

COMPLIANCE · PLD/CFT

# Prevenção à Lavagem de Dinheiro

Diretrizes, processos e responsabilidades para impedir o uso dos nossos produtos na lavagem de dinheiro e no financiamento do terrorismo.

CÓDIGO  
MACOM-001

VERSÃO  
1

ÁREA RESPONSÁVEL  
Compliance

VIGÊNCIA  
Junho de 2026

## Sumário

<b>1</b>	<b>Objetivo</b> .....	<b>3</b>
<b>2</b>	<b>Abrangência</b> .....	<b>3</b>
<b>3</b>	<b>Área responsável pelo documento</b> .....	<b>3</b>
<b>4</b>	<b>Conceitos</b> .....	<b>3</b>
<b>5</b>	<b>Indícios de lavagem de dinheiro e financiamento ao terrorismo</b> .....	<b>4</b>
<b>6</b>	<b>Abordagem baseada em risco (ABR)</b> .....	<b>5</b>
<b>7</b>	<b>Processo "Conheça seu Cliente"</b> .....	<b>6</b>
<b>8</b>	<b>Processo "Conheça seu Funcionário"</b> .....	<b>6</b>
<b>9</b>	<b>Processo "Conheça seu Fornecedor / Terceirizados"</b> .....	<b>6</b>
<b>10</b>	<b>Processo "Conheça seu Parceiro"</b> .....	<b>6</b>
<b>11</b>	<b>Avaliação de novos produtos e serviços</b> .....	<b>6</b>
<b>12</b>	<b>Monitoramento de transações</b> .....	<b>7</b>
<b>13</b>	<b>Comunicação de transações suspeitas</b> .....	<b>7</b>
<b>14</b>	<b>Manutenção de informações e registros</b> .....	<b>7</b>
<b>15</b>	<b>Treinamentos</b> .....	<b>7</b>
<b>16</b>	<b>Exceções</b> .....	<b>7</b>
<b>17</b>	<b>Responsabilidades</b> .....	<b>7</b>
<b>18</b>	<b>Referências</b> .....	<b>9</b>
<b>19</b>	<b>Glossário</b> .....	<b>10</b>

## 1 Objetivo

Esta Política de Prevenção à Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo tem como objetivo definir as diretrizes para que a Zaztech, por intermédio da área de Compliance e de todos os seus administradores, consolide princípios e regras que previnam práticas de lavagem de dinheiro e financiamento do terrorismo, em consonância com a legislação e a regulamentação vigentes e com as melhores práticas de mercado.

## 2 Abrangência

A Política deve ser respeitada, seguida e difundida em todos os setores da empresa, não se limitando a sócios, diretores, administradores, conselheiros, gestores, empregados, estagiários, agentes, fornecedores, representantes, parceiros comerciais e de negócios, aprendizes e prestadores de serviço terceirizado, ou ainda qualquer pessoa, física ou jurídica, que esteja agindo por conta ou em conjunto com a Zaztech.

## 3 Área responsável pelo documento

A área de Compliance da Zaztech é a responsável pela monitoria, revisão e atualização periódica desta Política.

## 4 Conceitos

### ● LAVAGEM DE DINHEIRO

Interpretada amplamente como a inserção de ativo financeiro obtido de forma ilícita nos produtos ou serviços dos arranjos de pagamento, a fim de dar-lhe aparência de origem lícita, bem como possibilitar o financiamento de atividades ilícitas, incluindo o terrorismo. O processo costuma envolver três etapas: **colocação** (introdução de valores provenientes de atividades ilícitas em instituições financeiras e não financeiras); **ocultação** (separação do ativo de sua origem, mascarando-a para dificultar o rastreamento); e **integração** (retorno dos recursos "lavados" à economia com aparência lícita). A Zaztech deve impedir rigorosamente que seus produtos sejam utilizados para a lavagem de dinheiro.

### ● FINANCIAMENTO AO TERRORISMO

Consiste na reunião de fundos e/ou capital para a realização de atividades terroristas. Esses fundos podem ser provenientes de doações ou de diversas atividades ilícitas, como tráfico de drogas, contrabando, extorsões, sequestros e fraudes.

### ● CORRUPÇÃO

Consiste em sugerir, oferecer, submeter, solicitar, aceitar ou receber vantagens indevidas, de forma direta ou indireta, de pessoas do setor público, privado ou de organizações do terceiro setor.

● **PESSOA POLITICAMENTE EXPOSTA (PEP)**

Agentes públicos que desempenham ou tenham desempenhado, nos últimos cinco anos, no Brasil ou no exterior, cargos, empregos ou funções públicas relevantes, assim como seus representantes, familiares e pessoas de relacionamento próximo. Uma pessoa natural com participação societária conjunta com uma PEP também é considerada PEP.

● **BENEFICIÁRIO FINAL**

Pessoa natural que, em última instância, de forma direta ou indireta, possui, controla ou influencia significativamente a estrutura empresarial, ou o representante que exerça o comando de fato sobre as atividades da pessoa jurídica. Excetuam-se companhias abertas, entidades sem fins lucrativos e cooperativas, cujas informações abrangem as pessoas naturais autorizadas a representá-las, controladores, administradores e diretores.

**5**

## **Indícios de lavagem de dinheiro e financiamento ao terrorismo**

É de suma importância que todos tenham conhecimento das operações que configuram indícios de lavagem de dinheiro e financiamento ao terrorismo. A lista abaixo é exemplificativa:

- 1 Valores, propostas e/ou operações incompatíveis com o perfil socioeconômico, a capacidade financeira ou a ocupação profissional do cliente, beneficiário, terceiros ou titular;
- 2 Movimentação de valores incompatíveis com o faturamento mensal das pessoas jurídicas;
- 3 Oscilação significativa no volume e/ou na frequência de negócios de qualquer das partes;
- 4 Desdobramentos que constituam artifício para burlar a identificação dos envolvidos, beneficiários, origem, destino ou responsáveis pelos recursos;
- 5 Movimentação de recursos de alto valor, de forma contumaz, em nome de terceiros;
- 6 Mudança repentina e injustificada nas modalidades operacionais usualmente utilizadas;
- 7 Operações com a finalidade de gerar perda ou ganho sem fundamento econômico;
- 8 Participação de pessoas ou entidades constituídas em países que não aplicam suficientemente as recomendações do GAFI;
- 9 Transferências privadas de recursos sem motivação aparente;
- 10 Transferências em que não seja possível identificar o beneficiário final;
- 11 Operações cujo grau de complexidade e risco sejam incompatíveis com a qualificação técnica do cliente ou de seu representante;

- 12 Resistência em fornecer as informações necessárias no início do relacionamento ou na atualização cadastral;
- 13 Fornecimento de informações falsas;
- 14 Representação de diferentes pessoas jurídicas pelos mesmos procuradores, sem justificativa;
- 15 Conta de pagamento de organização sem fins lucrativos com saldos ou movimentações sem fundamentação econômica ou legal;
- 16 Movimentação não usual de recursos de/para qualquer tipo de PEP ou PEP relacionado;
- 17 Solicitação ou indução para que funcionários não sigam os procedimentos formais de uma operação;
- 18 Declaração de diversas contas bancárias e/ou sua modificação com habitualidade;
- 19 Autorização de procurador que não apresente vínculo aparente;
- 20 Fragmentação de saques em espécie para burlar limites regulatórios de reporte;
- 21 Operações atípicas por pessoa natural ou jurídica relacionadas a licitações;
- 22 Operações atípicas relacionadas a patrocínio, propaganda, marketing, consultorias e capacitação oriundos de contratos com o setor público;
- 23 Operações envolvendo partidos políticos e campanhas eleitorais sem fundamento;
- 24 Operações envolvendo pessoas ou entidades listadas pelo CSNU, pela OFAC e pela União Europeia;
- 25 Operações com indícios de financiamento ao terrorismo;
- 26 Operações atípicas ou aparentemente sem fundamento em municípios de regiões de fronteira.

#### ● REPORTE

Assim que identificados, os casos de suspeita devem ser reportados ao Departamento de Compliance, responsável por respeitar o sigilo do reporte, averiguar os fatos e comunicar as autoridades competentes, quando pertinente.

**6**

## Abordagem baseada em risco (ABR)

Para identificar e mensurar o risco de utilização dos nossos produtos e serviços na lavagem de dinheiro e no financiamento do terrorismo, utilizamos a metodologia ABR (Abordagem Baseada em Riscos), considerando variáveis como cliente, localização, modelo de negócio, papel exercido (cliente, fornecedor, funcionário ou parceiro), produto e transação.

Essa metodologia permite categorizar o risco, concentrando maiores esforços nas situações de maior risco e adotando controles simplificados nas de menor risco. A avaliação de risco é revisada periodicamente e sempre que houver alterações nos perfis de risco.

## 7 Processo "Conheça seu Cliente"

Conjunto de ações realizadas pelas áreas cadastrais que asseguram a identificação e a qualificação do cliente, contemplando captura, verificação, atualização e armazenamento de informações cadastrais, incluindo procedimentos para identificação de beneficiários finais e de Pessoas Politicamente Expostas, e a verificação de representantes e estreitos colaboradores.

É proibido iniciar ou manter relacionamento com indivíduos ou entidades mencionados nas listas de sanções internacionais da ONU, da OFAC e da União Europeia, bem como com empresas de fachada. Após o cadastro, todos os clientes e seus beneficiários finais e representantes são submetidos a verificação em listas restritivas internas e externas. Conforme a classificação de risco, realiza-se diligência mais aprofundada e, havendo desabonos relevantes, o caso é submetido a alçada superior.

## 8 Processo "Conheça seu Funcionário"

Conjunto de regras, procedimentos e controles para seleção e acompanhamento do funcionário quanto à situação econômico-financeira e à idoneidade, visando evitar vínculo com pessoas envolvidas em atos ilícitos.

## 9 Processo "Conheça seu Fornecedor / Prestador de Serviços Terceirizados"

Conjunto de regras e procedimentos para identificação e aceitação de fornecedores e prestadores de serviços terceirizados, prevenindo a contratação de empresas ou pessoas inidôneas ou suspeitas de envolvimento em atividades ilícitas.

## 10 Processo "Conheça seu Parceiro"

Conjunto de regras, procedimentos e controles para identificação e aceitação de parceiros das unidades de negócios, visando prevenir negócios com contrapartes inidôneas ou suspeitas e assegurar que possuam procedimentos adequados de PLD/CFT, quando aplicável.

## 11 Avaliação de novos produtos e serviços

O Departamento de Compliance participa da análise prévia de novos produtos, serviços e tecnologias sob a ótica de PLD/CFT, com o objetivo de mitigar riscos regulatórios e o risco de que sejam utilizados para a prática de lavagem de dinheiro ou financiamento do terrorismo.

## 12 Monitoramento de transações

O Departamento de Compliance é responsável pelas rotinas de monitoramento das operações para identificação de indícios de lavagem de dinheiro e financiamento do terrorismo. O monitoramento é realizado por sistema que se integra aos sistemas internos de informações cadastrais, operacionais e de movimentação financeira, mediante parametrização de regras.

Gerada uma ocorrência, cabe ao Compliance analisar o cliente e suas operações para confirmar ou não os indícios. Qualquer identificação de indícios de lavagem de dinheiro, corrupção ou financiamento do terrorismo é levada à Direção da empresa para decisão sobre o reporte, o bloqueio da conta e/ou o término do relacionamento.

## 13 Comunicação de transações suspeitas aos órgãos reguladores

Operações, situações ou propostas com indícios de lavagem de dinheiro ou financiamento ao terrorismo devem ser comunicadas aos órgãos reguladores competentes, quando aplicável, de forma tempestiva. As comunicações de boa-fé, efetuadas conforme a legislação, não acarretam responsabilidade civil ou administrativa à Zaztech nem aos administradores. As informações sobre as comunicações são restritas, sigilosas e não divulgadas a clientes ou terceiros.

## 14 Manutenção de informações e registros

Os documentos cadastrais, as análises dos procedimentos “Conheça seu...” e os dossiês das operações e propostas selecionadas, comunicadas ou não ao COAF, devem ser arquivados pelo período mínimo de **dez anos**, contados a partir do primeiro dia do ano seguinte ao término do relacionamento, ao término da relação contratual ou à realização da operação.

## 15 Treinamentos

A Zaztech, por meio do Departamento de Compliance, aplica periodicamente treinamentos aos seus colaboradores, parceiros e prestadores de serviços terceirizados, para a disseminação da prevenção à lavagem de dinheiro e ao financiamento do terrorismo.

## 16 Exceções

As exceções deverão ser fundamentadas com as respectivas áreas interessadas e ter sempre a aprovação do Departamento de Compliance. Não havendo consenso entre os integrantes do Compliance, o caso será submetido à apreciação e deliberação da Diretoria.

## 17 Responsabilidades

Todos os colaboradores da Zaztech são responsáveis pela condução dos negócios nos termos da legislação aplicável e desta Política. Abaixo, as responsabilidades específicas de cada área:

## Diretoria Geral

- Avaliar os resultados das análises de prevenção a atos ilícitos em sua unidade de negócios;
- Incentivar a realização dos treinamentos de PLD/CFT pelos colaboradores;
- Garantir o cumprimento das determinações dos órgãos reguladores;
- Deliberar sobre o início de relacionamento de PEPs e relacionados, quando sinalizados pelo Compliance;
- Aprovar a Política e zelar por sua efetividade e melhoria contínua.

## Compliance

- Analisar clientes, colaboradores, fornecedores, prestadores e parceiros antes do relacionamento, identificando PEPs e relacionados;
- Promover a cultura de PLD/CFT e realizar treinamentos;
- Implementar ferramentas de apoio ao programa de prevenção;
- Realizar análise prévia de novos produtos, serviços e tecnologias;
- Monitorar o comportamento transacional dos clientes e os riscos à imagem da empresa;
- Rever e atualizar regras frente às exigências regulatórias;
- Avaliar e investigar indícios apurados no monitoramento;
- Assegurar a comunicação ao COAF dentro do prazo regulatório e manter as informações atualizadas;
- Rever os critérios da ABR e atualizar periodicamente a Política e o manual de procedimentos;
- Realizar a devida diligência de parceiros e fornecedores relevantes;
- Deliberar, com a Direção Geral, sobre a comunicação ao COAF.

## Diretoria Jurídica, Riscos e Regulatório

- Definir as diretrizes para a prevenção a atos ilícitos conforme as normas vigentes;
- Garantir o programa de treinamento e capacitação contínua;
- Garantir a avaliação de riscos no início do relacionamento com clientes, fornecedores e parceiros;
- Apoiar a avaliação de riscos sob a ótica jurídica;
- Envidar esforços para incluir, nas minutas padrão de contratos, cláusulas de PLD/CFT.

## Auditoria Interna

- Realizar, ao menos uma vez ao ano, avaliação independente da qualidade e efetividade da Política;
- Verificar o cumprimento das regras por meio de testes de aderência;
- Apontar desvios e reportar inconsistências aos responsáveis;
- Definir e executar testes de verificação dos controles adotados.

## Área de Cadastro

- Realizar e manter o cadastro atualizado, garantindo a integridade das informações;
- Obter, verificar e validar a autenticidade das informações de identificação do cliente;
- Vedar o início de relacionamento com cadastro incompleto e identificar beneficiários finais de PJ;

- Coletar informações de PEPs e equalizar o controle com o Compliance;
- Assegurar a adequação dos dados, com revisão de periodicidade máxima de um ano;
- Reportar ao Compliance qualquer atipicidade identificada.

### Área Comercial

- Seguir as melhores práticas do "Conheça seu Cliente" e comunicar atividades suspeitas;
- Garantir a coleta adequada de informações cadastrais de clientes, parceiros e fornecedores;
- Auxiliar na identificação de beneficiários finais e prestar esclarecimentos ao Compliance;
- Realizar visitas a clientes e estabelecimentos, quando necessário;
- Manter sigilo das investigações conduzidas pelo Compliance.

### Recursos Humanos

- Garantir a coleta e a atualização dos dados cadastrais dos novos colaboradores;
- Assegurar a realização dos treinamentos de PLD/CFT e apresentar relatórios de status;
- Verificar as informações dos colaboradores e informar suspeitas ao Compliance;
- Auxiliar no monitoramento do "Conheça seu Funcionário (KYE)".

### Tecnologia da Informação

- Garantir o funcionamento adequado dos sistemas de PLD/CFT, resolvendo falhas no menor tempo possível.

### Segurança da Informação

- Garantir a conformidade com as circulares aplicáveis à contratação de serviços de processamento, armazenamento de dados e computação em nuvem utilizados no monitoramento de operações suspeitas.

### Compras

- Auxiliar o Compliance no conhecimento dos fornecedores e prestar esclarecimentos;
- Captar informações e documentação com a diligência necessária à prevenção.

### Sócios e colaboradores

- Reportar ao Compliance toda proposta, operação ou situação atípica ou suspeita;
- Guardar sigilo sobre as comunicações feitas ao Compliance;
- Agir com diligência e probidade no suporte ao Compliance;
- Elaborar respostas aos apontamentos das auditorias e providenciar documentação solicitada;
- Disseminar a cultura de prevenção e participar dos treinamentos;
- Comunicar conflitos de interesse e a contratação de terceirizados suspeitos.

## 18

## Referências

- Lei nº 9.613, de 3 de março de 1998 (Lei de Lavagem de Capitais);
- Lei nº 12.683, de 9 de julho de 2012 (Lavagem de Dinheiro);

- Lei nº 12.865, de 9 de outubro de 2013 (Lei dos Arranjos de Pagamento);
- Circular nº 3.865, de 7 de dezembro de 2017 (Compliance);
- Resolução nº 4.282/2013 do Conselho Monetário Nacional;
- Circulares nº 3.680/13, 3.681/13 e 3.865/17 do Banco Central do Brasil;
- Lei nº 12.846, de 1º de agosto de 2013 (Lei Anticorrupção);
- Decreto nº 8.420, de 18 de março de 2015;
- Portarias nº 909/15 e 910/15 da Controladoria-Geral da União;
- Instruções Normativas nº 01/15 e 02/15 da Controladoria-Geral da União;
- Circulares nº 3.978/20 e 4.001/20 do Banco Central do Brasil;
- Lei nº 13.260, de 16 de março de 2016;
- Circular nº 3.858, de 14 de novembro de 2017;
- Cartas Circulares nº 3.409/2009, 3.430/2010 e 3.977/2019;
- Circular nº 3.942, de 21 de maio de 2019.

**19**

**Glossário**

**Programa de Compliance**

Conjunto de normativos, mecanismos e procedimentos internos de integridade, auditoria, incentivo à denúncia e aplicação do Código de Conduta, diretrizes de governança, políticas e normas, com o objetivo de detectar e sanar não conformidades.

**PLD/CFT**

Prevenção à Lavagem de Dinheiro / Combate ao Financiamento do Terrorismo.

**PEP**

Pessoa Politicamente Exposta.

**COAF**

Conselho de Controle de Atividades Financeiras — órgão criado pela Lei nº 9.613/1998 para disciplinar, aplicar penas administrativas, receber, examinar e identificar ocorrências suspeitas relacionadas à lavagem de dinheiro.

**OFAC**

Office of Foreign Assets Control — agência do Departamento do Tesouro dos Estados Unidos responsável por administrar e aplicar sanções contra países, regimes e indivíduos visados.

**CSNU**

Conselho de Segurança das Nações Unidas — órgão da ONU encarregado de zelar pela manutenção da paz e da segurança internacional, capaz de adotar decisões obrigatórias aos Estados-membros.

**União Europeia**

Por meio do Conselho Europeu, define, administra e aplica sanções financeiras, comerciais, políticas e de segurança internacional, incluindo a prevenção à lavagem de dinheiro e ao financiamento do terrorismo.



## Compromisso com a **conformidade.**

Identificou uma operação atípica ou suspeita? Reporte imediatamente ao Departamento de Compliance, que preserva o sigilo de cada comunicação.

### E-MAIL

[comercial@zaztech.com.br](mailto:comercial@zaztech.com.br)

### WHATSAPP COMERCIAL

(48) 99919-8061

### SITE

[www.zaztech.com.br](http://www.zaztech.com.br)

### RAZÃO SOCIAL

ZAZ Tecnologia Financeira Ltda.  
CNPJ 17.968.083/0001-00

### ENDEREÇO

Rua Elizeu Di Bernardi, 34 — Kplatz Corporate, Sala 405 — Kobrasol  
São José/SC — CEP 88101-030