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

1. INTRODUÇÃO

A presente Política tem como objetivo estabelecer as diretrizes adotadas pela BANVOX Distribuidora de Títulos e Valores Mobiliários LTDA “BANVOX”, “BANVOX DTVM”) na Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e ao Financiamento da Proliferação de Armas de Destruição em Massa (“PLD/FTP”), assim como definir os procedimentos a serem adotados desde a análise do cliente até a comunicação de uma operação atípica/suspeita aos órgãos reguladores competentes, em consonância com a legislação vigente.

As regras aqui descritas aplicam-se a todos os colaboradores (estagiários, menores aprendizes, funcionários, diretores e sócios), terceiros e prestadores de serviços, devendo sempre adotar as melhores práticas em suas atividades, e principalmente no cadastro de clientes, dedicando especial atenção aos conceitos e atividades que auxiliam na Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e ao Financiamento da Proliferação de Armas de Destruição em Massa.

2. ASPECTOS LEGAIS E REGULATÓRIOS

Vale ressaltar as principais normas legais e reguladoras do mercado financeiro no que tange a prevenção e combate à lavagem de dinheiro e financiamento ao terrorismo:

- 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;
- 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;
- 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;
- 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;

- 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);
- Normas emitidas pelo COAF – Conselho de Controle de Atividades Financeiras.

3. CONCEITOS

A legislação brasileira define como Crimes de Lavagem ou Ocultação de Bens, Direitos e Valores, ocultar ou dissimular a natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente, de infração penal.

Os responsáveis por esta operação fazem com que os valores obtidos por meio das atividades ilícitas e criminosas (como o tráfico de drogas, corrupção, comércio ilegal de armas, prostituição, crimes de estelionato, terrorismo, extorsão, fraude fiscal, entre outros) sejam dissimulados ou escondidos, retornando à economia como operações comerciais legais e que possam ser absorvidas pelo sistema financeiro, naturalmente.

Segue a definição dos principais conceitos pertinentes a prevenção a lavagem de dinheiro e financiamento do terrorismo.

3.1. Fases da Lavagem de Dinheiro

O processo mais comum utilizado no crime de Lavagem de Dinheiro e Ocultação de Bens e Valores é composto de três fases:

(i) Colocação: ingresso no sistema financeiro de recursos provenientes de atividade ilícitas, por meio de depósitos, compra de instrumentos financeiros ou compra de bens. Nesta fase, é comum a utilização de instituições financeiras para a introdução de recursos obtidos ilicitamente;
(ii) Ocultação: execução de múltiplas operações financeiras com os recursos já ingressados no sistema financeiro, visando a ocultação dos recursos ilegais, por meio de transações complexas e em grande número para dificultar o rastreamento, monitoramento e identificação da fonte ilegal do dinheiro;

(iii) Integração: incorporação formal do dinheiro no sistema econômico, por meio de investimento no mercado de capitais, imobiliário, obras de arte, entre outros. Nessa fase o recurso retorna à economia como recurso lícito.

3.2. Crimes de Financiamento ao Terrorismo

O Financiamento ao Terrorismo pode ser definido como a reunião de fundos ou de capital para a realização de atividades terroristas. Esses fundos podem ter origem legal, como: doações, ganho de atividades econômicas lícitas diversas; ou ilegal, como: as procedentes de atividades criminais (crime organizado, fraudes, contrabando, extorsões, sequestros etc.). Diferente do crime de lavagem de dinheiro, os recursos utilizados nos atos criminosos de terrorismo também podem ser provenientes de atos lícitos, não só de atos ilícitos.

A Lei nº 13.260 de 16/03/2016, define como terrorismo a prática por um ou mais indivíduos dos atos abaixo descritos, por razões de xenofobia, discriminação ou preconceito de raça, cor, etnia e religião, quando cometidos com a finalidade de provocar terror social ou generalizado, expondo a perigo pessoa, patrimônio, a paz pública ou a incolumidade pública.

São considerados atos de terrorismo:

- Usar ou ameaçar usar, transportar, guardar, portar ou trazer consigo explosivos, gases tóxicos, venenos, conteúdos biológicos, químicos, nucleares ou outros meios capazes de causar danos ou promover destruição em massa;
- Sabotar o funcionamento ou apoderar-se, com violência, grave ameaça a pessoa ou servindo-se de mecanismos cibernéticos, do controle total ou parcial, ainda que de modo temporário, de meio de comunicação ou de transporte, de portos, aeroportos, estações ferroviárias ou rodoviárias, hospitais, casas de saúde, escolas, estádios esportivos, instalações públicas ou locais onde funcionem serviços públicos essenciais, instalações de geração ou transmissão de energia, instalações militares, instalações de exploração, refino e processamento de petróleo e gás e instituições bancárias e sua rede de atendimento;
- Atentar contra a vida ou a integridade física de pessoa;
- Promover, constituir, integrar ou prestar auxílio, pessoalmente ou por interposta pessoa, a organização terrorista.
- Realizar atos preparatórios de terrorismo com o propósito inequívoco de consumar tal delito;
- Incorre nas mesmas penas o agente que, com o propósito de praticar atos de terrorismo:
- recrutar, organizar, transportar ou municiar indivíduos que viajem para país distinto daquelede sua residência ou nacionalidade;
- fornecer ou receber treinamento em país distinto daquele de sua residência ou nacionalidade.

3.3. Pessoa Politicamente Exposta (“PEP”)

Conforme Resolução CVM 50 31/08/2021 e Circular Bacen 3.978 de 23/01/2020, consideram-se pessoas politicamente expostas:

i. os detentores de mandatos eletivos dos Poderes Executivo e Legislativo da União;

ii. os ocupantes de cargo, no Poder Executivo da União, de:

a) Ministro de Estado ou equiparado;

b) Natureza Especial ou equivalente;

c) presidente, vice-presidente e diretor, ou equivalentes, de entidades da administração pública indireta;

d) Grupo Direção e Assessoramento Superiores (DAS), nível 6, ou equivalente;

iii. os membros do Conselho Nacional de Justiça, do Supremo Tribunal Federal, dos Tribunais Superiores, dos Tribunais Regionais Federais, dos Tribunais Regionais do Trabalho, dos Tribunais Regionais Eleitorais, do Conselho Superior da Justiça do Trabalho e do Conselho da Justiça Federal;

iv. os membros do Conselho Nacional do Ministério Público, o Procurador-Geral da República, o Vice- Procurador-Geral da República, o Procurador-Geral do Trabalho, o Procurador-Geral da Justiça Militar, os Subprocuradores-Gerais da República e os Procuradores Gerais de Justiça dos Estados e do Distrito Federal;

v. os membros do Tribunal de Contas da União, o Procurador-Geral e os Subprocuradores-Gerais do Ministério Público junto ao Tribunal de Contas da União;

vi. os presidentes e os tesoureiros nacionais, ou equivalentes, de partidos políticos;

vii. os Governadores e os Secretários de Estado e do Distrito Federal, os Deputados Estaduais e Distritais, os presidentes, ou equivalentes, de entidades da administração pública indireta estadual e distrital e os presidentes de Tribunais de Justiça, Tribunais Militares, Tribunais de Contas ou equivalentes dos Estados e do Distrito Federal; e

viii. os Prefeitos, os Vereadores, os Secretários Municipais, os presidentes, ou equivalentes, de entidades da administração pública indireta municipal e os Presidentes de Tribunais de Contas ou equivalentes dos Municípios.

São também consideradas expostas politicamente as pessoas que, no exterior, sejam:

i. chefes de estado ou de governo;

ii. políticos de escalões superiores;

iii. ocupantes de cargos governamentais de escalões superiores;

iv. oficiais-generais e membros de escalões superiores do Poder Judiciário;

v. executivos de escalões superiores de empresas públicas; ou

vi. dirigentes de partidos políticos.

vii. dirigentes de escalões superiores de entidades de direito internacional público ou privado.

São considerados ainda como “PEP Relacionado”:

I – familiares: os parentes, na linha direta, até o segundo grau, o cônjuge, o companheiro, a companheira, oenteado e a enteada; e

II – estreitos colaboradores:

a) pessoas naturais que são conhecidas por terem sociedade ou propriedade conjunta em pessoas jurídicas de direito privado ou em arranjos sem personalidade jurídica, que figurem como mandatárias, ainda que por instrumento particular, ou possuam qualquer outro tipo de estreita relação de conhecimento público com uma pessoa exposta politicamente; e

b) pessoas naturais que têm o controle de pessoas jurídicas de direito privado ou em arranjos sem personalidade jurídica, conhecidos por terem sido criados para o benefício de uma pessoa exposta politicamente.

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.

3.4. Beneficiários Finais

Segundo a Resolução CVM 50/2021, entende como beneficiário final para aplicação da norma, a pessoa natural ou pessoas naturais que, em conjunto, possuam, controlem ou influenciem significativamente, direta ou indiretamente a entidade Pessoa Jurídica, e que conduzam suas operações ou que dela se beneficiem. Inclusive, equivalem a beneficiário final os seus prepostos, procuradores ou representantes legais.

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 BANCO CENTRAL DO BRASIL;

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:

1. o número de cotistas seja igual ou superior a 100 (cem) e nenhum deles tenha influência significativa; e

2. 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.

4. RESPONSABILIDADES E ATRIBUIÇÕES

Todos os colaboradores dentro de suas correspondentes atividades têm funções e responsabilidade relacionadas ao Programa de PLD/FTP, e estão sujeitas as sanções impostas pelas Políticas internas da BANVOX, bem como da legislação vigente referente ao tema.

4.1. Organogramas da Estrutura Organizacional

Organograma DTVM

4.2. Alta Direção

A Alta Direção da BANVOX deve apoiar a disseminação do Programa de PLD/FTP, aos diversos níveis do Grupo, e aprovar a presente Política, bem como aprovar o Relatório Anual de Avaliação de Risco de LDFTP.

[ANEXAR ORGANOGRAMA]

4.3. Diretoria de Compliance e Controles Internos

O Diretor de Controles Internos é o responsável pela área de Compliance, que realiza as atividades pertinentes a PLD/FTP, assegurando a devida implementação do Programa de PLD/FTP na BANVOX. E deverá estar devidamente registrado no sistema UNICAD do Banco Central e na CVMWEB como responsável pelas atividades de PLD/FTP.

O referido Diretor deverá ainda, preparar relatório anual relativo à avaliação interna de risco de LDFTP, e submeter a aprovação da alta direção da BANVOX. O Relatório Anual de Avaliação de Risco de LDFTP deve ser emitido até o último dia útil do mês de abril do ano subsequente à data base.

4.4. Comitê de CCR

Conforme Política interna de Comitês, o Comitê de CCR (Compliance, Controles Internos e Risco) é o órgão interno responsável por deliberar quanto a questões referentes a PLD/FTP, bem como sobre os temas abaixo:

- Avaliação de mudanças e adaptações regulatórias;
- Monitoramento de obrigações regulatórias;
- Avaliação de operações / clientes com perfil atípico;
- Revisão dos parâmetros e enquadramento de risco;
- Apuração e deliberações quanto aos novos clientes e parceiros, quando necessário.

As deliberações do Comitê serão tomadas pela maioria de seus membros e se constituirão em recomendações ao departamento e/ou responsável pela área que tiver apontado dúvida ao Comitê.

4.5. Controles Internos

A área de Controles Internos da BANVOX é a responsável pela realização de testes periódicos para verificação da suficiência dos procedimentos relacionados à Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e ao Financiamento da Proliferação de Armas de Destruição em Massa.

A periodicidade dos testes é determinada com base na avaliação do nível de risco de cada processo conforme mapeamento documentado na matriz de risco.

4.6. Compliance

A área de Compliance da BANVOX é responsável por implementar e monitorar as diretrizes descritas nesta Política, sempre observando as boas práticas e os padrões éticos na condução dos negócios, no estabelecimento e na manutenção de relacionamento com os clientes, de forma objetiva e imparcial.

Sendo responsável ainda por:

- Desenvolver e realizar treinamentos internos de PLD/FTP;
- Desenvolver Política e Procedimentos internos de controle para a detecção e monitoramento de operações que caracterizem indício de ocorrência dos crimes de lavagem de dinheiro ou financiamento ao terrorismo;
- Definir a metodologia e os critérios de classificação dos clientes através de abordagem baseada em risco, para a realização das atividades de PLD/FTP;
- Realizar o processo de "Conheça seu Cliente", demandado informações quando necessário a área de Cadastro e/ou áreas responsáveis pelo cliente;
- Avaliar os processos internos das áreas com vistas à PLD/FTP;
- Criar mecanismos para monitoramento de clientes, com base nos normativos vigentes da CVM e BANCO CENTRAL DO BRASIL, bem como legislação vigente;
- Realizar atividades de monitoramento de PLD/FTP;
- Obter e analisar documentação relativa a processos de suspeita de crimes de LDFTP;
- Realizar apresentação de casos suspeitos de LDFTP ao Comitê de CCR;
- Realizar comunicação de situações identificadas como suspeita ao COAF;
- Reter toda a documentação de formalização dos processos de PLD/FTP pelo prazo regulatório de 10 (dez) anos; e
- Validar, formalizar e manter a guarda desta Política atualizada.

4.7. Auditoria Interna

A Auditoria Interna é responsável por revisar e avaliar a eficiência quanto à implementação e os controles da Política de PLD/FTP.

4.8. Cadastro

A área de Cadastro utiliza sistemas alternativos para efetuar o cadastro dos clientes. Além disso, desempenha a função de analisar os documentos cadastrais, assegurando a conformidade e regularidade da documentação dos clientes.

Cadastro de Clientes

a) Pessoa Física: Cliente Pessoa Física deverá acessar o app da BANVOX, e clicar no botão *"iniciar agora"*, o cliente deve preencher os dados cadastrais, tirar fotos do documento de identificação (RG ou CPF) e em seguida tirar uma Selfie. No processo de cadastramento, o cliente, deverá, além de informar seus dados, tomar ciência das declarações e aderir os contratos constantes no processo cadastral.

Feito isto, os documentos são encaminhados para verificação no sistema de *onboarding check* contratado, o sistema irá realizar a validação do documento encaminhado pelo cliente e Selfie enviada através de documentoscopia, prova de vida, legibilidade das fotos, *facematch*, além de consultas do CPF.

Após a aprovação no sistema, será iniciada a segunda etapa de pesquisa reputacional do cliente, que é realizada por sistema contratado para pesquisas de informações reputacionais em listas PEP e Relacionados, listas de sanções e restritivas (nacionais e internacionais), órgãos reguladores e autarquias, tribunais 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)"*.

Após o processo de pesquisa reputacional, o cliente é classificado por nível de risco, BAIXO, MÉDIO e ALTO. Clientes classificados com nível de risco baixo terão aprovação automática, clientes classificados com nível de risco médio deverão ser avaliados e aprovados pelo Compliance, e clientes classificados com nível de risco alto deverão ser avaliados e aprovados pelo compliance e diretoria.

b) Pessoa Jurídica: Para abertura de conta de pessoa jurídica, o cliente (ou representante) deve enviar para o Departamento de Cadastro o kit cadastral devidamente preenchido e respectivos documentos comprobatórios. Cabe destacar que antes do efetivo cadastramento do cliente, toda a documentação apresentada é avaliada pelos colaboradores da área de Cadastro. 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 finalização da análise da documentação, o time de cadastro deverá incluir a documentação cadastral no SharePoint para aprovação do compliance e diretoria. Necessária aprovação da diretoria, somente para clientes de classificação de risco Alta. Além da documentação cadastral, deverá incluir no SharePoint o dossiê gerado no sistema de pesquisas reputacionais e *check list* cadastral.

c) INR: Para abertura de conta de investidor não residente, o cliente (ou representante) deve enviar para o Departamento de Cadastro o kit cadastral devidamente preenchido e respectivos documentos comprobatórios. Cabe destacar que antes do efetivo cadastramento do cliente, toda a documentação apresentada é avaliada pelos colaboradores da área de Cadastro. A BANVOX DTVM utiliza o modelo de cadastro completo para Investidor não residente. Após finalização da análise da documentação, o time de cadastro deverá incluira documentação cadastral no SharePoint para aprovação do compliance e diretoria. Além da documentação cadastral, deverá ser incluso no SharePoint o dossiê gerado no sistema de pesquisas reputacionais e *check list* cadastral.

d) Atualização Cadastral e Recadastro: O processo de atualização cadastral seguirá as mesmas regras da abertura da conta. Pessoa Física via App, Pessoa Jurídica e INR via documentação física.

4.9. Recursos Humanos

- Solicitar ao candidato o preenchimento de Ficha Cadastral;
- Previamente à contratação submeter o candidato a análise da área de Compliance para verificação reputacional;
- Orientar o colaborador sobre a obrigatoriedade dos treinamentos obrigatórios;
- No início da atividade do funcionário encaminhar os treinamentos obrigatórios descritos no item 7 da presente Política.

4.10. Colaboradores

Para efeitos da presente Política são considerados Colaboradores; os funcionários, estagiários, jovens aprendizes, sócios e diretores da BANVOX, bem como terceiros contratados e prestadores de serviço relevante para os negócios da BANVOX.

Todos os Colaboradores devem observar as diretrizes da presente Política na execução de suas atividades junto à BANVOX, devendo ter especial atenção as atividades de captação, intermediação e negociação, adotando as melhores práticas no que tange o processo de "Conheça seu Cliente" e, ainda:

- Realizar o treinamento de Compliance sobre PLD/FTP;
- Comunicar a área de Compliance sobre operações suspeitas;
- Responder de forma tempestiva e objetiva as solicitações da área de Compliance.

5. DIRETRIZES INSTITUCIONAIS

O processo de análise e monitoramento de PLD/FTP da BANVOX abarca todos os tipos de relacionamentos e operações realizadas junto à instituição. Para tanto, seus clientes, fornecedores, colaboradores, prestadores de serviço e parceiros em geral são submetidos a uma análise criteriosa no início de seu relacionamento e são monitorados no decorrer de suas atividades junto à BANVOX.

Através de uma Abordagem Baseada em Risco, clientes e produtos são classificados com o objetivo de realizar um controle e identificação dos riscos.

5.1. Conheça seu Cliente (Know Your Client “KYC”)

O processo de “Conheça seu Cliente” ou “KYC”, inicia-se na recepção das informações do cliente e/ou da operação através da área de Cadastro, seja por meio digital ou físico.

A área de Cadastro da BANVOX executa rotinas de identificação e habilitação dos clientes, alteração de dados, atualização cadastral e efetivação de encerramento de contas mediante solicitação do cliente.

A análise de Cadastro consiste na validação das informações conforme disposto no item 4.8 da referida política.

O processo de atualização cadastral deverá ocorrer conforme o tipo de cliente PJ institucional, PJ não Financeira e Pessoa Física:

- PJ Institucional: Processo de atualização cadastral deverá ocorrer conforme a classificação de risco atribuído ao cliente em sistema, clientes classificados com nível de risco Alto deverão atualizar o cadastro em um prazo não superior a 24 meses, clientes com nível de risco Médio deverão atualizar o cadastro em um prazo não superior a 36 meses e clientes com nível de risco Baixo deverão atualizar o cadastro em um prazo não superior a 60 meses.
- PJ Não Financeira e Pessoa Física: Processo de atualização cadastral deverá ocorrer em um prazo que não seja superior a 24 meses, independentemente do nível de risco do cliente.

Os documentos atualizados são analisados pela área de Cadastro e repassados ao Compliance para realização de nova análise reputacional.

A área de Cadastro possui Políticas e Manuais próprios onde são descritos os procedimentos completos de suas atividades.

O potencial cliente ou as contrapartes de uma operação são submetidos a verificação em listas PPE (Pessoa Politicamente Exposta), Restritivas e Sanções, análise de processos judiciais, mídias negativas, inquéritos policiais, país de constituição e outras fontes de dados externos de informações. Para as pessoas jurídicas (PJ) a pesquisa se estende para a cadeia de participação societária até a identificação de seu beneficiário final.

Para realização de tal análise são utilizados sistemas contratados e pesquisa em sites de busca na rede mundial de computadores.

Na análise inicial de um cliente ou operação, cabe à área de Compliance, responsável pelo monitoramento de PLD/FTP, observar, mas não se limitando, os itens que seguem abaixo:

- Analisar as pesquisas de KYC e seus resultados quanto a possíveis situações que desabonem sua reputação, com especial atenção ao envolvimento com ilícitos;
- Identificar quem são os titulares beneficiários (intermediários e finais) – por meio de documentos comprobatórios, que explicitem a participação de pessoa natural até o fim da cadeia societária, ou até o percentual de 25% de participação acionária. Além do processo de identificação, os beneficiários finais deverão ser qualificados a partir da validação/verificação das informações de local de residência e capacidade financeira (incluindo a renda).

Quando não for possível identificar e/ou qualificar o beneficiário final, o cliente deverá ser submetido ao comitê de CCR para aprovação, caso o cliente seja aprovado em Comitê o mesmo deverá ser classificado como nível de risco ALTO. Serão parametrizados alertas de monitoramento específicos para clientes que não seja possível identificar e/ou qualificar o beneficiário final.

- Analisar a situação financeira do cliente e suas atividades profissionais;

Verificar se o cliente é uma Pessoa Politicamente Exposta (PEP) considerando a declaração feita pelo cliente e indícios obtidos nas pesquisas de lista PEP contratada, caso o cliente seja identificado como PEP, este deverá ser classificado nos sistemas internos como tal. Clientes identificados como PEP serão classificados no mínimo com nível de risco MÉDIO. Serão parametrizados alertas de monitoramento específicos para clientes identificados como PEP.

Verificar se o cliente é constituído como ONG (Organização Sem Fins Lucrativos), considerando a documentação entregue e avaliada pelo departamento de Cadastro. Clientes identificados como ONGs serão classificados minimamente com nível de risco MÉDIO e deverão ser avaliados pelo comitê de CCR para eventual aprovação. Ainda, serão parametrizados alertas de monitoramento específicos para clientes identificados como ONGs.

- Verificar se o cliente foi constituído em um paraíso fiscal;
- Verificar se o cliente reside em algum dos países não cooperantes ou países expostos a significativos riscos de lavagem de dinheiro ou financiamento ao terrorismo.

Após avaliação e verificação das informações do cliente obtém-se a classificação de Risco do mesmo, conforme descrito no item 5.8 da presente Política.

Nota: Clientes onde não seja possível identificar o beneficiário final, constituídos como ONGs e clientes identificados como PEP, as operações serão monitoradas conforme descrito no item 5.6.

5.2. Conheça seu Colaborador (Know Your Employee – “KYE”)

O processo de “Conheça seu Colaborador” da BANVOX inicia-se no processo de seleção e é finalizadoantes da admissão. Tal processo é realizado através da checagem de informações e obtenção de documentospessoais pela área de Recursos Humanos.

Com o recebimento das informações básicas do candidato (RG, CPF, dentre outros) a área de Recursos Humanos encaminha para análise da área de Compliance antes de efetivar a admissão do mesmo. As pesquisas são realizadas através de sistema contratado que gera um dossiê contendo informações relativas a pesquisas em mídias, tribunais, Polícia Federal, MPF, STJ, listas restritivas locais e internacionais, dentre outros.

Além das informações reputacionais, listas restritivas locais e internacionais, devem ser avaliadas as atividades que serão desenvolvidas pelo candidato, com base na classificação interna de riscos a elas associada e na relevância das informações envolvidas.

Áreas de front office (área de negócios em geral), cadastro e tecnologia devem ser consideradas atividades de risco de LD/FTP. Portanto, para candidatos a vagas nessas áreas, o processo de KYE deve ser executado de acordo com a criticidade das referidas atividades, tendo como base os critérios de probabilidade e impacto descritos na matriz de avaliação interna de risco.

Após análise e não sendo identificada nenhuma informação que desabone ou impeça a admissão do candidato, a área de recrutamento segue com o processo de contratação do candidato. No início de suas atividades, o colaborador receberá as Políticas internas e o Código de Ética e Conduta para leitura e aceite de seus termos.

A BANVOX adota processos contínuos de monitoramento de seus colaboradores para acompanhamento de mudanças no padrão financeiro, e treinamentos de atualização de sua Política de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e ao Financiamento da Proliferação de Armas de Destruição em Massa, bem como demais Políticas aplicáveis.

Deverão ser relatados à área de Compliance os casos suspeitos ou confirmados de envolvimento de colaboradores em transações ou operações consideradas atípicas.

5.3. Conheça seu parceiro (Know Your Partner – "KYP")

A BANVOX possui processos robustos de seleção e contratação de parceiros (fornecedores e prestadores de serviço), sempre atuando de forma diligente em observância às melhores práticas de mercado e à legislação aplicável a PLD/FTP, e adota procedimentos com o objetivo de mitigar alianças com parceiros cuja reputação possa afetar negativamente a imagem da instituição.

Para tanto, a BANVOX possui processo de análise de acordo com a natureza do relacionamento e serviços prestados, onde inicialmente é realizada análise reputacional verificando, através de sistemas contratados, se a empresa possui informações desabonadoras através de pesquisas quanto a situação socioeconômica, tribunais, mídias, polícia federal, MPF, STJ, listas restritivas locais e internacionais, dentre outros.

Além da pesquisa reputacional, de acordo com o tipo de relacionamento é realizada Due Diligence, visitas presenciais e inclusão de cláusulas contratuais com relação ao cumprimento das Leis 9.613 e 13.260 e do cumprimento do Código de Ética e Conduta da BANVOX, e demais leis e normas vigentes, quando aplicável. Após análise, o parceiro recebe uma classificação de risco conforme descrito no item 5.8 da presente Política.

Deverão ser relatados à área de Compliance os casos suspeitos ou confirmados de envolvimento de parceiros contratados em transações ou operações consideradas atípicas.

5.4. Situações Não Permitidas

Segue abaixo situações não permitidas na admissão de cliente e como contraparte em operações:

- Pessoa física ou jurídica, cuja identidade não possa ser confirmada;
- "Shell Bank" (instituição financeira constituída em um dado território ou jurisdição sem ter nele presença física e que não se encontre integrado a nenhum grupo financeiro regulamentado);
- Comércio Varejista de Combustível;
- Organizações Religiosas;
- Associações sindicais;
- Partidos políticos;
- Segmentos econômicos cuja renda seja proveniente de jogos de azar ou atividades afins;
- Segmentos econômicos cuja renda seja proveniente de crimes: terrorismo e seu financiamento; contrabando ou tráfico ilícito de armas e munições, de material destinado à sua produção e de substâncias entorpecentes; de extorsão mediante sequestro; contra o Sistema Financeiro Nacional e cometido por organização criminosa.

5.5. Produtos e Serviços

Os novos produtos e serviços são analisados de forma prévia pela área de Compliance e pela área de Risco da BANVOX, considerando a identificação de pontos de riscos e formalização do produto e/ou serviço.

Com relação aos produtos disponibilizados, são analisadas características relacionadas ao emissor, gestor e/ou outros prestadores de serviço (no caso de fundos de investimento), riscos relacionados e demais aspectos relevantes durante o processo de Due Diligence.

A análise de PLD/FTP do novo produto e/ou serviço, quando identificadas situações de atipicidade, é submetida ao Comitê Executivo para aprovação ou reprovação.

De acordo com a metodologia de Abordagem Baseada em Risco da BANVOX, todos os produtos e/ou serviços são classificados de acordo com sua complexidade e nível de risco.

5.6. Monitoramento e Análise de Operações

Todas as transações e operações financeiras, inclusive as propostas, realizadas pelos clientes, colaboradores ou não, devem ser monitoradas para apuração de situações que podem configurar indícios de ocorrência de lavagem de dinheiro ou financiamento do terrorismo. Para realização do monitoramento das operações, a área de Compliance utiliza sistemas contratados e previamente parametrizados para atender aos incisos dispostos na Resolução CVM nº 50/21 e normas do BANCO CENTRAL DO BRASIL. Os procedimentos de monitoramento das transações, propostas, operações e atipicidades que possam caracterizar indícios de lavagem de dinheiro e financiamento ao terrorismo englobam as operações de todos os clientes do Grupo.

Para realização do monitoramento de PLD/FTP, os alertas são parametrizados com base no CPF/CNPJ dos clientes e com periodicidade diária e/ou mensal, além da utilização de parâmetro alfabético (nome do cliente) para monitoramento junto às listas de sanções internacionais e nacionais. As regras de detecção de LDFT estão segmentadas por nível de risco baixo, médio e alto, como podemos observar na Matriz de Avaliação Interna de Risco.

As análises realizadas são registradas em sistema e/ou em planilha específica, caso seja necessário algum tipo de informação para conclusão das referidas análises, o analista encaminha solicitação para as áreas competentes solicitando justificativa para a atipicidade identificada referente ao cliente. A análise se baseará no produto operado e no risco do cliente para determinar a tomada de decisão e as sanções aplicáveis à situação.

Os critérios de análises e tomada de decisão considerando o nível de risco do cliente estão disponíveis nos manuais de PLD/FTP da BANVOX DTVM, de acordo com o seu ramo de atividade.

Clientes onde não seja possível identificar o beneficiário final, constituídos como ONGs e clientes identificados como PEP, as operações, mídias e listas restritivas serão analisadas para verificar atipicidades relacionadas a PLD/FTP. Caso sejam identificadas atipicidades, estes clientes serão comunicados ao COAF e poderão ter as contas bloqueadas para novas operações. Sendo identificada alguma situação de atipicidade sem justificativa, a área de Compliance poderá encaminhar para análise do Comitê de CCR, conforme descrito no item 6 da Política.

Todos os colaboradores (independente do seu nível hierárquico) e prestadores de serviços, caso sejam identificadas na prospecção, negociação ou durante o relacionamento propostas de operações (solicitação ou ordem) ou situações com indícios ou evidências de atos ilícitos relacionados a LD/FTP, devem comunicar imediatamente ao departamento de Compliance e/ou canal de denúncia.

As comunicações deverão ser enviadas, com o máximo de detalhes possíveis, para os seguintes canais: XXXXXXXXX e/ou XXXXXXXX. Caso o colaborador ou prestador prefira fazer um relato de maneira anônima, a BANVOX mantém o canal confidencial em seu site [SITE DA BANVOX], sendo que o formulário está disponível no rodapé do site.

5.7. Monitoramento das Sanções Impostas pela Lei nº 13.810/2019

Para realização do monitoramento dos clientes indicados na lista de sanções do CSNU (Conselho de Segurança das Nações Unidas) e demais países, a BANVOX utiliza sistemas previamente parametrizados para identificação dos clientes citados nas referidas listas.

Caso seja identificado cliente nas referidas listas, a BANVOX deverá executar as tratativas a seguir:

i. Verificar se o cliente citado possui posição financeira na BANVOX DTVM;

ii. Caso cliente possua posição, solicitar o bloqueio dos ativos, conforme disposto na lei nº 13810 de março de 2019;

iii. Fazer a comunicação do cliente ao COAF, BANCO CENTRAL DO BRASIL (via BC Correio), CVM e Ministério da Justiça e Segurança Pública (MJSP);

iv. Encaminhar para o comitê de CCR, informando da inclusão do cliente na lista de sanção do CSNU, bem como da comunicação do cliente ao COAF, BANCO CENTRAL DO BRASIL, CVM e MJSP.

5.8. Avaliação Interna de Risco (AIR)

A Abordagem Baseada em Risco (ABR) da BANVOX, no limite de suas atribuições, tem como objetivo identificar e mensurar os riscos na utilização de seus produtos e serviços na prática da lavagem de dinheiro e do financiamento do terrorismo.

Para definição da AIR (Avaliação Interna de Risco) a BANVOX considerou os seguintes perfis de risco:

- Dos clientes;
- Da BANVOX, incluindo o seu modelo de negócio e a área geográfica de atuação;
- Das operações, transações, produtos e serviços oferecidos e
- Das atividades exercidas pelos colaboradores, parceiros e prestadores de serviços terceirizados da BANVOX.

Os perfis de risco considerados para definição da AIR estão segmentados em Risco Baixo, Médio e Alto.

Para definição da metodologia da AIR, foram considerados os riscos quanto a sua probabilidade de ocorrência e à magnitude dos impactos financeiros, jurídico, reputacional e socioambiental para a BANVOX. No que diz respeito à classificação das atividades exercidas pelos colaboradores, parceiros e prestadores de serviços, a avaliação considera fatores como o poder de decisão/execução de operações financeiras, os potenciais conflitos de interesse (possíveis incentivos à prática de LD/FTP ou à conivência com esse tipo de irregularidade) e o acesso a informações financeiras.

Aplicação da referida metodologia pode ser consultada na matriz de avaliação interna de risco, disponível na Intranet da BANVOX.

O nível de risco dos clientes será reavaliado em um prazo não superior a 12 (doze) meses; clientes que no período tiverem até 2 (duas) ocorrências consideradas atípicas (operações, mídias e listas restritivas) serão reclassificados para nível de risco acima do atual.

Após reclassificação e não sendo identificados novos alertas considerados atípicos em um período de 12 (doze) meses, o nível de risco do cliente deverá ser reavaliado, podendo retornar para a classificação anterior.

5.9. Relatório de Avaliação Interna de Risco

Em atendimento ao disposto na regulamentação em da CVM e Banco Central, anualmente será formalizado o relatório de avaliação interna de risco de LD/FTP. Tal relatório tem por objetivo apresentar para alta administração a efetividade dos procedimentos e controles internos relacionados a prevenção à lavagem de dinheiro, ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa.

O relatório deverá ser elaborado e enviado a alta administração e ao comitê de auditoria interna até 31 (trinta e um) de março do ano seguinte ao da data-base e deverá conter as seguintes informações:

- Avaliação de efetividade dos procedimentos destinados a conhecer clientes, incluindo a verificação e a validação das informações dos clientes e a adequação dos dados cadastrais;
- Avaliação de efetividade dos procedimentos de monitoramento, seleção, análise e comunicação ao COAF, incluindo a avaliação de efetividade dos parâmetros de seleção de operações e de situações suspeitas;
- Avaliação de efetividade da governança da Política de PLD/FTP;
- Avaliação de efetividade das medidas de desenvolvimento da cultura organizacional voltadas à PLD/FTP e dos programas de capacitação periódica de pessoal;
- Avaliação de efetividade dos procedimentos destinados a conhecer os funcionários, parceiros e prestadores de serviços terceirizados; e
- Avaliação de efetividade de implementação das recomendações indicadas no relatório anterior e/ou apontamentos realizados pelos times de controles internos e auditoria interna.

Adicionalmente aos itens indicados acima, o relatório deverá conter:

- Identificação e análise das situações de risco de LD/FTP, considerando as respectivas ameaças, vulnerabilidades e consequências;
- Se aplicável, análise da atuação dos prepostos, assessores de investimento ou prestadores de serviços relevantes contratados, bem como a descrição da governança e dos deveres associados à manutenção do cadastro simplificado; e
- Tabela relativa ao ano anterior, contendo:
    i. Número consolidado das operações e situações atípicas detectadas, segregadas por cada hipótese;
    ii. Número de análises realizadas e comunicações ao COAF; e
    iii. Data do reporte da declaração negativa, se aplicável.

6. COMUNICAÇÃO DE SITUAÇÕES SUSPEITAS AOS ÓRGÃOS COMPETENTES

Durante o processo de análise e monitoramento, quando identificadas situações suspeitas de atipicidade, de acordo com as orientações descritas nas normas vigentes referentes a PLD/FTP, o cliente ou parceiro em questão deverá ser comunicado ao Conselho de Controle de Atividades Financeiras (COAF).

6.1. Comunicação ao COAF

Sempre que identificadas situações atípicas, caberá à área de Compliance analisar as evidências coletadas e apresentar para decisão do Comitê de CCR quanto a comunicação ou não aos órgãos competentes.

Após a conclusão da análise, se identificados indícios de ocorrência de crimes de lavagem de dinheiro ou financiamento ao terrorismo, a área de Compliance irá convocar um Comitê de CCR extraordinário. Os casos não considerados como indícios de lavagem de dinheiro ou financiamento ao terrorismo são encerrados e têm seus documentos arquivados pela área de Compliance.

Após decisão do Comitê de CCR quanto a comunicação aos órgãos reguladores competentes, a área de Compliance, em cumprimento à Lei, comunicará ao órgão regulador correspondente até o dia útil seguinte à operação analisada, todos os casos relativos às operações ou fatos suscetíveis de relação com a lavagem de dinheiro ou com o financiamento ao terrorismo, arquivando ainda a documentação de todos os casos analisados e reportados.

A partir do momento da identificação da situação suspeita, os procedimentos de análise não poderão exceder o prazo de quarenta e cinco dias, contados a partir da data da seleção da operação ou situação. E a comunicação da operação ou situação suspeita ao COAF deve ser realizada até o dia útil seguinte ao da decisão de comunicação.

Atenção: É vedado dar ciência aos envolvidos ou a terceiros quanto a sua comunicação ao COAF.

Atenção: Clientes identificados no monitoramento periódico em Listas de Sanções Internacionais serão comunicados imediatamente ao COAF e o Comitê de CCR será informado de sua comunicação.

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 BANVOX 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.

7. TREINAMENTOS

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

Os treinamentos são de participação obrigatória referente às Políticas abaixo:

- Código de Ética e Conduta e Política de Responsabilidade Social, Ambiental e Climática;
- Segurança da Informação e Segurança Cibernética;
- Política de PLD/FTP e Política Anticorrupção.

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.

Periodicamente é enviado o material contendo orientações revisadas/atualizadas a todos os colaboradores e uma avaliação é aplicada para verificar se o colaborador compreendeu os conceitos. A nota mínima para aprovação é 7 (sete).

8. VIGÊNCIA E REVISÃO

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

9. CONTROLE DE REVISÕES