



# i9ADVISORY

---

**POLÍTICA DE PREVENÇÃO E COMBATE  
AOS CRIMES DE LAVAGEM DE DINHEIRO E  
FINANCIAMENTO AO TERRORISMO**

Março de 2022



## **1. OBJETIVO**

A presente Política tem como objetivo estabelecer critérios a serem adotados pela i9Advisory e seus Colaboradores para coibir práticas de lavagem de dinheiro e financiamento ao terrorismo no âmbito das atividades de Consultoria de Investimentos. Cabe ao Diretor de Compliance da i9Advisory assegurar a aplicação da Política, nos termos da Resolução CVM 19 e da Resolução CVM 50 e demais normativos referentes ao assunto conforme expedidos pela CVM.

## **2. LAVAGEM DE DINHEIRO E FINANCIAMENTO AO TERRORISMO**

Constitui lavagem de dinheiro, a ocultação ou dissimulação da natureza, origem, localização, disposição, movimentação ou propriedade de bens, direito ou valores provenientes, direta ou indiretamente, de crime: (i) de tráfico ilícito de substâncias entorpecentes ou drogas afins; (ii) de terrorismo e seu financiamento; (iii) de contrabando ou tráfico de armas, munições ou material destinado à sua produção; (iv) de extorsão mediante sequestro; (v) contra a Administração Pública, inclusive a exigência, para si ou para outrem, direta ou indiretamente, de qualquer vantagem, como condição ou preço para a prática ou omissão de atos administrativos; (vi) contra o sistema financeiro nacional; (vii) praticado por organização criminosa; e (viii) praticado por particular contra a administração pública estrangeira (arts. 337-B, 337-C e 337- D do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal).

Incorre ainda no mesmo crime de lavagem de dinheiro quem, para ocultar ou dissimular a utilização de bens, direitos ou valores provenientes de atividades ilícitas: (i) os converte em ativos lícitos; (ii) os adquire, recebe, troca, negocia, dá ou recebe em garantia, guarda, tem em depósito, movimenta ou transfere; (iii) importa ou exporta bens com valores não correspondentes aos verdadeiros; (iv) utiliza, na atividade econômica ou financeira, bens, direitos ou valores que sabe



serem provenientes de qualquer dos crimes descritos acima; e (v) participa de grupo, associação ou escritório tendo conhecimento de que sua atividade principal ou secundária é dirigida à prática dos crimes descritos acima.

O financiamento do terrorismo consiste na destinação de recursos a terroristas, organizações terroristas ou atos terroristas. Os recursos podem ter origem lícita ou ilícita.

A i9Advisory deverá cooperar plenamente, de acordo com as leis aplicáveis, com os esforços dos órgãos governamentais competentes para evitar, detectar e processar situações que possam implicar em lavagem de dinheiro e/ou financiamento de terrorismo. A i9Advisory não poderá, conscientemente, fazer negócios com clientes existentes ou potenciais cujo dinheiro seja suspeito de ser proveniente de ou usado para, atividades criminosas ou terroristas. Se a i9Advisory souber de fatos que levem a uma suposição razoável de que algum cliente esteja envolvido em tais atividades, ou de que as transações de algum cliente sejam, elas próprias, criminosas em suas respectivas finalidades, deverão ser tomadas as devidas providências, de acordo com a lei. Tais providências poderão incluir, por exemplo, o cancelamento de transações comerciais com tal Cliente, o fechamento ou o congelamento das contas desse Cliente e o envio de relatórios às autoridades governamentais competentes.

### **3. GOVERNANÇA E ATRIBUIÇÕES DE RESPONSABILIDADES**

A i9Advisory possui estrutura de governança compatível com a complexidade dos produtos e serviços fornecidos conforme exigências da CVM, sendo que é do entendimento da consultoria que cada componente possui suas atribuições e responsabilidades na implementação desta Política.



A Alta Administração da i9Advisory é composta pelo Diretor de Consultoria de Valores Mobiliários e o Diretor de *Compliance*. Tais pessoas são responsáveis pelas rotinas de natureza diretiva/gerencial em suas respectivas áreas de competência, sendo os analistas das áreas técnicas e de compliance responsáveis pelas rotinas operacionais, respondendo diretamente ao diretor a cargo do respectivo departamento.

As atribuições de cada perfil de profissional para fins de implementação das regras contidas nesta Política, incluindo mas não se limitando ao processo de abordagem baseada em risco, estão devidamente descritas na **Diretriz de Atribuição de Responsabilidades para fins de Cumprimento da Política de PLDFT** da i9Advisory.

O Comitê de *Compliance* e PLDFT é o organismo interno da i9Advisory dedicado a deliberar sobre questões referentes à presente Política. O referido comitê é instalado mensalmente e possui como membros efetivos o Diretor de *Compliance* e os analistas do Departamento de *Compliance* sendo, portanto, totalmente independente da área de negócios da i9Advisory. Os assuntos discutidos e as deliberações tomadas são registradas em atas, sendo que o poder de decisão quanto às matérias deliberadas está concentrado no referido diretor.

#### **4. AVALIAÇÃO INTERNA DE RISCO**

É de conhecimento da i9Advisory que as atividades realizadas por essa no âmbito do mercado de capitais brasileiro implicam na assunção de riscos de lavagem de dinheiro e financiamento ao terrorismo, os quais deverão ser identificados, analisados, compreendidos e mitigados pelos colaboradores responsáveis pela implementação do Programa de PLDFT da instituição.

Diante deste cenário, tem-se que os fatores de riscos identificados referentes a tais atividades são: os clientes, os colaboradores, os parceiros e os prestadores de serviços relevantes. Tais fatores e/ou situações a esses relacionadas deverão ser classificados de acordo com a probabilidade de



potencial dano ao mercado de valores mobiliários e à instituição no que se refere à lavagem de dinheiro e financiamento ao terrorismo, nas categorias Baixo, Médio ou Alto de acordo com os parâmetros definidos na **Diretriz de Avaliação Interna de Risco** da i9Advisory, adotando-se uma abordagem baseada em risco para garantir que as medidas de prevenção e mitigação sejam proporcionais aos riscos identificados e assegurar o cumprimento da regulamentação em vigor, conforme metodologia lá detalhada.

O Diretor de *Compliance* deve elaborar relatório relativo à avaliação interna de risco de lavagem de dinheiro e financiamento ao terrorismo, a ser encaminhado para a Alta Administração até o último dia útil do mês de abril, contendo as seguintes informações: (i) classificação dos clientes por grau de risco de lavagem de dinheiro e financiamento ao terrorismo, segmentando-os minimamente em baixo, médio e alto risco; (ii) identificação e análise das situações de risco de lavagem de dinheiro e financiamento ao terrorismo, considerando as respectivas ameaças, vulnerabilidades e consequências; (iii) análise da atuação dos prepostos ou prestadores de serviços relevantes contratados; (iv) tabela relativa ao ano anterior, contendo (a) o número consolidado das situações atípicas detectadas; (b) o número de análises de operações realizadas; (c) o número de comunicações de operações suspeitas reportadas para a Unidade de Inteligência Financeira; e (d) a data do reporte da declaração negativa de comunicação de operações, se for o caso; (v) as medidas adotadas para o atendimento do disposto nas alíneas “b” e “c” do inciso II do art. 4º da Resolução CVM 50; (vi) a apresentação dos indicadores de efetividade nos termos definidos na política de PLDFT, incluindo a tempestividade acerca das atividades de detecção, análise e comunicação de operações ou situações atípicas; (vii) a apresentação, se for o caso, de recomendações visando mitigar os riscos identificados do exercício anterior que ainda não foram devidamente tratados, contendo (a) possíveis alterações nas diretrizes previstas na política de PLDFT; (b) aprimoramento das regras, procedimentos e controles internos, com o estabelecimento de cronogramas de saneamento; e (viii) a indicação da efetividade das recomendações adotadas referidas no item vi acima em relação ao relatório respectivamente anterior, de acordo com a metodologia de abordagem baseada em risco, registrando de forma individualizada os resultados.



O referido relatório deverá ficar disponível para a CVM na sede da i9Advisory.

## 5. PROCESSO DE CONHEÇA SEU CLIENTE (KYC)

Os colaboradores deverão empenhar seus esforços para determinar a verdadeira identidade de todos os Clientes, para ajudar a evitar que os sistemas financeiros e comerciais sejam usados como canais para financiar crimes e atividades terroristas.

Não poderão ser conduzidas transações comerciais com clientes que deixarem de fornecer comprovações adequadas das respectivas identidades, ou que tentarem enganar os órgãos regulamentares ou policiais ou a i9Advisory fornecendo informações incompletas, alteradas ou enganosas.

É de importância vital que todos os colaboradores compreendam plenamente que essas ações podem constituir infração às leis aplicáveis contra lavagem de dinheiro e financiamento do terrorismo e relatem qualquer irregularidade potencial.

Os colaboradores devem conhecer e aplicar na íntegra a legislação referente à prevenção e combate ao crime de lavagem de dinheiro, especialmente, a Lei nº 9.613/98, e demais normativos editados ou que venham a ser editados com relação à prevenção aos crimes de lavagem ou ocultação de bens, direitos e valores, bem como a política de prevenção e combate ao crime de lavagem de dinheiro.

O processo de Conheça o seu Cliente (KYC) adotado pela i9Advisory é composto por 04 (quatro) etapas, a saber (i) a identificação do Cliente; (ii) o cadastro e a identificação dos beneficiários finais; (iii) a avaliação reputacional e de enquadramento de PEP; e (iv) a condução de diligências devidas, conforme melhor detalhadas na **Diretriz do Processo de Conheça seu Cliente (KYC)** da i9Advisory.



Tais etapas foram delineadas com o objetivo de estabelecer um processo detalhado e constante de conhecimento dos clientes, assim como identificar e monitorar situações que impliquem maiores riscos para o início ou manutenção do relacionamento entre cliente e i9Advisory tais como a presença de entidades sem fins lucrativos ou pessoas expostas politicamente.

Os cadastros deverão ser elaborados contendo minimamente as informações requeridas no Anexo B da Resolução CVM 50 e atualizados periodicamente de acordo com a classificação de risco atribuída a cada cliente nos termos da metodologia de abordagem baseada em risco adotada pela consultora, observando o intervalo máximo de 05 (cinco) anos em relação ao cadastro inicial ou a sua última atualização. Tanto no cadastramento inicial de novos clientes quanto na atualização periódica serão verificadas as condições relativas à Pessoa Exposta Politicamente.

A I9Advisory adota a política de análise e identificação do investidor com o objetivo de conhecer seus clientes estabelecendo um conjunto de regras que propiciem identificar e conhecer a origem e constituição do patrimônio e dos recursos financeiros do cliente, assim como os beneficiários finais dos clientes organizados sob a forma de pessoa jurídica ou entes despersonalizados.

Todos os clientes da I9Advisory deverão ser previamente cadastrados antes do início do relacionamento de negócios com a i9Advisory. Caso os colaboradores suspeitarem de qualquer dado ou informação do cliente, deverá reportar tal acontecimento ao Diretor de *Compliance* para que seja determinado se o cliente deverá ou não ser aceito. O Diretor de *Compliance* da I9Advisory, a seu exclusivo critério, poderá vetar o início ou a manutenção do relacionamento da consultora com potenciais clientes ou clientes, conforme o caso, devido ao risco envolvido.

Na ocasião da implementação do primeiro cadastro, assim como em suas posteriores atualizações, é providenciada a análise reputacional dos clientes por meio da pesquisa de mídias negativas, processos judiciais e apontamentos em listas restritivas de alcance internacional tais como aquelas divulgadas pelo Escritório de Controle de Ativos Estrangeiros dos EUA, INTERPOL e Conselho das Nações Unidas e, também, de alcance nacional tais como aquelas divulgadas pelo Governo Federal



e outros organismos referentes a trabalho escravo, empresas inedôneas e suspeitas (CEIS), autuações e embargos ambientais de origem e aquisição (IBAMA), entidades sem fins lucrativos impedidas (CEPIM) e empresas punidas (CNEP). As pesquisas são realizadas por meio de consulta de bases de dados públicas e privadas e compiladas em relatório sujeito à aprovação do Diretor de de *Compliance*.

No caso de clientes, organizados sob a forma de pessoa jurídica, deverão ser identificados e verificados os respectivos beneficiários finais, os diretores e os procuradores, caso houver, devendo ser realizadas as avaliações reputacionais pertinentes.

A i9Advisory conta com o suporte de sistemas informatizados para coleta e verificação de dados cadastrais, reputacionais e quanto ao enquadramento dos clientes, seus beneficiários finais, representantes e procuradores, assim como seus familiares, estreitos colaboradores e pessoas de relacionamento próximo na condição de Pessoa Exposta Politicamente (PEP).

Os colaboradores do Departamento de *Compliance* da i9Advisory deverão estabelecer uma análise independente e assegurar um processo reforçado de “Due Diligence” e monitoramento das operações com relação às Pessoas Expostas Politicamente (PEP). A aceitação de Pessoa Exposta Politicamente como cliente da i9Advisory depende sempre da autorização do Diretor de *Compliance*.

## **6. PROCESSO DE CONHEÇA SEU PARCEIRO (KYP)**

O Processo de Conheça o seu Parceiro (KYP) tem como objetivo coletar e validar periodicamente dados cadastrais dos parceiros e prestadores de serviços relevantes que possuem ou possuem relacionamento comercial com a i9Advisory. Os critérios para análise, seleção, monitoramento e classificação de risco dos prestadores de serviços relevantes e parceiros estão devidamente descritos na **Diretriz para o Processo de Conheça seu Parceiro (KYP)** da i9Advisory. Os



procedimentos são implementados de acordo com o perfil e o propósito de relacionamento, visando prevenir a realização de negócios com pessoas declaradas inidôneas ou investigadas por envolvimento em atividades ilícitas.

São coletados dados cadastrais para a correta identificação do parceiro ou do prestador de serviço relevante, assim como seus sócios, diretores e procuradores e beneficiários finais os quais são ratificados por meio de pesquisas realizadas em base de dados públicas e/ou privadas. Os colaboradores do Departamento de *Compliance* no âmbito da implementação do Processo de Conheça seu Parceiro (KYP) serão responsáveis pela realização de avaliação reputacional da pessoa jurídica representada pelo parceiro ou prestador de serviço relevante, seus beneficiários finais, diretores e procuradores, quando aplicável, assim como pela identificação de Pessoas Expostas Politicamente na estrutura societária de tais pessoas jurídicas.

Caberá aos colaboradores do Departamento de *Compliance* a verificação da elaboração e implementação de políticas de PLDFT por parte dos parceiros e prestadores de serviços relevantes, realizando diligências nas estruturas físicas desses quando cabível.

## **7. PROCESSO DE CONHEÇA SEU EMPREGADO (KYE)**

O Processo de Conheça seu Empregado (KYE) consiste na condução de diligências para identificação e verificação dos colaboradores vinculados à i9Advisory. Tais diligências são condizentes ao perfil da posição que o colaborador ocupa e ao histórico das suas atividades profissionais e objetivam a realização de verificação de informações cadastrais em banco de dados públicos e/ou privados, assim como avaliação reputacional, nos termos da **Diretriz para o Processo de Conheça seu Empregado (KYE)** da i9Advisory.

Todos os Colaboradores da i9Advisory, independentemente de sua função, devem atender aos treinamentos e capacitação promovidos pela instituição, assim como ler, compreender e aderir à presente Política.



## 8. APROVAÇÃO DE NOVOS PRODUTOS, SERVIÇOS E TECNOLOGIAS

A aprovação de novos produtos, serviços ou tecnologias deverá ser analisada sob o ponto de vista de PLDFT pelo Comitê de *Compliance* e PLDFT, sendo que deverá ser elaborado e registrado na ata da reunião de avaliação e aprovação dos novos produtos, serviços ou tecnologias um cronograma com as exigências mínimas para implantação dos processos internos e rotinas operacionais, assim como os prazos para tal implantação.

Na avaliação de novos produtos, serviços e tecnologias deverá ser levado em consideração, a identificação, a avaliação, a mitigação e a compreensão dos riscos inerentes a situações de LDFT e a viabilidade da incorporação desses na **Diretriz Avaliação Interna de Risco**, assim como a aplicação da metodologia de abordagem baseada em risco da instituição.

## 9. CUMPRIMENTO DE SANÇÕES IMPOSTAS POR RESOLUÇÕES DO CSNU

A i9Advisory, no limite de suas atribuições, deverá cumprir, imediatamente, e sem aviso prévio aos sancionados, as medidas estabelecidas nas resoluções sancionatórias do CSNU ou as designações dos seus comitês de sanções que determinem a indisponibilidade de ativos de quaisquer valores, de titularidade, direta ou indireta, de pessoas naturais, de pessoas jurídicas ou de entidades, assim como determinações judiciais conforme previsto na regulamentação em vigor.

Ficará sob a responsabilidade do Departamento de *Compliance* (i) monitorar diretamente as determinações de indisponibilidade referidas no parágrafo anterior assim como eventuais informações a serem observadas para o seu adequado atendimento, inclusive o levantamento total ou parcial de tais determinações em relação a pessoas, entidades ou ativos, visando ao cumprimento imediato do quanto determinado, acompanhando, minimamente em períodos



mensais, para tanto, as informações divulgadas na página do CSNU na rede mundial de computadores; e (ii) comunicar imediatamente a indisponibilidade de ativos e as tentativas de sua transferência relacionadas às pessoas naturais, às pessoas jurídicas ou às entidades sancionadas por resolução do CSNU ou por designações de seus comitês de sanções, nos termos da legislação em vigor para a CVM ([listas@cvm.gov.br](mailto:listas@cvm.gov.br)), o Ministério da Justiça e Segurança Pública ([csnu@mj.gov.br](mailto:csnu@mj.gov.br)) e a Unidade de Inteligência Financeira; e (iii) manter sob verificação a existência ou o surgimento, em seu âmbito, de ativos alcançados pelas determinações de indisponibilidade para efeito de pôr tais ativos imediatamente, tão logo detectados, sob tal regime, nos termos da legislação em vigor.

## 10. INTERCÂMBIO DE INFORMAÇÕES

Para o cumprimento desta Política e suas diretrizes correlatas, a i9Advisory possui mecanismos de intercâmbio de informações com sociedades do mesmo grupo econômico que a consultora e parceiros que atuem como prestadores de serviços no mercado de capitais, tais como administradores fiduciários, custodiantes, escrituradores, controladores e auditores independentes. As informações intercambiadas são consideradas confidenciais e serão divulgadas preferencialmente de forma restrita em conteúdo suficiente para atendimento das normas de PLDFT, preservando a intimidade dos envolvidos. A condução dessas comunicações será de responsabilidade do Departamento de *Compliance*, sendo que essas serão realizadas por meio de correspondências eletrônicas.

## 11. IDENTIFICAÇÃO E COMUNICAÇÃO DE SITUAÇÕES ATÍPICAS

Eventuais operações ou situações atípicas e suspeitas com indícios da prática dos crimes de lavagem de dinheiro e financiamento ao terrorismo verificadas no âmbito da atividade de



consultoria de valores mobiliários exercidas pela i9 Advisory, deverão ser objeto de investigação por parte do Departamento *Compliance* por meio de diligências que objetivem identificar minimamente as pessoas envolvidas, a origem e o destino dos recursos movimentados, assim como o objetivo e o fundamento econômico das movimentações, além de outros parâmetros a serem definidos pelo Comitê de Compliance e PLDFT, conforme cada circunstância. Tal investigação deverá ser encerrada em até 45 (quarenta e cinco) dias da detecção da operação e/ou situação suspeita, sendo que todas as informações relacionadas ao processo investigativo deverão ser formalizadas na forma de relatório, havendo a conclusão acerca da ocorrência ou não de fortes indícios da prática dos crimes de lavagem de dinheiro e financiamento ao terrorismo. Tal relatório deverá ser apreciado pelo Comitê de Compliance e PLDFT que decidirá pela comunicação ou não às autoridades competentes.

Mediante análise fundamentada nos termos do parágrafo anterior, caso decidido pelo Comitê de Compliance e PLDFT, a i9Advisory, representada pelo Diretor de *Compliance*, deverá comunicar à Unidade de Inteligência Financeira, no prazo determinado pela regulamentação em vigor, todas as situações e operações detectadas ou propostas de operações que possam constituir-se em sérios indícios de lavagem de dinheiro e financiamento ao terrorismo. Tais comunicações deverão conter minimamente a data de início de relacionamento com a i9Advisory, com a pessoa envolvida na operação, a explicação fundamentada dos sinais de alerta identificados, a descrição e o detalhamento das características das operações realizadas, a apresentação das informações obtidas por meio das diligências devidas que qualifiquem os envolvidos, inclusive informando tratar-se ou não, de Pessoas Expostas Politicamente e que detalhem o comportamento da pessoa comunicada e a conclusão da análise, incluindo o relato fundamentado que caracterize os sinais de alerta identificados como uma situação suspeita a ser comunicada à Unidade de Inteligência Financeira, contendo minimamente as informações definidas acima.

## **12. INDICADOR DE EFETIVIDADE**



A efetividade dos processos previstos nesta Política é avaliada por meio de indicador específico que leva em consideração a adesão de cada processo à regulamentação em vigor e o seu cumprimento satisfatório considerando o seu objetivo com base nas exigências da referida regulamentação. Por meio de tais parâmetros, cada processo é analisado individualmente, devendo ser atribuída uma pontuação específica, conforme metodologia desenvolvida pelo Departamento de *Compliance*, sendo 0 (zero), o pior desempenho e 100 (cem), o melhor. A soma de todas as pontuações atribuídas a cada processo dividida pela quantidade de processos resultará no indicador de efetividade considerando os intervalos acima mencionados.

O processo de avaliação deverá ser conduzido pelos colaboradores do Departamento de *Compliance* e registrado por meio de relatório a ser aprovado pelo diretor do departamento acima mencionado.

### **13. CANAL DE DENÚNCIAS**

A i9Advisory dispõe de canal de denúncias para reporte de fraudes, irregularidades, situações com indícios de ilicitude de qualquer natureza, assim como possíveis desvios de conduta relacionados a esta Política e as diretrizes correlatas.

As investigações das denúncias reportadas deverão ser encerradas em até 45 (quarenta e cinco) dias do reporte, devendo ser registradas as conclusões da investigação em relatório específico a ser apreciado pelo Comitê de Compliance e PLDFT. Caberá ao Diretor de Compliance, caso aplicável, após a deliberação do Comitê de Compliance e PLDFT, efetuar a comunicação dos fatos analisados às autoridades competentes nos termos da regulamentação em vigor.



## **14. MANUTENÇÃO, REGISTRO E GUARDA DE INFORMAÇÕES E DOCUMENTOS**

Todas as informações e documentos previstos nesta Política para a efetiva implementação dos procedimentos internos de combate aos crimes de LDFT devem ser registrados e arquivados eletronicamente nos servidores da i9Advisory pelos Colaboradores do Departamento de *Compliance* pelo prazo estabelecido na regulamentação em vigor.

## **15. MONITORAMENTO DO PROGRAMA DE PLDFT E REVISÕES DA POLÍTICA**

A presente Política deverá ser revisada pelo Departamento de *Compliance* no mínimo a cada ano contado da sua publicação. As alterações da presente Política estão sujeitas à aprovação da Alta Administração. O monitoramento do Programa de PLDFT por meio do cumprimento por parte dos colaboradores das diretrizes e procesos previstos nesta Política e/ou nas diretrizes correlatas ficará a cargo do Departamento de *Compliance*.