POLÍTICA DE PREVENÇÃO À LAVAGEM DE DINHEIRO, AO FINANCIAMENTO DO TERRORISMO E AO FINANCIAMENTO DA PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA DA PROBVS CAPITAL

("Probvs Capital")

© Probvs Capital Gestora de Fundos e Investimentos Ltda. – Todos os direitos reservados.

1 INTRODUÇÃO

A Probvs Capital compromete-se a adotar as melhores práticas no combate à lavagem de dinheiro (LD), ao financiamento do terrorismo (FT) e ao financiamento da proliferação de armas de destruição em massa (FADM), em conformidade com as disposições legais e regulamentares nacionais e internacionais aplicáveis. Reconhecendo o impacto potencial desses ilícitos no mercado financeiro e na segurança global, a instituição estabelece a presente Política de Prevenção com o objetivo de proteger a integridade de suas operações, garantindo a observância dos mais elevados padrões de conformidade e ética.

A Política visa assegurar que a Probvs Capital implemente controles adequados, e procedimentos de monitoramento de transações, com vistas a identificar, prevenir e mitigar quaisquer riscos associados à lavagem de dinheiro, ao financiamento do terrorismo e à proliferação de armas de destruição em massa. Ademais, a instituição se compromete a manter mecanismos eficazes de detecção e reporte de atividades suspeitas, colaborando com as autoridades competentes sempre que necessário, em alinhamento com os princípios de prevenção e combate a crimes financeiros.

A presente Política é de observância obrigatória para todos os colaboradores, prestadores de serviços, parceiros comerciais e qualquer pessoa ou entidade que atue em nome da Probvs Capital. Vale ressaltar, que seu cumprimento é essencial para assegurar as obrigações legais, bem como para preservar a confiança e reputação da instituição no mercado.

2 LEIS E NORMAS REGULAMENTARES

A prevenção à lavagem de dinheiro (LD) e ao financiamento do terrorismo (FT) no Brasil é regida por um conjunto robusto de normas legais e regulamentares que buscam garantir a integridade do sistema financeiro e a segurança do país. Dentre as principais, destacam-se as seguintes:

(i) Lei nº 9.613 de 03/03/1998 - Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os respectivos ilícitos, e cria o COAF - Conselho de Controle de Atividades Financeiras;

(ii) Lei nº 13.260 de 16/03/2016 - Regulamenta o disposto no inciso XLIII do art. 5º da Constituição Federal, disciplinando o terrorismo, tratando de disposições investigatórias e processuais e reformulando o conceito de organização terrorista.

(iii) Resolução CVM nº 50 de 31/08/2021 - Dispõe sobre a Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e ao Financiamento da Proliferação de Armas de Destruição em Massa – PLD/FTP no âmbito do mercado de valores mobiliários.

(iv) Circular Bacen nº 3978 de 23/01/2020 - Dispõe sobre a política, os procedimentos e os controles internos a serem adotados pelas instituições autorizadas a funcionar pelo BANCO CENTRAL DO BRASIL visando à prevenção da utilização do sistema financeiro para a prática dos crimes de "lavagem" ou ocultação de bens, direitos e valores, de que trata a Lei nº 9.613, de 3 de março de 1998, e de financiamento do terrorismo, previsto na Lei nº 13.260, de 16 de março de 2016.

(v) Carta-Circular Bacen nº 4.001 de 31/01/2020- Divulga relação de operações e situações que podem configurar indícios de ocorrência dos crimes de "lavagem" ou ocultação de bens, direitos e valores, de que trata a Lei nº 9.613, de 3 de março de 1998, e de financiamento ao terrorismo, previstos na Lei nº 13.260, de 16 de março de 2016, passíveis de comunicação ao Conselho de Controle de Atividades Financeiras (COAF); e

(vi) Normas emitidas pelo COAF – Conselho de Controle de Atividades Financeiras.

2.1 CONCEITOS

A legislação brasileira, por meio da Lei nº 9.613/1998, define os crimes de lavagem de dinheiro ou ocultação de bens, direitos e valores como qualquer ação destinada a ocultar ou dissimular a natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente, de infrações penais. Nesse contexto, a lavagem de dinheiro configura-se como o processo pelo qual valores obtidos em decorrência de atividades ilícitas, tais como tráfico de entorpecentes, corrupção, comércio ilegal de armas, tráfico de pessoas, crimes de estelionato, terrorismo, extorsão, fraudes fiscais, entre outros, são "limpos", ou seja, disfarçados de modo que se apresentem como legítimos, com o objetivo de reintegrá-los ao sistema econômico formal.

As atividades criminosas originadoras desses bens e valores, ao serem dissimuladas, buscam inserir tais valores no sistema financeiro ou em outras áreas da economia legal, por meio de operações comerciais ou financeiras aparentemente legítimas. Ao longo do processo de lavagem, os criminosos empregam uma série de operações financeiras complexas, tais como transferências bancárias, compra e venda de bens de alto valor, utilização de empresas de fachada e outras manobras, com a finalidade de dificultar a rastreabilidade da origem ilícita dos recursos.

Além disso, é relevante destacar que os crimes de lavagem de dinheiro envolvem a utilização de estruturas financeiras e instituições reguladas que, sem os devidos mecanismos de monitoramento e controle, podem ser utilizadas para reintegrar os valores ilícitos à economia, tornando-os indistinguíveis de recursos provenientes de atividades legais.

A seguir, são apresentadas as definições e conceitos jurídicos essenciais relacionados à prevenção à lavagem de dinheiro e ao financiamento do terrorismo, com base nas disposições legais e regulamentares pertinentes, visando a delinear as obrigações das instituições financeiras e demais entidades sujeitas à regulamentação.

2.2 FASES DA LAVAGEM DE DINHEIRO

(i) COLOCAÇÃO (PLACEMENT): é o estágio inicial do processo de lavagem de dinheiro, em que os valores oriundos de atividades ilícitas são inseridos no sistema financeiro ou em outras áreas da economia formal. Nessa etapa, os criminosos buscam introduzir o dinheiro sujo de forma discreta, evitando despertar suspeitas. Para tanto, os criminosos frequentemente utilizam bancos, instituições financeiras, casas de câmbio, empresas de fachada, casas de leilão e negócios de alto valor, como imóveis, automóveis e joias, para realizar transações em montantes que, individualmente, não chamem atenção das autoridades.

(ii) OCULTAÇÃO (LAYERING): visa dificultar ainda mais a rastreabilidade dos fundos ilícitos. Após a introdução dos recursos no sistema financeiro, os criminosos buscam separar e disfarçar a origem dos valores por meio de uma série de transações complexas e sucessivas, com o objetivo de tornar as conexões entre o dinheiro e a infração original mais difíceis de identificar. Nessa fase, os envolvidos podem realizar transferências bancárias entre várias contas, movimentações internacionais de recursos, compra e venda de ativos (como ações, imóveis e outros bens), falsificação de documentos e disfarce da identidade dos beneficiários. O objetivo é criar camadas de transações que tornem o processo de rastreamento mais complexo e que dificultem a identificação da origem ilícita dos recursos. Além disso, a ocultação pode envolver o uso de empresas de fachada, trusts, offshores e outras estruturas jurídicas que dificultam a identificação dos verdadeiros beneficiários finais das operações. Quanto mais complexas e opacas as transações, mais difícil se torna a identificação das atividades ilícitas.

(iii) INTEGRAÇÃO (INTEGRATION): a última etapa da lavagem de dinheiro, em que os recursos obtidos a partir de atividades ilícitas são finalmente reintegrados à economia formal, de modo que possam ser utilizados sem levantar suspeitas. O dinheiro "lavado" já se apresenta como proveniente de fontes legítimas e, por isso, pode ser utilizado livremente em negócios, investimentos ou despesas do dia a dia. Nesta fase, o criminoso pode utilizar os recursos em operações comerciais legítimas, aquisição de imóveis ou investimentos financeiros. Também é comum a utilização de empréstimos ou garantias como forma de reverter os recursos em produtos financeiros ou patrimoniais que possam ser facilmente convertidos em dinheiro ou outros ativos de valor. A principal característica da integração é que o criminoso consegue utilizar o dinheiro disfarçado sem que haja a necessidade de ocultá-lo, uma vez que, ao ser

reintegrado à economia formal, o recurso já é considerado legítimo aos olhos do sistema financeiro.

A prevenção à lavagem de dinheiro exige uma atuação eficiente e contínua em todas as fases desse processo, desde a colocação até a integração dos recursos ilícitos. A Probvs Capital compromete-se a adotar políticas de monitoramento e verificação adequadas, a fim de identificar, impedir e relatar qualquer tentativa de utilização do sistema financeiro para a prática de crimes de lavagem de dinheiro ou financiamento ao terrorismo, em conformidade com as normas e regulamentações legais aplicáveis.

Essas medidas são essenciais para preservar a integridade e a segurança das operações financeiras, bem como para garantir a conformidade com as obrigações legais e regulatórias, protegendo a reputação da empresa e contribuindo para um mercado financeiro mais seguro e ético.

3 CRIMES DE FINANCIAMENTO AO TERRORISMO

O financiamento ao terrorismo é definido como a ação de angariar, fornecer ou reunir fundos ou outros meios financeiros com o intuito de viabilizar a prática de atos terroristas. Esses recursos podem ter origem tanto legal quanto ilegal. No âmbito legal, os fundos podem advir de doações ou de atividades econômicas lícitas de diversas naturezas, tais como negócios e investimentos legítimos. Por outro lado, no contexto ilegal, os recursos podem ter origem em atividades criminosas, incluindo, mas não se limitando a crime organizado, fraudes, contrabando, extorsões, sequestros, entre outras práticas delituosas.

Diferente da lavagem de dinheiro, que se caracteriza pela ocultação da origem ilícita de recursos financeiros, o financiamento ao terrorismo distingue-se pelo fato de que os fundos utilizados nos atos terroristas podem ser provenientes, simultaneamente, tanto de ações ilícitas quanto de ações lícitas. Este aspecto diferencia a natureza do financiamento terrorista, uma vez que a própria finalidade dos recursos — a promoção de atos de terror — é o que caracteriza a sua ilegalidade, independentemente da origem dos fundos.

A Lei nº 13.260, de 16 de março de 2016, estabelece, em seu artigo 2º, a definição jurídica de terrorismo no ordenamento jurídico brasileiro. A referida legislação considera como terrorismo a prática de atos violentos ou ameaçadores cometidos por uma ou mais pessoas, com motivações de xenofobia, discriminação ou preconceito com base em raça, cor, etnia ou religião, e que tenham como objetivo gerar terror social ou generalizado, colocando em risco a vida, o patrimônio, a paz pública ou a incolumidade pública.

São considerados atos de terrorismo aqueles que envolvem ações destinadas a provocar pânico generalizado, ou ainda que ameaçam a segurança nacional, mediante o uso de violência ou ameaça,

com o objetivo de desestabilizar as estruturas sociais, políticas ou governamentais, em conformidade com os princípios da referida legislação.

Esses atos, conforme especificado na legislação, incluem, mas não se limitam a, ações como explosões, sequestros, assaltos armados a instituições públicas ou privadas, e outros comportamentos que atentem contra a ordem pública e a segurança das pessoas. O financiamento de tais atividades configura-se como uma violação grave dos princípios da ordem pública, da segurança nacional e dos direitos humanos, sendo objeto de rigorosa vigilância e repressão pelas autoridades competentes.

São atos terroristas:

(i) Utilizar ou ameaçar utilizar, transportar, armazenar, portar ou carregar consigo explosivos, gases tóxicos, venenos, agentes biológicos, agentes químicos, materiais nucleares ou quaisquer outros meios que possuam capacidade para causar danos ou provocar destruição em massa.

(ii) Sabotar o funcionamento ou, mediante violência, grave ameaça à pessoa ou utilizando-se de meios cibernéticos, apoderar-se, de forma total ou parcial (ainda que de modo temporário), do controle de meios de comunicação ou de transportes; de portos, aeroportos, estações ferroviárias ou rodoviárias; de hospitais, casas de saúde, escolas, estádios esportivos, instalações públicas ou locais onde se prestem serviços públicos essenciais; de instalações de geração ou transmissão de energia; de instalações militares; de instalações de exploração, refino ou processamento de petróleo e gás; ou de instituições bancárias e suas respectivas redes de atendimento.

(iii) Atentar contra a vida ou a integridade física de qualquer pessoa.

(iv) Promover, constituir, integrar ou fornecer assistência, pessoalmente ou por meio de interposta pessoa, a organizações terroristas.

(v) Realizar atos preparatórios com a intenção manifesta de perpetrar um ato de terrorismo, com o objetivo de consumar o referido delito.

(vi) Incorrer nas mesmas penalidades o agente que, com a finalidade específica de praticar atos terroristas, recrutar, organizar, transportar ou municiar indivíduos com destino a um país diferente daquele de sua residência ou nacionalidade.

(vii) Fornecer ou receber treinamento em um país distinto daquele de sua residência ou nacionalidade, com a intenção de realizar atividades terroristas.

4 CADASTRO

O processo de cadastro de clientes é conduzido pela Diretoria de Risco e Compliance, que analisa a documentação cadastral e verifica sua conformidade com as normas aplicáveis, assegurando a regularidade e atualização das informações.

(i) CADASTRO PESSOA FÍSICA: O cliente pessoa física deverá encaminhar as informações e documentos necessários para sua identificação, incluindo comprovante de identidade, endereço e informações financeiras relevantes. Posteriormente, a Diretoria de Risco e Compliance realizará a análise de todas as informações prestadas, bem como a regularidade dos documentos encaminhados. Após a aprovação, será iniciada a segunda etapa de pesquisa reputacional do cliente, que é realizada em fontes públicas e listas restritivas, incluindo Pessoas Politicamente Expostas (PEP), sanções nacionais e internacionais e mídias adversas. Os resultados obtidos por meio da pesquisa reputacional são utilizados pelo departamento de Compliance para execução do processo de Conheça seu Cliente "Know Your Client (KYC)". Todos os cadastros e revisões de clientes, independentemente da classificação de risco, são submetidos à aprovação conjunta da Diretoria de Gestão e da Diretoria de Compliance e Risco, refletindo o modelo de atuação personalizada e o compromisso da Probvs Capital com o acompanhamento direto de cada relacionamento.

(ii) CADASTRO PESSOA JURÍDICA: O cliente pessoa jurídica ou seu representante, deverá encaminhar as informações e documentos necessários para sua identificação e qualificação, incluindo contrato social, comprovantes de inscrição e documentos dos administradores e representantes. Posteriormente, a Diretoria de Risco e Compliance realizará a análise de todas as informações prestadas, bem como a regularidade dos documentos encaminhados. Após a análise, será iniciada a segunda etapa de pesquisa reputacional da pessoa jurídica, que é realizada em fontes públicas e listas restritivas, em conformidade com os mesmos critérios aplicados às pessoas físicas. Cabe destacar que antes do efetivo cadastramento do cliente, toda a documentação apresentada é avaliada pela área de Compliance. As informações cadastrais relativas ao cliente pessoa jurídica abrangerão as pessoas naturais autorizadas a representá-la, bem como a cadeia de participação societária, até alcançar a pessoa natural caracterizada como beneficiário final.

Após a análise e verificação da documentação e das informações do cliente, a Diretoria de Compliance e Risco elabora o registro cadastral e submete o processo à aprovação conjunta da Diretoria de Gestão e da Diretoria de Compliance e Risco.

Essa dupla aprovação reflete o modelo de atuação personalizada da Probvs Capital, em que cada relação com o cliente é avaliada diretamente pelos diretores responsáveis.

Toda a documentação e os registros de análise são arquivados em ambiente corporativo de nuvem segura, de modo organizado e rastreável, garantindo integridade e disponibilidade para eventual consulta pelas autoridades competentes.

(iii) INVESTIDOR NÃO-RESIDENTE ("INR"): O investidor e/ou seu representante domiciliado no Brasil, deverá encaminhar:

a. as informações e documentos necessários à sua identificação e qualificação, incluindo comprovantes de identidade, domicílio e representação legal.

b. A Diretoria de Risco e Compliance analisa a documentação, verifica a regularidade das informações e realiza pesquisa reputacional do investidor e de seu representante, consultando fontes públicas e listas restritivas (PEP, sanções nacionais e internacionais, e mídias adversas).

c. As informações cadastrais devem abranger as pessoas naturais e jurídicas autorizadas a representar o investidor, bem como a cadeia societária até o beneficiário final, conforme a regulamentação aplicável.

d. Concluída a análise, o cadastro é submetido à aprovação conjunta da Diretoria de Gestão e da Diretoria de Compliance e Risco, em linha com o modelo de relacionamento direto e personalizado da Probvs Capital.

e. Toda a documentação e os registros da análise são arquivados em ambiente corporativo de nuvem segura, de forma organizada e rastreável, garantindo a integridade e a disponibilidade das informações.

(iv) ATUALIAÇÃO CADASTRAL E RECADASTRAMENTO: Os procedimentos para atualização cadastral e recadastramento dos clientes, deverão seguir os mesmos procedimentos iniciais descritos nos itens acima.

5 PESSOAS POLITICAMENTE EXPOSTAS (PEP)

Em conformidade com a Resolução CVM nº 50, de 31 de agosto de 2021, e a Circular Bacen nº 3.978, de 23 de janeiro de 2020, as Pessoas Politicamente Expostas (PEPs) são definidas como aquelas que, por sua posição ou função, exercem ou exerceram, no âmbito nacional ou estrangeiro, funções públicas de relevância, bem como seus familiares e pessoas de seu círculo próximo.

Consideram-se PEPs, para efeitos de prevenção à lavagem de dinheiro e ao financiamento do terrorismo:

(i) Pessoas ocupantes de cargos públicos relevantes:

a) Chefe de Estado ou de Governo, ministros de Estado e secretários de alto escalão;

b) Membros do legislativo, judiciário ou órgãos equivalentes em outros países, incluindo parlamentares, juízes, membros de tribunais superiores, procuradores-gerais e promotores de justiça;

c) Dirigentes de instituições militares de alta patente, como generais ou outros cargos de comando de forças armadas e segurança pública;

d) Diretores e membros da administração de empresas estatais ou entidades públicas relevantes.

(ii) Familiares próximos:

a) Cônjuges, companheiros(as) ou parentes de até segundo grau (pais, filhos, avós, irmãos, sogros, cunhados, etc.) das pessoas ocupantes de cargos públicos relevantes, conforme descrito no item (i) acima

(iii) Pessoas que mantêm relações estreitas:

a) Pessoas que tenham ou tenham tido uma relação de proximidade com indivíduos que ocupam ou ocuparam funções públicas relevantes, como assessores diretos, consultores e outros membros de círculos íntimos ou pessoais

A condição de pessoa exposta politicamente deve ser aplicada pelos cinco anos seguintes à data em que a pessoa deixou de se enquadrar nas categorias descritas acima.

6 BENEFICIÁRIOS FINAIS

De acordo com a Resolução CVM nº 50/2021, para os fins de aplicação das normas de prevenção à lavagem de dinheiro e ao financiamento do terrorismo, considera-se beneficiário final a pessoa natural ou o conjunto de pessoas naturais que, direta ou indiretamente, possuam, controlem ou exerçam influência significativa sobre a entidade Pessoa Jurídica, conduzindo suas operações ou sendo as principais beneficiárias de suas atividades. Em outras palavras, o beneficiário final é a pessoa ou grupo

de pessoas que, em última instância, controla ou se beneficia economicamente da entidade, independentemente de sua posição formal dentro da estrutura corporativa.

Além disso, são igualmente considerados beneficiários finais as pessoas jurídicas que atuam como prepostos, procuradores ou representantes legais da pessoa ou grupo de pessoas que efetivamente controlam ou se beneficiam da entidade.

No entanto, conforme as normas vigentes, existem exceções específicas para a obrigação de identificar a pessoa natural como beneficiário final, previstas nas situações e tipos de empresas a seguir, conforme os critérios aplicáveis.

São considerados exceções referentes à obrigação de identificação da pessoa natural caracterizada como beneficiário final, conforme normas aplicáveis, as empresas e situações abaixo:

(i) pessoa jurídica constituída como companhia aberta no Brasil;

(ii) fundos e clubes de investimento nacionais registrados, desde que:

a) não seja fundo exclusivo;

b) obtenham recursos de investidores com o propósito de atribuir o desenvolvimento e a gestão de uma carteira de investimento a um gestor qualificado que deve ter plena discricionariedade na representação e na tomada de decisão junto às entidades investidas, não sendo obrigado a consultar os cotistas para essas decisões e tampouco indicar os cotistas ou partes a eles ligadas para atuar nas entidades investidas; e

c) seja informado o número do CPF/MF ou de inscrição no Cadastro Nacional de Pessoa Jurídica – CNPJ de todos os cotistas para a Receita Federal do Brasil na forma definida em regulamentação específica daquele órgão;

(iii) instituições financeiras e demais entidades autorizadas a funcionar pelo BACEN;

(iv) seguradoras, entidades abertas e fechadas de previdência complementar e de regimes próprios de previdência social;

(v) os investidores não residentes classificados como:

a) bancos centrais, governos ou entidades governamentais, assim como fundos soberanos ou companhias de investimento controladas por fundos soberanos e similares;

b) organismos multilaterais;

c) companhias abertas ou equivalentes;

d) instituições financeiras ou similares, agindo por conta própria;

e) administradores de carteiras, agindo por conta própria;

f) seguradoras e entidades de previdência; e

g) fundos ou veículos de investimento coletivo, desde que, cumulativamente: (I) o número de cotistas seja igual ou superior a 100 (cem) e nenhum deles tenha influência significativa; e (II) a administração da carteira de ativos seja feita de forma discricionária por administrador profissional sujeito à regulação de órgão regulador que tenha celebrado com a CVM acordo de cooperação mútua.

7 RESPONSABILIDADE E ATRIBUIÇÕES

Todos os colaboradores, no âmbito de suas respectivas funções e responsabilidades, devem atuar em conformidade com as diretrizes do Programa de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (PLD/FTP), sendo igualmente sujeitos às sanções previstas nas políticas internas, bem como às disposições da legislação vigente aplicável à matéria.

Para efeitos da presente Política são considerados colaboradores todos os profissionais que atuam em nome da Probvs Capital, incluindo seus diretores, sócios e prestadores de serviço relevantes. Todos os colaboradores devem observar as diretrizes da presente Política, com especial atenção à identificação e acompanhamento dos clientes e das operações sob gestão, em conformidade com os princípios de "Conheça seu Cliente – Know Your Client (KYC)" e, ainda comunicar a área de Compliance sobre operações suspeitas, bem como responder de forma tempestiva e objetiva as solicitações da área de Compliance.

8 CONHEÇA SEU CLIENTE (KNOW YOUR CLIENT – KYC)

A Política de Conheça Seu Cliente (KYC- Know Your Customer) tem como objetivo estabelecer um conjunto de medidas e procedimentos para garantir que a empresa conheça adequadamente seus clientes, de forma a prevenir e combater crimes financeiros como lavagem de dinheiro, financiamento do terrorismo e fraudes. Através do KYC, a empresa assegura que todas as transações sejam realizadas de forma transparente e em conformidade com as normas legais e regulatórias aplicáveis.

O processo de "Conheça seu Cliente" inicia-se na recepção das informações do cliente e/ou da operação através dos procedimentos descritos no capítulo 4 acima – Cadastro, seja por meio digital ou físico.

O processo de atualização cadastral deverá ocorrer conforme o tipo de cliente, sendo eles: Pessoa Jurídica Institucional, Pessoa Jurídica Não Financeira e Pessoa Física.

(i) PESSOA JURÍDICA INSTITUCIONAL: Processo de atualização cadastral deverá ocorrer conforme a classificação de risco atribuído ao cliente, clientes classificados com nível de risco "Alto", deverão atualizar o cadastro em um prazo não superior a 24 (vinte e quatro) meses. Clientes com nível de risco "Médio", deverão atualizar o cadastro em um prazo não superior a 36 (trinta e seis) meses e clientes com nível de risco "Baixo", deverão atualizar o cadastro em um prazo não superior a 60 meses.

(ii) PESSOA JURÍDICA NÃO FINANCEIRA: Independente da classificação de risco atribuída, o processo de atualização cadastral deverá ocorrer em um prazo que não seja superior a 24 (vinte e quatro) meses.

(iii) PESSOA FÍSICA: Independente da classificação de risco atribuída, o processo de atualização cadastral deverá ocorrer em um prazo que não seja superior a 24 (vinte e quatro) meses.

Salienta-se, que neste procedimento de atualização, os documentos atualizados serão analisados, será feito nova pesquisa reputacional, bem como dependerão de nova aprovação.

São princípios fundamentais do KYC:

(i) Identificação do Cliente: A empresa realizará a identificação de todos os clientes, sejam pessoas físicas ou jurídicas, coletando dados como nome, endereço, data de nascimento (no caso de pessoas físicas), CPF/CNPJ, documentos oficiais de identificação, e outras informações relevantes para confirmar sua identidade. No caso de clientes pessoas jurídicas, também serão coletadas informações sobre a estrutura societária, documentos de registro e identificação dos sócios e administradores.

(ii) Verificação de Identidade: A verificação da identidade do cliente será realizada por meio da análise de documentos oficiais (como RG, CPF, passaporte, ou certidão de constituição de empresa, dependendo da natureza do cliente). A empresa utilizará tecnologia e métodos adequados para garantir a autenticidade desses documentos e evitar fraudes.

(iii) **Análise de Risco:** No âmbito do processo de Conheça Seu Cliente (KYC), a **Probvs Capital** realizará a análise de risco dos clientes com base em critérios objetivos e proporcionais à natureza das operações, conforme previsto nos art. 17 e 18 da Resolução CVM nº 50/2021. A **Probvs Capital** realizará uma avaliação de risco baseada no perfil do cliente, levando em consideração fatores tais como a verificação da identidade do cliente e, quando aplicável, de seus beneficiários finais; a compreensão da natureza e finalidade da relação comercial; monitoramento contínuo das operações realizadas; origem dos recursos; o tipo de transação; aplicação de diligência simplificada, normal ou reforçada, conforme o grau de risco identificado; e o histórico de transações.

Os clientes serão classificados em três categorias de risco: **alto, médio e baixo**, com base em critérios tais como: (i) Alto; (ii) Médio; e (iii) Baixo, com base em critérios como:

(i) País de origem ou residência;
(ii) Setor econômico de atuação;
(iii) Tipo empresarial;
(iv) Volume e frequência das operações;
(v) Presença em listas de sanções nacionais ou internacionais; e
(vi) Utilização de estruturas complexas de propriedade ou controle.

A classificação dos clientes é realizada com base nos seguintes critérios, em consonância com o art. 4º, inciso II da Resolução CVM nº 50/2021:

Serão considerados de Baixo risco:

(i) Clientes com renda e patrimônio compatíveis com os produtos contratados;

(ii) Operações padronizadas, de baixo valor ou baixa frequência;

(iii) Perfil de investidor com objetivos conservadores e histórico financeiro estável;

(iv) Pessoas físicas ou jurídicas domiciliadas em jurisdições com efetiva supervisão e cooperação internacional no âmbito de PLDFT.

Serão considerados de Médio risco:

(i) Clientes com estrutura societária mais complexa ou beneficiário final não evidente;

(ii) Operações com valores mais expressivos ou com frequência elevada;

(iii) Envolvimento em setores econômicos mais vulneráveis a riscos de PLDFT;

(iv) Residentes ou domiciliados em jurisdições consideradas de risco elevado ou com histórico de fragilidades regulatórias.

Os clientes com características divergentes ao disposto acima, serão considerados de alto risco, como por exemplo: pessoas politicamente expostas (PEPs) ou residentes de países com alta incidência de crimes financeiros, terão sua transação e relação comercial monitoradas com mais rigor. As medidas de diligência aplicadas a cada cliente serão proporcionais à sua classificação de risco.

(iv) Monitoramento Contínuo: A empresa implementará processos contínuos de monitoramento das contas e das transações de seus clientes, com o objetivo de identificar atividades suspeitas ou irregulares. Qualquer transação que se desvie do padrão ou que apresente risco de envolvimento em atividades ilícitas será investigada e, se necessário, reportada às autoridades competentes.

(v) Atualização de Dados: A empresa estabelecerá um processo de atualização periódica das informações dos clientes, garantindo que os dados coletados permaneçam precisos e atuais. Alterações significativas no perfil de um cliente, como mudanças no endereço, atividade profissional ou estrutura societária, deverão ser comunicadas e verificadas pela empresa.

(vi) Conformidade Legal e Regulamentar: A empresa seguirá todas as leis e regulamentações locais e internacionais relacionadas ao KYC, incluindo a Lei de Lavagem de Dinheiro, a Lei Antiterrorismo e as diretrizes emitidas pelos órgãos reguladores financeiros. Além disso, qualquer cliente que se recuse a fornecer as informações solicitadas ou que se mostre relutante em seguir as exigências do KYC poderá ter sua conta suspensa ou encerrada.

(vii) Treinamento e Conscientização: Todos os colaboradores da empresa envolvidos no processo de KYC serão treinados regularmente para reconhecer sinais de atividades suspeitas e garantir o cumprimento das políticas internas. A empresa também incentivará uma cultura de conformidade e transparência em todas as áreas, promovendo a conscientização sobre a importância da política de KYC.

(viii) Privacidade e Proteção de Dados: A empresa se compromete a proteger a privacidade e a confidencialidade dos dados pessoais dos clientes. Todos os dados coletados serão tratados de acordo com as leis de proteção de dados vigentes (como a Lei Geral de Proteção de Dados - LGPD, no Brasil), garantindo que a informação seja utilizada apenas para fins de conformidade e prevenção de riscos financeiros.

9 CONHEÇA SEU COLABORADOR (KNOW YOUR EMPLOYEE – KYE)

A política de *Conheça Seu Colaborador* (KYE- Know Your Employee) visa implementar práticas rigorosas para conhecer adequadamente todos os colaboradores da empresa, garantindo a segurança e integridade dos processos internos e a conformidade com as regulamentações do mercado financeiro. Através dessa política, a empresa busca mitigar riscos internos, como fraudes, conflitos de interesse, vazamento de informações sensíveis e outras práticas ilícitas que possam afetar a reputação e a operação da organização.

São princípios fundamentais do KYE:

(i) Seleção Rigorosa de Colaboradores: A empresa adota um processo seletivo criterioso para contratação de colaboradores, com ênfase na verificação de antecedentes profissionais e comportamentais. Isso inclui a análise de históricos de emprego, referências profissionais, e a realização de verificações de antecedentes criminais e financeiros, quando aplicável. O objetivo é garantir que os candidatos contratados possuam a qualificação necessária e um histórico compatível com os valores e exigências do mercado financeiro.

(ii) Verificação de Conflitos de Interesse: A empresa implementará um processo contínuo de monitoramento e avaliação para identificar potenciais conflitos de interesse entre colaboradores e a organização. Isso inclui a análise de relações comerciais, interesses pessoais ou familiares que possam afetar a imparcialidade do colaborador no desempenho de suas funções. Qualquer situação de conflito de interesse será tratada com transparência e, quando necessário, serão adotadas medidas corretivas.

(iii) Avaliação de Perfil e Risco: Antes do início da relação contratual, é realizada uma verificação reputacional dos profissionais e prestadores relevantes, incluindo pesquisa pública de antecedentes e integridade. Essa verificação poderá ser atualizada sempre que houver indício de risco ou mudança relevante na relação contratual.

(iv) Treinamento e Conscientização: Os diretores e prestadores de serviço relevantes participam, ao menos uma vez por ano, de treinamento e orientação sobre ética, Compliance e conformidade com a legislação vigente, incluindo prevenção à lavagem de dinheiro, combate ao financiamento do terrorismo, e proteção de dados. A conscientização sobre a importância de manter altos padrões éticos e legais é essencial para a cultura organizacional da empresa.

(v) Monitoramento e Controles Internos: As atividades internas são periodicamente revisadas pela Diretoria de Risco e Compliance, de forma a assegurar que os registros, acessos e decisões estejam em conformidade com as normas e políticas internas.

(vi) **Gestão de Acessos e Privacidade:** A empresa estabelecerá uma política de gestão de acessos rigorosa, garantindo que os colaboradores tenham acesso apenas às informações e sistemas necessários para o desempenho de suas funções. A gestão de acessos será revista regularmente para assegurar que as permissões de acesso sejam apropriadas, limitando o risco de vazamento de dados ou uso indevido de informações confidenciais.

(vii) **Processo de Desligamento e Encerramento de Acessos:** Quando um colaborador deixar a empresa, seja por demissão voluntária ou por iniciativa da organização, a empresa tomará medidas imediatas para garantir que todos os acessos e privilégios sejam revogados de forma eficaz e segura. Isso inclui a devolução de equipamentos, a revogação de senhas e credenciais, e a destruição de informações confidenciais que possam ter sido acessadas durante o período de trabalho.

(viii) **Acompanhamento de Performance e Conduta:** A conduta dos diretores e prestadores de serviço é acompanhada de forma contínua pela Diretoria de Risco e Compliance, que avalia eventuais ocorrências, comportamentos inadequados ou indícios de descumprimento das políticas internas, adotando as medidas corretivas cabíveis.

(ix) **Confidencialidade e Proteção de Dados:** Os colaboradores da **Probvs Capital** estarão sujeitos a políticas rigorosas de confidencialidade, especialmente no que diz respeito ao manuseio de informações sensíveis, tanto de clientes quanto da própria organização. A empresa promoverá a proteção de dados e o sigilo absoluto sobre informações confidenciais, de acordo com as normas de proteção de dados pessoais e a legislação aplicável.

(x) **Transparência e Canal de Denúncias:** A **Probvs Capital** mantém canal confidencial para comunicação de eventuais irregularidades, disponível por meio do endereço eletrônico: denuncias@probvscapital.com.br. O canal é administrado exclusivamente pela Diretoria de Risco e Compliance, que assegura o sigilo das informações e a ausência de qualquer forma de retaliação.

1. CONHEÇA SEU COLABORADOR (KNOW YOUR PARTNER – KYP)

A Política de Conheça Seu Parceiro (KYP- Know Your Partner) tem como objetivo assegurar que todos os parceiros comerciais, fornecedores, intermediários e outras entidades com as quais a empresa mantém relações comerciais, sejam devidamente avaliados e monitorados de forma compatível com o porte da instituição, garantindo integridade, conformidade e alinhamento ético. O KYP busca minimizar riscos de envolvimento com práticas ilícitas, como lavagem de dinheiro, financiamento do terrorismo e fraudes financeiras, além de proteger a integridade da empresa e seus clientes.

São princípios fundamentais do KYP:

(i) Diligência Prévia: Antes da contratação de qualquer prestador ou parceiro relevante, a Probvs Capital realiza verificação de integridade e reputação, incluindo pesquisa pública sobre antecedentes, regularidade cadastral e histórico profissional.

(ii) Verificação de Integridade e Conformidade: São priorizados parceiros que adotem boas práticas de governança, ética e conformidade, especialmente em temas relacionados à prevenção à lavagem de dinheiro, financiamento do terrorismo e proteção de dados.

(iii) Análise de Risco e Perfil do Parceiro: A empresa realizará uma avaliação de risco detalhada de cada parceiro, considerando o país de origem, a natureza dos negócios, o segmento de atuação e os possíveis vínculos com práticas ilegais ou suspeitas. Parceiros de alto risco, como aqueles localizados em jurisdições com alta incidência de corrupção ou que operam em setores vulneráveis, terão um acompanhamento mais rigoroso e frequente.

(iv) Monitoramento Contínuo da Relação: A Diretoria de Compliance e Risco revisa anualmente a lista de prestadores e parceiros relevantes, verificando sua regularidade e eventual ocorrência de fatos reputacionais adversos.

(v) Política de Transparência e Integridade: A empresa estabelecerá critérios claros de transparência e integridade para a escolha de seus parceiros. Quaisquer sinais de práticas antiéticas ou ilegais, como subornos, fraudes ou manipulação de informações, resultam na revisão e possível rescisão do contrato com o parceiro. A empresa também se compromete a exigir que todos os seus parceiros comerciais implementem políticas similares em relação à ética e conformidade regulatória.

(vi) Exigências contratuais e de compliance: Todos os contratos firmados com parceiros comerciais incluirão cláusulas específicas de compliance e responsabilidades relacionadas à conformidade com as leis de prevenção à lavagem de dinheiro, financiamento do terrorismo e outras regulamentações financeiras. Os parceiros devem se comprometer a adotar práticas de conformidade e fornecer à empresa acesso a documentos e registros quando solicitado para auditorias e verificações.

(vii) Avaliação Periódica da Relação Comercial: A empresa realizará revisões anuais das relações comerciais com seus parceiros, considerando fatores como desempenho, conformidade contínua e a manutenção de boas práticas de governança. Essas avaliações garantirão que a

relação com os parceiros seja sempre vantajosa e esteja alinhada com os padrões da empresa em termos de risco, compliance e ética.

(viii) **Rescisão de Contrato em Caso de Inconformidade:** Caso um parceiro descumpra qualquer aspecto relevante da política de KYP ou ainda, seja identificado com envolvimento em práticas ilícitas, a empresa tomará as medidas necessárias para a rescisão imediata do contrato, além de adotar ações legais cabíveis. A empresa pode, ainda, reportar a situação às autoridades competentes, dependendo da gravidade da infração.

10 MONITORAMENTO E ANÁLISE DE OPERAÇÕES

Todas as transações e operações financeiras, incluindo, mas não se limitando, às propostas apresentadas, realizadas por clientes, colaboradores ou terceiros, deverão ser submetidas a monitoramento contínuo, com o intuito de identificar e apurar eventuais indícios de práticas que possam configurar crimes de lavagem de dinheiro ou financiamento ao terrorismo.

O monitoramento é conduzido pela Diretoria de Risco e Compliance, de forma compatível com o porte e a natureza das atividades da gestora, utilizando planilhas e registros internos, bem como informações fornecidas pelos administradores fiduciários e custodiante, que executam os controles operacionais de PLD/FT.

Os procedimentos de monitoramento abrangem as propostas e operações de todos os clientes vinculados a instituição, bem como quaisquer atipicidades que possam sugerir a ocorrência de lavagem de dinheiro (LD) ou financiamento do terrorismo (FT). O monitoramento é conduzido pela área de Compliance utilizando registros e controles internos, além de consultas periódicas a lista de sanções internacionais e nacionais, com base no CPF ou CNPJ dos clientes. As regras para a detecção de operações suspeitas estão segmentadas conforme o nível de risco atribuído ao cliente, sendo classificados como baixo, médio ou alto.

Todas as análises realizadas são devidamente registradas em planilhas ou controles internos específicos. Caso a análise de uma operação revele alguma atipicidade que demande esclarecimentos adicionais, a Diretoria de Risco e Compliance poderá solicitar informações complementares aos responsáveis pela relação com o cliente, para que forneçam justificativas relativas à irregularidade identificada, no que diz respeito ao cliente em questão. A análise será conduzida com base no tipo de produto operado e no perfil de risco do cliente, a fim de determinar as medidas cabíveis à situação identificada.

Nos casos de clientes para os quais não seja possível identificar o beneficiário final, incluindo aqueles constituídos sob a forma de Organizações Não Governamentais (ONGs) e clientes classificados como

Pessoas Politicamente Expostas (PEP), as operações, bem como as mídias e listas restritivas, serão submetidas a uma análise minuciosa para detectar possíveis atipicidades relacionadas à prevenção à lavagem de dinheiro (PLD) e ao financiamento do terrorismo (FTP). Caso sejam identificadas transações ou comportamentos suspeitos, esses clientes serão imediatamente comunicados ao Conselho de Controle de Atividades Financeiras (COAF) e poderão ter suas contas bloqueadas para a realização de novas operações.

Todos os colaboradores, independentemente de seu nível hierárquico, bem como prestadores de serviços, têm a obrigação de comunicar imediatamente ao departamento de Compliance e/ou ao canal de denúncias qualquer proposta de operação (solicitação ou ordem) ou situação identificada durante a prospecção, negociação ou no curso do relacionamento comercial, que apresente indícios ou evidências de atos ilícitos relacionados à lavagem de dinheiro (LD) ou ao financiamento do terrorismo (FTP). Essa comunicação deve ocorrer de forma tempestiva, garantindo a adoção das medidas corretivas e de investigação adequadas, em conformidade com as normas internas e regulatórias aplicáveis. Quando verificados indícios de irregularidades relevantes, a Probvs comunicará o fato ao Conselho de Controle de Atividades Financeiras (COAF), observando os procedimentos previstos na Resolução CVM nº 50/2021.

Todos os diretores, colaboradores e prestadores de serviço têm o dever de comunicar, de forma imediata e confidencial, à Diretoria de Compliance e Risco, qualquer proposta, operação ou fato que possa configurar indício de lavagem de dinheiro, financiamento do terrorismo ou outras práticas ilícitas. Essa comunicação pode ser feita também pelo canal de denúncias institucional (denuncias@probvscapital.com.br), garantindo o sigilo e a ausência de retaliação.

11 COMUNIÇÃO AO COAF

Sempre que forem identificadas situações atípicas, caberá à área de Compliance realizar a análise das evidências coletadas e submeter o caso à Diretoria, para deliberar sobre a necessidade de comunicação aos órgãos competentes. Após a conclusão da análise preliminar, caso sejam identificados indícios suficientes que sugiram a prática de crimes relacionados à lavagem de dinheiro ou ao financiamento do terrorismo, a área de Compliance em estrita conformidade com a legislação vigente, procederá à comunicação ao órgão regulador pertinente até o dia útil subsequente à operação ou fato analisado, sendo ainda responsável pelo arquivamento de toda a documentação relativa aos casos investigados e reportados.

A partir da identificação de qualquer operação ou situação suspeita, os procedimentos de análise não poderão ultrapassar o prazo de quarenta e cinco dias corridos, contados a partir da data de seleção da operação ou ocorrência. A comunicação ao Conselho de Controle de Atividades Financeiras (COAF), quando pertinente, deverá ser realizada até o dia útil seguinte à decisão do compliance.

ATENÇÃO: É VEDADO DAR CIÊNCIA AOS ENVOLVIDOS OU A TERCEIROS QUANTO A SUA COMUNICAÇÃO AO COAF.

DEVERÁ HAVER CONFIDENCIALIDADE EM TODAS AS COMUNICAÇÕES, CONFORME DETERMINA A LEI 9.613/98, PORTANTO, EM NENHUMA HIPÓTESE DEVERÁ SER REVELADA, AOS CLIENTES OU A TERCEIROS, A TRANSMISSÃO DE INFORMAÇÕES AO REGULADOR OU O EXAME PELA INSTITUIÇÃO DE ALGUMA OPERAÇÃO CONSIDERADA INCOMUM.

AS DECISÕES E PROCESSOS DE COMUNICAÇÃO DEVERAM SER GUARDADOS PELO PERÍODO REGULATÓRIO DE 10 (DEZ) ANOS, CONTADOS A PARTIR DO PRIMEIRO DIA DO ANO SEGUINTE AO DO ENCERRAMENTO DO RELACIONAMENTO OU DA CONCLUSÃO DAS OPERAÇÕES.

12 CONSIDERAÇÕES FINAIS

A presente política deverá ser atualizada pela área de Compliance uma vez ao ano ou sempre que houver necessidade de atualização, por demanda interna pela instituição ou devido a alterações na legislação e normativos vigentes. No processo de atualização serão reavaliados os critérios relacionados à classificação de risco de clientes, produtos, serviços e situações de mercado.

O controle e revisão desta política deverá ser realizada por colaboradores da área de Compliance da instituição e validada pelo diretor de Compliance.

A área de Compliance é responsável por realizar treinamento para todos os colaboradores da instituição, em sua admissão, com atualização anual, ou sempre que ocorrer alteração da legislação vigente.

Demais treinamentos que se verifiquem necessários a fim de desenvolver conhecimentos específicos poderão ser realizados. Em relação ao treinamento sobre PLD/FTP, as orientações aplicadas têm por objetivo reforçar a importância do combate ao crime de lavagem de dinheiro e financiamento do terrorismo e na detecção de operações que caracterizem indícios deste crime.

Manual vigente a partir de novembro de 2025.