MANUAL OPERACIONAL DE KYC

(CONHEÇA SEU CLIENTE)

IZA Seguradora S.A.

Sumário

MANUAL OPERACIONAL DE KYC (CONHEÇA SEU CLIENTE) 4
1. Objetivo 4
2. Abrangência 5
3. Fluxo Operacional de KYC 7
Etapa 1: Coleta de Informações 7
Checklist Obrigatório e Orientações: 7
Procedimentos Especiais de Coleta: 9
Etapa 4: Aprovação de Cadastro 9
Pré-requisitos para aprovação: 10
A) Clientes de Baixo Risco 10
B) Clientes de Médio Risco 10
C) Clientes de Alto Risco 11
Recusa de Cadastro: 12
Fluxo de Exceção (Overruling): 12
Etapa 5: Monitoramento Contínuo 13
A) Comportamentais e Operacionais: 14
B) Financeiros e Patrimoniais: 14
Procedimento de Análise de Alertas: 15
Fluxo de Reporte (Resumo Visual): 17
Etapa 6: Reporte de Operações Suspeitas 19
1. Análise da Operação 19
2. Registro Interno 20
3. Comunicação ao COAF (Quando Aplicável) 21
4. Arquivamento do Dossiê 22
4. Regras Específicas 24
4.1 Pessoas Politicamente Expostas (PEP) 25
4.2 Clientes de Alto Risco 26
4.4 Disposições Gerais 27
5. Atualização Cadastral 28
5.1 Periodicidade da Atualização 29

5.2 Procedimento de Atualização 30
5.2.1 Fluxo Operacional 30
5.2.2 Procedimentos Detalhados 30
5.3 Documentação Exigida na Atualização 31
5.4 Tratamento de Não Resposta 31
5.5 Atualização por Iniciativa do Cliente 32
5.6 Penalidades por Cadastro Desatualizado 32
5.7 Registro e Guarda de Documentos 33
5.8 Indicadores de Efetividade (KPIs) 33
5.9 Disposições Gerais 33
6. Registro e Evidências 34
6.1 Documentos e Evidências a Serem Registrados 34
6.2 Prazo de Guarda 35
6.3 Formato e Qualidade da Guarda 36
6.3.1 Meio de Armazenamento 36
6.3.2 Sistemas Utilizados 37
6.4 Controles de Acesso e Sigilo 37
6.5 Política de Retenção e Descarte 38
6.5.1 Retenção Ativa 38
6.5.2 Descarte Seguro 38
6.5.3 Suspensão do Descarte 39
6.6 Responsabilidades Específicas 39
6.7 Trilha de Auditoria (Audit Trail) 40
6.8 Check-list de Conformidade (para auditorias internas) 40
6.9 Disposições Gerais 40
7. Responsabilidades 41
7.1 Estrutura das Linhas de Defesa 41
7.2 Responsabilidades Detalhadas por Área 42
7.2.1 Comercial (1ª Linha de Defesa) 42
7.2.2 Atendimento / Cadastro (1ª Linha de Defesa) 42
7.2.3 Compliance (2ª Linha de Defesa) 43
7.2.4 Diretoria (Alta Administração) 44

7.3 Responsabilidades Complementares (Outras Áreas) 46
7.4 Matriz de Responsabilidades (RACI) 46
7.5 Responsabilidade Solidária e Consequências 47
7.5.1 Responsabilidade Solidária 47
7.5.2 Consequências do Descumprimento 47
7.6 Canal de Reporte (Linha Ética) 48
7.7 Disposições Gerais 49
8. Treinamento 49
8.1 Periodicidade e Carga Horária 50
8.2 Conteúdo Programático 50
8.2.1 Treinamento Básico (Obrigatório para Todos) 50
8.2.2 Treinamento Específico por Área 51
8.3 Metodologia e Formatos 53
8.4 Registro e Controle 53
8.5 Avaliação de Efetividade 53
8.6 Treinamento para Parceiros e Prestadores de Serviço 54
8.7 Cronograma Anual de Treinamentos 54
8.8 Consequências da Não Participação 55
8.9 Disposições Gerais 56
8.10 Indicadores de Treinamento (KPIs) 56
9. Auditoria e Controles 57
9.1 Estrutura de Controles 57
9.2 Auditoria Interna Periódica 58
9.2.2 Metodologia da Auditoria 59
9.2.3 Amostragem 59
9.3 Testes de Aderência 59
9.3.1 Tipos de Testes 60
9.3.2 Roteiro de Testes de Aderência (Exemplos) 60
9.4 Indicadores de Efetividade (KPIs) 60
9.4.1 Indicadores de Processo 61
9.4.2 Indicadores de Monitoramento 61
9.4.3 Indicadores de Reporte 61

9.4.4 Indicadores de Treinamento 62
9.5 Painel de Controle (Dashboard) 62
9.6 Plano de Ação Corretiva 62
9.7 Reporte à Alta Administração 63
9.8 Melhoria Contínua 63
9.9 Disposições Gerais 64
10. Penalidades 65
10.1 Infrações e Classificação de Gravidade 65
10.2 Sanções Internas (Colaboradores) 65
10.2.1 Procedimento Disciplinar 66
10.3 Sanções para Parceiros e Prestadores de Serviço 66
10.4 Sanções Regulatórias (SUSEP / COAF) 67
10.4.1 Sanções Previstas na Lei 9.613/98 67
10.4.2 Sanções Previstas na Circular SUSEP nº 612/2020 68
10.4.3 Consequências Acessórias 68
10.5 Responsabilização Individual dos Administradores 68
10.6 Matriz de Responsabilização e Penalidades 69
10.7 Agravantes e Atenuantes 69
10.8 Comunicação de Penalidades 70
10.9 Programa de Integridade (Compliance) 70
10.10 Disposições Gerais 70
10.11 Termo de Ciência e Compromisso (Modelo) 71
11. Vigência 72

1. Objetivo

Estabelecer procedimentos operacionais detalhados para identificação, qualificação, classificação de risco e monitoramento de clientes, assegurando conformidade com a Circular SUSEP nº 612/2020 e demais normativos de PLD/FT.

O presente Manual tem como objetivo estabelecer as diretrizes e os procedimentos operacionais padronizados para a efetiva implementação da política de "Conheça seu Cliente" (KYC - Know Your Customer) no âmbito da IZA Seguradora S.A.

Este documento visa garantir a identificação inequívoca, a qualificação detalhada (incluindo a cadeia de envolvidos, como representantes, beneficiários e prestadores de serviço), a adequada classificação do perfil de risco e o monitoramento contínuo de todos os relacionamentos comerciais.

Ao formalizar estas etapas, a Seguradora busca:

- Mitigar riscos reputacionais, legais e operacionais, prevenindo o uso de seus produtos e serviços para atividades ilícitas como lavagem de dinheiro e financiamento do terrorismo.
- Assegurar a conformidade estrita com a legislação vigente, especialmente as disposições da Circular SUSEP nº 612/2020, da Lei nº 9.613/1998 e alterações posteriores, e demais normativos aplicáveis ao mercado de seguros.
- Promover a integridade e a transparência nas relações contratuais, assegurando que a IZA Seguradora S.A. opere apenas com contrapartes idôneas e cuja origem e destino dos recursos sejam compatíveis com sua capacidade econômico-financeira e atividade declarada.
- Subsidiar a área de Compliance e a Alta Administração com informações precisas para a tomada de decisão, a manutenção de cadastros de qualidade e a tempestiva comunicação de operações suspeitas ao órgão regulador (COAF/SUSEP).

Em suma, o objetivo deste manual não é apenas o cumprimento de uma obrigação normativa, mas a consolidação de uma cultura de prevenção, onde a diligência na identificação e no monitoramento do cliente é a primeira e

mais importante linha de defesa da Seguradora contra o envolvimento em crimes financeiros.

---

2. Abrangência

Este Manual e as diretrizes da Política "Conheça seu Cliente" são de observância obrigatória para todas as áreas, colaboradores, parceiros e terceirizados que, direta ou indiretamente, interajam com dados, informações ou negociações envolvendo clientes da IZA Seguradora S.A.

Compreendendo que a prevenção à lavagem de dinheiro e o conhecimento do cliente são responsabilidades difusas e permanentes, este normativo aplica-se de forma transversal a todas as fases do ciclo de vida do cliente, abrangendo, mas não se limitando, às seguintes áreas e suas respectivas responsabilidades:

- **Comercial (Front Line):** Responsável pela primeira barreira de prevenção. Deve aplicar a due diligence inicial na prospecção, coletar a documentação obrigatória no primeiro contato, e estar atenta a sinais de alerta ou comportamentos atípicos que possam indicar tentativas de burlar os controles da seguradora.
- **Subscrição:** Deve incorporar a análise de risco do cliente (KYC) e a verificação de background (inclusive de pessoas expostas politicamente - PEP) como parte intrínseca do processo de aceitação do risco. A decisão de emitir ou não uma apólice deve considerar não apenas o risco atuarial, mas também o risco de integridade do cliente.
- **Sinistros:** Atua como uma linha de defesa crítica, onde o risco de fraude e lavagem de dinheiro pode se materializar. Deve verificar a consistência das informações do segurado e beneficiário no momento do pagamento, assegurando que os recursos sejam destinados à pessoa correta e que a ocorrência do sinistro seja legítima.
- **Atendimento:** Responsável pela interface direta e contínua com o cliente ao longo da vigência do contrato. Deve aproveitar cada interação (seja para emissão de boletos, emissão de segunda via de documentos, alterações contratuais ou simples esclarecimento de dúvidas) para validar a consistência das informações cadastrais, confirmar meios de contato e identificar comportamentos atípicos que possam ter passado despercebidos nas etapas iniciais. O atendimento é o "termômetro" da saúde do relacionamento com o cliente.

- **Compliance:** Atua como função central de supervisão e segunda linha de defesa. É responsável por elaborar e revisar o manual, definir os critérios de classificação de risco, homologar as ferramentas de screening, treinar as demais áreas, realizar o monitoramento automatizado e reportar as operações suspeitas aos órgãos reguladores.
- **Tecnologia da Informação (TI)**: Parceiro estratégico essencial. Deve prover e manter as ferramentas tecnológicas (sistemas de cadastro, bases de dados de PEP e listas restritivas, sistemas de BI para monitoramento) que viabilizem a automação dos controles, a rastreabilidade das ações e a segurança das informações tratadas.
- **Jurídico:** Atua em conjunto com o Compliance na interpretação das normas, na análise de casos limítrofes e na fundamentação legal para eventuais comunicações ao COAF, além de apoiar na elaboração de cláusulas contratuais que reforcem as obrigações de KYC.

Responsabilidade Solidária:

A IZA Seguradora entende que o conhecimento do cliente não é uma ação pontual, mas um processo integrado. A falha em qualquer uma destas áreas pode comprometer todo o sistema de prevenção. Portanto, a responsabilidade pela aplicação deste manual é solidária e compartilhada entre todas as áreas listadas, que devem atuar de maneira coordenada, comunicando imediatamente à área de Compliance qualquer inconsistência, omissão ou indício de irregularidade identificado em suas respectivas etapas de atuação.

---

3. Fluxo Operacional de KYC

O processo de "Conheça seu Cliente" (KYC) na IZA Seguradora S.A. estrutura-se em etapas sequenciais e complementares, garantindo a diligência necessária em cada fase do relacionamento com o cliente. A observância rigorosa deste fluxo é condição indispensável para a emissão de propostas, renovação de apólices e pagamento de sinistros.

Etapa 1: Coleta de Informações

Responsáveis: Comercial (prospecção e captação inicial) e Atendimento (validação e complementação cadastral)

Objetivo: Obter, de forma completa e fidedigna, o conjunto mínimo de dados cadastrais que permita à Seguradora conhecer a real identidade, capacidade financeira e propósito do cliente na contratação do seguro.

Diretrizes Gerais:

1. Proibição de Cadastros Incompletos: É vedado o início de qualquer relacionamento comercial (emissão de proposta, cotação vinculante ou emissão de apólice) sem o preenchimento integral de todos os campos obrigatórios definidos neste manual.

2. Obrigatoriedade de Documentos: Todos os documentos listados abaixo deverão ser apresentados em cópia digital legível (ou física, quando aplicável) e conferidos com o original pelo responsável da coleta.

3. Atualização e Validade: O cliente é responsável pela veracidade das informações prestadas. A Seguradora reserva-se o direito de solicitar documentos complementares sempre que julgar necessário para a correta qualificação do risco.

Checklist Obrigatório e Orientações:

A) Para Pessoas Físicas (Segurado, Beneficiário, Representante Legal ou Procurador)

- Nome Completo: Exigir o nome civil completo, sem abreviações, conforme consta no documento de identificação.

- CPF (Cadastro de Pessoas Físicas): Obrigatório e deve ser validado quanto à situação cadastral na base da Receita Federal (regular, suspensa, cancelada, etc.).

- Documento de Identificação com Foto (RG, CNH, Passaporte ou RNE):
✔ Exigir cópia nítida da frente e verso.
✔ Verificar a data de expedição e a validade do documento.
✔ No caso de procurador, anexar também o instrumento particular de procuração com poderes específicos
.
- Data de Nascimento: Fundamental para o cálculo de risco atuarial e para a triagem em bases de monitoramento (menores de idade

requerem representantes; maiores de 60 anos podem exigir cuidados especiais).

- Endereço Completo: Logradouro, número, complemento, bairro, CEP, cidade e estado.
- Exigir comprovante de residência atualizado (últimos 90 dias) em nome do cliente. Caso o comprovante seja em nome de cônjuge ou pais, solicitar documentação que comprove o vínculo (certidão de casamento, por exemplo).

- Profissão e Renda Estimada:

✔ A profissão deve ser detalhada (ex: "Engenheiro Civil" ao invés de apenas "Engenheiro"; "Médico Cardiologista" ao invés de "Médico").

✔ A renda estimada deve ser compatível com o prêmio do seguro e com o capital segurado contratado. Discrepâncias gritantes devem ser reportadas ao Compliance.

B) Para Pessoas Jurídicas (Segurado Tomador / Estipulante)

- Razão Social: Nome completo da empresa, exatamente como registrado no CNPJ.
- Nome Fantasia (se houver): Para correta identificação comercial.
- CNPJ (Cadastro Nacional da Pessoa Jurídica): Obrigatório, com validação da situação cadastral (ativa, baixada, suspensa, etc.) na Receita Federal.
- Contrato Social e/ou Estatuto Social (consolidado):

✔ Exigir a última alteração contratual consolidada ou o contrato social vigente.

✔ Verificar o objeto social da empresa: a atividade declarada é compatível com o risco a ser segurado?

- **Quadro Societário (composição):**

✔ Coletar a relação completa de todos os sócios com participação relevante (conforme definição interna, geralmente acima de 10% ou 25%, ou conforme limite legal).

✔ Para sociedades anônimas de capital aberto, essa diligência pode ser simplificada, focando nos acionistas controladores.

- **Identificação do Beneficiário Final:**

- ✔ Conceito: Pessoa(s) natural(is) que, direta ou indiretamente, possua(m), controle(m) ou influencie(m) significativamente a entidade. Aplica-se o conceito de "Pessoa Exposta" nos termos da regulamentação.

- ✔ Obrigação: Identificar a cadeia de participação até chegar à(s) pessoa(s) física(s). Se, após todos os esforços, não for possível identificar o beneficiário final, a pessoa que exerce o controle gerencial (diretor presidente ou similar) deverá ser assim qualificada, e o caso deverá ser submetido à análise de Compliance para risco elevado.

- Endereço da Sede (Completo): Logradouro, número, complemento, bairro, CEP, cidade e estado, com comprovante de endereço em nome da empresa (conta de consumo, contrato de locação, etc.).

Procedimentos Especiais de Coleta:

- Pessoas Expostas Politicamente (PEP): Durante a coleta, o sistema ou o colaborador deverá verificar se o cliente (ou seu beneficiário final) se enquadra como PEP (conforme definição da Susep). Em caso positivo, a proposta deverá ser encaminhada para análise aprofundada pela Subscrição/Compliance.

- Clientes Não Residentes: Para estrangeiros sem domicílio no Brasil, exigir passaporte, visto vigente e comprovante de endereço no exterior. A avaliação de risco será elevada.

- Recusa de Fornecimento: Caso o cliente se recuse a fornecer qualquer informação ou documento obrigatório, o atendimento deverá ser imediatamente interrompido, a proposta recusada e o fato comunicado formalmente à área de Compliance para registro.

Etapa 4: Aprovação de Cadastro

Objetivo: Formalizar a validação definitiva do cadastro do cliente, assegurando que a decisão de estabelecer ou manter o relacionamento comercial seja tomada pela instância adequada, conforme o nível de risco previamente classificado nas etapas de coleta e triagem.

Pré-requisitos para aprovação:

- Todas as informações obrigatórias da Etapa 1 (Coleta) foram preenchidas e validadas.
- A triagem da Etapa 2 (Background Check) foi concluída, com verificação em bases restritivas, PEP e listas de sanções.
- O cliente foi devidamente classificado na Etapa 3 (Classificação de Risco) como Baixo, Médio ou Alto Risco.

Fluxo Decisório por Nível de Risco:

A) Clientes de Baixo Risco

Responsável pela Aprovação: Automático (via sistema) ou Subscrição (em casos de parametrização específica).

- **Procedimento:**

✔ Aprovação Automática: Para clientes que atendam a todos os critérios objetivos de baixo risco (ex: fontes de renda claras, profissão de baixo risco, sem ocorrências em listas restritivas, compatibilidade entre renda e prêmio), o sistema poderá liberar a emissão da apólice de forma automática, sem intervenção humana adicional.

✔ Validação pela Subscrição: Em casos onde o sistema identifique a necessidade de uma análise técnica (mesmo para baixo risco), a Subscrição poderá aprovar o cadastro de forma simplificada, desde que não haja qualquer suspeita ou alerta não endereçado.

- **Tempo de Resposta: Imediato ou até 24 horas úteis.**

B) Clientes de Médio Risco

- Responsável pela Aprovação: Subscrição (com ciência do Compliance, se parametrizado).

- **Procedimento:**

✔ A Subscrição deverá realizar uma análise aprofundada das informações, verificando a coerência entre os dados declarados e os documentos apresentados.

✔ Poderão ser solicitados documentos complementares para esclarecimento de pontos específicos (ex: comprovante de capacidade financeira, declaração de origem dos recursos).

✔ A aprovação somente poderá ocorrer após o saneamento de todos os alertas de nível moderado identificados na triagem.

✔ O Compliance deverá ter acesso ao parecer da Subscrição e poderá, a seu critério, solicitar reanálise ou elevação da classificação de risco.

- **Tempo de Resposta: Até 48 horas úteis**

C) Clientes de Alto Risco

- **Responsável pela Aprovação**: Compliance + Diretoria (aprovadores formais).

- **Procedimento:**

✔ Análise pelo Compliance: A área de Compliance receberá o dossiê completo do cliente, incluindo toda a documentação, histórico de triagem e justificativa comercial para a contratação. Deverá elaborar um parecer técnico detalhado, contemplando:

✔ Análise da origem dos recursos.

✔ Contextualização da exposição política (se PEP).

✔ Avaliação do propósito do seguro e sua adequação ao perfil do cliente.

✔ Identificação de redes de relacionamento ou estruturas societárias complexas.

✔ Análise de background expandida (buscas em mídias, bases internacionais, etc.).

- **Deliberação da Diretoria**: Após parecer do Compliance, o processo será submetido à instância diretiva competente (Diretor de Operações, Diretor de Riscos ou Comitê de Compliance, conforme definido no organograma de alçadas).

✔ A Diretoria poderá: (i) aprovar o cadastro, com ou sem restrições; (ii) solicitar diligências adicionais; ou (iii) rejeitar o cadastro e negar o estabelecimento do relacionamento.

✔ Comunicação e Registro: Todas as decisões relativas a clientes de alto risco deverá ser formalizadas em ata ou documento específico, com a

devida justificativa, e arquivadas pelo Compliance para eventual auditoria ou fiscalização.

- **Tempo de Resposta**: Até 5 dias úteis (podendo ser estendido mediante complexidade).

Disposições Gerais sobre Aprovação:			
Nível de Risco	Responsável pela Aprovação	Alçada Decisória	Exigência de Documentação
Baixo Risco	Automático Subscrição	Operacional	Mínima obrigatória
Médio Risco	Subscrição	Tática	Complementar (se necessário)
Alto Risco	Compliance + Diretoria	Estratégica	Reforçada e justificada

Recusa de Cadastro:

A IZA Seguradora reserva-se o direito de recusar o cadastro e, consequentemente, não estabelecer o relacionamento comercial nas seguintes situações:

1. Falta de informações: Cliente se recusa a fornecer dados ou documentos obrigatórios.

2. Inconsistência grave: Discrepância insanável entre as informações prestadas e os documentos apresentados.

3. Ocorrência em listas restritivas: Presença em listas de sanções internacionais (ONU, OFAC, União Europeia) ou condenações por crimes de lavagem de dinheiro, corrupção ou terrorismo.

4. Atividade incompatível: Objeto social ou atividade profissional incompatível com os valores ou apetite de risco da Seguradora.

5. Parecer negativo do Compliance: Fundamentação técnica pela área de Compliance contraindique o relacionamento.

Fluxo de Exceção (Overruling):

Em situações excepcionais e devidamente justificadas, a Diretoria (ou instância superior) poderá autorizar a aprovação de cadastro mesmo com parecer inicial desfavorável de área técnica, desde que:

- Haja justificativa comercial robusta e documentada.
- Sejam estabelecidos controles adicionais de monitoramento para o cliente.
- A decisão seja formalizada e arquivada pelo Compliance, com ciência do Conselho de Administração (se aplicável).

Encadeamento das Etapas (visão geral do fluxo completo):			
Etapa	Descrição	Responsável Principal	Entregável
1	Coleta de Informações	Comercial / Atendimento	Dossiê do cliente completo
2	Triagem e Verificação	Compliance / Automação (TI)	Relatório de background check
3	Classificação de Risco	Compliance / Subscrição	Classe de risco definida (Baixo/Médio/Alto)
4	Aprovação de Cadastro	Automático / Subscrição / Compliance + Diretoria	Cadastro aprovado ou recusado
5	Monitoramento Contínuo	Compliance / Áreas de Negócio	Alertas tratados e atualizações periódicas

---

Etapa 5: Monitoramento Contínuo

Responsável: Compliance (gestão do processo e análise de alertas), com suporte de TI (parametrização de sistemas) e áreas de negócio (reporte de atipicidades identificadas no dia a dia).

Objetivo: Acompanhar permanentemente as operações realizadas pelos clientes, identificando comportamentos atípicos ou inconsistentes que possam indicar indícios de lavagem de dinheiro, financiamento do terrorismo, fraude ou outras irregularidades, bem como assegurar a atualização periódica das informações cadastrais.

Diretrizes Gerais:

1. Monitoramento Baseado em Risco: A frequência e a profundidade do monitoramento serão proporcionais ao nível de risco do cliente. Clientes de alto risco serão submetidos a revisões mais frequentes e criteriosas.
2. Ferramentas Tecnológicas: A IZA Seguradora utilizará sistemas automatizados de monitoramento, parametrizados conforme os gatilhos de alerta definidos neste manual, para rastrear operações e gerar alertas para análise humana.
3. Registro e Rastreabilidade: Todas as análises realizadas (alertas confirmados, descartados ou em investigação) deverão ser devidamente registradas em sistema ou documento próprio, garantindo a rastreabilidade e o histórico das decisões.
4. Tempestividade: Os alertas gerados deverão ser analisados pelo Compliance em prazo compatível com a criticidade da situação, não superior a 30 (trinta) dias corridos, salvo justificativa fundamentada.

Gatilhos de Alerta Parametrizáveis:

A área de Compliance, em conjunto com a TI, deverá implementar e manter os seguintes gatilhos de alerta mínimos no sistema de monitoramento:

A) Comportamentais e Operacionais:

Gatilho de Alerta	Descrição	Possíveis Indícios
Fracionamento de operações	Diversas contratações de apólices, endossos ou pagamentos de prêmio em valores fracionados, realizados em curto espaço de tempo, que somados ultrapassam limites significativos.	Tentativa de burlar limites de identificação obrigatória ou ocultar a real capacidade financeira.
Cancelamentos recorrentes	Cliente que contrata e cancela apólices com frequência incomum, especialmente seguros de vida ou prestamista.	Possível tentativa de utilizar o cancelamento para recebimento de valores (devolução de prêmio) de forma
Alterações cadastrais frequentes	Múltiplas solicitações de mudança de endereço, telefone, e-mail ou beneficiários em curto intervalo de tempo.	Possível tentativa de utilizar o cancelamento para recebimento de valores (devolução de prêmio) de forma pulverizada.
Sinistros atípicos	Ocorrência de sinistros logo após o início da vigência da apólice (período de carência recém-cumprido) ou com documentação inconsistente.	Fraude ou tentativa de recebimento de indenização com base em informações falsas.
Beneficiários incomuns	Indicação de beneficiários sem vínculo familiar ou econômico aparente com o segurado, especialmente em seguros de vida.	Possível ocultação de parte interessada ou tentativa de transferência de recursos para terceiros não

B) Financeiros e Patrimoniais:

Gatilho de Alerta	Descrição	Possíveis Indícios
Incompatibilidade financeira	Contratação de prêmios ou capitais segurados manifestamente incompatíveis com a renda declarada, patrimônio conhecido ou atividade profissional do cliente.	Possível utilização de recursos de origem ilícita ou declaração falsa de capacidade financeira.
Pagamentos por terceiros não autorizados	Pagamento de prêmios por pessoas físicas ou jurídicas sem relação contratual direta com o seguro, sem justificativa plausível.	Ocultação do real beneficiário ou origem dos recursos (laranja).
Utilização de meios de pagamento atípicos	Pagamentos frequentes em espécie de valores elevados (acima do limite regulatório) ou utilização de contas de terceiros para liquidação de prêmios.	Indício de lavagem de dinheiro ou evasão fiscal.
Movimentação incomum em produtos de acumulação	Aportes ou resgates atípicos em produtos com componente de investimento ou acumulação (VGBL, PGBL), sem justificativa econômica.	Possível ocultação de patrimônio ou movimentação de recursos de origem duvidosa.

Procedimento de Análise de Alertas:

Ao receber um alerta gerado pelo sistema, a área de Compliance deverá seguir o seguinte fluxo:

1. **Triagem Inicial:**

✔ Verificar a consistência do alerta (falso positivo ou alerta real).
✔ Reunir toda a documentação e histórico do cliente.
✔ Consultar as áreas de negócio (Comercial, Atendimento, Subscrição) para obter contexto adicional sobre a operação.

2. **Análise Aprofundada (se aplicável):**

✔ Realizar pesquisas adicionais em bases públicas, mídias e listas restritivas.
✔ Solicitar esclarecimentos ao cliente (quando cabível e sem alertar sobre a investigação de PLD).
✔ Elaborar relatório preliminar de análise.

3. **Conclusão e Classificação:**

✔ Alertas Justificados (Falso Positivo): O analista registra a justificativa pela não confirmação da suspeita e arquiva o caso, mantendo o histórico.
✔ Alertas Confirmados (Suspeita Fundada): O analista aprofunda a investigação e prepara um dossiê para deliberação.

4. **Comunicação ao COAF (quando aplicável):**

✔ Confirmada a suspeita de lavagem de dinheiro ou financiamento do terrorismo, o Compliance deverá elaborar a comunicação negativa ao

Conselho de Controle de Atividades Financeiras (COAF), nos termos da regulamentação vigente.

- ✔ A comunicação deverá ser realizada em até 24 horas (para casos de financiamento do terrorismo) ou no prazo estabelecido na Circular Susep (para demais operações suspeitas).
- ✔ A decisão de comunicar deverá ser formalizada e aprovada pelo Diretor responsável.

5. Atualização do Perfil de Risco:

- ✔ Caso a análise confirme indícios relevantes (mesmo sem comunicação ao COAF), o Compliance poderá reclassificar o cliente para um nível de risco superior, submetendo-o a monitoramento mais rigoroso.
- ✔ Em situações extremas, poderá ser recomendado o encerramento do relacionamento comercial.

Atualização Cadastral Periódica (Refresh):

O monitoramento contínuo inclui também a obrigação de manter os dados cadastrais atualizados. A periodicidade da revisão cadastral seguirá o nível de risco:

Nível de Risco	Periodicidade da Atualização Cadastral
Baixo Risco	A cada 36 meses (3 anos)
Médio Risco	A cada 24 meses (2 anos)
Alto Risco	A cada 12 meses (1 ano)

Procedimento de Refresh:

- O sistema deverá emitir alerta para a área de Atendimento/Compliance sobre a data de vencimento da atualização cadastral.
- Será realizado contato com o cliente para confirmação e atualização dos dados.

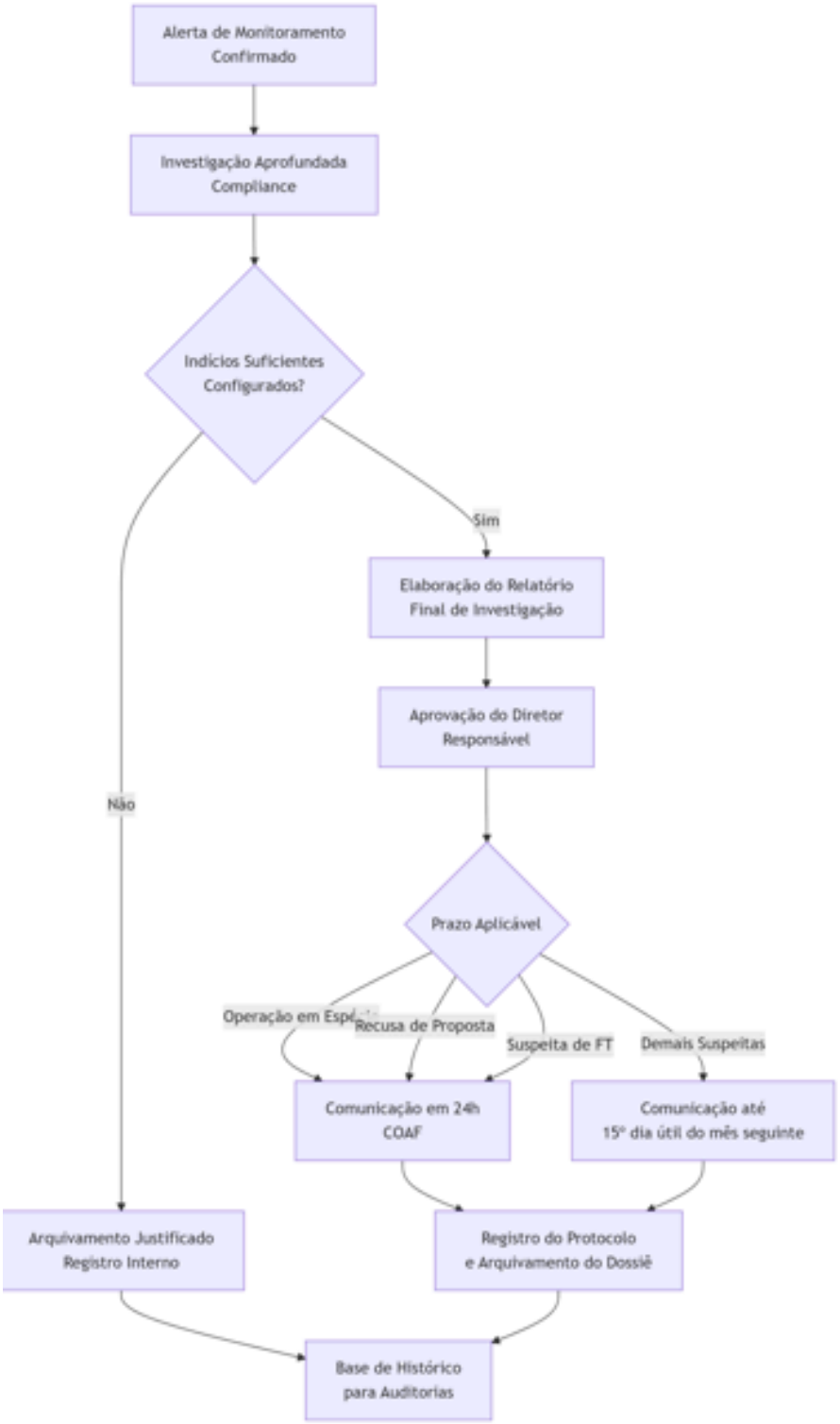
- A não atualização no prazo poderá ensejar a suspensão de novas contratações, endossos ou pagamentos de sinistros, até a regularização da situação cadastral.

Reporte à Alta Administração:

O Compliance deverá elaborar, com periodicidade mínima trimestral, um relatório gerencial de monitoramento contendo:

- Número de alertas gerados x analisados.
- Principais tipologias identificadas.
- Casos reclassificados para alto risco.
- Comunicações realizadas ao COAF.
- Propostas de aprimoramento dos controles.

Fluxo de Reporte (Resumo Visual):


Alerta de Monitoramento Confirmado
Investigação Aprofundada Compliance
Indícios Suficientes Configurados?
Não
Sim
Elaboração do Relatório Final de Investigação
Aprovação do Diretor Responsável
Prazo Aplicável
Operação em Espé
Recusa de Proposta
Suspeita de FT
Demais Suspeitas
Comunicação em 24h COAF
Comunicação até 15º dia útil do mês seguinte
Arquivamento Justificado Registro Interno
Registro do Protocolo e Arquivamento do Dossiê
Base de Histórico para Auditorias

Disposições Importantes:

- Comunicações por Decisão de Diretoria: Mesmo sem indícios robustos, se a Diretoria entender que a operação é sensível ou pode gerar dano reputacional, poderá autorizar a comunicação a título de cautela.

- Responsabilidade do Compliance: O analista de Compliance é responsável pela qualidade técnica da comunicação. Informações incompletas ou imprecisas podem prejudicar a análise do COAF e expor a Seguradora a sanções.

- Proibição de Vazamento: Qualquer colaborador que, de qualquer forma, divulgar a existência de uma comunicação ao COAF para o cliente ou terceiros não autorizados estará sujeito a sanções disciplinares internas, além das sanções legais cabíveis.

Etapa 6: Reporte de Operações Suspeitas

Responsável: Compliance

Objetivo: Formalizar a identificação de operações com indícios de lavagem de dinheiro ou financiamento do terrorismo, garantindo o cumprimento das obrigações legais e regulatórias perante o COAF e a SUSEP.

Fluxo Resumido:

Fase	Descrição	Responsável Principal	Prazo
1	Recebimento do alerta confirmado	Compliance	Imediato
2	Análise aprofundada da operação	Compliance	Até 15 dias
3	Decisão de comunicar ou arquivar	Compliance / Diretoria	Imediato após análise
4	Registro interno da decisão	Compliance	24h após decisão
5	Comunicação ao COAF (se aplicável)	Compliance	Conforme prazo legal
6	Arquivamento do dossiê	Compliance	10 anos

1. Análise da Operação

Atividades detalhadas:

- Reunir todo o dossiê do cliente (documentação KYC, histórico de interações, propostas, apólices, sinistros).
- Consolidar os alertas de monitoramento que originaram a suspeita.
- Realizar pesquisas complementares em bases públicas, mídias e listas restritivas.
- Consultar áreas internas (comercial, subscrição, sinistros) para obter contexto factual, sem revelar a suspeita de PLD.
- Elaborar relatório preliminar com a descrição dos fatos, inconsistências identificadas e fundamentação legal.

Critérios para aprofundamento da análise:

- Movimentações incompatíveis com a capacidade financeira do cliente
- Estruturas societárias complexas ou opacas
- Envolvimento de pessoas expostas politicamente (PEP)
- Operações fracionadas que sugerem burla a controles
- Indícios de utilização de "laranjas" ou interpostas pessoas
- Atipicidade em relação ao perfil declarado pelo cliente

2. Registro Interno

A) Hipótese de Arquivamento:

Quando a análise concluir que **não há elementos suficientes** para configurar uma suspeita fundada:

Atividade	Detalhamento
Justificativa	Elaborar nota técnica explicando os motivos do arquivamento (ex: alerta falso positivo, justificativa apresentada pelo cliente, documentação complementar saneadora).
Aprovação	Submeter à validação do supervisor imediato do Compliance.
Registro	Inserir no sistema de monitoramento a decisão, a justificativa e os documentos comprobatórios.
Prazo de guarda	Manter o registro por 10 anos para consultas futuras e auditorias.

B) Hipótese de Comunicação:

Quando a análise confirmar **indícios suficientes** de lavagem de dinheiro ou financiamento do terrorismo:

Atividade	Detalhamento
Relatório final	Elaborar documento conclusivo consolidando todas as evidências, a narrativa dos fatos e a fundamentação legal.
Aprovação diretiva	Submeter o relatório à aprovação formal do Diretor responsável (estatutário).
CI do Diretor	Obter ciência expressa do Diretor, preferencialmente por meio eletrônico ou assinatura em documento físico.
Preparação da comunicação	Estruturar as informações no leiaute exigido pelo sistema do COAF (SISCOAF).

3. Comunicação ao COAF (Quando Aplicável)

Prazos legais (Circular SUSEP nº 612/2020):

Tipo de Operação	Prazo para Comunicação
Operações em espécie acima de R$ 50.000,00	24 horas
Propostas de contratação recusadas por suspeita de PLD/FT	24 horas
Operações suspeitas de financiamento do terrorismo	24 horas
Demais operações suspeitas (art. 9º da Circular)	Até o 15º dia útil do mês seguinte à conclusão da análise

Procedimento de comunicação:

1. Acessar o SISCOAF com o certificado digital da IZA Seguradora.

2. Selecionar o tipo de comunicação adequado:
✔ Comunicação automática (espécie)
✔ Comunicação de recusa
✔ Comunicação por suspeita

3. **Preencher os campos obrigatórios:**
✔ Qualificação completa do(s) envolvido(s)
✔ Descrição detalhada da(s) operação(ões)
✔ Valores, datas e formas de pagamento
✔ Narrativa da suspeita (fundamentação)

4. **Revisar as informações para garantir precisão e completude**.

5. **Transmitir a comunicação e aguardar o protocolo de recebimento.**

6. **Salvar o comprovante (protocolo) para juntada ao dossiê.**

4. Arquivamento do Dossiê

Documentos obrigatórios na pasta do caso:

✔ Cópia da comunicação realizada no SISCOAF (protocolo)
✔ Relatório final de investigação
✔ Parecer do Compliance e aprovação da Diretoria
✔ Documentação completa de KYC do cliente
✔ Evidências que embasaram a suspeita (extratos, prints, planilhas)
✔ Registro de consultas a áreas internas (se houver)
✔ Comprovante de arquivamento (se for o caso)

Prazo de guarda: Mínimo de 10 (dez) anos a contar da data da comunicação ou arquivamento.

Forma de guarda: Preferencialmente digital, com backup e controle de acesso restrito à área de Compliance.

Alertas de Compliance:

Atenção	Descrição
Confidencialidade	O cliente NÃO PODE ser informado sobre a existência de uma comunicação. A quebra de sigilo constitui crime (art. 10 da Lei 9.613/98).
Imunidade	A comunicação de boa-fé ao COAF não gera responsabilidade civil ou administrativa à Seguradora (art. 11 da Lei 9.613/98).
Qualidade da informação	Comunicações incompletas ou imprecisas podem prejudicar a análise do COAF e expor a IZA Seguradora a sanções.
Atualização normativa	Prazos e limites podem ser alterados pelos órgãos reguladores. Manter-se atualizado via canais oficiais.

RELATÓRIO DE INVESTIGAÇÃO Nº [XXX/ANO]

Cliente: [Nome/Razão Social]

CPF/CNPJ: [Número]

Classificação de Risco: [Alto/Médio]

Data da Análise: [DD/MM/AAAA]

Analista Responsável: [Nome]

1. HISTÓRICO DO ALERTA:

- Data do alerta: [DD/MM/AAAA]
- Tipo de alerta: [Fracionamento / Incompatibilidade / etc.]
- Valor envolvido: R$ [XXX]

2. DESCRIÇÃO DOS FATOS:

[Narrativa objetiva das operações realizadas]

3. ANÁLISE DOCUMENTAL:

[Confronto entre as operações e a documentação KYC]

4. PESQUISAS COMPLEMENTARES:

[Resultado de consultas em bases públicas, mídias, etc.]

5. FUNDAMENTAÇÃO:

[Base legal para a suspeita]

6. CONCLUSÃO:

[ ] Arquivamento (justificativa)

[ ] Comunicação ao COAF

7. APROVAÇÕES:

Analista: _____

Supervisor Compliance: _____

Diretor: _____

Este formato mais enxuto tem como objetivo facilitar a consulta pelos colaboradores, e garante que todas as informações essenciais estejam disponíveis para a correta execução do processo de reporte.

---

4. Regras Específicas

A IZA Seguradora aplica tratamentos diferenciados a determinadas categorias de clientes que, por sua natureza, posição ou atividade, apresentam risco potencialmente mais elevado de envolvimento em lavagem de dinheiro, financiamento do terrorismo ou corrupção. As regras abaixo complementam o fluxo geral de KYC e devem ser rigorosamente observadas.

4.1 Pessoas Politicamente Expostas (PEP)

Definição (conforme Circular SUSEP nº 612/2020): Consideram-se pessoas politicamente expostas os agentes públicos que desempenham ou tenham desempenhado, nos últimos cinco (5) anos, cargos, empregos ou funções públicas relevantes, no Brasil ou no exterior, bem como seus representantes, familiares e estreitos colaboradores.

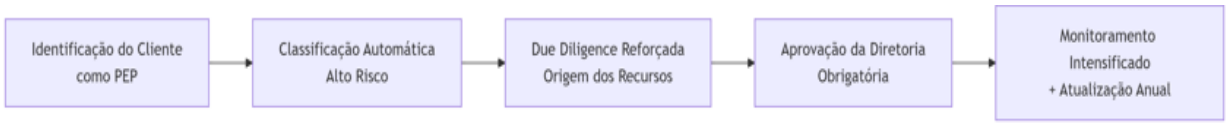
Abrangência: O conceito de PEP inclui:

- O próprio agente público.
- Os familiares (parentes até o segundo grau: cônjuges, companheiros, filhos, pais, irmãos).
- Estreitos colaboradores (sócios, procuradores, representantes legais).

Classificação e Tratamento:

Requisito	Procedimento
Classificação automática	**Clientes identificados como PEP (ou com beneficiário final PEP) serão automaticamente classificados como Alto Risco** no sistema, independentemente de outros critérios.
Identificação	**A triagem inicial (Etapa 2) deverá verificar obrigatoriamente bases de dados oficiais de PEP. O comercial e o atendimento também devem estar atentos a indícios de exposição política durante a coleta de informações.**
Due diligence reforçada	**A coleta de informações deverá incluir a origem detalhada dos recursos e a compatibilidade entre a função pública exercida e o patrimônio/renda declarados.**
Aprovação obrigatória da Diretoria	**Nenhum contrato com cliente classificado como PEP poderá ser firmado sem a aprovação formal e expressa da Diretoria (ou Comitê de Compliance), conforme alçadas definidas.**
Monitoramento reforçado	**As operações de clientes PEP serão submetidas a monitoramento contínuo intensificado, com revisão periódica das transações e análise de qualquer movimentação atípica.**
Atualização cadastral	**A cada 12 (doze) meses, no mínimo, o cadastro de clientes PEP deverá ser revisado e atualizado.**

Procedimento para PEP:



Observação: A exposição política não impede, por si só, o relacionamento comercial. No entanto, a decisão de contratar com PEP deve ser sempre documentada, justificada e aprovada pela instância máxima de governança da Seguradora.

4.2 Clientes de Alto Risco

Definição: Além dos PEP (classificados automaticamente como alto risco), serão considerados de alto risco os clientes que, na Etapa 3 (Classificação de Risco), apresentarem um ou mais dos seguintes critérios:

- Setores de atividade sensíveis: Comércio de armas, joias, pedras preciosas, obras de arte, casas de câmbio, jogos e apostas, etc.

- Jurisdições de risco: Clientes residentes, sediados ou com operações em países considerados paraísos fiscais ou com deficiências na prevenção à lavagem de dinheiro (listas do GAFI, por exemplo).

- Estruturas societárias complexas: Empresas com cadeia de participação opaca, utilização de trusts, offshores em jurisdições de risco ou dificuldade de identificação do beneficiário final.

- Comportamento atípico: Clientes que se recusam a fornecer informações, apresentam documentação fraudulenta ou realizam operações incompatíveis com seu perfil.

- Histórico negativo: Envolvimento prévio em crimes de lavagem de dinheiro, corrupção, fraudes ou inclusão em listas restritivas (mesmo após reabilitação).

Tratamento Diferenciado:

Requisito	Procedimento
Due diligence reforçada	A coleta de informações deve ir além do básico, incluindo: comprovação da origem dos recursos, declaração de capacidade financeira assinada, referências bancárias ou comerciais, e pesquisa aprofundada de background.
Aprovação escalada	Clientes de alto risco devem obrigatoriamente ser aprovados pelo Compliance e pela Diretoria, conforme definido na Etapa 4.
Atualização cadastral anual	O cadastro de clientes de alto risco deve ser revisado e atualizado a cada 12 (doze) meses, no máximo. A não atualização no prazo enseja a suspensão de novas contratações.
Monitoramento contínuo intensificado	As operações de clientes de alto risco serão monitoradas com maior frequência e profundidade, incluindo: análise trimestral das movimentações, verificação recorrente em bases de dados e acompanhamento próximo pela área de Compliance.
Revisão do relacionamento	Anualmente, a área de Compliance deverá emitir parecer sobre a manutenção do relacionamento com cada cliente de alto risco, recomendando a continuidade ou o encerramento do vínculo.

Due Diligence Reforçada (Checklist adicional):

Para clientes de alto risco, além dos documentos obrigatórios da Etapa 1, deverão ser solicitados:

- Comprovante de origem dos recursos (declaração de IR, contratos de venda de ativos, comprovantes de herança, etc.)
- Declaração de capacidade financeira assinada pelo cliente
- Referências bancárias ou comerciais (quando aplicável)
- Estrutura societária completa até o beneficiário final (com documentação de todas as camadas societárias)
- Pesquisa de background expandida (incluindo mídias e bases internacionais)
- Justificativa comercial para a contratação (memorando da área de negócios)

4.4 Disposições Gerais

1. Listas Oficiais: A IZA Seguradora S.A. utilizará bases de dados oficiais e atualizadas para a identificação de PEP e jurisdições de risco, incluindo, mas não se limitando:

- Portal da Transparência (CGU)
- Lista de PEP do COAF
- Listas do GAFI (países com deficiências estratégicas)
- Listas de sanções da ONU e OFAC

2. Atualização de Critérios: A área de Compliance revisará anualmente os critérios de classificação de alto risco e as listas de setores sensíveis, propondo ajustes sempre que necessário.

4. Registro das Decisões: Todas as decisões relativas a clientes de alto risco (aprovações, recusas, condições especiais) deverão ser formalizadas em ata, parecer ou documento equivalente, com a assinatura dos responsáveis, e arquivadas pelo prazo mínimo de 10 anos.

5. Exceções justificadas: Eventual reclassificação de um cliente de alto risco para médio ou baixo risco somente poderá ocorrer mediante

parecer fundamentado do Compliance e aprovação da Diretoria, com registro detalhado dos motivos que justificam a alteração.

Esta seção estabelece um tratamento claro e proporcional ao risco, demonstrando o compromisso da IZA Seguradora S.A. com as melhores práticas de prevenção à lavagem de dinheiro e com a conformidade regulatória.

---

5. Atualização Cadastral

Responsável: Compliance (gestão do processo e validação de alterações sensíveis) / Atendimento (execução da coleta de atualização) / TI (suporte tecnológico e alertas automáticos)

Objetivo: Manter as informações dos clientes permanentemente atualizadas, garantindo que a IZA Seguradora conheça, em tempo real, alterações relevantes no perfil, capacidade financeira, composição societária ou exposição política de seus clientes, assegurando a eficácia do monitoramento contínuo.

5.1 Periodicidade da Atualização

A frequência da atualização cadastral é proporcional ao nível de risco do cliente, conforme classificação estabelecida na Etapa 3:

Nível de Risco	Periodicidade da Atualização	Responsável pela
Alto Risco (inclui PEP)	A cada 12 meses	Atendimento / Compliance
Médio Risco	A cada 24 meses	Atendimento
Baixo Risco	A cada 36 meses	Atendimento (automatizado)

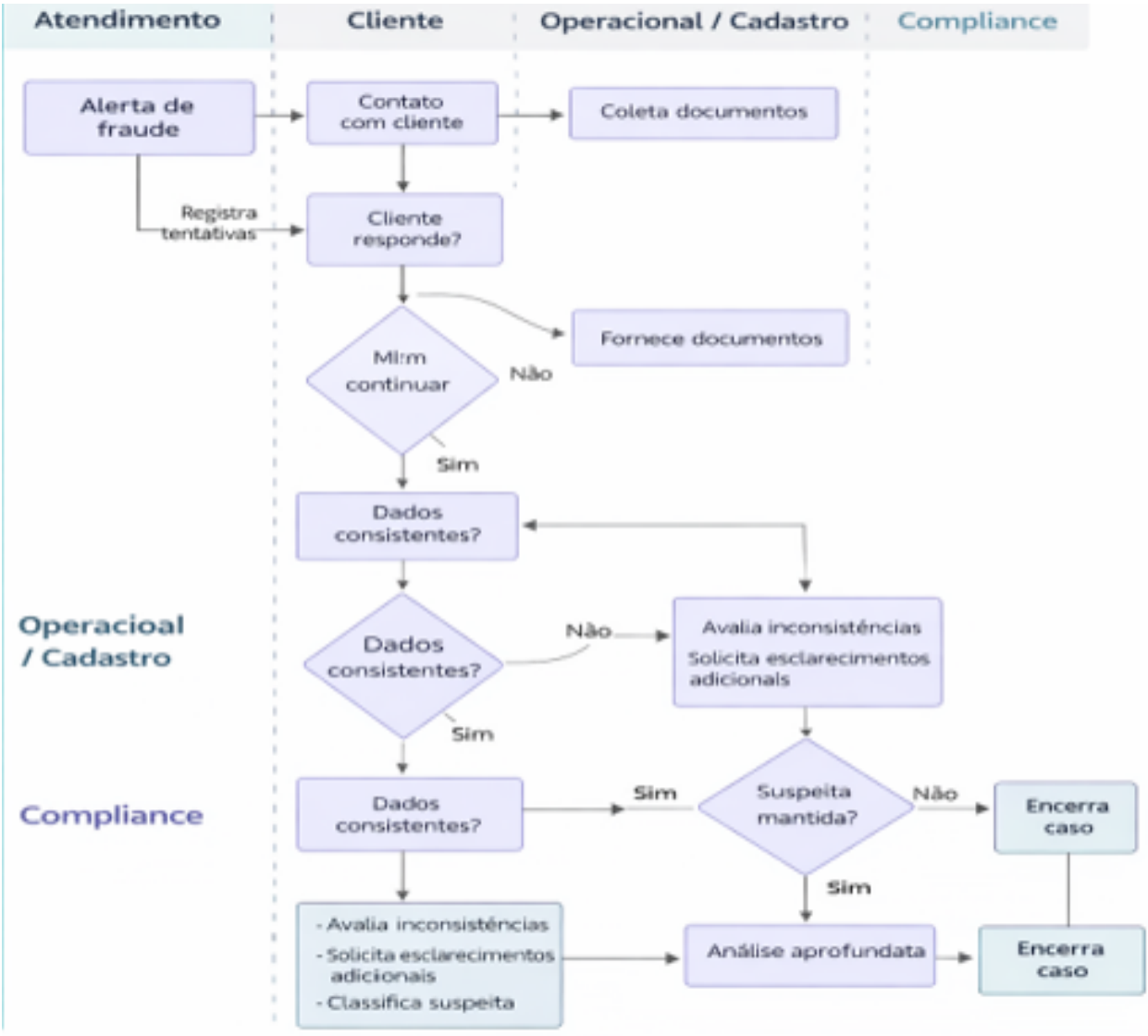
Disposições importantes:

- O prazo é contado a partir da data da última atualização cadastral (seja a coleta inicial ou a última revisão periódica).
- O sistema de gestão de clientes deverá emitir alerta automático com 60 (sessenta) dias de antecedência do vencimento da atualização, para que a área responsável programe o contato com o cliente.

- Clientes que não realizarem a atualização no prazo estabelecido poderão ter seu cadastro bloqueado temporariamente para novas contratações, endossos ou pagamentos de sinistros, até a regularização da situação.

5.2 Procedimento de Atualização

5.2.1 Fluxo Operacional



5.2.2 Procedimentos Detalhados

Etapa	Atividade	Detalhamento
1	Alerta automático	Sistema identifica clientes com cadastro próximo do vencimento e gera lista de trabalho para o Atendimento.
2	Contato com o cliente	Atendimento realiza contato proativo (telefone, e-mail, WhatsApp, carta) solicitando a atualização cadastral e orientando sobre os documentos necessários.
3	Coleta de documentos	Cliente deve apresentar os mesmos documentos da coleta inicial, atualizados (comprovante de residência recente, documentos com foto, etc.).
4	Validação	Atendimento confere a consistência dos documentos e a compatibilidade com as informações já constantes no cadastro.
5	Atualização no sistema	Informações são inseridas no sistema, substituindo os dados anteriores. O histórico deve ser preservado para consulta futura.
6	Registro da data-base	Sistema registra a nova data de atualização para contagem do próximo ciclo.

5.3 Documentação Exigida na Atualização

A documentação exigida na atualização cadastral é a mesma da coleta inicial (Etapa 1), devendo ser apresentada com data recente:

Tipo de Cliente	Documentos Obrigatórios
Pessoa Física	-Documento de identidade com foto (atualizado) - Comprovante de residência (últimos 90 dias) - Comprovante de renda atualizado (se houver alteração significativa) - Declaração de atualização de dados assinada
Pessoa Jurídica	- Cartão CNPJ (comprovante de situação cadastral) - Contrato social e alterações (consolidadas) - Comprovante de endereço da sede (últimos 90 dias) - Declaração de beneficiário final atualizada - Documentos dos sócios e representantes legais

Observação: Para clientes de alto risco, a exigência documental é reforçada, podendo ser solicitados:

- Declaração de Imposto de Renda (com recibo de entrega)
- Extratos bancários dos últimos 3 meses
- Declaração de origem dos recursos para movimentações atípicas
- Documentação comprobatória de alterações societárias

5.4 Tratamento de Não Resposta

Caso o cliente não atenda às solicitações de atualização cadastral, aplica-se o seguinte fluxo:

Prazo	Ação
Até 30 dias antes do vencimento	**Atendimento realiza contatos proativos (mínimo 3 tentativas por canais diferentes).**
Data do vencimento	**Caso não haja resposta, o sistema gera alerta para o Compliance.**
Até 30 dias após o vencimento	**Compliance avalia o histórico do cliente e define ação: nova tentativa, bloqueio ou reclassificação de risco.**
Após 30 dias do vencimento	**Cadastro é bloqueado temporariamente** para novas operações (novas apólices, endossos, pagamento de sinistros). A liberação só ocorre após a regularização.
Após 90 dias do vencimento	**Compliance avalia o encerramento do relacionamento, notificando o cliente formalmente sobre a suspensão definitiva.**

5.5 Atualização por Iniciativa do Cliente

Além da atualização periódica, o cliente pode, a qualquer tempo, solicitar a alteração de seus dados cadastrais. Neste caso:

1. O Atendimento deve coletar a solicitação e os documentos comprobatórios.

2. Verificar a autenticidade da solicitação (evitar fraudes por terceiros).

3. Atualizar o cadastro no sistema.

4. Registrar a nova data-base (reiniciando o ciclo de contagem).

5. Comunicar o Compliance se a alteração for relevante e envolver cliente de alto risco ou se houver indícios de irregularidade.

Alterações que exigem atenção do Compliance:

- Mudança frequente de endereço em curto espaço de tempo
- Inclusão de novos sócios em empresa de alto risco
- Alteração de beneficiários em apólices de vida
- Qualquer modificação que sugira tentativa de ocultação ou burla

5.6 Penalidades por Cadastro Desatualizado

A IZA Seguradora S.A. não operará com cadastros desatualizados. As seguintes restrições aplicam-se:

Situação	Consequência
Cadastro vencido (até 30 dias)	Alertas internos, mas operações ainda permitidas
Cadastro vencido (31 a 90 dias)	Bloqueio de novas contratações e endossos
Cadastro vencido (acima de 90 dias)	Bloqueio total, incluindo sinistros (até regularização)
Recusa reiterada em atualizar	Encerramento do relacionamento comercial

5.7 Registro e Guarda de Documentos

- Todos os documentos coletados nas atualizações cadastrais deverão ser armazenados no sistema de gestão documental da IZA Seguradora.
- O histórico de versões do cadastro deve ser preservado, permitindo a consulta à evolução das informações do cliente ao longo do tempo.

- Prazo de guarda: 10 (dez) anos contados do encerramento do relacionamento ou da última movimentação, conforme regulamentação.

5.8 Indicadores de Efetividade (KPIs)

A área de Compliance deverá monitorar e reportar trimestralmente à Diretoria os seguintes indicadores:

Indicador	Meta
% de cadastros de alto risco atualizados no prazo	> 95%
% de cadastros de médio risco atualizados no praz	> 90%
% de cadastros de baixo risco atualizados no prazo	> 85%
Tempo médio de regularização de cadastros vencidos	< 30 dias
Nº de clientes desligados por cadastro desatualizado	Reportar variações

5.9 Disposições Gerais

1. A atualização cadastral é obrigatória e condição indispensável para a manutenção do relacionamento comercial com a IZA Seguradora.

2. O cliente será informado, no momento da contratação, sobre a política de atualização cadastral e as consequências do não cumprimento.

3. A área de Compliance poderá, a qualquer tempo e independentemente do prazo regular, solicitar a atualização cadastral de qualquer cliente sempre que houver indícios de alteração relevante no perfil de risco.

4. Casos de não atualização envolvendo clientes de alto risco deverá ser reportados individualmente à Diretoria, com proposta de ação.

Esta seção estabelece um processo claro e estruturado para a atualização cadastral, garantindo que a IZA Seguradora mantenha sempre informações precisas e atualizadas sobre seus clientes, em linha com as melhores práticas de mercado e as exigências regulatórias.

---

6. Registro e Evidências

Responsável: Todas as áreas envolvidas no processo de KYC (Comercial, Atendimento, Subscrição, Sinistros, Compliance, TI) são responsáveis pela geração e guarda adequados dos documentos e evidências relativos às suas respectivas etapas. A guarda centralizada e a gestão do prazo de retenção são de responsabilidade do Compliance.

Objetivo: Assegurar a rastreabilidade, a transparência e a auditabilidade de todo o processo de "Conheça seu Cliente", garantindo que a IZA Seguradora possa comprovar, a qualquer tempo, a diligência empregada na identificação, qualificação, classificação e monitoramento de seus clientes.

6.1 Documentos e Evidências a Serem Registrados

Todo o ciclo de vida do cliente deve ser documentado, desde o primeiro contato até o eventual encerramento do relacionamento. Abaixo, a relação mínima de documentos e evidências que devem ser preservados:

Etapa do Processo	Documentos/Evidências Obrigatórios	Formato de Guarda
Coleta de Informações (Etapa 1)	• Ficha cadastral preenchida • Documento de identidade (frente e verso) • CPF/CNPJ • Comprovante de residência • Contrato social (PJ) • Dedaração de beneficiário final • Procurações (se houver) • Comprovantes de renda/patrimônio	Digital (PDF/A ou imagem)
Triagem e Verificação (Etapa 2)	• Relatório de consulta em bases PEP • Relatório de consulta em listas restritivas • Prints de telas com resultados das consultas • Protocolos de consulta (quando aplicável) • Evidências de pesquisas complementares	Digital (PDF ou imagem)
Classificação de Risco (Etapa 3)	• Matriz de classificação preenchida • Justificativa técnica para a classificação • Parecer do Compliance (para casos especiais) • Registro da classificação no sistema	Digital / Log de sistema
Aprovação de Cadastro (Etapa 4	• Registro de aprovação automática (log) • Aprovação formal da Subscrição (e-mail ou sistema) • Parecer do Compliance (alto risco) • Aprovação da Diretoria (alto risco) • Decisão de recusa (se aplicável)	Digital / Log de sistema / PDF assinado
Monitoramento Contínuo (Etapa 5)	• Logs de alertas gerados • Relatórios de análise de alertas • Justificativas de arquivamento • Evidências de investigações • Relatórios de monitoramento periódico	Digital (PDF) com controle de acesso
Reporte de Operações Suspeitas (Etapa 6)	• Relatório final de investigação • Parecer do Compliance • Aprovação da Diretoria • Protocolo de comunicação ao COAF • Dossiê completo do caso	Digital (PDF) com controle de acesso
Atualização Cadastral (Etapa 5.2)	• Documentos atualizados (mesmos da coleta) • Registro de contatos com o diente • Justificativas para bloqueios • Decisões de encerramento	Digital / Log de sistema

6.2 Prazo de Guarda

ATENÇÃO: A Circular SUSEP nº 612/2020 estabelece o prazo mínimo de guarda de 5 (cinco) anos. No entanto, a IZA Seguradora, alinhada às melhores práticas de mercado e à Lei nº 9.613/98, adotará o prazo de 10 (dez) anos como regra geral, contados do encerramento da relação comercial ou da última movimentação cadastrada.

Tipo de Documento	Prazo Mínimo	Início da Contagem
Documentos cadastrais (coleta e atualizações)	10 anos	Data do encerramento do relacionamento
Registros de apólices e operações	10 anos	Data da última movimentação
Relatórios de triagem e monitoramento	10 anos	Data da geração do relatório
Comunicações ao COAF	10 anos	Data da comunicação
Decisões de recusa ou encerramento	10 anos	Data da decisão
Logs de sistema (acessos, alterações)	5 anos (mínimo legal)	Data do registro

Observações importantes:

- Caso o cliente permaneça com relacionamento ativo por período superior a 10 anos, os documentos devem ser mantidos enquanto durar o vínculo, somando-se mais 10 anos após o encerramento.
- Em caso de processos judiciais, administrativos ou auditorias em andamento, os documentos relacionados devem ser preservados até a conclusão definitiva do caso, independentemente dos prazos acima.

- A contagem do prazo inicia-se na data do desligamento do cliente ou da última operação registrada.

6.3 Formato e Qualidade da Guarda
6.3.1 Meio de Armazenamento

A IZA Seguradora S.A. adotará preferencialmente o meio digital para guarda dos documentos e evidências, observando:

Digitalização com qualidade: Os documentos digitalizados devem ser legíveis, com resolução mínima de 200 DPI, em preto e branco ou colorido quando necessário.

- Formato padrão: Preferencialmente PDF/A (formato de preservação de longo prazo) ou imagens (JPEG, PNG) quando aceitável.

- Indexação: Os documentos devem ser indexados por cliente, tipo de documento e data, permitindo busca e recuperação eficientes.

- Backup: O repositório digital deve contar com política de backup regular (diário, semanal) e armazenamento em local seguro, preferencialmente com replicação em nuvem ou data center distinto.

6.3.2 Sistemas Utilizados

Sistema	Finalidade
Sistema de Gestão de Clientes (CRM)	Registro de dados cadastrais, histórico de interações, documentos anexados
Sistema de Monitoramento	Logs de alertas, análises realizadas, decisões de arquivamento
Repositório Documental (DMS)	Armazenamento de PDFs, imagens, relatórios e comunicações
Sistema de Protocolo	Registro de comunicações ao COAF e protocolos
Logs de Sistema	Trilhas de auditoria (quem, quando, o que alterou)

6.4 Controles de Acesso e Sigilo

Os documentos e evidências relacionados ao processo de KYC e PLD/FT contêm informações sensíveis e devem ter seu acesso rigorosamente controlado:

Perfil de Acesso	Documentos Permitidos	Restrições
Comercial/Atendimento	Documentos cadastrais básicos, histórico de interações	Sem acesso a investigações, comunicações ao COAF ou análises de suspeita
Subscrição/Sinistros	Documentos necessários para análise técnica	Acesso restrito ao necessário para a função
Compliance	Acesso integral a todos os documentos e evidências	Acesso exclusivo para análises e investigações
Auditoria Interna/Externa	Acesso mediante autorização formal e acompanhamento	Leitura, sem possibilidade de alteração ou exclusão
Diretoria	Relatórios gerenciais e casos de alto risco	Acesso mediante solicitação ou em reuniões de comitê

Princípios de acesso:

- Mínimo privilégio necessário para o exercício da função
- Rastreabilidade de acessos (logs de quem acessou o quê e quando)
- Confidencialidade reforçada para casos de comunicação ao COAF

6.5 Política de Retenção e Descarte

6.5.1 Retenção Ativa

Durante o período de retenção ativa (enquanto o cliente mantém relacionamento ou nos primeiros anos após o encerramento), os documentos devem estar prontamente acessíveis para consulta pelas áreas autorizadas e para atendimento a solicitações de órgãos reguladores.

6.5.2 Descarte Seguro

Após o decurso do prazo de guarda (10 anos), os documentos poderão ser descartados, observando:

1. Autorização prévia do Compliance para o descarte.

2. Registro da destruição: Ata ou documento formal listando os documentos destruídos, com data e assinatura dos responsáveis.

3. Método seguro de destruição:

✔ Documentos físicos: fragmentação (triturador industrial) ou incineração controlada.

✔ Documentos digitais: exclusão segura com sobrescrita de dados ou destruição física da mídia (quando aplicável).

6.5.3 Suspensão do Descarte

O descarte de documentos de clientes envolvidos em:

- Investigações internas em andamento

- Comunicações ao COAF

- Processos judiciais ou administrativos

- Solicitações de órgãos reguladores

deverá ser **imediatamente suspenso** até a conclusão definitiva do caso, independentemente do prazo de guarda já ter sido atingido.

6.6 Responsabilidades Específicas

Área	Responsabilidade
Comercial	Garantir que os documentos coletados na origem estejam legíveis e completos antes de enviar para digitalização/armazenamento.
Atendimento	Assegurar que as atualizações cadastrais sejam acompanhadas dos documentos comprobatórios e que estes sejam corretamente anexados ao sistema.
Subscrição/Sinistros	Registrar no sistema as decisões tomadas e os pareceres emitidos, anexando evidências quando necessário.
Compliance	Manter o repositório central de investigações e comunicações ao COAF, com controle de acesso restrito; monitorar a conformidade dos prazos de guarda; autorizar descartes.
TI	Garantir a integridade, disponibilidade e backup dos sistemas e repositórios; manter logs de acesso; implementar política de retenção técnica.
Todos os colaboradores	Abster-se de destruir ou alterar qualquer documento relacionado a processos de KYC sem autorização expressa do Compliance.

6.7 Trilha de Auditoria (Audit Trail)

A IZA Seguradora S.A. assegurará que todos os sistemas utilizados no processo de KYC mantenham trilhas de auditoria completas, registrando:

- Data e hora de cada ação (inclusão, alteração, exclusão, consulta)
- Usuário responsável pela ação (login individual, nunca compartilhado)
- IP e estação de trabalho de origem (quando aplicável)
- Conteúdo anterior e posterior à alteração (para modificações de dados)

Estes logs deverão ser preservados pelo prazo mínimo de 5 (cinco) anos e estar disponíveis para auditorias internas e externas mediante solicitação.

6.8 Check-list de Conformidade (para auditorias internas)

Item	Atende	Evidência
Todos os clientes possuem documentação completa e legível?		
As classificações de risco estão registradas no sistema?		
As aprovações de alto risco estão formalizadas e assinadas?		
Os alertas de monitoramento foram analisados e registrados?		
As comunicações ao COAF possuem dossiê completo?		
Os prazos de guarda estão sendo cumpridos?		
Os acessos aos documentos são controlados e rastreados?		
Há política de descarte segura e formalizada?		

6.9 Disposições Gerais

1. A ausência de documentação ou evidência de qualquer etapa do processo de KYC será considerada falha grave nos processos de auditoria interna e poderá sujeitar a IZA Seguradora S.A. a sanções regulatórias.

2. Em caso de fusão, aquisição ou transferência de carteira, todos os documentos e evidências deverão ser transferidos integralmente à nova entidade, observando os prazos de guarda remanescentes.

3. A área de Compliance realizará, com periodicidade mínima anual, auditoria amostral da documentação armazenada para verificar a conformidade com esta política.

4. Dúvidas sobre prazos de guarda, documentos a preservar ou procedimentos de descarte devem ser encaminhadas à área de Compliance.

---

7. Responsabilidades

Objetivo: Definir de forma clara e objetiva as atribuições de cada área envolvida no processo de "Conheça seu Cliente" e Prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo (PLD/FT), estabelecendo as linhas de defesa da IZA Seguradora e garantindo a segregação de funções.

Princípio Fundamental: A prevenção à lavagem de dinheiro é responsabilidade de todos os colaboradores da IZA Seguradora S.A., independentemente do cargo ou área de atuação. Qualquer suspeita ou irregularidade identificada deve ser imediatamente reportada à área de Compliance.

7.1 Estrutura das Linhas de Defesa

A IZA Seguradora S.A. adota o modelo de Três Linhas de Defesa para gestão de riscos de PLD/FT:

Linha de Defesa	Áreas Envolvidas	Função Principal
1ª Linha	Comercial, Atendimento, Subscrição, Sinistros	Identificação e mitigação de riscos no dia a dia operacional
2ª Linha	Compliance	Supervisão, orientação e monitoramento
3ª Linha	Auditoria Interna	Avaliação independente da eficácia dos controles

7.2 Responsabilidades Detalhadas por Área

7.2.1 Comercial (1ª Linha de Defesa)

Missão: Atuar como a primeira barreira de prevenção, garantindo que a coleta inicial de informações seja completa, precisa e fidedigna.

Atribuição	Detalhamento
Coleta inicial de dados	Obter todos os documentos e informações obrigatórios listados na Etapa 1, no primeiro contato com o cliente, antes da emissão de qualquer proposta ou apólice.
Identificação de PEP	Estar atento a indícios de exposição política durante a interação com o cliente e sinalizar imediatamente no sistema ou para o Compliance.
Primeira triagem de alertas	Identificar comportamentos suspeitos na prospecção (ex: pressa incomum para contratar, desinteresse nas condições do seguro, foco apenas em valores) e comunicar ao Compliance.
Qualidade da informação	Assegurar que os documentos coletados estejam legíveis, completos e dentro do prazo de validade antes de encaminhar para validação.
Registro no sistema	Inserir corretamente os dados do cliente nos sistemas da seguradora, sem abreviações ou informações inconsistentes.

Responsabilização: O comercial responderá por falhas na coleta inicial que resultem em cadastros incompletos ou documentos insuficientes, especialmente se tais falhas impedirem a correta classificação de risco do cliente.

7.2.2 Atendimento / Cadastro (1ª Linha de Defesa)

Missão: Garantir a integridade e a atualização permanente dos dados cadastrais, atuando como guardião da qualidade da informação.

Atribuição	Detalhamento
Validação documental	Conferir a autenticidade, a legibilidade e a consistência dos documentos apresentados pelo cliente, confrontando com as informações declaradas.
Atualização cadastral	Executar o processo de atualização periódica dos cadastros, conforme prazos definidos na Etapa 5, realizando contato proativo com os clientes.
Identificação de inconsistências	Reportar imediatamente ao Compliance qualquer discrepância relevante entre os documentos e as informações declaradas, ou indícios de falsificação.
Registro de interações	Documentar no sistema todos os contatos realizados com o cliente para fins de atualização cadastral ou esclarecimento de dúvidas.
Gestão de bloqueios	Aplicar os bloqueios cadastrais previstos para clientes que não atualizam seus dados no prazo, conforme orientação do Compliance.

Responsabilização: O atendimento responderá por falhas na validação documental que permitam a manutenção de cadastros inconsistentes ou desatualizados, bem como pela não aplicação dos bloqueios previstos.

7.2.3 Compliance (2ª Linha de Defesa)

Missão: Supervisionar, orientar e monitorar todo o processo de KYC e PLD/FT, atuando como autoridade técnica e guardião da conformidade regulatória.

Atribuição	Detalhamento
Classificação de risco	Definir os critérios objetivos para classificação de risco (baixo, médio, alto), revisá-los periodicamente e aplicar a classificação final nos casos de alto risco ou situações limítrofes.
Monitoramento contínuo	Gerir o sistema de monitoramento automatizado, analisar os alertas gerados, investigar casos suspeitos e documentar as conclusões (arquivamento ou aprofundamento).
Reportes regulatórios	Elaborar e transmitir as comunicações obrigatórias ao COAF e à SUSEP, nos prazos legais, mantendo dossiês completos de cada caso.
Gestão de PEP e listas restritivas	Manter atualizadas as bases de consulta de PEP e listas de sanções, garantindo a integração com os sistemas operacionais.
Elaboração e revisão de normas	Redigir, revisar e atualizar este Manual, bem como demais normativos internos relacionados a PLD/FT, submetendo à aprovação da Diretoria.
Treinamento e conscientização	Promover capacitação periódica para todas as áreas envolvidas, garantindo que os colaboradores compreendam seus papéis e as obrigações regulatórias.
Atendimento a órgãos reguladores	Ser o ponto focal para auditorias, fiscalizações e solicitações da SUSEP, COAF e demais autoridades.
Gestão de riscos de PLD/FT	Manter matriz de riscos atualizada, identificando vulnerabilidades e propondo melhorias nos controles.
Pareceres técnicos	Emitir pareceres sobre casos complexos, clientes de alto risco, PEP e operações suspeitas, subsidiando a decisão da Diretoria.

Responsabilização: O Compliance responderá pela efetividade do programa de PLD/FT, pela tempestividade e precisão das comunicações aos órgãos reguladores, e pela adequação contínua dos controles aos normativos vigentes.

7.2.4 Diretoria (Alta Administração)

Missão: Patrocinar a cultura de conformidade, aprovar os casos críticos e garantir os recursos necessários para a efetiva implementação do programa de PLD/FT.

Atribuição	Detalhamento
Aprovação de casos críticos	Aprovar formalmente o relacionamento com clientes de alto risco e PEP, após análise e parecer do Compliance, conforme alçadas definidas na Etapa 4.
Decisão sobre comunicações	Dar ciência e aprovar as comunicações de operações suspeitas ao COAF, especialmente nos casos de maior complexidade ou valor.
Aprovação de normas	Aprovar este Manual e suas atualizações, bem como a política institucional de PLD/FT.
Alocação de recursos	Assegurar que as áreas de Compliance, TI e negócios disponham de recursos humanos, tecnológicos e financeiros adequados para execução dos controles de PLD/FT.
Patrocínio da cultura	Liderar pelo exemplo, demonstrando compromisso com a integridade e a conformidade em todas as decisões estratégicas.
Ciência de relatórios	Receber e analisar os relatórios periódicos de monitoramento e os indicadores de efetividade (KPIs) apresentados pelo Compliance.

Responsabilização: A Diretoria responderá, perante os órgãos reguladores e acionistas, pela adequação e efetividade do sistema de prevenção à lavagem de dinheiro da IZA Seguradora, nos termos do art. 10 da Circular SUSEP nº 612/2020.

7.3 Responsabilidades Complementares (Outras Áreas)

Área	Atribuições Específicas
Subscrição	Incorporar a análise de risco de PLD/FT na aceitação de riscos; validar a coerência entre perfil do cliente e contratação; reportar atipicidades ao Compliance.
Sinistros	Verificar a consistência das informações de beneficiários; identificar indícios de fraude ou lavagem de dinheiro nos pagamentos; reportar casos suspeitos ao Compliance.
Tecnologia da Informação (TI)	Garantir a disponibilidade, integridade e segurança dos sistemas; implementar e manter as ferramentas de monitoramento automatizado; preservar logs e trilhas de auditoria.
Jurídico	Apoiar o Compliance na interpretação de normas e na fundamentação legal para comunicações ao COAF; assessorar em processos administrativos ou judiciais relacionados.
Recursos Humanos	Incluir temas de PLD/FT nos programas de integração de novos colaboradores; comunicar ao Compliance sobre afastamentos ou desligamentos de colaboradores-chave.
Auditoria Interna (3ª Linha)	Avaliar periodicamente a eficácia dos controles de PLD/FT; reportar à Diretoria e ao Conselho de Administração as conclusões e recomendações.

7.4 Matriz de Responsabilidades (RACI)

A matriz abaixo resume as responsabilidades de cada área nas principais atividades do processo de KYC:

Atividade	Comercial	Atendimento	Subscrição	Sinistros	Compliance	TI	Diretoria
Coleta inicial de dados	R	C	I	I	C	-	-
Validação documental	C	R	C	I	C	-	-
Triagem em bases restritivas	-	-	-	-	R	C	-
Classificação de risco	-	-	C	-	R	-	I
Aprovação de baixo risco	C	C	R	-	I	-	-
Aprovação de médio risco	C	C	R	-	C	-	-
Aprovação de alto risco	C	I	C	-	R	-	A
Monitoramento contínuo	I	C	I	C	R	C	I
Análise de alertas	-	-	-	-	R	-	-
Comunicação ao COAF	-	-	-	-	R	-	A
Atualização cadastral	C	R	I	I	C	-	-
Gestão de documentos	C	C	C	C	R	C	-
Treinamento	C	C	C	C	R	I	C
Auditoria	I	I	I	I	C	I	R

Legenda:

- R = Responsável pela execução
- A = Aprovador (quem decide)
- C = Consultado (deve ser ouvido)
- I = Informado (deve ser comunicado)

7.5 Responsabilidade Solidária e Consequências

7.5.1 Responsabilidade Solidária

A IZA Seguradora S.A. entende que a prevenção à lavagem de dinheiro é um esforço integrado. A falha em qualquer das áreas pode comprometer todo o sistema. Assim:

- Todas as áreas são solidariamente responsáveis pela qualidade e integridade das informações que produzem ou processam.
- A omissão no reporte de situações suspeitas, ainda que fora da alçada direta do colaborador, será tratada como falha grave.

7.5.2 Consequências do Descumprimento

O descumprimento das obrigações previstas neste manual poderá acarretar:

Nível	Consequência
Colaborador	Advertência, suspensão ou demissão por justa causa, conforme gravidade da falha e reincidência, sem prejuízo de responsabilização civil ou criminal cabível.
Gestor	Responsabilização por falhas sistêmicas em sua área, falta de supervisão ou omissão no reporte de irregularidades.
Área	Exposição a riscos reputacionais, legais e regulatórios; necessidade de planos de ação corretivos; auditorias especiais.

7.6 Canal de Reporte (Linha Ética)

Qualquer colaborador que identifique:

- Descumprimento das regras deste manual
- Falhas nos controles de KYC
- Suspeitas de lavagem de dinheiro não endereçadas
- Solicitações inadequadas de aprovação de cadastros

deverá reportar imediatamente, de forma sigilosa e anônima, se desejado, pelos seguintes canais:

Canal	Detalhamento
E-mail exclusivo	compliance@iza.com.vc
Linha Ética	**0800 XXX XXXX**
Canal presencial	**Reunião com a área de Compliance, mediante agendamento**
Sistema de denúncias	**[link para sistema específico, se houver]**

7.7 Disposições Gerais

1. As responsabilidades aqui definidas devem constar nas descrições de cargos e nos programas de treinamento de cada área.

2. Gestores são responsáveis por assegurar que seus times conheçam e cumpram as atribuições previstas neste manual.

3. Em caso de dúvida sobre a quem compete determinada ação, o colaborador deve consultar o Compliance para orientação.

4. Este capítulo será revisado sempre que houver alterações significativas na estrutura organizacional da IZA Seguradora.

---

8. Treinamento

Responsável: Compliance (conteúdo e gestão do programa) / Recursos Humanos (logística, registro e integração)

Objetivo: Capacitar permanentemente todos os colaboradores, parceiros e prestadores de serviço relevantes sobre as obrigações legais, regulatórias e internas relacionadas à prevenção à lavagem de dinheiro e ao financiamento do terrorismo (PLD/FT), assegurando que cada um compreenda seu papel na proteção da IZA Seguradora S/A.

Princípios Fundamentais:

- Obrigatoriedade: O treinamento é condição indispensável para o exercício de atividades na IZA Seguradora S/A.
- Periodicidade: Deve ser realizado anualmente, no mínimo, com reforços sempre que necessário.
- Proporcionalidade: O conteúdo deve ser adequado ao nível de exposição e às responsabilidades de cada área.
- Efetividade: O treinamento deve ser mensurável, com mecanismos de avaliação da aprendizagem.

8.1 Periodicidade e Carga Horária

Tipo de Treinamento	Periodicidade	Carga Horária Mínima	Público-Alvo
Treinamento Obrigatório Anual	Anual	2 horas	Todos os colaboradores
Treinamento de Integração (Onboarding)	Na admissão	1 hora	Novos colaboradores
Treinamento Específico por Área	Anual ou sob demanda	1 a 2 horas	Comercial, Atendimento, Subscrição, Sinistros
Treinamento Aprofundado	Anual	4 horas	Compliance, Diretoria, Auditores
Reforços pontuais	Quando necessário	Variável	Áreas específicas

Observação: O treinamento anual deve ser realizado, preferencialmente, no primeiro trimestre de cada ano, garantindo que todos os colaboradores estejam atualizados antes de eventuais auditorias ou fiscalizações.

8.2 Conteúdo Programático

8.2.1 Treinamento Básico (Obrigatório para Todos)

Módulo	Conteúdo	Carga Horária
1. Contexto e Importância	• O que é lavagem de dinheiro? • Consequências sociais e econômicas • Por que a IZA Seguradora se preocupa? • Riscos reputacionais, legais e operacionais	20 min
2. Base Legal e Regulatória	• Lei 9.613/98 e alterações • Circular SUSEP nº 612/2020 • Papel do COAF • Consequências do descumprimento (multas, sanções, responsabilização criminal)	20 min
3. Políticas Internas	• Apresentação do Manual "Conheça seu Cliente" • Obrigações de cada colaborador • Canais de reporte (Linha Ética)	20 min
4. Sinais de Alerta (Red Flags)	• Comportamentos suspeitos mais comuns • O que observar no dia a dia? • Exemplos práticos e estudos de caso	15 min
5. Consequências do Não Cumprimento	• Sanções internas (advertência a demissão) • Responsabilização individual • Impacto para a empresa	15 min
6. Avaliação de Aprendizagem	• Questionário objetivo (mínimo 70% de acerto para aprovação)	15 min

8.2.2 Treinamento Específico por Área

Comercial e Atendimento (adicional ao básico):

Módulo	Conteúdo
Coleta de documentos	Checklist completo, cuidados com falsificações, validação de autenticidade
Identificação de PEP	Como identificar, o que perguntar, quando suspeitar
Abordagem ao cliente	Como solicitar informações sem constranger, como lidar com recusas
Sinais de alerta na prospecção	Pressa incomum, desinteresse nas condições, foco apenas em valores

Subscrição e Sinistros (adicional ao básico):

Módulo	Conteúdo
Análise de risco integrada	Como incorporar PLD/FT na análise atuarial
Incompatibilidades	Identificação de discrepâncias entre perfil e contratação
Beneficiários suspeitos	Análise de beneficiários em sinistros de vida
Fraude x Lavagem	Diferenças e interseções

Compliance e Diretoria (adicional ao básico):

Módulo	Conteúdo
Aprofundamento legal	Jurisprudência, interpretação de normas, tendências regulatórias
Comunicação ao COAF	Técnicas de redação, prazos, cuidados legais
Investigação avançada	Técnicas de análise, fontes de informação, cruzamento de dados
Gestão de risco de PLD/FT	Matriz de riscos, indicadores, reporte à alta administração

8.3 Metodologia e Formatos

A IZA Seguradora S/A adotará múltiplos formatos de treinamento para garantir acessibilidade, engajamento e efetividade:

Formato	Descrição	Aplicação
EAD (Ensino a Distância)	Plataforma online com vídeos, textos interativos e questionários	Treinamento obrigatório anual e integração
Presencial ou ao Vivo (Webinar)	Sessões com especialistas, permitindo interação e perguntas	Treinamentos específicos, aprofundamentos, lançamento de novas normas
Estudos de caso práticos	Análise de situações reais (anonimizadas) em grupo	Treinamentos por área
Newsletters e comunicados	Reforços pontuais, lembretes de sinais de alerta, atualizações normativas	Periódico (bimestral)
Cartilhas e materiais de apoio	Guias rápidos, checklists, infográficos	Disponíveis permanentemente na intranet

8.4 Registro e Controle

A área de Recursos Humanos, em conjunto com o Compliance, deverá manter registro detalhado de todos os treinamentos realizados:

Informação	Detalhamento
Colaborador	Nome completo, cargo, área, data de admissão
Treinamento	Título, data, carga horária, formato (EAD/presencial)
Conteúdo	Grade programática ou referência ao material utilizado
Avaliação	Nota obtida, aprovação/reprovação, tentativas
Registro de participação	Certificado ou declaração assinada (presencial) / log de conclusão (EAD)

Prazo de guarda: Mínimo de 5 (cinco) anos para os registros de treinamento, contados da data de realização.

8.5 Avaliação de Efetividade

Para garantir que o treinamento não seja mera formalidade, a IZA Seguradora S/A adotará mecanismos de avaliação de efetividade:

Nível de Avaliação	Indicador	Meta	Periodicidade
Reação	Satisfação do participante (pesquisa pós-treinamento)	Média > 4,5 (escala 1-5)	Após cada treinamento
Aprendizagem	Nota média na avaliação final	Média > 8,0	Após cada treinamento
Comportamento	Redução de erros operacionais relacionados a KYC	Redução anual > 10%	Anual
Resultado	Número de alertas gerados por colaboradores (reportes espontâneos)	Aumento anual > 5%	Anual

8.6 Treinamento para Parceiros e Prestadores de Serviço

Corretores, correspondentes e outros parceiros que atuem em nome da IZA Seguradora S/A também devem ser capacitados:

Tipo de Parceiro	Exigência de Treinamento	Responsável
Corretores credenciados	Treinamento anual obrigatório, com certificação	Compliance / Parcerias
Prestadores de serviço	Treinamento específico conforme atividade exercida	Gestor do contrato / Compliance
Terceirizados com acesso a dados	Treinamento básico de PLD/FT e proteção de dados	Gestor do contrato / Compliance

Cláusula contratual: Todos os contratos com parceiros devem conter cláusula obrigando a participação nos treinamentos e o cumprimento das políticas de PLD/FT da IZA Seguradora S/A.

8.7 Cronograma Anual de Treinamentos

Período	Atividade	Público-Alvo
Janeiro-Fevereiro	Planejamento e atualização dos conteúdos	Compliance / RH
Março	Lançamento do treinamento obrigatório anual	Todos os colaboradores
Abril	Prazo final para conclusão do treinamento anual	Todos os colaboradores
Maio	Relatório de conclusão e ações de reforço para áreas com baixa adesão	Compliance / RH
Junho	Treinamento específico para novas contratações (integração)	Novos colaboradores
Agosto	Treinamento aprofundado para Compliance e Diretoria	Compliance / Diretoria
Outubro	Treinamento específico para Comercial e Atendimento	Comercial / Atendimento
Dezembro	Balanço anual e planejamento do próximo ciclo	Compliance / RH

8.8 Consequências da Não Participação

A participação no treinamento obrigatório anual é condição para o exercício regular das atividades na IZA Seguradora S/A:

Situação	Consequência
Não realização no prazo	Notificação formal do gestor e do colaborador, com novo prazo estipulado
Não realização após 2ª chamada	Suspensão de acessos a sistemas até a regularização
Não realização por período superior a 3 meses	Advertência formal e registro em pasta funcional
Reincidência	Sanções disciplinares, podendo chegar à demissão por justa causa

Exceções: Afastamentos legais (férias, licença saúde) serão considerados para recalendarização, desde que devidamente comprovados.

8.9 Disposições Gerais

O conteúdo do treinamento será revisado anualmente pelo Compliance, incorporando:

- Alterações na legislação ou regulamentação
- Novas tipologias de lavagem de dinheiro identificadas no mercado
- Casos concretos ocorridos na IZA Seguradora (anonimizados)
- Resultados das avaliações de efetividade

A área de Compliance manterá um banco de casos (anonimizados) para utilização em treinamentos, extraídos de situações reais identificadas no monitoramento.

Os colaboradores que atuam em áreas de maior risco (Comercial, Atendimento, Subscrição, Sinistros) devem receber reforços periódicos além do treinamento anual, por meio de comunicados, alertas e reuniões de equipe.

A participação nos treinamentos será considerada nos processos de avaliação de desempenho e promoção.

8.10 Indicadores de Treinamento (KPIs)

A área de Compliance reportará trimestralmente à Diretoria os seguintes indicadores:

Indicador	Fórmula	Meta
Taxa de conclusão do treinamento anual	(Colaboradores treinados / Total de colaboradores) x 100	> 95%
Taxa de aprovação na avaliação	(Aprovados / Total avaliados) x 100	> 90%
Tempo médio para conclusão	Média de dias entre liberação e conclusão	< 30 dias
Satisfação com o treinamento	Média das notas de reação	> 4,5
Reportes espontâneos pós-treinamento	Comparativo com período anterior	Aumento anual

---

9. Auditoria e Controles

Responsável: Auditoria Interna (execução dos trabalhos de auditoria) / Compliance (monitoramento de controles e geração de indicadores) / Diretoria (ciência e deliberação sobre resultados)

Objetivo: Estabelecer mecanismos sistemáticos de avaliação, verificação e melhoria contínua dos controles internos relacionados ao processo de "Conheça seu Cliente" e Prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo, assegurando que os procedimentos descritos neste manual sejam efetivamente cumpridos e que os riscos sejam adequadamente gerenciados.

Princípios Fundamentais:

- **Independência:** A auditoria deve ser realizada por área independente das funções auditadas.
- **Periodicidade:** Os controles devem ser avaliados em intervalos regulares e sempre que houver mudanças significativas.
- **Materialidade:** A profundidade dos testes deve ser proporcional ao risco identificado.

- **Melhoria contínua:** Os resultados devem subsidiar aperfeiçoamentos no programa de PLD/FT.

9.1 Estrutura de Controles

A IZA Seguradora S/A adota um modelo de controles em camadas, envolvendo diferentes níveis de verificação:

Camada	Descrição	Responsável
1ª Camada: Autocontrole	Verificação diária realizada pelos próprios executores dos processos	Comercial, Atendimento, Subscrição, Sinistros
2ª Camada: Monitoramento	Supervisão e testes realizados pela área de Compliance	Compliance
3ª Camada: Auditoria Interna	Avaliação independente e sistemática	Auditoria Interna
4ª Camada: Auditoria Externa	Verificação por firma de auditoria independente	Auditoria Externa
5ª Camada: Órgãos Reguladores	Fiscalização direta pela SUSEP, COAF e outros	SUSEP / COAF

9.2 Auditoria Interna Periódica

9.2.1 Escopo da Auditoria

A auditoria interna anual deverá avaliar, no mínimo:

Área de Avaliação	Itens Verificados
Governança	• Política de PLD/FT aprovada pela Diretoria • Designação de diretor responsável • Estrutura da área de Compliance • Atas de reuniões e decisões sobre casos críticos
Processo de KYC	• Cumprimento do checklist documental • Qualidade da validação de documentos • Classificação de risco adequada • Aprovação dentro das alçadas definidas
Monitoramento	• Parametrização dos sistemas de alerta • Análise tempestiva dos alertas gerados • Registro das decisões de arquivamento • Investigação de casos suspeitos
Comunicações ao COAF	• Tempestividade das comunicações • Qualidade e completude das informações • Dossiês completos e bem fundamentados • Protocolos de envio arquivados
Atualização Cadastral	• Cumprimento dos prazos por nível de risco • Efetividade dos contatos com dientes • Bloqueios aplicados corretamente
Treinamento	• Taxa de conclusão do treinamento anual • Qualidade do conteúdo • Registros de participação
Documentação e Registros	• Prazos de guarda cumpridos • Organização e acessibilidade dos documentos • Controles de acesso

9.2.2 Metodologia da Auditoria

Etapa	Atividade
Planejamento	Definição do escopo, cronograma, equipe e amostras a serem testadas
Execução	Aplicação de testes, entrevistas, análise documental, revisão de sistemas
Achados	Identificação de não conformidades, fragilidades ou oportunidades de melhoria
Relatório	Documento formal com conclusões, recomendações e prazos para implementação
Plano de Ação	Resposta das áreas auditadas com cronograma de correção
Follow-up	Verificação posterior da implementação das ações corretivas

9.2.3 Amostragem

A auditoria deverá utilizar critérios de amostragem estatística ou julgamental, garantindo cobertura adequada:

Critério	Percentual Mínimo da Carteira
Clientes de alto risco	100% (quando factível) ou amostra representativa
Clientes médio risco	Mínimo 10% ou amostra estatisticamente válida
Clientes baixo risco	Mínimo 5% ou amostra estatisticamente válida
Comunicações ao COAF	100% dos casos do período
Aprovações de Diretoria	100% das decisões do período

9.3 Testes de Aderência

Os testes de aderência são verificações pontuais realizadas pelo Compliance (2ª linha) para avaliar se os processos estão sendo executados conforme o manual.

9.3.1 Tipos de Testes

Tipo de Teste	Descrição	Frequência
Teste de Conformidade	Verifica se o procedimento seguiu exatamente o que está no manual	Trimestral
Teste de Efetividade	Avalia se o controle atingiu o objetivo pretendido	Semestral
Teste de Qualidade	Analisa a qualidade das informações e decisões registradas	Trimestral
Teste de Tempestividade	Verifica se os prazos foram cumpridos	Mensal

9.3.2 Roteiro de Testes de Aderência (Exemplos)

Processo	Teste	Critério de Aceitação
Teste de Conformidade	Verifica se o procedimento seguiu exatamente o que está no manual	Trimestral
Teste de Efetividade	Avalia se o controle atingiu o objetivo pretendido	Semestral
Teste de Qualidade	Analisa a qualidade das informações e decisões registradas	Trimestral
Teste de Tempestividade	Verifica se os prazos foram cumpridos	Mensal

9.4 Indicadores de Efetividade (KPIs)

A área de Compliance deverá monitorar e reportar trimestralmente à Diretoria um conjunto de indicadores que permitam avaliar a saúde e a efetividade do programa de PLD/FT.

9.4.1 Indicadores de Processo

KPI	Definição	Fórmula	Meta	Frequência
% de cadastros completos	Proporção de clientes ativos com toda a documentação obrigatória anexada e válida	(Clientes com cadastro completo / Total de clientes ativos) x 100	> 98%	Mensal
% de cadastros com documentação vencida	Proporção de clientes com documentos fora do prazo de validade	(Clientes com doc. vencida / Total de clientes ativos) x 100	< 2%	Mensal
% de clientes classificados por risco	Proporção de clientes que possuem classificação de risco atribuída	(Clientes classificados / Total de clientes) x 100	100%	Mensal
Distribuição por nível de risco	Percentual de clientes em cada categoria	• Alto: (Qtd alto risco / Total) x 100 • Médio: (Qtd médio risco / Total) x 100 • Baixo: (Qtd baixo risco / Total) x 100	Reportar variações	Trimestral
% de atualizações cadastrais em dia	Proporção de clientes com cadastro atualizado dentro do prazo	(Clientes com atualização em dia / Total de clientes) x 100	> 95%	Mensal

9.4.2 Indicadores de Monitoramento

KPI	Definição	Fórmula	Meta	Frequência
Nº de alertas gerados	Total de alertas emitidos pelo sistema de monitoramento no período	Contagem absoluta	Reportar tendência	Mensal
Nº de alertas analisados	Total de alertas que receberam análise no período	(Alertas analisados / Alertas gerados no período) x 100	> 95%	Mensal
Tempo médio de análise de alertas	Média de dias entre a geração do alerta e a conclusão da análise	Soma dos dias de análise / Total de alertas analisados	< 15 dias	Mensal
Taxa de confirmação de alertas	Proporção de alertas que resultaram em suspeita confirmada	(Alertas confirmados / Alertas analisados) x 100	Reportar variação	Trimestral
Nº de investigações aprofundadas	Casos que demandaram investigação além da análise inicial	Contagem absoluta	Reportar tendência	Trimestral

9.4.3 Indicadores de Reporte

KPI	Definição	Fórmula	Meta	Frequência
Nº de comunicações ao COAF	Total de comunicações realizadas no período	Contagem absoluta	Reportar justificativa	Trimestral
Comunicações por tipo	Detalhamento por categoria: espécie, recusa, suspeita	Contagem por categoria	Reportar justificativa	Trimestral
Tempestividade das comunicações	Proporção de comunicações realizadas dentro do prazo legal	(Comunicações no prazo / Total de comunicações) x 100	100%	Trimestral
Nº de comunicações por cliente	Casos de múltiplas comunicações envolvendo o mesmo cliente	Contagem	Reportar para investigação	Semestral

9.4.4 Indicadores de Treinamento

KPI	Definição	Fórmula	Meta	Frequência
Taxa de conclusão do treinamento	Proporção de colaboradores que concluíram o treinamento obrigatório	(Concluintes / Total de colaboradores) x 100	> 95%	Trimestral
Nota média na avaliação	Média das notas obtidas pelos colaboradores nos testes	Soma das notas / Total de avaliados	> 8,0	Anual
Nº de reportes espontâneos	Comunicações de suspeitas realizadas por colaboradores das áreas	Contagem absoluta	Aumento anual	Trimestral

9.5 Painel de Controle (Dashboard)

A área de Compliance deverá manter um painel de controle (dashboard) atualizado mensalmente, com visualização gráfica dos principais indicadores, acessível à Diretoria e à Auditoria.

Layout do dashboard:

PAINEL PLD/FT - MÊS/ANO

CADASTROS	MONITORAMENTO	REPORTES
% Completo: 98% % Vencidos: 1,5% Distribuição: • Alto: 3% • Médio: 22% • Baixo: 75%	Alertas mês: 245 % Analisados: 97% Tempo médio: 8d Tx Confirmação: 5% Inv. Aprofundadas: 12	Comunic. COAF: 3 - Espécie: 1 - Recusa: 1 - Suspeita: 1 Tempestividade: 100%

ATUALIZAÇÃO CADASTRAL	TREINAMENTO
% Atualiz. em dia: 96% • Alto risco: 100% • Médio risco: 97% • Baixo risco: 95%	% Conclusão: 98% Nota média: 8,7 Reportes espontâneos: 23 (+15%)

9.6 Plano de Ação Corretiva

Quando os testes de aderência, auditorias ou indicadores apontarem não conformidades ou fragilidades, a área responsável deverá elaborar um Plano de Ação Corretiva:

Campo	Descrição
Não conformidade	Descrição clara do problema identificado
Causa raiz	Análise da origem do problema
Ação corretiva	O que será feito para resolver
Responsável	Área ou pessoa que executará a ação
Prazo	Data limite para implementação
Evidência	Como será comprovada a correção
Status	Em andamento / Concluído / Atrasado

Acompanhamento: O Compliance deverá monitorar a execução dos planos de ação e reportar à Diretoria os casos de atraso ou não implementação.

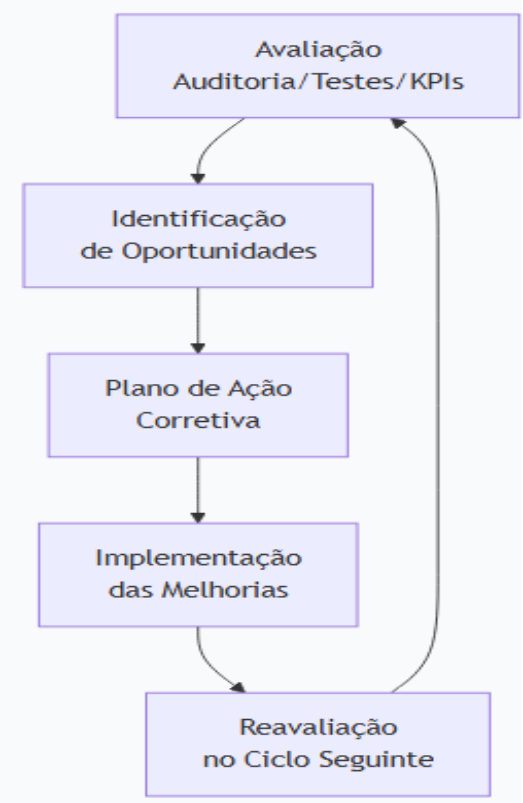
9.7 Reporte à Alta Administração

A área de Compliance deverá apresentar à Diretoria, com periodicidade trimestral, um relatório executivo contendo:

1. Sumário executivo (principais destaques do período)
2. Painel de indicadores (KPIs atualizados)
3. Análise de tendências (evolução dos indicadores ao longo do tempo)
4. Principais casos (síntese de investigações relevantes, comunicações ao COAF)
5. Resultados de auditorias e testes (achados e planos de ação)
6. Recomendações (propostas de melhoria nos controles)
7. Aprovações pendentes (casos de alto risco aguardando deliberação)

9.8 Melhoria Contínua

Os resultados das auditorias, testes e indicadores devem alimentar um ciclo de melhoria contínua do programa de PLD/FT:



Atualização do Manual: Anualmente, ou sempre que necessário, o Compliance deverá propor atualizações neste Manual incorporando:

- Melhorias identificadas a partir de auditorias e testes
- Novas exigências regulatórias
- Novas tipologias de lavagem de dinheiro
- Lições aprendidas com casos concretos

9.9 Disposições Gerais

1. **Independência:** A Auditoria Interna deve reportar-se funcionalmente ao Conselho de Administração ou ao Comitê de Auditoria, garantindo sua independência em relação à gestão executiva.
2. **Recursos:** A Diretoria deve assegurar que as áreas de Auditoria e Compliance disponham de recursos adequados para execução de suas atribuições.

3. **Transparência:** Os relatórios de auditoria e os planos de ação devem estar disponíveis para consulta dos órgãos reguladores, quando solicitados.
4. **Confidencialidade:** Os resultados de auditorias e investigações devem ser tratados com o devido sigilo, restritos às instâncias de governança.

---

10. Penalidades

Objetivo: Estabelecer de forma clara e transparente as consequências do descumprimento das normas, procedimentos e controles estabelecidos neste manual, abrangendo tanto as sanções internas aplicáveis aos colaboradores quanto as sanções regulatórias que podem recair sobre a IZA Seguradora e seus administradores.

Princípios Fundamentais:

- **Proporcionalidade:** As penalidades devem ser proporcionais à gravidade da infração, à reincidência e ao dano potencial ou efetivo causado.
- **Isonomia:** Tratamento igualitário para infrações de mesma natureza e gravidade.
- **Devido processo legal:** Garantia de ampla defesa e contraditório antes da aplicação de qualquer penalidade.
- **Dissuasão:** As penalidades devem desestimular condutas inadequadas e reforçar a cultura de conformidade.

10.1 Infrações e Classificação de Gravidade

As infrações ao disposto deste manual são classificadas em três níveis de gravidade:

Nível	Descrição	Exemplos
Leve	Falhas pontuais, sem dolo ou má-fé, que não resultam em dano efetivo à Seguradora ou a terceiros, e que são prontamente corrigidas.	• Atraso não justificado na atualização cadastral • Documento anexado com baixa qualidade, mas legível • Esquecimento pontual de procedimento, sem consequências
Média	Falhas recorrentes ou que, embora sem dolo, criam risco potencial de dano à Seguradora ou comprometem a efetividade dos controles.	• Reincidência em infrações leves • Coleta incompleta de documentos obrigatórios • Classificação de risco incorreta por negligência • Atraso na análise de alertas sem justificativa
Grave	Condutas dolosas, fraudulentas ou com negligência extrema, que resultam em dano efetivo ou expõem a Seguradora a riscos regulatórios, legais ou reputacionais significativos.	• Omissão intencional de informações relevantes • Falsificação ou adulteração de documentos • Quebra do sigilo sobre comunicações ao COAF • Conivência com operações suspeitas • Reincidência em infrações médias

10.2 Sanções Internas (Colaboradores)

Os colaboradores que descumprirem as obrigações previstas neste manual estarão sujeitos às seguintes sanções disciplinares, aplicadas pela área de Recursos Humanos em conjunto com a gestão direta e com ciência do Compliance:

Gravidade	Sanções Aplicáveis	Responsável pela Aplicação
Leve	• Advertência verbal (com registro) • Orientação formal e reforço de treinamento	Gestor imediato, com comunicação ao RH
Média	• Advertência escrita formal • Suspensão de até 5 dias • Realocação de funções (se cabível) • Monitoramento temporário reforçado	RH + Gestor, com ciência do Compliance
Grave	• Suspensão de 6 a 30 dias • Demissão por justa causa • Comunicação aos órgãos reguladores (se aplicável) • Representação criminal (em casos de dolo)	RH + Diretoria + Jurídico + Compliance

10.2.1 Procedimento Disciplinar

Etapa	Descrição
1. Apuração	Compliance ou gestor identificam a infração e reúnem evidências.
2. Notificação	Colaborador é notificado formalmente sobre a infração e as evidências, sendo garantido prazo para defesa prévia (mínimo 5 dias úteis).
3. Defesa	Colaborador apresenta sua versão dos fatos, podendo juntar documentos e indicar testemunhas.
4. Decisão	Com base nas evidências e na defesa, a instância competente decide pela aplicação ou não da penalidade.
5. Registro	A penalidade é registrada na pasta funcional do colaborador, com todos os documentos do processo.
6. Recursos	Cabem recursos à instância superior (Diretoria) no prazo de 5 dias úteis.

10.3 Sanções para Parceiros e Prestadores de Serviço

Corretores, correspondentes, prestadores de serviço e outros parceiros que atuem em nome da IZA Seguradora S/A, também estão sujeitos a sanções contratuais em caso de descumprimento das obrigações de PLD/FT:

Infração	Sanção Contratual
Descumprimento leve (pontual)	Notificação formal e exigência de correção imediata
Descumprimento médio (recorrente)	Suspensão temporária do credenciamento / Multa contratual
Descumprimento grave (doloso ou com dano)	Rescisão unilateral do contrato / Descredenciamento / Comunicação aos órgãos reguladores
Envolvimento em atividades ilícitas	Rescisão imediata + Representação criminal + Comunicação ao COAF

Cláusula contratual: Todos os contratos com parceiros devem prever expressamente a possibilidade de aplicação das sanções acima em caso de descumprimento das obrigações de PLD/FT.

10.4 Sanções Regulatórias (SUSEP / COAF)

O descumprimento das obrigações previstas na Circular SUSEP nº 612/2020 e demais normativos pode sujeitar a IZA Seguradora, seus administradores e membros do Conselho Fiscal a severas sanções administrativas.

10.4.1 Sanções Previstas na Lei 9.613/98

Infração	Sanção
Deixar de comunicar operações suspeitas	• Advertência • Multa de até R$ 20.000.000,00 (vinte milhões de reais) • Inabilitação temporária para exercício de cargos de administração
Deixar de identificar clientes ou manter registros	• Advertência • Multa de até R$ 20.000.000,00 • Proibição de realizar novas operações
Quebrar sigilo sobre comunicações ao COAF	• Multa • Responsabilização criminal (art. 10 da Lei 9.613/98)
Reincidência	• Multa em dobro • Cassação da autorização para funcionar

10.4.2 Sanções Previstas na Circular SUSEP nº 612/2020

Infração	Sanção
Falhas nos procedimentos de KYC	• Advertência • Multa (valor variável conforme porte da empresa)
Ausência de monitoramento adequado	• Multa • Determinação de implementação de controles
Não designação de diretor responsável	• Multa • Inabilitação temporária
Descumprimento de prazos de comunicação	• Advertência • Multa

10.4.3 Consequências Acessórias

Além das sanções pecuniárias, o descumprimento pode acarretar:

- **Dano reputacional:** Perda de confiança do mercado, clientes e parceiros
- **Restrições operacionais:** Impedimento de comercializar determinados produtos
- **Auditorias especiais:** Determinação de contratação de auditoria externa às expensas da empresa
- **Responsabilização criminal:** Para administradores e colaboradores envolvidos em condutas dolosas

10.5 Responsabilização Individual dos Administradores

Nos termos do art. 10 da Circular SUSEP nº 612/2020, o diretor responsável designado responde solidariamente pela implementação e efetividade dos controles de PLD/FT. Sua responsabilização pode ocorrer:

Hipótese	Consequência
Falha sistêmica nos controles	Multa pessoal / Inabilitação temporária
Conivência com irregularidades	Multa / Inabilitação / Responsabilização criminal
Omissão na supervisão	Advertência / Multa

10.6 Matriz de Responsabilização e Penalidades

Conduta	Responsável	Penalidade Interna	Penalidade Regulatória
Deixar de coletar documento obrigatório	Comercial	Advertência (média)	Multa para a empresa
Classificar risco incorretamente	Subscrição/Compliance	Advertência/suspensão (média/grave)	Multa para a empresa
Ignorar alerta de monitoramento	Compliance	Suspensão/demissão (grave)	Multa + inabilitação
Quebrar sigilo de comunicação ao COAF	Qualquer colaborador	Demissão por justa causa (gravíssima)	Multa + responsabilização criminal
Aprovar cliente de alto risco sem alçada	Diretoria	Advertência formal	Multa + inabilitação
Não implementar controles determinados	Diretoria/Compliance	Avaliação do Conselho	Multa + inabilitação

10.7 Agravantes e Atenuantes

Na aplicação das penalidades, serão considerados:

Agravantes	Atenuantes
• Reincidência	• Primariedade
• Dolo evidente	• Culpa leve (negligência, não dolo)
• Cargo de liderança (exemplo negativo)	• Comunicação espontânea da falha
• Dano efetivo à Seguradora	• Adoção de medidas corretivas imediatas
• Envolvimento de valores elevados	• Colaboração com a investigação
• Tentativa de ocultar a infração	• Ausência de dano efetivo

10.8 Comunicação de Penalidades

As penalidades aplicadas a colaboradores por infrações graves relacionadas a PLD/FT deverão ser comunicadas:

1. **Internamente:** À Diretoria e ao Comitê de Compliance, para ciência e registro.
2. **Externamente**: Aos órgãos reguladores, quando a infração envolver conduta que também constitua violação regulatória (ex: quebra de sigilo, envolvimento em lavagem de dinheiro).

10.9 Programa de Integridade (Compliance)

A IZA Seguradora S/A manterá um Programa de Integridade robusto, contemplando:

- **Canal de denúncias** acessível e confidencial
- **Proteção ao denunciante de boa-fé** (non-retaliation)
- **Due diligence de colaboradores e terceiros**
- **Treinamento contínuo** sobre ética e conformidade
- **Monitoramento de clima ético**

10.10 Disposições Gerais

1. Ciência do colaborador: Todos os colaboradores devem assinar termo de ciência e compromisso com as normas deste manual no momento da admissão e sempre que houver atualizações relevantes.

2. Divulgação: Este capítulo sobre penalidades deve ser amplamente divulgado, inclusive nos treinamentos anuais, para que todos conheçam as consequências do descumprimento.

3. Revisão: As penalidades aqui previstas não excluem a possibilidade de aplicação de outras sanções previstas na legislação brasileira, inclusive na esfera criminal.

4. Casos omissos: Situações não previstas neste capítulo serão decididas pela Diretoria, com base nos princípios da proporcionalidade e da razoabilidade, ouvido o Compliance.

10.11 Termo de Ciência e Compromisso (Modelo)

TERMO DE CIÊNCIA E COMPROMISSO

Eu, _____, CPF nº _____,

colaborador da IZA Seguradora S.A., declaro para os devidos fins que:

1. Recebi, li e compreendi integralmente o conteúdo do Manual "Conheça seu Cliente" da IZA Seguradora S.A., especialmente o capítulo referente às Penalidades.

2. Comprometo-me a cumprir rigorosamente todas as normas, procedimentos e controles estabelecidos no referido manual, sob pena de sujeitar-me às sanções disciplinares internas e legais cabíveis.

3. Estou ciente de que o descumprimento das obrigações de prevenção à lavagem de dinheiro e financiamento do terrorismo pode sujeitar a empresa, seus administradores e colaboradores a severas sanções regulatórias, incluindo multas e inabilitação.

4. Comprometo-me a comunicar imediatamente à área de Compliance qualquer irregularidade, suspeita ou violação das normas de que venha a ter conhecimento.

5. Autorizo a IZA Seguradora S/A a manter este termo em minha pasta funcional, pelo prazo de 10 (dez) anos após o encerramento do meu vínculo com a empresa.

Local e data: _____, ____ de _____ de 202__.

Assinatura: _____

11. Vigência

Objetivo: Estabelecer a data de entrada em vigor deste Manual, bem como as regras para sua revisão, atualização e comunicação às partes interessadas, garantindo que todos os colaboradores e parceiros da IZA Seguradora S/A, tenham ciência das normas aplicáveis e das versões vigentes.

11.1 Data de Entrada em Vigor

Este Manual "Conheça seu Cliente" entra em vigor na data de sua aprovação pela Diretoria da IZA Seguradora S.A., conforme assinatura constante na folha de aprovação.

Versão	Data de Aprovação	Data de Início de Vigência	Responsável pela Aprovação
1.0	23 de março de 2026	23 de março de 2026	Diretoria IZA Seguradora S/A

IZA Seguradora S.A.
Área de Compliance