



BITRUST



***Política de Prevenção à Lavagem de Dinheiro e
Combate ao Financiamento do Terrorismo***

2021



Assunto: Política de Prevenção à Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo

Sumário

OBJETIVO	3
ABRANGÊNCIA	3
RESPONSABILIDADES	3
DIRETRIZES	4
4.1. GESTÃO E CONTROLES	4
4.1.1. Cadastro de Clientes	4
4.1.2. Pessoas Expostas Politicamente (PEP's)	5
4.2. PROCESSOS DE ANÁLISES	5
4.2.1. Conheça o seu Cliente (Know Your Customer - KYC)	5
4.2.2 Conheça seu Funcionário (Know Your Employee - KYE)	5
4.2.3 Conheça seu Parceiro / Fornecedor (Know Your Partner - KYP / Know Your Supplier - KYS)	6
4.2.4. Avaliação de Novos Produtos, Serviços e Operações	6
4.3. CLASSIFICAÇÃO E MONITORAMENTO	6
4.3.1. Critério para Classificação de Clientes	6
4.3.2. Monitoramento de Operações	8
4.3.3. Comunicação de Ocorrências e Situações Suspeitas	8
4.3.4. Controles e Avaliação Interna de Riscos	8
TREINAMENTO E ACULTURAMENTO	9
PENALIDADES	10
DISPOSIÇÕES FINAIS	10
REFERÊNCIAS	10



1. OBJETIVO

Esta Política tem por finalidade estabelecer as responsabilidades e os processos a serem observados na prevenção à lavagem de dinheiro e combate ao financiamento do terrorismo.

2. ABRANGÊNCIA

Esta Política aplica-se a todos os administradores, colaboradores, estagiários e prestadores de serviços e seus subcontratados.

3. RESPONSABILIDADES

Diretoria de Compliance

- Coordenar o programa de Prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo;
- Conduzir o processo de verificação dos clientes (“Conheça seu Cliente”), fornecedores (“Conheça seu Fornecedor), colaborador (“Conheça seu Funcionário”) e parceiros de negócios (“Conheça seu Parceiro”), por meio da análise de integridade;
- Analisar e monitorar continuamente as operações dos clientes com indícios de atipicidade;
- Adotar as providências cabíveis para os casos suspeitos de ilicitude;
- Analisar os novos produtos e serviços a fim de identificar os riscos de utilização destes em qualquer tipo de ato ilícito;
- Assegurar a conformidade com a legislação, normas e regulamentos que disciplinam esses assuntos; e
- Desenvolver e promover programas de treinamento e de conscientização dos administradores, funcionários, colaboradores, estagiários e dos prestadores de serviços terceirizados relevantes.

Áreas de Negócios

- Estabelecer relação de proximidade com os clientes para conhecer suas características, operações e negócios; e
- Identificar e reportar para a área de Compliance propostas de operações suspeitas, bem como indícios de práticas de atos ilícitos.

Atendimento

- Manter e identificar corretamente os dados cadastrais dos clientes;
- Realizar o processo de “Conheça seu Cliente” para os de baixo e médio riscos; e
- Reportar para a área de Compliance os clientes classificados como alto e extremo riscos para análise.



Recursos Humanos

- Informar à área de Compliance as novas contratações para que seja realizado o processo de “Conheça seu Funcionário”.

O gestor do colaborador deve acompanhá-lo, dentro do possível, atentando para qualquer mudança comportamental habitual, que possa indicar possível atividade irregular por parte deste, e comunicá-la à área de Compliance.

Jurídico

- Apoiar a área de Compliance a manter atualizada a matriz de regulamentações, com base nos normativos estabelecidos pelos órgãos reguladores aplicáveis.

Colaboradores

- Informar a área de Compliance sobre as novas contratações com parceiros de negócios e fornecedores para que sejam realizadas as análises de integridade; e
- Comunicar à área de Compliance quaisquer irregularidades ou suspeitas de ato ilícito que tomarem conhecimento.

4. DIRETRIZES

4.1. GESTÃO E CONTROLES

4.1.1. Cadastro de Clientes

A área de Atendimento é responsável pela análise, registro das informações e documentos de identificação dos clientes com os quais a Instituição mantém relacionamento por meio dos serviços e produtos financeiros. Muitas dessas informações essenciais são feitas por meio de busca automatizada em fontes de dados para pessoas física e jurídica visando agilizar o processo de “onboarding digital” de clientes, sem comprometer a segurança e o sigilo da informação.

Todas as informações cadastrais deverão estar atualizadas, de acordo com os dados apresentados pelo cliente, e revisadas periodicamente, por um prazo inferior a 24 (vinte e quatro) meses. As responsabilidades cadastrais abrangem:

- Conferência, custódia da documentação de cadastro exigida, análise e registro das informações bem como dos documentos de identificação dos clientes;
- Verificar as informações acerca de renda mensal e patrimônio, no caso de pessoas naturais, e de faturamento médio mensal dos 12 (doze) meses anteriores, no caso de pessoas jurídicas;
- Validação dos documentos (CNPJ e outros);
- Efetuar a identificação de clientes PEP's; e



- Monitorar as renovações dos cadastros e dos relatórios de “Conheça Seu Cliente”.

4.1.2. Pessoas Expostas Politicamente (PEP's)

Consideram-se PEP's os agentes públicos que desempenham ou tenham desempenhado, nos últimos 5 (cinco) anos, no Brasil ou em países, territórios e dependências estrangeiras, cargos, empregos ou funções públicas relevantes, assim como seus representantes, familiares e outras pessoas de seu relacionamento próximo.

Os processos a serem observados para o estabelecimento de relação de negócios e acompanhamento das movimentações financeiras de PEPs, são estruturados de forma a possibilitar a sua identificação, bem como a origem dos fundos envolvidos nas transações. Não obstante, como tal pesquisa está concentrada nas pessoas físicas que desempenharam funções públicas, é de fundamental importância atentar para os representantes e controladores, quando se tratar de cliente pessoa jurídica.

4.2. PROCESSOS DE ANÁLISES

4.2.1. Conheça o seu Cliente (*Know Your Customer - KYC*)

O processo “Conheça seu Cliente” é adequado às características e especificações dos negócios, objetivando prevenir que o cliente utilize a Bitrust para atividades ilegais ou impróprias. Assim, tem por premissa permitir que a Bitrust conheça as propriedades e especificidades do cliente, para que fique clara a origem e o destino dos ativos digitais movimentados, aferir a compatibilidade entre a operação e o perfil da outra parte do negócio, bem como classificar o risco do cliente frente à utilização do serviço de custódia digital.

A metodologia de verificação de antecedentes do cliente poderá conter pesquisa de informações públicas como situação cadastral na Receita Federal, antecedentes criminais e processos judiciais, protestos, análise de situação econômico-financeira, a participação em quadro societário de empresas, situação eleitoral perante o Tribunal Superior Eleitoral (TSE), enquadramento como Pessoa Exposta Politicamente (PEP), bem como eventual presença em lista de inabilitados em instituições financeiras e listas de sanções internacionais.

4.2.2 Conheça seu Funcionário (*Know Your Employee - KYE*)

No processo de contratação de colaboradores, são adotados processos que incluem mecanismos de análises, desde a contratação até o seu comportamento, visando proteger a Instituição de possíveis práticas de atos ilícitos.

Os eventos para conhecer os colaboradores tem como diretrizes:

- Alteração inusitada nos padrões de vida e de comportamento sem causa aparente;



- Realização de qualquer negócio de modo diverso aos procedimentos formais;
- Fornecimento de auxílio ou informações, remunerados ou não, para cliente em prejuízo do programa de prevenção à lavagem de dinheiro e combate ao financiamento do terrorismo ou auxílio para estruturar ou fracionar operações, burlar limites regulamentares, operacionais entre outros.

4.2.3 Conheça seu Parceiro / Fornecedor (*Know Your Partner - KYP / Know Your Supplier - KYS*)

A Instituição adota processos para identificação e aceitação de parceiros e fornecedores, com a finalidade de prevenir a realização de negócios com parceiros inidôneos ou suspeitos de envolvimento em atividades ilícitas. Além disso, também tem como objetivo assegurar que possuam práticas adequadas de prevenção à lavagem de dinheiro e combate ao financiamento do terrorismo.

4.2.4. Avaliação de Novos Produtos, Serviços e Operações

Os novos produtos e serviços são analisados e aprovados previamente pelas áreas de Produtos, Operações e de Compliance tendo como premissa a ótica de prevenção à lavagem de dinheiro e combate ao financiamento do terrorismo. Assim, são observadas a estruturação do novo produto ou serviço, considerando todas as variáveis de riscos de ocorrência de práticas de atos ilícitos, incluindo, mas não se limitando, à operacionalização, investidores, prestadores de serviços e tipos de ativos envolvidos.

4.3. CLASSIFICAÇÃO E MONITORAMENTO

4.3.1. Critério para Classificação de Clientes

Na qualificação do nível de risco do cliente, são considerados entre outros fatores:

- Informações cadastrais e financeiras, sendo verificada a profissão ou a atividade da empresa;
- Informações de geolocalização, incluindo o endereço completo, que considera se a cidade é de fronteira, ou se o país está na lista de países com restrição pelo Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo (GAFI/FATF), ou se o país apresenta nível de risco alto;
- Mídias negativas, listas sancionadoras, incluindo a lista de sanções impostas pelo Conselho de Segurança das Nações Unidas (CSNU);
- Processos criminais, administrativos dentre outros; e
- Enquadramento na condição de PEP.



Adicionalmente são realizadas verificações em bases públicas e privadas para avaliação se há processos ou outros fatos desabonadores. Após aplicação de todos os filtros e critérios acima descritos, o cliente é classificado quanto ao seu grau de risco.

A classificação possui 4 (quatro) categorias de risco sendo baixo, médio, alto e extremo:

Os clientes que apresentarem risco extremo são aqueles que apresentam os seguintes enquadramentos:

- Processos criminais ou administrativos com trânsito em julgado com decisão pela condenação sem possibilidade de qualquer recurso contra a decisão judicial, pelo ato ilícito cometido; e
- Listas sancionadoras, ramos de atividade impeditivos e países com restrição no GAFI.

Os clientes que apresentarem risco alto são aqueles que apresentam os seguintes enquadramentos:

- Processos criminais ou administrativos junto ao BACEN com trânsito em julgado com decisão pela condenação e com possibilidade de recorrer contra a decisão judicial, pelo ato ilícito cometido;
- Processos em andamento na esfera criminal ou administrativa; e
- Mídia negativa e com enquadramento na condição de PEP, e com enquadramento de país de alto risco.

Os clientes que apresentarem risco médio são aqueles que apresentam os seguintes enquadramentos:

- Mídia com até 03 (três) anos de publicação;
- Profissão de risco ou ramo de atividade sensível; e
- Residentes em cidade de fronteira.

Os clientes que apresentarem risco baixo são aqueles que apresentam os seguintes enquadramentos:

- Mídia com mais de 03 (três) anos da data de publicação;
- Não possuam processo criminal, administrativo junto ao BACEN, ou que apresentam processo na categoria civil, trabalhista ou fiscal;
- Processo criminal, administrativo junto ao BACEN, com trânsito em julgado com absolvição;
- Exerça profissão de risco, ramo de atividade sensível ou impeditivo, país de alto risco e/ou cidade de fronteira.

4.3.2. Monitoramento de Operações



A **Bitrust** realiza o monitoramento de todas as movimentações realizadas em seu serviço de custódia digital, realizando o processo de “Conheça a sua Transação” (“Know Your Transaction” - KYT), dessa forma é possível identificar movimentações que apresentam algum tipo de irregularidade. As informações monitoradas são de caráter sigiloso e de acesso restrito das áreas responsáveis pelos processos e da Diretoria, sendo esta responsável pela guarda delas.

Na hipótese de indício ou certeza de que qualquer operação, desvia do objetivo da operação ou que o conjunto de operações se constitui ou está relacionado à lavagem de dinheiro ou ao financiamento de terrorismo, a área de Compliance deverá ser comunicada imediatamente.

4.3.3. Comunicação de Ocorrências e Situações Suspeitas

A documentação e as informações que amparam a tomada de decisão de efetuar ou não as comunicações serão formalizadas com o devido acompanhamento da área de Compliance. O dossiê com a documentação e as informações obtidas nas análises poderá conter um conjunto de documentos que amparam a decisão a exemplo de:

- Registro da ocorrência;
- Dossiê do KYC;
- Ficha cadastral e documentação apresentada pelo cliente;
- Relatório de movimentação contendo posições detidas na Instituição e registro de operações e serviços prestados aos clientes;
- E-mail de comunicação entre as áreas envolvidas; e
- Outros documentos que amparam a tomada de decisão.

A **Bitrust** comunicará ao COAF, após a efetiva análise da ocorrência, qualquer transação que apresentar indícios de lavagem ou ocultação de bens, direitos e valores. A legislação impõe ainda à **Bitrust** abster-se de fornecer, aos respectivos clientes, informações sobre eventuais comunicações efetuadas em decorrência de indícios de crime de lavagem de dinheiro e o financiamento do terrorismo.

Em caso de não ocorrência de transações passíveis de comunicação ao COAF, deve-se realizar uma “Declaração Negativa” na periodicidade e forma definidas pelo órgão regulador.

4.3.4. Controles e Avaliação Interna de Riscos

A **Bitrust** atentar-se, de maneira efetiva, quando do cadastramento, monitoramento ou da revisão cadastral do cliente e de suas movimentações, se há indícios de crime, ou suspeitas de atividades ilícitas, nas seguintes situações:



- As movimentações cujos valores se apresentem incompatíveis com a ocupação profissional, os rendimentos e/ou a situação patrimonial/financeira de quaisquer das partes envolvidas, tomando-se por base as informações cadastrais respectivas;
- As movimentações que evidenciem oscilação significativa em relação ao volume e/ou frequência de negócios de quaisquer das partes envolvidas;
- As movimentações cujas características e/ou desdobramentos evidenciem atuação, de forma contumaz, em nome de terceiros; e
- Aquelas movimentações que evidenciem mudança repentina e objetivamente injustificada relativamente às modalidades operacionais usualmente utilizadas pelos envolvidos.

Em especial atenção, os clientes que se enquadram em uma ou mais situações descritas abaixo:

- Movimentações cujas características, pela falta de fundamento econômico ou legal, indiquem risco de ocorrência dos crimes previstos na legislação de lavagem de dinheiro e financiamento do terrorismo, ou com eles relacionados;
- Propostas de início de relacionamento e operações com PEP's de nacionalidade brasileira e as oriundas de países com os quais o Brasil possua elevado número de transações financeiras e comerciais, fronteiras comuns ou proximidade étnica, linguística ou política;
- Clientes em que não seja possível identificar o beneficiário final quando aplicável;
- Transações com clientes oriundos de países que aplicam insuficientemente as recomendações do GAFI; e
- Situações em que não seja possível manter atualizadas as informações cadastrais de seus clientes.

5. TREINAMENTO E ACULTURAMENTO

O treinamento periódico sobre o Programa Prevenção à Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo, ocorrerá de acordo com a programação definida anualmente pela área de Compliance, e deverá abordar:

- O que é a lavagem de dinheiro e financiamento ao terrorismo e seus riscos, tanto para a Instituição quanto para os seus colaboradores;
- Exemplificar a lavagem de dinheiro e o financiamento do terrorismo para que possam ser reconhecidas operações e atividades incomuns;
- Conhecer as políticas e os processos da Instituição, bem como os requerimentos legais relacionados à prevenção da lavagem de dinheiro e ao combate de financiamento do terrorismo; e
- Indicar os procedimentos a serem adotados diante de transações suspeitas.



A instituição aplicará treinamentos contínuos destacando a regulamentação de PLDFT, sob os pontos de vista teórico e prático. Até o final de cada exercício, os novos profissionais que ainda não passaram pelo treinamento ou os profissionais que estão em período de renovação passarão pelo processo.

6. PENALIDADES

O descumprimento desta Política sujeita os infratores às ações disciplinares e legais cabíveis. A negligência e a falha voluntária são também consideradas descumprimento desta Política, sendo passíveis de aplicação de medidas disciplinares.

7. DISPOSIÇÕES FINAIS

A Instituição se compromete a submeter seus conteúdos e suas práticas a processos de avaliação e revisão periódicos.

Quaisquer dúvidas, esclarecimentos ou exceções sobre a aplicação desta Política poderão ser enviadas para a área de Compliance.

8. REFERÊNCIAS

Lei nº 9.613, alterada pela Lei 12.683/12	Dispõe sobre lavagem de dinheiro e financiamento do terrorismo.
Lei 13.260/16	Disciplina o terrorismo, tratando de disposições investigatórias e processuais e reformulando o conceito de organização terrorista.
Resolução nº 10/01 do Ministério da Fazenda - COAF	Dispõe sobre os procedimentos a serem observados pelas pessoas jurídicas não financeiras prestadoras de serviços de transferência de numerário.





