

POLÍTICA DE PREVENÇÃO À LAVAGEM DE DINHEIRO E AO FINANCIAMENTO DO TERRORISMO (PLD/FT)

1. OBJETIVO, ABRANGÊNCIA E BASE LEGAL

1.1 Objetivo

A presente Política de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (PLD/FT) tem como objetivo estabelecer princípios, diretrizes, responsabilidades e procedimentos destinados à prevenção, detecção, análise, monitoramento e comunicação de operações ou situações que possam configurar indícios de lavagem de dinheiro ou financiamento do terrorismo no âmbito do Instituto Ambev de Previdência Privada – IAPP.

A Política visa assegurar que a Entidade não seja utilizada, direta ou indiretamente, para a prática de ilícitos financeiros, garantindo a conformidade com a legislação vigente, a integridade dos processos institucionais e a proteção de seus participantes, assistidos, patrocinadores e demais partes interessadas.

Adicionalmente, busca promover uma cultura organizacional pautada em elevados padrões éticos, transparência, integridade e diligência na condução das atividades, alinhada às melhores práticas de governança, riscos e compliance.

1.2 Abrangência

Esta Política aplica-se a todos os membros dos órgãos de governança, dirigentes, colaboradores, estagiários, prestadores de serviços, parceiros, patrocinadores, participantes, assistidos e quaisquer terceiros que, de forma direta ou indireta, mantenham relacionamento com o IAPP.

As diretrizes aqui estabelecidas devem ser observadas em todos os processos e atividades da Entidade que envolvam operações financeiras, contratações, relacionamento com participantes, assistidos, patrocinadores, fornecedores e colaboradores, bem como no desenvolvimento de produtos, serviços e uso de tecnologias.

1.3 Base Legal e Normativa

Esta Política está fundamentada nas seguintes legislações e normativos, sem prejuízo de outras normas aplicáveis:

- Lei nº 9.613, de 03 de março de 1998 (Lei de Prevenção à Lavagem de Dinheiro);
- Lei nº 13.260, de 16 de março de 2016 (Lei de Combate ao Financiamento do Terrorismo);
- Lei Complementar nº 109, de 29 de maio de 2001;
- Resolução PREVIC nº 23, de 14 de agosto de 2023;
- Resolução PREVIC nº 25, de 15 de outubro de 2024;
- Demais normativos emitidos pela Superintendência Nacional de Previdência Complementar – PREVIC e pelo Conselho de Controle de Atividades Financeiras – COAF.

1.4 Diretrizes Gerais

O IAPP adota abordagem baseada em risco para prevenção à lavagem de dinheiro e ao financiamento do terrorismo, considerando seu porte, perfil e complexidade operacional, de forma a assegurar a implementação de controles proporcionais aos riscos identificados.

Adicionalmente, esta Política deve ser redigida e mantida em linguagem clara, objetiva e acessível, de modo a possibilitar sua adequada compreensão pelos públicos a que se destina.

2. PRINCÍPIOS E DIRETRIZES DE PREVENÇÃO À LAVAGEM DE DINHEIRO E AO FINANCIAMENTO DO TERRORISMO

2.1 Princípios Gerais

A atuação do IAPP na prevenção à lavagem de dinheiro e ao financiamento do terrorismo é orientada pelos seguintes princípios:

- **Legalidade:** cumprimento integral da legislação e regulamentação aplicáveis;
- **Ética e Integridade:** adoção de conduta baseada em transparência, boa-fé e responsabilidade;
- **Abordagem baseada em risco:** implementação de controles proporcionais ao nível de risco identificado;
- **Diligência:** adoção de medidas preventivas para identificação e mitigação de riscos;
- **Segregação de funções:** definição clara de responsabilidades e alçadas;
- **Confidencialidade:** preservação do sigilo das informações, especialmente nos processos de análise e comunicação de operações suspeitas;
- **Rastreabilidade:** manutenção de registros que permitam a verificação das operações realizadas;
- **Melhoria contínua:** revisão periódica e aprimoramento dos controles e procedimentos.

2.2 Diretrizes de Prevenção e Detecção

O IAPP estabelece diretrizes para prevenir e detectar operações ou situações que possam caracterizar indícios de lavagem de dinheiro ou financiamento do terrorismo, contemplando:

- A identificação, análise e monitoramento contínuo de operações e comportamentos atípicos;
- A implementação de procedimentos para **prevenção, detecção, análise, reporte e monitoramento** de eventos suspeitos;
- A adoção de controles internos que permitam identificar inconsistências, incompatibilidades financeiras e indícios de irregularidades;
- A manutenção de registros e evidências que suportem as análises realizadas;
- A comunicação tempestiva às autoridades competentes, quando aplicável.

2.3 Diretrizes de Avaliação de Riscos

O IAPP deve identificar e avaliar os riscos de lavagem de dinheiro e financiamento do terrorismo nos seus processos, considerando, no mínimo:

- Perfil de clientes (participantes, assistidos, patrocinadores);
- Natureza dos produtos e serviços oferecidos;
- Canais de relacionamento e transação;
- Terceiros e prestadores de serviços;
- Uso de tecnologias e sistemas;
- Aspectos regulatórios.

Os riscos identificados devem ser classificados, avaliados e monitorados, de modo a subsidiar a definição e o aprimoramento dos controles internos.

2.4 Diretrizes de Monitoramento e Reporte

O IAPP deverá:

- Monitorar operações e situações que possam indicar práticas ilícitas;
- Estabelecer critérios objetivos para identificação de operações suspeitas;
- Assegurar que as análises sejam realizadas de forma tempestiva e documentada;
- Comunicar ao COAF, no prazo regulamentar, as operações suspeitas ou aquelas que atendam aos critérios legais;
- Realizar comunicação negativa à PREVIC, quando aplicável;
- Garantir que os processos de comunicação sejam realizados com sigilo e independência.

2.5 Diretrizes de Prevenção nos Processos Institucionais

As práticas de prevenção à lavagem de dinheiro e ao financiamento do terrorismo devem estar incorporadas aos principais processos do IAPP, incluindo:

- Cadastro e relacionamento com clientes;
- Contratação e gestão de fornecedores e prestadores de serviços;
- Atuação e gestão de colaboradores cedidos;
- Desenvolvimento de produtos e serviços;
- Utilização de novas tecnologias e sistemas;
- Gestão financeira e operacional.

2.6 Diretrizes de Ação Preventiva e Corretiva

Quando identificados indícios de lavagem de dinheiro ou financiamento do terrorismo, o IAPP deverá:

- Adotar medidas preventivas para mitigar os riscos identificados;
- Revisar processos, controles e responsabilidades, quando necessário;
- Registrar e documentar as análises e decisões tomadas;
- Avaliar a necessidade de comunicação aos órgãos competentes;
- Implementar ações corretivas para evitar recorrência.

2.7 Diretrizes de Capacitação e Conscientização

O IAPP promoverá a disseminação da cultura de prevenção à lavagem de dinheiro e ao financiamento do terrorismo, por meio de:

- Programas de treinamento periódicos;
- Ações de conscientização direcionadas aos públicos internos;
- Divulgação de orientações e boas práticas;
- Atualização contínua dos envolvidos sobre riscos e controles.

3. ABORDAGEM BASEADA EM RISCO E AVALIAÇÃO INTERNA DE RISCO

3.1 Abordagem Baseada em Risco

O IAPP adota abordagem baseada em risco para prevenção à lavagem de dinheiro e ao financiamento do terrorismo, de modo a assegurar que os controles internos sejam proporcionais ao nível de risco identificado, considerando o porte, a complexidade e o perfil operacional da Entidade.

Essa abordagem tem por objetivo direcionar os esforços e recursos para as áreas de maior exposição a riscos, permitindo maior efetividade na prevenção, detecção e mitigação de práticas ilícitas.

3.2 Avaliação Interna de Risco

O IAPP deve realizar Avaliação Interna de Risco com o objetivo de identificar, analisar, classificar e monitorar os riscos de lavagem de dinheiro e financiamento do terrorismo aos quais está exposto.

A avaliação deve contemplar, no mínimo:

- Identificação dos processos e atividades da Entidade;
- Mapeamento dos riscos de lavagem de dinheiro e financiamento do terrorismo associados a esses processos;
- Avaliação do nível de risco, considerando impacto e probabilidade;
- Identificação e avaliação dos controles existentes;

- Definição de planos de ação para mitigação de riscos, quando necessário.

3.3 Classificação de Risco

Os riscos identificados deverão ser classificados de acordo com os parâmetros de avaliação vigentes, observando os critérios e escalas definidos pela Entidade para mensuração do impacto, da frequência/probabilidade e do nível de risco resultante.

Os parâmetros utilizados na avaliação de riscos serão revisados no início de cada ciclo de avaliação, de forma a refletir o contexto organizacional, regulatório e operacional da Entidade, e estarão detalhados nos documentos complementares de gestão de riscos, especialmente no Dicionário de Riscos e no documento de Critérios de Avaliação de Riscos.

3.4 Integração com Controles Internos

Os resultados da Avaliação Interna de Risco devem ser utilizados para:

- Definir e aprimorar controles internos;
- Estabelecer critérios de monitoramento e análise de operações;
- Priorizar ações de mitigação de riscos;
- Subsidiar a tomada de decisão da Diretoria e dos órgãos de governança;
- Apoiar a elaboração e revisão da presente Política.

3.5 Periodicidade e Atualização

A Avaliação Interna de Risco deve ser realizada, no mínimo, anualmente, para analisar:

- Alterações relevantes nos processos, produtos ou serviços;
- Mudanças no ambiente regulatório;
- Identificação de novos riscos;
- Ocorrência de eventos relevantes relacionados à lavagem de dinheiro ou financiamento do terrorismo.

4. GOVERNANÇA E RESPONSABILIDADES

4.1 Estrutura de Governança

O IAPP deve manter estrutura de governança adequada para assegurar a implementação, execução, monitoramento e melhoria contínua das práticas de prevenção à lavagem de dinheiro e ao financiamento do terrorismo.

A governança deve observar princípios de segregação de funções, independência, rastreabilidade e responsabilidade, garantindo que os processos relacionados à PLD/FT sejam conduzidos de forma estruturada e eficaz.

4.2 Conselho Deliberativo

Compete ao Conselho Deliberativo:

- Aprovar a Política de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo e suas atualizações;
- Acompanhar a implementação e o cumprimento das diretrizes estabelecidas nesta Política;
- Tomar ciência dos resultados da Avaliação Interna de Risco (AIR);
- Tomar ciência dos relatórios de avaliação de efetividade dos controles;
- Apoiar a adoção de medidas necessárias ao aprimoramento dos controles internos relacionados à PLD/FT.

4.3 Conselho Fiscal

Compete ao Conselho Fiscal:

- Fiscalizar o cumprimento das obrigações legais e regulamentares relacionadas à PLD/FT;
- Acompanhar a adequação e a efetividade dos controles internos;
- Tomar ciência dos resultados da Avaliação Interna de Risco (AIR);
- Tomar ciência dos relatórios de avaliação de efetividade da Política e dos controles;
- Recomendar melhorias nos processos e controles, quando necessário.

4.4 Diretoria Executiva

Compete à Diretoria Executiva:

- Garantir a implementação e o cumprimento das diretrizes estabelecidas nesta Política;
- Aprovar e acompanhar a Avaliação Interna de Risco (AIR);
- Assegurar a existência e a aplicação de controles internos adequados e proporcionais aos riscos identificados;
- Coordenar, de forma integrada, as atividades relacionadas à governança, riscos e compliance no âmbito da PLD/FT;
- Deliberar sobre situações relevantes, incluindo casos de operações suspeitas;
- Garantir a comunicação tempestiva às autoridades competentes, quando aplicável;
- Promover a cultura de prevenção à lavagem de dinheiro e ao financiamento do terrorismo na Entidade;
- Assegurar a elaboração de registros e relatórios relacionados à PLD/FT.

4.5 Execução Operacional

Considerando a estrutura reduzida do IAPP, as atividades operacionais relacionadas à prevenção à lavagem de dinheiro e ao financiamento do terrorismo são desempenhadas de forma compartilhada entre os colaboradores, com apoio de prestadores de serviços e terceiros responsáveis por processos operacionais da Entidade, sem prejuízo da responsabilidade final da Diretoria Executiva pelas obrigações de PLD/FT.

Compete aos colaboradores:

- Cumprir as diretrizes estabelecidas nesta Política;
- Acompanhar e supervisionar as atividades executadas por terceiros;
- Executar, quando aplicável, os procedimentos de cadastro, atualização cadastral e conferência de informações;
- Monitorar as operações realizadas no âmbito de suas atividades e aquelas executadas por terceiros;
- Identificar e comunicar à Diretoria Executiva situações atípicas ou suspeitas;
- Manter registros e evidências das atividades executadas;
- Apoiar a implementação e o aprimoramento dos controles internos;
- Atuar com diligência e atenção redobrada nos processos com maior exposição ao risco de PLD/FT.

4.6 Colaboradores, Prestadores de Serviços e Terceiros

Compete a todos os colaboradores, prestadores de serviços e terceiros:

- Conhecer e cumprir as diretrizes desta Política;
- Atuar com diligência, ética e responsabilidade;
- Comunicar imediatamente quaisquer indícios ou suspeitas de irregularidades;
- Participar dos treinamentos e ações de conscientização;
- Colaborar com auditorias, avaliações e investigações internas.

4.7 Segregação de Funções

O IAPP deve assegurar a adequada segregação de funções nos processos relacionados à PLD/FT, de forma a evitar conflitos de interesse e garantir a independência nas atividades de:

- Cadastro e relacionamento;
- Monitoramento e análise;
- Aprovação e decisão;
- Comunicação de operações suspeitas.
-

5. CONHEÇA SEU CLIENTE, FORNECEDOR E COLABORADOR (KYC, KYP e KYE)

5.1 Diretrizes Gerais

O IAPP deve adotar procedimentos destinados à identificação, qualificação, classificação e atualização cadastral de clientes, fornecedores, prestadores de serviços e colaboradores, com o objetivo de prevenir a utilização da Entidade para práticas de lavagem de dinheiro e financiamento do terrorismo.

Esses procedimentos devem assegurar:

- A obtenção de informações completas, atualizadas e fidedignas;
- A verificação da consistência das informações prestadas;
- A identificação de situações de risco, incluindo Pessoas Expostas Politicamente (PEP);
- A rastreabilidade das informações e das alterações cadastrais;
- A aplicação de diligência proporcional ao nível de risco identificado.

5.2 Cadastro e Dados Mínimos

O IAPP deve manter cadastro atualizado de clientes, fornecedores e colaboradores, contendo, no mínimo, as seguintes informações:

a) Pessoas físicas:

- Nome completo;
- CPF;
- Documento de identificação (RG ou equivalente);
- Data de nascimento;
- Nacionalidade;
- Estado civil (quando aplicável);
- Ocupação profissional (quando aplicável);
- Endereço completo;
- Telefone e e-mail;
- Informação sobre enquadramento como Pessoa Exposta Politicamente (PEP).

b) Pessoas jurídicas:

- Razão social;
- CNPJ;
- Endereço completo;
- Atividade econômica;

- Dados dos sócios e administradores (incluindo CPF);
- Estrutura societária;

5.3 Atualização Cadastral

As informações cadastrais devem ser mantidas atualizadas, sendo:

- Atualizadas periodicamente ou sempre que houver alteração relevante;
- Revisadas em processos que envolvam movimentações financeiras, concessão de benefícios ou contratação de serviços;
- Validadas quanto à sua consistência e completude.

5.4 Alterações Cadastrais de Dados Críticos

As alterações cadastrais consideradas críticas devem observar procedimentos de controle, incluindo:

- Validação das informações por meio de documentação comprobatória;
- Conferência por colaborador responsável;
- Registro da alteração realizada, com identificação do responsável;
- Quando aplicável, aprovação pela Diretoria Executiva.

São considerados dados críticos, entre outros:

- Dados bancários;
- Dados de identificação pessoal;
- Alterações relacionadas a beneficiários ou representantes.

5.5 Conheça seu Cliente (KYC)

O IAPP deve adotar procedimentos destinados ao conhecimento de seus clientes (participantes, assistidos e patrocinadores), incluindo:

- Identificação e qualificação no momento do cadastro;
- Atualização periódica das informações;
- Verificação de compatibilidade entre perfil e movimentações;
- Identificação de situações atípicas ou inconsistentes;
- Aplicação de diligência adicional em casos de maior risco.

5.6 Conheça seu Fornecedor (KYP)

No processo de contratação e manutenção de fornecedores e prestadores de serviços, o IAPP deve:

- Realizar a identificação e qualificação cadastral;
- Verificar a reputação e idoneidade dos envolvidos;
- Identificar sócios e beneficiários finais;
- Realizar consultas, quando aplicável, a:
 - Listas restritivas nacionais e internacionais;
 - Bases relacionadas a crimes econômicos e financeiros;
 - Listas de sanções e outras fontes públicas disponíveis;
- Avaliar o risco associado à contratação;
- Manter registro das análises realizadas.

5.7 Conheça seu Colaborador (KYE)

O IAPP deve manter informações cadastrais básicas dos colaboradores que atuam na Entidade, ainda que cedidos por patrocinadores, assegurando:

- A identificação e qualificação cadastral;
- O conhecimento das funções exercidas;
- A ciência desta Política e de suas responsabilidades;
- A aplicação de controles proporcionais ao nível de risco da função exercida.

5.8 Registro e Rastreabilidade

Todos os procedimentos relacionados ao cadastro, atualização cadastral e diligência devem ser:

- Formalmente registrados;
- Mantidos pelo prazo mínimo exigido pela legislação;
- Disponibilizados para fins de auditoria e fiscalização, quando necessário.

6. PESSOAS EXPOSTAS POLITICAMENTE (PEP)

6.1 Definição

Para fins desta Política, considera-se Pessoa Exposta Politicamente (PEP) a pessoa natural que desempenha ou tenha desempenhado, nos últimos 5 (cinco) anos, cargo, emprego ou função pública relevante, no Brasil ou no exterior, bem como seus representantes, familiares e pessoas de seu relacionamento próximo, conforme definido na legislação aplicável.

6.2 Identificação de PEP

O IAPP deve adotar procedimentos para identificar Pessoas Expostas Politicamente nos processos de:

- Cadastro de clientes (participantes, assistidos, patrocinadores e instituidores);
- Contratação de fornecedores e prestadores de serviços, mediante verificação da condição de PEP dos sócios, administradores, representantes legais ou demais pessoas naturais que exerçam controle ou influência relevante sobre a pessoa jurídica contratada;
- Contratação, designação ou cessão de profissionais para o exercício de funções na Entidade, especialmente em cargos, funções ou atividades com maior exposição a riscos de PLD/FT.

A identificação de PEP deve ocorrer por meio de:

- Declaração do próprio interessado;
- Atualização cadastral periódica;
- Consulta a bases públicas e, quando aplicável, bases especializadas.

6.3 Classificação de Risco

Pessoas Expostas Politicamente devem ser consideradas, como regra, de **maior risco**, sendo sujeitas a procedimentos de diligência reforçada.

6.4 Diligência Reforçada

Nos casos em que houver identificação de PEP, o IAPP deve adotar medidas adicionais, tais como:

- Análise mais detalhada das informações cadastrais;
- Verificação da origem dos recursos, quando aplicável;
- Monitoramento mais rigoroso das operações realizadas;
- Avaliação da necessidade de aprovação por alçada superior, quando aplicável;
- Registro das análises realizadas.

6.5 Monitoramento de Operações

As operações realizadas por PEP devem ser monitoradas com maior nível de atenção, com o objetivo de identificar:

- Movimentações incompatíveis com o perfil declarado;
- Operações atípicas ou incomuns;
- Situações que possam indicar indícios de irregularidades.

6.6 Registro e Atualização

As informações relativas à condição de PEP devem:

- Ser registradas no cadastro;
- Ser mantidas atualizadas;
- Ser revisadas periodicamente ou sempre que houver alteração relevante.

6.7 Comunicação de Situações Suspeitas

Caso sejam identificadas operações ou situações suspeitas envolvendo PEP, o IAPP deve:

- Realizar análise detalhada;
- Registrar as evidências;
- Avaliar a necessidade de comunicação ao COAF, conforme regulamentação aplicável.

7. DUE DILIGENCE DE TERCEIROS E CONSULTAS A LISTAS RESTRITIVAS

7.1 Diretrizes Gerais

O IAPP deve adotar procedimentos de due diligence no processo de contratação e manutenção de relacionamento com fornecedores, prestadores de serviços e parceiros, incluindo aqueles responsáveis pela execução de atividades operacionais terceirizadas, com o objetivo de prevenir a contratação de pessoas físicas ou jurídicas envolvidas, direta ou indiretamente, em atividades ilícitas, incluindo lavagem de dinheiro e financiamento do terrorismo.

A diligência deve ser proporcional ao risco associado à natureza da contratação, ao grau de exposição da atividade e à relevância do terceiro para a execução dos processos da Entidade.

7.2 Identificação e Qualificação de Terceiros

Antes da contratação, o IAPP deve realizar a identificação e qualificação dos terceiros, incluindo, no mínimo:

- Dados cadastrais da pessoa física ou jurídica;
- Identificação de sócios, administradores e, quando aplicável, beneficiário final;
- Verificação da atividade econômica;
- Avaliação da compatibilidade entre o objeto do contrato e a atividade do fornecedor.

7.3 Consultas a Listas Restritivas e Bases Públicas

No processo de due diligence, o IAPP deve realizar, sempre que aplicável, consultas ao CNPJ e CPF dos envolvidos, incluindo sócios e administradores, em bases públicas e listas restritivas, tais como:

- Listas de sanções nacionais e internacionais;
- Listas relacionadas a crimes financeiros e econômicos;
- Cadastros de inidoneidade ou restrição (quando disponíveis);

- Informações públicas que indiquem envolvimento em atividades ilícitas.

As consultas devem ser registradas e arquivadas como evidência do processo de diligência.

7.4 Verificação de Pessoas Expostas Politicamente (PEP)

Deve ser verificado, no processo de contratação, se os terceiros, seus sócios ou administradores se enquadram como Pessoas Expostas Politicamente (PEP), sendo aplicados, nesses casos, procedimentos de diligência reforçada, conforme disposto nesta Política.

7.5 Classificação de Risco de Terceiros

Os terceiros devem ser avaliados quanto ao risco de lavagem de dinheiro e financiamento do terrorismo, considerando:

- Natureza do serviço prestado;
- Grau de acesso a recursos financeiros ou informações sensíveis;
- Complexidade da operação;
- Exposição a riscos regulatórios.

Quando identificado maior nível de risco, devem ser aplicados controles adicionais.

7.6 Monitoramento e Reavaliação

O IAPP deve, sempre que necessário:

- Reavaliar os terceiros contratados;
- Atualizar informações cadastrais;
- Monitorar eventuais alterações relevantes que possam impactar o risco da relação;
- Reavaliar a continuidade do relacionamento em caso de indícios de irregularidades.

7.7 Vedação de Contratação

O IAPP poderá deixar de contratar, restringir ou reavaliar a manutenção do relacionamento com terceiros que:

- Apresentem indícios relevantes de envolvimento em atividades ilícitas, incluindo lavagem de dinheiro, financiamento do terrorismo, corrupção ou fraude;
- Estejam incluídos em listas restritivas ou de sanções aplicáveis, após análise do caso concreto;
- Não forneçam informações suficientes para sua adequada identificação, qualificação ou realização dos procedimentos de due diligence.

As situações identificadas deverão ser avaliadas considerando o contexto, a materialidade, os riscos envolvidos e as evidências disponíveis, podendo resultar na adoção de diligências adicionais antes da decisão sobre a contratação ou manutenção do relacionamento.

7.8 Registro e Evidência

Todos os procedimentos de due diligence devem ser:

- Formalmente registrados;
- Mantidos como evidência;
- Disponibilizados para fins de auditoria e fiscalização, quando solicitado.

8. MONITORAMENTO E IDENTIFICAÇÃO DE OPERAÇÕES E SITUAÇÕES SUSPEITAS

8.1 Diretrizes Gerais

O IAPP deve manter procedimentos de monitoramento contínuo de suas operações e relacionamentos, com o objetivo de identificar, analisar e tratar situações que possam indicar indícios de lavagem de dinheiro ou financiamento do terrorismo.

O monitoramento deve ser proporcional ao risco identificado, considerando os resultados da Avaliação Interna de Risco (AIR).

8.2 Monitoramento de Operações

O monitoramento deve abranger, no mínimo:

- Contribuições realizadas aos planos de benefícios;
- Aportes realizados por terceiros;
- Pagamentos a fornecedores e prestadores de serviços;
- Operações financeiras relevantes realizadas no âmbito da Entidade;
- Alterações cadastrais relevantes;
- Movimentações incompatíveis com o perfil do participante, assistido ou terceiro.

8.3 Critérios para Identificação de Situações Suspeitas

Devem ser consideradas situações de atenção, entre outras:

- Operações com valores incompatíveis com a capacidade financeira declarada;
- Movimentações financeiras atípicas, incomuns ou sem justificativa aparente;
- Fragmentação de operações com o objetivo de evitar controles;
- Utilização de terceiros para realização de operações;
- Recusa ou dificuldade na prestação de informações cadastrais;
- Alterações cadastrais frequentes ou inconsistentes;

- Operações envolvendo Pessoas Expostas Politicamente (PEP) sem justificativa adequada;
- Envolvimento com pessoas ou entidades com histórico ou indícios de irregularidades.

8.4 Monitoramento de Enriquecimento Súbito

O IAPP deve dispensar atenção a situações que possam indicar enriquecimento súbito de colaboradores, especialmente aqueles que exerçam funções com maior exposição a riscos financeiros ou operacionais.

Quando identificados indícios, devem ser realizadas análises adicionais, com o devido registro das evidências, e, quando necessário, adotadas medidas preventivas ou corretivas.

8.5 Análise de Situações Atípicas

As situações identificadas como atípicas ou suspeitas devem ser:

- Analisadas de forma tempestiva;
- Documentadas, com registro das evidências;
- Avaliadas quanto à necessidade de adoção de medidas adicionais;
- Submetidas à Diretoria Executiva, quando aplicável.

8.6 Registro e Rastreabilidade

Todas as análises realizadas devem ser:

- Formalmente registradas;
- Mantidas com documentação de suporte;
- Arquivadas pelo prazo mínimo exigido pela legislação;
- Disponibilizadas para fins de auditoria e fiscalização.

8.7 Ações Preventivas e Corretivas

Quando identificados indícios de lavagem de dinheiro ou financiamento do terrorismo, o IAPP deve:

- Adotar medidas preventivas, incluindo revisão de processos e controles;
- Avaliar a continuidade do relacionamento com as partes envolvidas;
- Reforçar os controles internos aplicáveis;
- Implementar ações corretivas para evitar recorrência;
- Avaliar a necessidade de comunicação aos órgãos competentes.

8.8 Integração com a Gestão de Riscos

As situações identificadas no monitoramento devem ser consideradas no processo de gestão de riscos da Entidade, contribuindo para:

- Atualização da Avaliação Interna de Risco (AIR);
- Aprimoramento dos controles internos;
- Priorização de ações de mitigação.

9. COMUNICAÇÃO AO COAF E À PREVIC

9.1 Diretrizes Gerais

O IAPP deve realizar a comunicação de operações e situações suspeitas de lavagem de dinheiro ou financiamento do terrorismo aos órgãos competentes, em conformidade com a legislação e regulamentação aplicáveis, garantindo tempestividade, sigilo e rastreabilidade das informações.

9.2 Comunicação ao COAF

O IAPP deve comunicar ao Conselho de Controle de Atividades Financeiras (COAF), por meio do sistema Siscoaf, no prazo de até 24 (vinte e quatro) horas a contar da conclusão da análise, as seguintes situações:

- Operações ou propostas de operações que possam constituir indícios de lavagem de dinheiro ou financiamento do terrorismo;
- Operações realizadas com um mesmo participante ou assistido que sejam iguais ou superiores a R\$ 50.000,00 (cinquenta mil reais), exceto aquelas decorrentes de pagamento de benefícios, empréstimos ou portabilidade, conforme regulamentação vigente.

A comunicação deve ser realizada independentemente de ciência ou autorização das partes envolvidas.

9.3 Comunicação Negativa à PREVIC

O IAPP deve comunicar à Superintendência Nacional de Previdência Complementar (PREVIC) a não ocorrência de operações ou situações passíveis de comunicação ao COAF, quando aplicável, observando os prazos e procedimentos estabelecidos na regulamentação vigente.

9.4 Sigilo das Informações

As comunicações realizadas ao COAF e à PREVIC devem ser tratadas com caráter sigiloso, sendo vedada a divulgação de sua existência ou conteúdo às partes envolvidas ou a terceiros não autorizados.

9.5 Registro e Evidência

O IAPP deve manter registro das comunicações realizadas, bem como das análises que as fundamentaram, garantindo:

- Rastreabilidade das decisões;
- Armazenamento das evidências;
- Disponibilidade para fins de auditoria e fiscalização.

9.6 Responsabilidade pela Comunicação

A comunicação ao COAF e à PREVIC é de responsabilidade da Diretoria Executiva, podendo ser operacionalizada por colaborador designado, sob sua supervisão.

10. PREVENÇÃO À LAVAGEM DE DINHEIRO E AO FINANCIAMENTO DO TERRORISMO NO DESENVOLVIMENTO DE PRODUTOS E SERVIÇOS

10.1 Diretrizes Gerais

O IAPP deve considerar os riscos de lavagem de dinheiro e financiamento do terrorismo no desenvolvimento, alteração ou revisão de produtos, serviços e processos, de forma a prevenir a utilização da Entidade para práticas ilícitas.

10.2 Avaliação de Riscos

Antes da implementação de novos produtos, serviços ou alterações relevantes, o IAPP deve avaliar, de forma proporcional ao seu porte e complexidade:

- Possíveis vulnerabilidades relacionadas à lavagem de dinheiro e ao financiamento do terrorismo;
- O perfil dos públicos envolvidos;
- A natureza das operações e movimentações financeiras;
- A necessidade de implementação ou adequação de controles internos.

10.3 Implementação de Controles

Quando identificados riscos, o IAPP deve:

- Definir e implementar controles compatíveis com o nível de risco identificado;
- Estabelecer critérios de monitoramento das operações associadas;
- Avaliar a necessidade de revisão de procedimentos existentes.

10.4 Registro das Avaliações

As análises realizadas devem ser registradas de forma simplificada, garantindo:

- Evidência da avaliação de risco;

- Rastreabilidade das decisões;
- Disponibilidade para eventual verificação.

11. PREVENÇÃO À LAVAGEM DE DINHEIRO E AO FINANCIAMENTO DO TERRORISMO NO USO DE NOVAS TECNOLOGIAS

11.1 Diretrizes Gerais

O IAPP deve considerar os riscos de lavagem de dinheiro e financiamento do terrorismo na utilização de novas tecnologias, sistemas e ferramentas, de forma a evitar vulnerabilidades que possam ser exploradas para práticas ilícitas.

11.2 Avaliação de Riscos Tecnológicos

Sempre que houver implementação ou alteração relevante em sistemas, ferramentas ou soluções tecnológicas, o IAPP deve avaliar, de forma proporcional ao seu porte:

- Possíveis riscos relacionados à segurança da informação e integridade dos dados;
- Impactos sobre os processos de cadastro, monitoramento e controle;
- Potenciais vulnerabilidades que possam facilitar fraudes, inconsistências ou ocultação de informações.

11.3 Controles e Mitigações

Quando identificados riscos, o IAPP deve:

- Adotar medidas de controle compatíveis com o nível de risco identificado;
- Garantir a integridade, confiabilidade e rastreabilidade das informações;
- Assegurar que os sistemas utilizados permitam a adequada identificação e registro das operações.

11.4 Registro das Avaliações

As análises realizadas devem ser registradas de forma simplificada, garantindo evidência da avaliação e suporte às decisões adotadas.

12. AÇÕES PREVENTIVAS E CORRETIVAS

12.1 Diretrizes Gerais

O IAPP deve adotar ações preventivas e corretivas sempre que forem identificados indícios, fragilidades ou situações que possam representar risco de lavagem de dinheiro ou financiamento do terrorismo, com o objetivo de mitigar riscos e evitar recorrência.

12.2 Ações Preventivas

As ações preventivas consistem na adoção de medidas para reduzir ou eliminar riscos identificados, podendo incluir, entre outras:

- Revisão e aprimoramento de processos;
- Ajuste de controles internos;
- Reforço de procedimentos de cadastro e monitoramento;
- Orientação aos colaboradores sobre boas práticas;
- Implementação de medidas adicionais de verificação, quando necessário.

12.3 Ações Corretivas

As ações corretivas devem ser adotadas quando identificadas falhas ou ocorrências relacionadas a possíveis irregularidades, incluindo:

- Análise detalhada da situação identificada;
- Registro das evidências e das decisões adotadas;
- Correção de inconsistências ou falhas operacionais;
- Avaliação da necessidade de comunicação aos órgãos competentes;
- Adoção de medidas para evitar a repetição da ocorrência.

12.4 Tratamento e Acompanhamento

As ações preventivas e corretivas devem:

- Ser registradas de forma adequada;
- Ter responsáveis definidos, quando aplicável;
- Ser acompanhadas até sua conclusão;
- Ser consideradas nos processos de avaliação de riscos e de efetividade dos controles.

13. PREVENÇÃO À LAVAGEM DE DINHEIRO E AO FINANCIAMENTO DO TERRORISMO NA ATUAÇÃO DOS COLABORADORES

13.1 Diretrizes Gerais

O IAPP deve assegurar que os colaboradores que atuam na Entidade, ainda que cedidos por patrocinadores, observem as diretrizes de prevenção à lavagem de dinheiro e ao financiamento do terrorismo, garantindo a integridade, a ética e a conformidade nas atividades desempenhadas.

13.2 Conhecimento das Diretrizes de PLD/FT

O IAPP deve assegurar que os colaboradores:

- Tenham ciência desta Política e de suas responsabilidades;
- Recebam orientações básicas sobre prevenção à lavagem de dinheiro e ao financiamento do terrorismo;
- Estejam aptos a identificar situações atípicas no exercício de suas atividades.

13.3 Conduta e Responsabilidades

Os colaboradores devem:

- Atuar com ética, diligência e responsabilidade;
- Cumprir os procedimentos estabelecidos nesta Política;
- Comunicar situações atípicas ou suspeitas à Diretoria Executiva;
- Manter suas informações cadastrais atualizadas, quando aplicável.

13.4 Medidas em Caso de Irregularidades

Caso sejam identificados indícios de irregularidades envolvendo colaboradores, o IAPP deve:

- Realizar análise da situação;
- Registrar as evidências;
- Adotar as medidas cabíveis, conforme a gravidade do caso;
- Avaliar a necessidade de comunicação aos órgãos competentes.

14. AVALIAÇÃO DE EFETIVIDADE

14.1 Diretrizes Gerais

O IAPP deve realizar, no mínimo anualmente, a avaliação de efetividade da Política, dos procedimentos e dos controles internos relacionados à prevenção à lavagem de dinheiro e ao financiamento do terrorismo, em conformidade com a regulamentação vigente.

14.2 Objetivo da Avaliação

A avaliação de efetividade tem como objetivo verificar se os controles implementados são adequados e suficientes para prevenir, detectar e tratar riscos de lavagem de dinheiro e financiamento do terrorismo no âmbito da Entidade.

14.3 Realização da Avaliação

A avaliação de efetividade deverá ser realizada periodicamente, podendo ser conduzida com o apoio de terceiros especializados, quando aplicável.

14.4 Utilização dos Resultados

Os resultados da avaliação de efetividade devem subsidiar:

- A identificação de oportunidades de melhoria;
- O aprimoramento dos controles internos;
- A atualização da Avaliação Interna de Risco (AIR);
- A revisão desta Política, quando necessário.

15. TREINAMENTO E CAPACITAÇÃO

15.1 Diretrizes Gerais

O IAPP deve promover a capacitação dos colaboradores quanto às práticas de prevenção à lavagem de dinheiro e ao financiamento do terrorismo, de forma proporcional ao porte da Entidade e às atividades desempenhadas.

15.2 Objetivo do Treinamento

Os treinamentos têm como objetivo:

- Disseminar as diretrizes desta Política;
- Orientar sobre a identificação de situações atípicas ou suspeitas;
- Reforçar a importância da prevenção à lavagem de dinheiro e ao financiamento do terrorismo;
- Promover a atuação ética e diligente dos colaboradores.

15.3 Realização dos Treinamentos

Os treinamentos devem ser realizados periodicamente, podendo ocorrer por meio de:

- Orientações internas;
- Reuniões de alinhamento;
- Materiais informativos;
- Outras formas compatíveis com a estrutura da Entidade.

15.4 Registro

O IAPP deve manter registro das ações de treinamento realizadas, de forma a evidenciar a disseminação das diretrizes desta Política.

16. SANÇÕES E CONSEQUÊNCIAS

16.1 Diretrizes Gerais

O descumprimento das diretrizes estabelecidas nesta Política sujeita os envolvidos às medidas cabíveis, conforme a natureza e a gravidade da irregularidade, observadas as normas internas do IAPP e a legislação aplicável.

16.2 Aplicação de Medidas

Nos casos de descumprimento, poderão ser adotadas, entre outras, as seguintes medidas:

- Orientação e reforço das diretrizes aplicáveis;
- Registro da ocorrência;
- Comunicação à patrocinadora, quando envolver colaborador cedido;
- Adoção de medidas administrativas cabíveis;
- Avaliação da necessidade de comunicação aos órgãos competentes.

16.3 Responsabilização

Os envolvidos em práticas relacionadas à lavagem de dinheiro ou financiamento do terrorismo poderão ser responsabilizados nas esferas administrativa, civil e penal, nos termos da legislação vigente.

17. DIVULGAÇÃO E DISSEMINAÇÃO

17.1 Diretrizes Gerais

O IAPP deve assegurar que esta Política seja devidamente divulgada e disseminada, considerando as funções desempenhadas pelos colaboradores e a sensibilidade das informações.

17.2 Público Interno

A Política deve ser disponibilizada a todos os colaboradores que atuam na Entidade, de forma a garantir:

- A ciência das diretrizes estabelecidas;
- A compreensão das responsabilidades individuais;
- O alinhamento das atividades com os princípios de prevenção à lavagem de dinheiro e ao financiamento do terrorismo.

17.3 Partes Interessadas

Sempre que aplicável, o IAPP poderá disponibilizar as diretrizes desta Política às partes interessadas relevantes, tais como prestadores de serviços e parceiros, especialmente quando houver impacto direto nas atividades desempenhadas.

17.4 Forma de Divulgação

A divulgação da Política poderá ser realizada por meio de:

- Disponibilização em meio eletrônico;
- Compartilhamento interno;
- Outras formas compatíveis com a estrutura da Entidade.

18. REVISÃO PERIÓDICA

18.1 Periodicidade

Esta Política deve ser revisada, no mínimo, anualmente, ou sempre que houver:

- Alterações na legislação ou regulamentação aplicável;
- Mudanças relevantes nos processos ou na estrutura do IAPP;
- Identificação de necessidade de aprimoramento.

18.2 Registro das Revisões

As revisões realizadas devem ser devidamente registradas, incluindo a data de atualização e, quando aplicável, a descrição das alterações realizadas.