnicas em uma arquitetura governada, e não da adoção indiscriminada da tecnologia mais recente.

Uma fronteira emergente é a identidade de agentes digitais. KYC, KYB e identificação de beneficiários finais continuam essenciais, mas o uso de agentes capazes de interagir e executar atividades delegadas insere perguntas adicionais: quem controla o agente, em nome de quem ele atua, que permissões ele recebeu e como sua ação pode ser auditada?

Essas questões vão muito além de de identificar o usuário que iniciou uma sessão. Um agente pode atuar por horas, recorrer a ferramentas externas e encadear tarefas que não estavam explicitamente visíveis no primeiro comando. Para garantir segurança, a instituição precisará associar sua identidade a um responsável, limitar escopos de atuação, registrar delegações e prever revogação de permissões. A mesma identidade digital que permite eficiência operacional deve constituir uma fronteira de controle, não um caminho alternativo para contorná-la.

A discussão conhecida como Know Your Agent (KYA) é uma extensão conceitual de identidade, autenticação e autorização, não uma exigência criada pela Resolução Susep 99/2026. O NIST publicou, em fevereiro de 2026, um documento conceitual sobre identidade e autoridade de agentes de software e IA, abordando questões de autenticação, controles de acesso, auditoria e

responsabilização.

Imagine um agente autorizado a consultar uma apólice ou acompanhar uma solicitação em nome de um segurado. Essa autorização permitiria também alterar beneficiários ou solicitar resgates? A resposta exige mecanismos proporcionais de delegação, restrição de privilégios e validação adicional para operações sensíveis. Conhecer o cliente seguirá sendo fundamental; conhecer quem – ou o que – age em seu nome será parte crescente da confiança digital.

Inteligência proporcional também significa custo previsível

A adoção de IA generativa acrescenta também uma variável econômica: consumo de tokens, processamento, latência, integrações, reprocessamentos e revisão humana podem produzir custos flutuantes. Nem toda operação, porém, exige um grande modelo generativo. Muitas tarefas podem ser resolvidas com regras, classificadores, algoritmos de detecção ou modelos preditivos mais simples.

Arquiteturas híbridas podem classificar a tarefa e encaminhá-la ao mecanismo adequado, recorrendo a modelos generativos menores ou maiores apenas quando seu valor adicional justificar o custo e o risco.

Trabalhos como FrugalGPT e RouteLLM (ICLR 2025) investigam estratégias de seleção e escalonamento de modelos para equilibrar qualidade e custo. Os resultados de pesquisa não equivalem, naturalmente, a garantias universais em produção.

Há ainda uma oportunidade de converter padrões repetitivos identificados com apoio de modelos generativos em regras ou modelos tradicionais, desde que submetidos a validação, monitoramento e revisão. Isso pode diminuir chamadas desnecessárias a serviços mais caros e aumentar a previsibilidade do custo por decisão. Importante lembrar que baixa complexidade técnica não significa baixo risco regulatório: uma operação simples pode demandar diligência reforçada.

Esse roteamento pode considerar métricas como confiança da classificação, custo estimado, tempo de resposta, criticidade da decisão e necessidade de revisão humana. Tarefas bem definidas podem seguir fluxos determinísticos; situações ambíguas podem passar por modelos especializados; casos mais exigentes podem ser escalonados para modelos avançados ou especialistas. O gerenciamento dessa complexidade também facilita projeções de capacidade, orçamentos e acordos de nível de serviço. A arquitetura deve, contudo, ser testada em dados representativos antes de entrar em produção.

O objetivo não é minimizar tokens a qualquer preço, mas selecionar a inteligência adequada à natureza e ao risco de cada decisão, sem sacrificar qualidade, governança ou segurança.

Efetividade: medir decisões, não apenas atividades

Programas de PLD/FTP acompanham volumes de alertas, casos analisados e comunicações efetuadas – indicadores úteis, mas insuficientes para demonstrar efetividade. Eles também importam cobertura dos cenários de risco, qualidade dos dados, consistência de classificações, tempo de resposta, resultados de validações, rastreabilidade e capacidade de detectar comportamentos relevantes.

Com a automação, passa a fazer sentido medir também a estabilidade de modelos, escalonamentos para revisão especializada, custo por caso e qualidade das evidências produzidas. O objetivo não é simplesmente reduzir alertas ou ampliar comunicações: é identificar, analisar e tratar riscos de maneira proporcional, preservando os deveres legais e a capacidade de explicar decisões. Tecnologia só agrega valor quando seus resultados podem ser avaliados.

Isso exige fechar o ciclo de aprendizado. Resultados de investigações, revisões independentes, exceções e alterações no ambiente de ameaças devem retroalimentar políticas e modelos, com

testes de eficácia e controle de mudanças. Um sistema que reduz o tempo de análise, mas deixa de identificar padrões relevantes, não é necessariamente mais eficiente. A métrica mais útil combina desempenho operacional com qualidade das decisões, cobertura de riscos e comprovação de que o controle cumpriu sua finalidade.

Uma agenda comum para o mercado segurador e financeiro

Bancos, seguradoras, entidades de previdência e cooperativas operam sob regras e estruturas distintas, mas compartilham desafios de governança, crimes financeiros, identidade, dados e decisões automatizadas. A aproximação entre esses debates não pressupõe superioridade de um setor sobre o outro, mas abre espaço para o intercâmbio de experiências e para soluções que respeitem as particularidades de cada negócio.

É nesse contexto que a realização conjunta dos congressos PLDFT e GRISC da FEBRABAN, em 17 e 18 de novembro de 2026, em São Paulo, se torna oportuna. A programação oficial reúne debates sobre supervisão, governança, riscos, IA, qualidade da informação e prevenção a crimes financeiros. Para o mercado segurador, é uma oportunidade de ampliar o diálogo com outros participantes do sistema financeiro.

No dia 18 de novembro, das 11h05 às 11h35, participarei, pelo SAS, com Camila Vieira, do Santander Brasil, da sessão “Enterprise Decisioning: o custo das decisões desconectadas”. A discussão examinará os efeitos de decisões isoladas sobre perdas, capital e solvência, além do papel de dados, analytics, IA e políticas de negócio na construção de decisões mais coordenadas.

O encontro pode ser um espaço útil para profissionais do setor segurador examinarem como esses desafios se manifestam em diferentes modelos de negócio. As experiências não são intercambiáveis automaticamente: produtos, marcos regulatórios e perfis de risco variam. Mas a discussão sobre governança, coordenação entre linhas de defesa, qualidade informacional e decisão baseada em risco é suficientemente transversal para justificar uma agenda de colaboração entre mercados.

Conectar riscos, informações e decisões

A Resolução Susep 99/2026 oferece um momento oportuno para revisitar a integração de PLD/FTP com gestão de riscos, controles internos e processos de negócio. Sua implementação não se resume à adoção de tecnologia, nem implica substituir o julgamento profissional ou afastar as responsabilidades de cada linha de defesa.

A transformação relevante é outra: usar melhor as informações disponíveis, tornar decisões verificáveis ao longo do tempo, governar a atuação de identidades humanas e digitais e empregar a complexidade tecnológica de forma justificável.

Afinal, uma decisão que parece adequada isoladamente continua sendo a melhor quando consideramos seus efeitos sobre toda a organização – hoje e no futuro?



Por Ricardo Saponara

SOBRE O AUTOR

Ricardo Saponara é executivo do SAS, com atuação na América Latina em soluções e estratégias de gestão de riscos, prevenção a fraudes e compliance. Atuário, mestre em Economia e professor de pós-graduação, possui experiência em analytics, inteligência artificial, gestão de riscos e transformação dos processos decisórios em instituições financeiras, seguradoras, governos, telecomunicações e outros setores da economia.

(09.11.2026)