Política de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa (PLD/FTP)

AZIMUT BRASIL
Versão 11

azimut

Conteúdo

1. Introdução

A **AZIMUT BRASIL ("AZBR")**, em conformidade com as diretrizes do Grupo Azimut, estabeleceu a presente Política de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo, aplicável a todas as instituições integrantes do Grupo Azimut no Brasil, bem como, indistintamente, a todos os seus Colaboradores, terceirizados, correspondentes e demais pessoas que mantenham vínculo com a Azimut.

Todos os abrangidos por esta Política têm o dever de identificar, monitorar e reportar eventuais situações de potencial conflito de interesseque possam surgir no exercício de suas atividades, contribuindo para a preservação da integridade, transparência e conformidade nas relações institucionais e profissionais.

2. Objetivo

A Política de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e ao Financiamento da Proliferação de Armas de Destruição em Massa tem como objetivo estabelecer as diretrizes, responsabilidades e controles adotados pela **AZBR** para prevenir, identificar, monitorar, tratar e reportar situações que possam representar indícios de lavagem de dinheiro, financiamento do terrorismo, financiamento da proliferação de armas de destruição em massa, violação de sanções ou outras práticas ilícitas.

3. Definições

ABR - Abordagem Baseada em Risco: metodologia utilizada para identificar, avaliar, classificar, monitorar e mitigar riscos de PLD/FTP de forma proporcional à natureza, porte, complexidade e perfil de risco das atividades da AZBR.

AIR - Avaliação Interna de Risco: processo periódico de identificação e avaliação dos riscos de PLD/FTP aos quais a AZBR está exposta, considerando clientes, produtos, serviços, operações, canais, contrapartes, terceiros, jurisdições, novas tecnologias e ativos virtuais.

ANBIMA - Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais: autorreguladora do mercado financeiro.

Ativos Virtuais: representação digital de valor que pode ser negociada ou transferida por meios eletrônicos e utilizada para pagamentos, investimentos ou outras finalidades permitidas pela regulamentação aplicável.

B3: Bolsa de valores brasileira: onde são negociados ativos como ações, fundos, derivativos e títulos.

BACEN - Banco Central do Brasil: órgão responsável por regular e supervisionar o sistema financeiro nacional.

Beneficiário Final: pessoa natural que, em última instância, possui, controla ou influencia significativamente cliente, contraparte, estrutura societária, veículo de investimento ou operação.

Blockchain Analytics: ferramenta ou processo utilizado para apoiar a análise, rastreabilidade e monitoramento de transações envolvendo ativos virtuais, *wallets*, endereços, entidades e demais fatores de risco.

Bridges: Protocolos que permitem transferir ativos virtuais entre diferentes redes blockchain.

Cloud: Serviços de computação em nuvem usados para armazenamento, processamento e operação de sistemas.

COAF: Conselho de Controle de Atividades Financeiras, unidade de inteligência financeira responsável por receber, examinar e identificar ocorrências suspeitas de atividades ilícitas, nos termos da legislação aplicável.

Colaborador(es): todos os que atuam em nome ou representação da Azimut, incluindo acionistas, sócios, administradores, conselheiros, diretores, empregados, estagiários, aprendizes, terceirizados, correspondentes e demais pessoas abrangidas por esta Política.

Compliance: Área responsável por garantir conformidade com leis, normas, políticas internas e boas práticas.

Contraparte: pessoa natural ou jurídica, instituição, parceiro, fornecedor, prestador de serviço ou terceiro relevante que mantenha relação operacional, comercial, contratual ou transacional com a Azimut.

CVM - Comissão de Valores Mobiliários: órgão que regula e fiscaliza o mercado de valores mobiliários no Brasil.

CSNU: Conselho de Segurança das Nações Unidas.

Custódia de ativos virtuais: serviço de guarda e controle dos instrumentos que permitam o exercício de direitos relativos aos ativos virtuais, incluindo controles sobre carteiras, chaves, movimentações, registros e conciliações.

DTVM - Distribuidora de Títulos e Valores Mobiliários: instituição autorizada a intermediar operações no mercado financeiro.

Due Diligence: Processo de análise e verificação de informações para avaliar riscos antes ou durante uma relação comercial.

Exchanges: Plataformas utilizadas para compra, venda, troca ou custódia de ativos virtuais.

FEBRABAN - Federação Brasileira de Bancos: entidade representativa do setor bancário brasileiro.

Financiamento do Terrorismo - FT: disponibilização, movimentação ou utilização de recursos, bens ou valores, direta ou indiretamente, com a finalidade de financiar atos terroristas, organizações terroristas ou pessoas a elas relacionadas.

Financiamento da Proliferação de Armas de Destruição em Massa — FPADM: disponibilização, movimentação ou utilização de recursos, bens ou valores destinados, direta ou indiretamente, à proliferação de armas nucleares, químicas, biológicas ou outros meios de destruição em massa, conforme regulamentação aplicável.

GAFI/FATF: Grupo de Ação Financeira Internacional, organismo internacional responsável por emitir recomendações e padrões globais de prevenção à lavagem de dinheiro, ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa.

Hash: Código único gerado para identificar uma transação ou informação em ambiente digital ou blockchain.

Head of Compliance: Profissional responsável por liderar a área de Compliance e supervisionar o cumprimento de normas.

KYC — Conheça seu Cliente: conjunto de procedimentos destinados à identificação, qualificação, classificação de risco, atualização cadastral e monitoramento de clientes.

KYE — Conheça seu Colaborador: conjunto de procedimentos destinados à análise, avaliação e monitoramento de colaboradores, conforme suas funções e exposição a riscos.

KYP — Conheça seu Parceiro: conjunto de procedimentos destinados à análise e avaliação de parceiros comerciais, contrapartes e demais terceiros relevantes.

KYS — Conheça seu Fornecedor/Prestador de Serviço: conjunto de procedimentos destinados à análise, seleção, contratação e monitoramento de fornecedores e prestadores de serviços.

KYT — Conheça sua Transação: conjunto de procedimentos destinados ao monitoramento, análise e classificação de risco de operações e transações, incluindo, quando aplicável, informações financeiras, transacionais, on-chain e comportamentais.

Lavagem de Dinheiro — LD: processo de ocultação ou dissimulação da natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente, de infração penal.

LGPD - Lei Geral de Proteção de Dados: norma brasileira que regula o tratamento de dados pessoais.

Mixers: Ferramentas que dificultam o rastreamento da origem e destino de ativos virtuais.

On-chain: Operação registrada diretamente em uma rede blockchain.

PEP — Pessoa Exposta Politicamente: pessoa natural que desempenha ou tenha desempenhado função pública relevante, no Brasil ou no exterior, bem como seus familiares, estreitos colaboradores e pessoas jurídicas relacionadas, nos termos da regulamentação aplicável.

PLD/FTP: prevenção à lavagem de dinheiro, ao financiamento do terrorismo e, quando aplicável, ao financiamento da proliferação de armas de destruição em massa.

Red flags: Sinais de alerta que indicam possível risco, irregularidade ou atividade suspeita.

Sanções: medidas restritivas impostas por autoridades nacionais ou internacionais, incluindo aquelas relacionadas à indisponibilidade de ativos, restrições operacionais, financeiras ou comerciais.

SPSAV: Sociedade Prestadora de Serviços de Ativos Virtuais, conforme regulamentação do Banco Central do Brasil.

Stablecoins: Ativos virtuais cujo valor busca acompanhar uma moeda ou outro ativo de referência.

SUSEP - Superintendência de Seguros Privados: órgão que regula e fiscaliza o mercado de seguros no Brasil.

TI- Tecnologia da Informação: área responsável por sistemas, infraestrutura e segurança tecnológica.

Token: Código ou credencial digital usado para autenticação, acesso ou representação de ativo.

Wallet ou Carteira de Ativos Virtuais: endereço, conta, solução tecnológica ou mecanismo utilizado para armazenar, controlar, transferir ou movimentar ativos virtuais.

Originador: pessoa natural ou jurídica que emite a instrução de transferência de ativos virtuais ou de recursos e que, conforme aplicável, é titular da conta, wallet ou carteira de origem da transação.

Beneficiário de transferência de ativos virtuais: pessoa natural ou jurídica destinatária da transferência de ativos virtuais ou de recursos e que, conforme aplicável, é titular da conta, wallet ou carteira de destino da transação.

PSAV: prestadora de serviços de ativos virtuais, autorizada ou sujeita ao regime regulatório aplicável, que participe da prestação de serviços relacionados a ativos virtuais.

Travel Rule: obrigação regulatória aplicável a transferências de ativos virtuais, destinada à coleta, validação, transmissão, recepção, verificação e guarda de informações de originadores e beneficiários das transações, conforme regulamentação vigente.

Carteira não custodial: carteira de ativos virtuais sob controle direto de seu titular, sem custódia ou intermediação por prestadora de serviços de ativos virtuais.

Mecanismos de ofuscação: recursos, protocolos ou ferramentas que dificultam a identificação, rastreabilidade, investigação ou monitoramento da origem, destino ou titularidade de ativos virtuais, incluindo, conforme aplicável, mixers, tumblers, embaralhadores ou instrumentos similares.

4. Diretrizes

4.1 Abordagem Baseada em Risco (ABR) e Avaliação Interna de Risco (AIR)

A Azimut adota a Abordagem Baseada em Risco - ABR, que possibilita identificar, avaliar, compreender, monitorar e mitigar os riscos de LD/FTP aos quais esteja sujeita no desenvolvimento de suas atividades. Esta abordagem assegura que as medidas de prevenção e combate implementadas sejam proporcionais aos riscos identificados no processo de aceitação, monitoramento e manutenção de relacionamento.

A ABR constitui diretriz central do Programa de PLD/FTP da Azimut e assegura que os procedimentos, controles internos, medidas de diligência, monitoramento e mitigação sejam proporcionais à natureza, ao porte, à complexidade, ao perfil de risco e ao modelo de atuação da instituição.

A Azimut realiza Avaliação Interna de Risco – AIR, considerando suas atividades, produtos, serviços, canais de distribuição, ambientes de negociação, base de clientes, contrapartes, parceiros, prestadores de serviços, fornecedores, áreas geográficas de atuação, novas tecnologias, modelos de negócio emergentes e operações envolvendo ativos virtuais.

No contexto da atuação da Azimut como prestadora de serviços de ativos virtuais, nas modalidades de intermediação e custódia, a avaliação considera os riscos associados a ativos virtuais, *wallets*, *stablecoins*, transferências *on-chain*, *exchanges*, custodiantes ou subcustodiantes, ferramentas de *blockchain analytics*, protocolos descentralizados, *mixers*, *bridges*, jurisdições de maior risco e sanções.

A Avaliação Interna de Risco será conduzida com base em metodologia que compreende, no mínimo, as seguintes etapas:

- **Identificação do risco inerente:** identificação dos riscos atuais e potenciais aos quais a Azimut está exposta, considerando informações internas e fontes externas relevantes;
- **Análise de vulnerabilidades:** avaliação da adequação da estrutura organizacional, das medidas preventivas e dos mecanismos de monitoramento em relação aos riscos identificados;
- **Determinação do risco residual:** avaliação do nível de risco remanescente, considerando o risco inerente e a efetividade das medidas de prevenção, detecção, monitoramento e mitigação adotadas;
- **Ação corretiva e aprimoramento contínuo**: definição e implementação de planos de ação, medidas adicionais de controle para a prevenção e a mitigação dos riscos de lavagem de dinheiro, financiamento do terrorismo e exposição a sanções.

4.2 Identificação e Classificação de Risco

A Azimut identifica, avalia e classifica os riscos de LD/FTP com base em critérios internos, abordagem baseada em risco e diretrizes estabelecidas na Avaliação Interna de Risco.

A classificação de risco é aplicada, conforme o caso, a clientes, beneficiários finais, empregados, prestadores de serviços terceirizados, fornecedores, parceiros, contrapartes, produtos, serviços, operações, canais de distribuição, ambientes de negociação, ativos analisados e demais elementos sujeitos à avaliação de PLD/FTP.

Na avaliação e classificação de risco, a Azimut considera, no mínimo, os seguintes fatores:

- Clientes e beneficiários finais: perfil cadastral, atividade econômica, estrutura societária, beneficiário final, condição de PEP, cliente não residente, histórico reputacional, exposição a sanções e compatibilidade econômico-financeira.
- Operações: volume de transações, valores envolvidos, frequência, finalidade econômica e identificação de operações atípicas ou incompatíveis com o perfil do cliente.
- Produtos, serviços e canais: natureza, complexidade, forma de contratação, canais de distribuição e características dos produtos e serviços oferecidos, bem como o público-alvo a que se destinam.
- Contrapartes, terceiros e jurisdições: perfil e localização de contrapartes, parceiros, *exchanges*, custodiantes, subcustodiantes, fornecedores e prestadores de serviços, especialmente quando relacionados a países ou territórios de maior risco.
- Ativos virtuais: tipo de ativo virtual, rede ou *blockchain* utilizada, *wallet* de origem ou destino, titularidade da *wallet*, origem dos recursos e dos ativos virtuais, bem como exposição a fatores de risco identificados por ferramenta de *blockchain analytics* ou processo equivalente.

Com base nesses critérios, os clientes e demais elementos avaliados são classificados, no mínimo, como risco baixo, médio ou alto. A classificação orienta o nível de diligência, monitoramento, atualização cadastral e eventuais medidas de restrição, bloqueio ou encerramento de relacionamento.

As análises reputacionais e cadastrais são renovadas, em regra, nos seguintes prazos:

- **Risco Alto: atualização anual;**
- **Risco Médio: atualização a cada dois anos;**
- **Risco Baixo: atualização a cada três anos.**

A periodicidade pode ser reduzida diante de alterações relevantes no cadastro, perfil transacional, beneficiário final, exposição a sanções, mídia negativa ou riscos relacionados a ativos virtuais, contrapartes ou jurisdições de maior risco.

4.3 Monitoramento Contínuo

A Azimut realiza monitoramento contínuo de clientes, beneficiários finais, contrapartes, terceiros relevantes, operações, transações e situações atípicas, de forma compatível com a classificação de risco atribuída e com a abordagem baseada em risco adotada pela instituição.

O monitoramento pode incluir, conforme aplicável, triagens em listas restritivas, sanções, PEP e mídia negativa, acompanhamento de operações financeiras e transacionais, análise de alertas gerados por sistemas internos ou ferramentas especializadas, inclusive blockchain analytics, solicitação de informações adicionais e escalonamento de situações relevantes à área de Compliance, à Comissão de PLD/FTP ou à Diretoria responsável.

Diante de indícios de irregularidade, incompatibilidade com o perfil de risco, exposição a sanções, ausência de informações ou suspeita de LD/FTP, a Azimut poderá adotar medidas proporcionais ao risco, incluindo diligência reforçada, restrição operacional, bloqueio preventivo, retenção, recusa de operação, encerramento de relacionamento ou comunicação às autoridades competentes, conforme aplicável.

4.4 *Due Diligence* de Contrapartes e Terceiros Relevantes

A Azimut adota procedimentos de due diligence de contrapartes, parceiros, fornecedores, prestadores de serviço e terceiros relevantes, de forma proporcional ao risco, à natureza da relação, à criticidade do serviço prestado e à exposição regulatória, operacional, reputacional, tecnológica e de PLD/FTP.

A análise pode abranger, conforme aplicável, identificação cadastral, estrutura societária, beneficiários finais, reputação, sanções, mídia negativa, situação regulatória, histórico de incidentes, controles de PLD/FTP, segurança da informação, proteção de dados, capacidade operacional, obrigações contratuais e aderência aos requisitos legais e regulatórios aplicáveis.

No contexto da prestação de serviços de ativos virtuais, a Azimut aplica diligência reforçada a terceiros críticos, incluindo exchanges, provedores de liquidez, custodiantes, subcustodiantes, provedores de wallet, ferramentas de blockchain analytics, prestadores de tecnologia, cloud e demais participantes relevantes da cadeia operacional.

A Azimut poderá solicitar informações adicionais, revisar a classificação de risco, restringir, suspender ou encerrar o relacionamento quando identificar riscos incompatíveis com esta Política, com os procedimentos internos ou com a regulamentação aplicável. As análises, decisões e evidências devem ser registradas e arquivadas conforme os procedimentos internos.

4.5 Informações sobre Transferências de Ativos Virtuais

Nas operações envolvendo ativos virtuais, a Azimut DTVM adota controles para coleta, registro, verificação, armazenamento e, quando aplicável, transmissão de informações relativas ao originador e ao beneficiário da operação, observada a regulamentação aplicável.

Esses controles devem ser executados de forma integrada aos procedimentos de Travel Rule, KYC, KYT, sanções, monitoramento transacional, prevenção a fraudes, segurança da informação e proteção de dados pessoais.

A ausência, inconsistência ou insuficiência de informações relacionadas à transferência de ativos virtuais, bem como operações envolvendo carteiras não custodiais, contrapartes de maior risco, mecanismos de ofuscação, endereços suspeitos ou exposição relevante a ilícitos, poderá ensejar diligência adicional, limitação operacional, retenção, bloqueio preventivo, recusa, devolução, escalonamento interno ou comunicação às autoridades competentes, conforme a abordagem baseada em risco e os procedimentos internos aplicáveis.

A Azimut DTVM manterá Procedimento Operacional de Travel Rule para disciplinar responsabilidades, campos mínimos, fluxos de transmissão e recepção, validações, autodeclarações, tratamento de carteiras não custodiais, retenções, bloqueios preventivos, comunicações, guarda de evidências e prazos regulatórios aplicáveis.

4.6 Pessoa Exposta Politicamente (PEP)

A Azimut adota procedimentos para identificação, análise e monitoramento de Pessoas Expostas Politicamente — PEP, bem como de seus familiares, estreitos colaboradores e pessoas jurídicas relacionadas, conforme a regulamentação aplicável.

A identificação de PEP é considerada fator relevante na classificação de risco e pode ensejar diligência reforçada, monitoramento mais próximo e aprovação em alçada competente, de acordo com a abordagem baseada em risco adotada pela Azimut.

4.7 Operações e Situações Suspeitas

A Azimut considera como potenciais indícios de LD/FTP as operações, propostas de operações ou situações que apresentem incompatibilidade com o perfil cadastral, econômico-financeiro, transacional ou reputacional do cliente, contraparte ou terceiro relacionado.

Entre outros fatores, são considerados sinais de alerta:

- impossibilidade de manter informações cadastrais atualizadas ou de identificar o beneficiário final;
- incompatibilidade entre renda, patrimônio, faturamento, atividade econômica, objeto social ou perfil declarado e as operações realizadas;
- operações sem fundamento econômico ou legal aparente, fracionamento, alteração abrupta de padrão transacional ou tentativa de burlar controles internos;
- movimentações envolvendo terceiros, contas, wallets ou estruturas sem justificativa plausível;
- operações com pessoas, entidades, wallets, contrapartes ou jurisdições sujeitas a sanções, listas restritivas, mídia negativa ou deficiências relevantes de PLD/FTP;
- exposição a PEP, processos, notícias desabonadoras ou registros reputacionais relevantes;
- operações envolvendo ativos virtuais, wallets, exchanges, bridges, mixers, tumblers, protocolos descentralizados, stablecoins ou transações on-chain incompatíveis com o perfil do cliente ou com exposição relevante a fatores de risco.

4.8 Identificação e Tratamento de Alertas

Os alertas, comunicações internas, operações atípicas ou situações suspeitas devem ser analisados pela área de Compliance ou pelas áreas competentes, conforme a natureza do caso, de forma diligente, sigilosa, documentada e proporcional ao risco identificado.

A análise pode envolver verificação cadastral, reputacional, econômico-financeira, transacional e operacional, consulta a sistemas internos, listas restritivas, ferramentas de monitoramento ou blockchain analytics, solicitação de informações adicionais e avaliação da compatibilidade da operação com o perfil do cliente, contraparte ou terceiro.

Com base na análise realizada, a Azimut poderá arquivar o alerta, aplicar diligência reforçada, restringir ou limitar operações, reter ou bloquear preventivamente transações, recusar ou devolver operações, encerrar relacionamento, escalonar o caso às instâncias competentes ou realizar comunicação às autoridades, conforme aplicável.

Os alertas e situações atípicas devem ser tratados nos prazos regulatórios e internos aplicáveis, observada a vedação de comunicação ao cliente ou a terceiros sobre eventual análise, investigação ou reporte.

A Azimut comunicará tempestivamente ao Banco Central do Brasil, quando aplicável, eventuais dificuldades relevantes de controle ou monitoramento de operações com ativos virtuais decorrentes de práticas adotadas por outras instituições autorizadas, especialmente quando tais práticas comprometerem a identificação, rastreabilidade, análise ou mitigação dos riscos de PLD/FTP.

4.9 Ausência ou Desatualização de Informações Cadastrais

Quando forem identificadas informações cadastrais ausentes, desatualizadas, inconsistentes ou insuficientes, a Azimut poderá solicitar atualização cadastral, documentos adicionais ou esclarecimentos ao cliente.

Enquanto não forem sanadas as inconsistências, a Azimut poderá restringir novas operações, limitar movimentações, submeter o caso à análise de *Compliance*, aplicar diligência reforçada ou avaliar a manutenção do relacionamento, conforme a abordagem baseada em risco.

Nos casos envolvendo ativos virtuais, a ausência de informações sobre titularidade de *wallet*, origem dos recursos, origem dos ativos virtuais ou finalidade econômica da operação poderá ensejar restrição, bloqueio ou recusa da operação.

4.10 Sanções e Indisponibilidade de Ativos

A Azimut adota procedimentos para identificação, monitoramento e tratamento de pessoas, entidades, operações, ativos ou *wallets* sujeitos a sanções nacionais ou internacionais, incluindo sanções impostas pelo Conselho de Segurança das Nações Unidas e demais listas aplicáveis.

Quando identificada obrigação de indisponibilidade de ativos ou restrição legal ou regulatória, a Azimut adota as providências cabíveis, sem aviso prévio ao cliente ou à parte envolvida, observando a legislação aplicável, os procedimentos internos e as comunicações exigidas às autoridades competentes.

No contexto de ativos virtuais, os procedimentos de sanções podem abranger clientes, beneficiários finais, contrapartes, exchanges, *wallets*, endereços, transações *on-chain* e demais entidades identificadas por ferramentas de monitoramento ou *blockchain analytics*.

A Azimut poderá consultar, utilizar ou compartilhar informações relativas a listas de suspeição e listas restritivas, nos termos da legislação e regulamentação aplicáveis, inclusive no âmbito do Sistema Financeiro Nacional, do Sistema de Pagamentos Brasileiro e do mercado de ativos virtuais.

4.11 Comunicação ao Coaf

Após a análise de operações, propostas de operações ou situações atípicas, caso a área de Compliance conclua pela existência de indícios de LD/FTP, violação de sanções ou demais situações sujeitas a reporte, a comunicação ao Coaf será realizada nos prazos, formas e condições previstos na regulamentação aplicável.

A análise que fundamentar a comunicação deve ser registrada e conter, quando aplicável, a descrição dos sinais de alerta identificados, as características da operação, as diligências realizadas, as informações obtidas, a identificação das partes envolvidas, a exposição a PEP, sanções ou ativos virtuais e a conclusão fundamentada da suspeição.

Nas situações envolvendo ativos virtuais, a análise poderá incluir informações adicionais, como ativo virtual envolvido, rede ou blockchain utilizada, wallet de origem ou destino, hash da transação, exposição a entidades de risco, resultado de blockchain analytics, dados de Travel Rule e demais evidências disponíveis.

A Azimut observa o dever de sigilo e a vedação de comunicação ao cliente ou a terceiros sobre eventual análise, decisão ou comunicação ao Coaf.

5. Tratamento de Dados Pessoais

Os procedimentos de segurança da informação e proteção de dados são mantidos atualizados e compatíveis com o tipo de dados pessoais tratados, em conformidade com a legislação e regulamentação brasileira aplicável à privacidade e à proteção de dados pessoais, especialmente a Lei nº 13.709, de 14 de agosto de 2018 (“Lei Geral de Proteção de Dados Pessoais” ou “LGPD”).

Os dados pessoais são utilizados apenas para finalidades legítimas e compatíveis com sua coleta, incluindo o cumprimento de obrigações legais e regulatórias relacionadas à prevenção à lavagem de dinheiro, ao financiamento do terrorismo e demais ilícitos. O tratamento de dados pessoais observa as diretrizes da Política Interna de Proteção de Dados Pessoais e da Política de Privacidade da Azimut, incluindo medidas técnicas e organizacionais destinadas a prevenir acesso não autorizado, vazamentos, perdas, destruição ou tratamento indevido.

A Azimut mantém registros das operações de tratamento aplicáveis, avalia riscos relacionados à proteção de dados pessoais e assegura meios para o exercício dos direitos dos titulares, conforme a legislação vigente.

6. Responsabilidades

6.1 Governança Corporativa

O Grupo Azimut mantém uma estrutura de governança compatível com suas atividades, com definição clara de funções e responsabilidades relacionadas à PLD/FTP

A governança de PLD/FTP é promovida por meio de:

- Atribuição formal de responsabilidades às áreas envolvidas no Programa de PLD/FTP e no cumprimento de sanções; designação de um Diretor responsável pelo cumprimento normativo (*Head of Compliance*), supervisionado pelo Conselho de Administração;
- disseminação de cultura de conformidade, integridade e prevenção a ilícitos em todas as áreas da instituição; estabelecimento de fluxos de reportes, garantindo canais eficazes para comunicar atividades suspeitas, incidentes ou violações, promovendo uma comunicação transparente e oportuna; e
- garantia de recursos humanos competentes e tecnologia adequada para a implementação eficaz das políticas de PLD/FT, incluindo treinamento contínuo, atualizações tecnológicas e supervisão adequada para assegurar a conformidade constante com as regulamentações aplicáveis.

6.2 Funções e responsabilidade do Conselho de Administração

O Conselho de Administração aprova e avalia periodicamente as direções estratégicas e as políticas de governança de riscos relacionadas à lavagem de dinheiro e ao financiamento do terrorismo. Especialmente, o Conselho de Administração:

- Estabelece e adota uma Política que delineia e justifica as decisões referentes a aspectos relevantes das estruturas organizacionais, procedimentos internos e controles, verificação de dados apropriada e retenção, de acordo com o princípio da proporcionalidade e a exposição real aos riscos de LD/FT;
- Define o apetite de risco de LD/FT da empresa;
- Garante regularmente que os riscos de LD/FT aos quais a empresa está exposta estejam alinhados com o seu apetite de risco de LD/FT;
- Estabelece a função do Departamento de *Compliance*, definindo suas tarefas, responsabilidades e métodos de coordenação e colaboração com outras funções de controle corporativo, mantendo um papel de supervisão sobre essa função;
- Define e aprova diretrizes para um sistema abrangente e coordenado de controle interno destinado a detectar e gerenciar prontamente o risco de lavagem de dinheiro, garantindo sua eficácia contínua;
- Define e aprova princípios para gerenciar relacionamentos com clientes classificados como "alto risco";
- Nomeia e demite o Diretor de *Compliance*;
- Garante que tarefas e responsabilidades relacionadas à lavagem de dinheiro e ao financiamento do terrorismo (LD/FT) sejam claramente e adequadamente alocadas, com funções operacionais e de controle separadas e dotadas de recursos qualitativos e quantitativos;
- Garante a implementação de um fluxo de informações adequado, abrangente e oportuno entre órgãos corporativos e funções de controle;
- Garante a confidencialidade no âmbito do procedimento de reporte de transações suspeitas;
- Revisa anualmente relatórios sobre as atividades conduzidas pelo *Head of Compliance* e os controles realizados por funções relevantes, bem como o documento sobre os resultados da autoavaliação de risco de lavagem de dinheiro;
- É responsável por tomar todas as medidas necessárias para garantir a eficácia da organização e dos controles implementados para o cumprimento do quadro aplicável de LD/FT;
- Garante que deficiências e anomalias identificadas em vários níveis de controles sejam prontamente levadas à sua atenção e promove a adoção de medidas corretivas adequadas, avaliando sua eficácia;
- Supervisiona a aderência às regulamentações e a minúcia, eficácia e suficiência dos sistemas de controle contra lavagem de dinheiro;
- Garante a implementação de um sistema de controle interno que permita a detecção e gerenciamento oportunos de riscos de LD/FT, garantindo sua eficácia contínua com base nos resultados do exercício de autoavaliação de risco;
- Implementa ferramentas apropriadas para verificar as atividades dos funcionários a fim de detectar quaisquer anomalias que possam surgir, especialmente no comportamento, na qualidade das comunicações direcionadas a representantes e estruturas da empresa, bem como interações com clientes;

- Garante a adoção de Procedimentos de TI específicos para o cumprimento das regulamentações contra lavagem de dinheiro em casos de operações remotas (por exemplo, realizadas por meio de canais digitais).

6.3 Departamento de *Compliance* e responsabilidades

Compete à área de *Compliance* implementar, supervisionar e aprimorar continuamente a Política de prevenção à lavagem de dinheiro, ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa (PLD/FTP), bem como os procedimentos e controles internos a ela relacionados, bem como identificar a regulamentação aplicável e avaliar seus impactos sobre os processos e procedimentos internos:

- implementar, acompanhar e submeter à anuência dos membros do Comitê de Riscos e *Compliance* eventuais atualizações normativas e atividades de controle regulatório;
- submeter à anuência dos membros da Comissão de PLDFT análises reputacionais de clientes classificados como de alto risco;
- promover a conscientização dos vinculados quanto à importância das atividades de prevenção à lavagem de dinheiro e de combate ao financiamento do terrorismo;
- analisar a efetividade desta Política, bem como dos procedimentos e controles internos a ela associados, propondo melhorias contínuas;
- identificar a regulamentação aplicável e avaliar seus impactos sobre os processos e procedimentos internos;
- colaborar na definição e no aprimoramento do sistema de controles internos voltado à prevenção e ao combate aos riscos de LD/FT;
- verificar continuamente a adequação do processo de gerenciamento de riscos de LD/FT, propondo ajustes organizacionais e procedimentais sempre que necessário;
- realizar verificações quanto à funcionalidade dos processos de reporte e à adequação das avaliações realizadas pela primeira linha de defesa em relação às operações dos clientes;
- auxiliar na definição e atualização das políticas relacionadas ao gerenciamento dos riscos de LD/FT e às diferentes etapas do processo de gestão de riscos;
- participar, em conjunto com outras funções corporativas relevantes, da autoavaliação anual dos riscos de lavagem de dinheiro enfrentados pela instituição;
- prestar suporte e assessoria aos órgãos corporativos e ao Conselho de Administração;
- fornecer relatórios periódicos sobre o andamento das atividades aos órgãos corporativos e ao Conselho de Administração;
- realizar atividades de *due diligence* de clientes e de monitoramento, conforme previsto nesta Política;
- avaliar os riscos de LD/FT associados à introdução de novos produtos e serviços;
- verificar a confiabilidade dos sistemas de informação, assegurando conformidade com as obrigações de *due diligence*, retenção de dados e comunicação de operações suspeitas;

- comunicar à autoridade pública competente, inclusive ao Conselho de Controle de Atividades Financeiras (COAF), inconsistências cadastrais, operações ou situações suspeitas, notícias desabonadoras envolvendo clientes ou vinculados, bem como atender comunicações e requisições de órgãos reguladores, conforme a regulamentação aplicável;
- elaborar o Relatório Anual de Avaliação Interna de Riscos, nos termos da Resolução nº 50 da CVM e alterações posteriores;
- elaborar o Relatório Anual de Avaliação de Efetividade, conforme exigido pela Circular nº 3.978, de 23 de janeiro de 2020, do Banco Central do Brasil, e suas alterações, avaliando a efetividade da Política, dos procedimentos e dos controles internos;
- auxiliar, em coordenação com outras funções corporativas, na elaboração e implementação de um plano de treinamento contínuo para os colaboradores;
- relatar prontamente aos órgãos corporativos quaisquer violações ou deficiências relevantes identificadas no exercício de suas atribuições;
- desenvolver e apresentar recomendações contínuas para a atualização e o aprimoramento desta Política;
- manter contatos institucionais e de emergência permanentemente atualizados para atendimento de demandas do Banco Central do Brasil e demais autoridades competentes, conforme aplicável.

6.4 Encarregado pelo reporte de transações suspeitas

O Grupo Azimut designa o Diretor de Compliance como encarregado pelo reporte de transações, operações ou situações suspeitas relacionadas à prevenção à lavagem de dinheiro, ao financiamento do terrorismo, ao financiamento da proliferação de armas de destruição em massa e ao cumprimento de sanções.

O encarregado atua com independência, autoridade, autonomia de julgamento e observância às obrigações de confidencialidade, sigilo e vedação de comunicação ao cliente ou a terceiros sobre eventual análise, investigação ou reporte realizado às autoridades competentes.

6.4.1 Procedimentos de Comunicação e Tratamento de Ocorrências

As denúncias, comunicações internas, alertas ou ocorrências recebidas pela área de Compliance devem ser tratadas de forma ética, sigilosa, imparcial e documentada, preservada a confidencialidade das informações e a identidade do denunciante, quando aplicável. A Azimut não tolera qualquer forma de retaliação contra pessoas que, de boa-fé, reportem suspeitas, indícios ou ocorrências relacionadas a esta Política.

Após análise interna, caso sejam identificados indícios de lavagem de dinheiro, financiamento do terrorismo, financiamento da proliferação de armas de destruição em massa, violação de sanções ou outras situações sujeitas a reporte regulatório, a comunicação será realizada aos órgãos competentes, nos prazos e formas previstos na regulamentação aplicável.

Quando os indícios não forem confirmados, a ocorrência poderá ser encerrada e arquivada, com o devido registro da análise realizada, das evidências consideradas e da decisão adotada. As informações relacionadas a suspeitas, análises, comunicações e decisões são confidenciais e não devem ser disponibilizadas a clientes, terceiros ou pessoas não autorizadas.

As comunicações realizadas aos órgãos competentes, incluindo o Coaf, não devem ser levadas ao conhecimento do cliente ou de terceiros envolvidos, observada a vedação de tipping-off e os deveres de sigilo previstos na legislação e regulamentação aplicáveis.

Quando as ocorrências envolverem colaboradores, administradores, parceiros comerciais, fornecedores ou prestadores de serviço, a Azimut poderá adotar medidas disciplinares ou contratuais cabíveis, incluindo advertência, suspensão, desligamento, rescisão contratual ou destituição, conforme a gravidade do caso, a legislação aplicável, os normativos internos e o direito de defesa, quando cabível.

Também poderão estar sujeitos a medidas disciplinares os colaboradores que deliberadamente omitirem informações relevantes, deixarem de reportar situações suspeitas ou dificultarem a apuração de ocorrências relacionadas a esta Política.

As decisões sobre medidas disciplinares, comunicações às autoridades, arquivamento ou demais providências relevantes poderão ser submetidas à Comissão de PLD/FTP, ao Comitê de Riscos e Compliance, à Diretoria ou às demais instâncias competentes, conforme a natureza, criticidade e impacto da ocorrência.

6.5 Comitê de Riscos, *Compliance* e Comissão de PLD/FTP

O Comitê de Riscos e *Compliance*, em conjunto com a Comissão de Prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo (PLD/FTP), é responsável pela supervisão, deliberação e tomada de decisões estratégicas relacionadas à gestão de riscos, à conformidade regulatória e à prevenção à lavagem de dinheiro e ao financiamento do terrorismo no âmbito da Azimut.

Compete a essas instâncias:

- aprovar políticas, procedimentos, medidas, orientações corporativas e relatórios periódicos regulatórios;
- assegurar, em nível corporativo, a aderência às diretrizes internas da organização e às regulamentações aplicáveis em matéria de prevenção à lavagem de dinheiro e combate ao financiamento do terrorismo;
- garantir a observância, por vinculados e contrapartes, do Programa de *Compliance* da companhia;
- discutir, analisar e aprovar assuntos relacionados às áreas de *Compliance* e Risco;
- analisar casos classificados como de alto risco, especialmente aqueles que apresentem *red flags* identificadas no processo de monitoramento;
- deliberar sobre decisões a serem adotadas em operações que apresentem indícios de lavagem de dinheiro ou financiamento do terrorismo;
- deliberar sobre a aprovação de cadastros de clientes Pessoas Expostas Politicamente (PEPs) que apresentem mídias negativas, processos desabonadores e/ou ocupem cargos de alta relevância;

- deliberar sobre casos que envolvam mídias negativas, processos sensíveis, presença em listas restritivas ou quaisquer outras informações que representem risco reputacional para a instituição.

6.6 Auditoria

Compete à função de Auditoria, no âmbito da Azimut:

- avaliar de forma independente a aderência da instituição à legislação aplicável, às normas emitidas pelos órgãos reguladores e autorreguladores, bem como às políticas e diretrizes internas;
- revisar e avaliar a efetividade dos controles internos, com foco na mitigação de riscos operacionais, regulatórios e de conformidade;
- realizar testes periódicos sobre processos, procedimentos e controles, inclusive aqueles relacionados à prevenção à lavagem de dinheiro e ao financiamento do terrorismo;
- avaliar a adequação da segregação de funções, com o objetivo de identificar potenciais conflitos de interesse;
- analisar a conformidade dos processos de classificação de riscos, verificando a aderência à metodologia e à matriz de riscos definida pela instituição;
- verificar a consistência e a qualidade das informações utilizadas nos reportes regulatórios;
- acompanhar e apoiar os trabalhos de auditores externos, incluindo o atendimento a demandas, requisições e esclarecimentos;
- identificar deficiências, fragilidades ou não conformidades nos controles e processos auditados;
- recomendar planos de ação corretivos para endereçar as deficiências identificadas e acompanhar sua implementação;
- reportar os resultados das auditorias e avaliações aos órgãos de governança competentes, de forma clara, tempestiva e documentada.

6.7 Jurídico

Compete à área Jurídica:

- analisar os requisitos legais e regulatórios aplicáveis, bem como seus impactos sobre os negócios;
- prestar suporte à área de *Compliance* na interpretação e no entendimento das questões regulatórias relacionadas aos controles de PLDFT e demais temas de *Compliance*;
- apoiar a avaliação de riscos, sob a ótica jurídica, e adotar as providências necessárias para o tratamento de ocorrências envolvendo transações ou operações suspeitas de lavagem de dinheiro;
- participar das discussões e decisões dos Comitês de Prevenção à Lavagem de Dinheiro (PLD) e de Riscos, fornecendo subsídios jurídicos para a deliberação de casos relevantes, especialmente aqueles que envolvam riscos regulatórios, legais ou reputacionais.

7. Análise de *KYC* - Avaliação de Risco e Procedimento de Conheça seu cliente

A Azimut adota procedimento de Conheça seu cliente – *KYC* no início e ao longo do relacionamento comercial, com o objetivo de identificar, qualificar e manter atualizadas as informações cadastrais, econômico-financeiras, reputacionais e transacionais dos clientes, conforme a regulamentação aplicável e a abordagem baseada em risco.

A área de *Compliance* é responsável por analisar as informações e documentos apresentados no processo de *KYC*, avaliar sua suficiência e consistência, solicitar complementações quando necessário e apoiar a classificação de risco do cliente, em conjunto com as áreas responsáveis pelo cadastro e relacionamento. Quando aplicável, a Azimut poderá utilizar processos de cadastro eletrônico, desde que sejam passíveis de verificação e permitam a adequada identificação do cliente, de seus representantes, procuradores, beneficiários finais e demais pessoas relacionadas.

A Azimut avalia, conforme sua metodologia interna e a regulamentação aplicável, se o Cliente se enquadra em critérios de *due diligence* simplificada, regular ou reforçada, considerando seu perfil de risco e eventuais indicadores de maior risco. Além das hipóteses em que a classificação de risco decorra de exigência legal ou regulatória, o Departamento de *Compliance* realiza avaliação adicional dos fatores de risco aplicáveis, com o objetivo de obter uma visão consolidada do perfil do Cliente.

O perfil de risco do Cliente é determinado com base nos seguintes fatores:

- Risco do Cliente, considerando sua natureza, estrutura, idade, atividade econômica, beneficiário final, histórico reputacional, condição de PEP, exposição a sanções, processos e condenações por crimes financeiros e compatibilidade econômico-financeira;
- Risco geográfico, relacionado ao país ou região de residência, domicílio, operação, origem ou destino de recursos, especialmente quando envolver jurisdições de maior risco;
- Risco de produtos, serviços e canais, considerando a natureza, complexidade, forma de contratação, canais utilizados e grau de exposição dos produtos e serviços contratados;
- Risco transacional, considerando volume, frequência, finalidade econômica e compatibilidade das operações com o perfil cadastral e econômico-financeiro do Cliente;
- Risco relacionado a ativos virtuais, quando aplicável, considerando wallets, origem dos recursos, origem dos ativos virtuais, rede ou *blockchain* utilizada, exposição a sanções, *exchanges* não reguladas ou outros fatores identificados por ferramenta de *blockchain analytics* ou processo equivalente.

A cada fator de risco é atribuída uma pontuação, conforme a metodologia de risco adotada pela Azimut, variando de:

- **Baixo risco.**
- **Médio risco.**
- **Alto risco.**

A pontuação geral do risco do Cliente é obtida a partir da soma das pontuações atribuídas a cada um dos fatores de risco mencionados. Com base no resultado, o Cliente é classificado em faixas específicas de risco, as quais determinam:

- o nível de diligência aplicável (simplificada, regular ou reforçada);
- a frequência de atualização cadastral e de *due diligence*;
- o grau de monitoramento contínuo das operações;
- a necessidade de aprovação por instâncias superiores, quando aplicável.

A periodicidade poderá ser reduzida diante de evento relevante, alteração cadastral significativa, mudança de perfil transacional, mídia negativa, exposição a sanções, alteração de beneficiário final ou identificação de risco relevante relacionado a ativos virtuais, contrapartes ou jurisdições de maior risco.

8. Análise de *KYE, KYP e KYS*

A Azimut adota procedimentos de Conheça seu Colaborador — KYE, Conheça seu Parceiro — KYP, e Conheça seu Fornecedor/Prestador de Serviço — KYS de forma proporcional ao risco, à natureza da relação mantida com a instituição, à criticidade da atividade desempenhada e à exposição regulatória, operacional, reputacional e de PLD/FTP.

Esses procedimentos têm como objetivo apoiar a identificação, avaliação, classificação, monitoramento e revisão dos riscos relacionados a colaboradores, parceiros, fornecedores, prestadores de serviço, terceiros relevantes, contrapartes e transações, em complemento aos procedimentos de KYC aplicáveis a clientes e pessoas jurídicas.

As análises podem incluir, conforme aplicável, verificação cadastral, análise reputacional, avaliação de histórico profissional ou societário, estrutura societária, beneficiários finais, situação regulatória, exposição a sanções, PEP, mídias negativas, conflitos de interesse, aderência a padrões de integridade, capacidade operacional, controles de PLD/FTP, segurança da informação, proteção de dados e demais fatores relevantes ao risco da relação.

Nos procedimentos de KYC, KYE, KYP e KYS, a Azimut realiza consultas, conforme aplicável, a listas restritivas e bases nacionais e internacionais voltadas à prevenção à lavagem de dinheiro, ao financiamento do terrorismo, ao financiamento da proliferação de armas de destruição em massa e ao cumprimento de sanções, incluindo listas do CSNU, OFAC, União Europeia, PEP, mídias negativas e outras bases reputacionais, regulatórias ou internas aplicáveis.

No contexto da prestação de serviços de ativos virtuais, as análises podem abranger wallets, endereços, contrapartes, exchanges, provedores de liquidez, custodiantes, subcustodiantes, provedores de wallet, ferramentas de blockchain analytics, prestadores de tecnologia, cloud e demais participantes relevantes da cadeia operacional, especialmente quando classificados como terceiros críticos ou de maior risco.

O monitoramento de transações envolvendo ativos virtuais poderá considerar fatores como origem e o destino dos recursos ou ativos virtuais, titularidade ou declaração de titularidade de wallet, rede blockchain utilizada, exposição a wallets sancionadas, endereços associados a ransomware, darknet, mixers, tumblers, fraudes, golpes, ilícitos on-chain ou outros fatores de risco identificados por ferramenta de blockchain analytics ou processo equivalente.

Quando forem identificadas inconsistências, ausência de informações, exposição relevante a risco ou incompatibilidade com o perfil esperado, a Azimut poderá solicitar informações adicionais, aplicar diligência reforçada, revisar a classificação de risco, limitar ou restringir operações, reter ou bloquear preventivamente transações, suspender ou

encerrar relacionamento, escalonar o caso às instâncias competentes ou realizar comunicação às autoridades, conforme aplicável.

As análises, classificações de risco, revisões, consultas realizadas, decisões e evidências relacionadas a colaboradores, parceiros, fornecedores, prestadores de serviço, terceiros relevantes, contrapartes, transações e ativos virtuais devem ser registradas e arquivadas conforme os procedimentos internos da Azimut e a regulamentação aplicável.

9. Manutenção dos Documentos

A Azimut mantém documentos, dados, registros e evidências relevantes para fins de PLD/FTP, de forma a permitir a prevenção, detecção, monitoramento, análise de operações e atendimento a solicitações de autoridades competentes.

Os registros são mantidos em sistemas ou repositórios adequados, observando critérios de segurança, integridade, autenticidade, rastreabilidade, disponibilidade e proteção contra perda, alteração indevida ou acesso não autorizado.

A Azimut preserva documentos cadastrais, registros de operações, análises, comunicações, decisões, consultas a listas restritivas, sanções, PEP, mídias negativas, relatórios de blockchain analytics e demais evidências relacionadas ao cumprimento das obrigações de PLD/FTP pelo prazo mínimo de 5 anos, contado da realização da operação, do encerramento do relacionamento ou da conclusão da análise, conforme aplicável e nos termos da legislação vigente.

No caso de operações envolvendo ativos virtuais, a Azimut mantém, quando aplicável, registros sobre originador, beneficiário, wallet, ativo virtual, montante, hash da transação, rede blockchain, data, finalidade declarada, autodeclarações, dados de Travel Rule, alertas, análises, decisões e evidências de monitoramento, pelo prazo mínimo de 5 anos, à disposição do Banco Central do Brasil, do Coaf e das demais autoridades competentes.

10. Treinamento

A Azimut realiza treinamentos periódicos em PLD/FTP, compatíveis com as funções e responsabilidades dos colaboradores, com o objetivo de fortalecer a capacidade de identificação, tratamento e reporte de situações suspeitas.

Os treinamentos incluem capacitação inicial para novos colaboradores e reciclagens periódicas, especialmente para áreas com contato direto com clientes, operações e Compliance. Os registros de participação são mantidos pelas áreas responsáveis e ficam disponíveis para fins de controle, auditoria e atendimento a autoridades competentes.

A Azimut poderá disponibilizar conteúdos informativos a clientes, usuários, fornecedores, prestadores de serviços e demais partes relacionadas, com o objetivo de disseminar boas práticas e informações sobre riscos associados às operações com ativos virtuais, incluindo segurança, prevenção a fraudes, golpes, sanções, *wallets*, transferências on-chain e demais temas relevantes.

11. Base Legal

Legislação Federal

- Lei nº 9.613, de 3 de março de 1998
- Lei nº 12.683, de 9 de julho de 2012
- Lei nº 13.260, de 16 de março de 2016
- Lei nº 13.810, de 8 de março de 2019
- Lei nº 13.974, de 7 de janeiro de 2020
- Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD)
- Lei nº 14.478, de 21 de dezembro de 2022
- Decreto nº 11.563, de 13 de junho de 2023

Banco Central do Brasil (BACEN)

- Circular BCB nº 3.978, de 23 de janeiro de 2020
- Carta Circular BCB nº 4.001, de 29 de janeiro de 2020
- Resolução BCB nº 44, de 24 de novembro de 2020
- Resolução BCB nº 131, de 20 de agosto de 2021
- Resolução BCB nº 519, de 10 de novembro de 2025
- Resolução BCB nº 520, de 10 de novembro de 2025
- Resolução BCB nº 521, de 10 de novembro de 2025

Comissão de Valores Mobiliários (CVM)

- Resolução CVM nº 50, de 31 de agosto de 2021

Normas e Padrões Internacionais

- Recomendações do Grupo de Ação Financeira (GAFI/FATF)

12. Disposições Gerais

Este material foi elaborado pela **AZIMUT BRASIL ("AZBR")** e aplica-se a todas as empresas integrantes do grupo, não podendo ser alterado, copiado, impresso, reproduzido ou distribuído sem a prévia e expressa anuência das referidas empresas.

Esta Política deve ser lida em conjunto com os procedimentos de PLD/FTP, KYC, KYE, KYP, KYS, KYT, Travel Rule, Prevenção a Atos Ilícitos e Fraudes.