POLÍTICA DE PREVENÇÃO E COMBATE À LAVAGEM DE DINHEIRO E AO FINANCIAMENTO DO TERRORISMO (PLD/FT)

1. INTRODUÇÃO E OBJETIVOS 3
2. ESCOPO E RESPONSABILIDADES 3
3. TERMOS E DEFINIÇÕES 4
Lavagem de dinheiro 4
Financiamento do Terrorismo 6
4. DIRETRIZES 6
4.1 Estrutura Organizacional 6
4.2 Riscos 7
4.3 Devida Diligência (Due Diligence) 7
4.3.1 Devida Diligência Simplificada 8
4.3.2 Devida Diligência Padrão 8
4.3.3 Devida Diligência Reforçada 9
4.3.4 A Localpayment não fará negócio com: 10
4.3.5. Sanções 11
4.3.6 Revisão de Compliance 12
4.4 Armazenamento de dados 13
4.4.1 Atualização cadastral 13
4.4.2 Informações de transações 13
4.4.3 Treinamentos 13
4.4.4 Tomada de decisões 13
4.5 Monitoramento 14
4.6 Encerramento de Relacionamento 15
4.7 Treinamentos e Capacitações 16
4.8 Auditoria Interna 16
4.9 Medidas disciplinares 17
4.10 Reporte de atividades suspeitas 17
5. VERIFICAÇÃO E EFETIVIDADE DA POLÍTICA PLD-FT 18
5.1 Avaliação Interna de Risco 19
5.2 Avaliação de Efetividade 19
6. PUBLICAÇÃO E DISTRIBUIÇÃO DE POLÍTICAS 19

1. INTRODUÇÃO E OBJETIVOS

Esta Política é uma extensão do Código de Conduta da Localpayment e todas as suas subsidiárias, e tem como objetivo estabelecer as condutas esperadas dos colaboradores e empregados quanto ao tema da Prevenção e Combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo.

A Localpayment tem tolerância zero com relação à lavagem de dinheiro e está comprometida em mitigar os riscos de lavagem de dinheiro, seguindo todas as regulamentações locais e internacionais aplicáveis. Além disso, tomará as medidas preventivas necessárias, investigará prontamente qualquer suspeita de lavagem de dinheiro e cooperará de forma irrestrita com as autoridades competentes. A Alta Administração da Localpayment apoia, supervisiona e está comprometida com a eficácia e a melhoria contínua do Programa PLD/FTP.

A Política Prevenção e Combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo é revisada no mínimo anualmente, a fim de atingir as melhores práticas para a Localpayment. A revisão é efetuada por meio de:

- Revisão regular de relatos de mídia relevantes para o setor ou a jurisdição em que a Localpayment atue;
- Revisão regular de alertas e relatórios sobre aplicação da lei;
- Atenção a mudanças de alertas de terror e de regimes de sanções assim que ocorrerem;
- Revisão de publicações temáticas e similares publicadas pelas autoridades competentes;
- Revisão das diretrizes nacionais, do Reino Unido, da UE, dos EUA e das organizações intergovernamentais, como o GAFI/FATF, que desenvolvem políticas para combater PLD/FTP. Essas diretrizes são ajustadas para atender aos requisitos específicos de cada jurisdição onde a Localpayment atua, a fim de definir regras, políticas e procedimentos eficazes contra a lavagem de dinheiro e o financiamento do terrorismo. Onde não houver orientação, o time de Compliance buscará orientação do advogado (interno/externo) e validará formalmente as opiniões fornecidas antes da implementação.

2. ESCOPO E RESPONSABILIDADES

Este documento aplica-se à LP do Brasil Instituição de Pagamento Ltda., às demais subsidiárias do grupo Localpayment, bem como a todos os seus sócios, administradores, diretores, colaboradores,

empregados, prestadores de serviços e parceiros comerciais, independentemente da localidade onde atuem.

As responsabilidades relacionadas à prevenção à lavagem de dinheiro e ao financiamento do terrorismo são atribuídas conforme a estrutura de governança da instituição e estão detalhadas a seguir.

2.1 Conselho de Diretoria e Compliance Officer

O conselho de Diretoria da empresa, junto ao Compliance Officer, são responsáveis por assegurar a implementação e a efetividade desta Política, garantindo a disponibilização de recursos humanos, tecnológicos e financeiros compatíveis com o porte, a complexidade, o perfil de risco e o modelo de negócios da instituição.

O Diretor responsável pela Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (PLD-FT), formalmente designado perante o Banco Central do Brasil, é o responsável pela supervisão do cumprimento das obrigações previstas na regulamentação aplicável, incluindo a implementação de controles internos, o monitoramento de operações, a comunicação de operações suspeitas ao COAF e o reporte periódico à administração.

2.2 Área de Compliance

A área de Compliance é responsável pela execução dos procedimentos previstos nesta Política, pela avaliação de riscos, pela condução de análises cadastrais e de monitoramento de transações, bem como pela manutenção dos registros e evidências necessárias ao cumprimento regulatório.

As áreas operacionais e de suporte devem observar e cumprir os procedimentos estabelecidos, reportando tempestivamente quaisquer indícios de irregularidade ou operação atípica identificados no exercício de suas atividades.

Todos os envolvidos nas atividades da instituição têm o dever de conhecer, cumprir e colaborar com a efetividade desta Política.

3. TERMOS E DEFINIÇÕES

Lavagem de dinheiro

Lavagem de dinheiro refere-se ao processo de disfarçar a origem ilícita de ativos financeiros ou bens, provenientes de atividades criminosas, a fim de integrá-los ao sistema econômico formal como se fossem legítimos. Qualquer recurso obtido através de atividades ilícitas pode ser objeto de lavagem de dinheiro.

Exemplos de crimes frequentemente associados à lavagem de dinheiro incluem: roubo, fraude, corrupção, suborno, comércio de informações privilegiadas, tráfico de drogas, contrabando, peculato, sonegação de impostos, entre outros.

Os três estágios da lavagem de dinheiro costumam ser:

- Colocação: é a primeira fase da lavagem de dinheiro. Envolve a inserção, na economia formal, do ativo proveniente de atividade ilegal.
- Ocultação: esta segunda fase consiste em afastar ainda mais os ativos ilícitos da sua origem por meio da criação de camadas complexas de transações financeiras desenhadas para disfarçar a rastreabilidade do dinheiro e permitir o anonimato.
- Integração: a fase final consiste em dar aparente legitimidade aos ativos provenientes de crimes. Se a fase da dissimulação foi bem-sucedida, esquemas de integração inserem o dinheiro lavado de volta à economia de uma maneira que esses ativos permaneçam no sistema financeiro aparentando ser fundos cuja origem é regular e lícita.

A Localpayment emprega controles específicos para identificar, interromper e reportar atividades suspeitas em cada uma das etapas de lavagem de dinheiro, incluindo ferramentas tecnológicas de monitoramento e a análise detalhada de transações.

Com base em diversas leis, regulamentações e orientações regulatórias da Financial Action Task Force (FATF) e de outras boas práticas internacionais aplicáveis, a Localpayment assegura o cumprimento das regulamentações internacionais e locais aplicáveis, adotando sempre os padrões mais rigorosos entre eles. Quando as regulamentações locais forem mais estritas do que os padrões desta Política, estas prevalecerão.

Caso os padrões mínimos estabelecidos nesta Política não puderem ser aplicados em algum país, porque sua aplicação iria de encontro à legislação local ou porque não poderiam ser impostos por outras razões legais, a Localpayment não iniciará, continuará, nem conduzirá relações de negócios nesse território. Se já existir uma relação de negócios nesse país, a Localpayment deve garantir que ela seja encerrada, independentemente de outras obrigações contratuais ou legais.

Financiamento do Terrorismo

Financiamento do terrorismo é definido como todo e qualquer envolvimento, direto ou indireto, com recursos ou propriedades que certamente ou provavelmente sejam utilizados para propósitos terroristas, independente da regularidade ou legalidade da sua origem.

Para efeito desta Política, o financiamento do terrorismo está diretamente relacionado à lavagem de dinheiro, incluindo quaisquer atividades que envolvam suporte financeiro ou material para atos terroristas ou grupos relacionados.

A Localpayment segue as recomendações da Financial Action Task Force (FATF) e regulamentações locais e internacionais para identificar, prevenir e mitigar riscos relacionados ao financiamento do terrorismo, adotando uma abordagem de tolerância zero.

4. DIRETRIZES

4.1 Estrutura Organizacional

Os processos de Compliance estão centralizados na estrutura de Legal, Risk & Compliance, que é responsável por definir as diretrizes gerais e implementar os processos relacionados à PLD/FTP. As subsidiárias e coligadas da Localpayment devem respeitar essas diretrizes, incluindo a criação de documentos normativos específicos para adequação ao modelo de negócios de cada uma, se necessário. Dessa forma, a Localpayment garante o respeito à gestão global e a independência dos segmentos de Compliance.

Para garantir que os controles de PLD/FTP necessários sejam efetivamente implantados, a Auditoria da Localpayment realiza avaliações anuais do Programa de PLD/FTP, fornecendo relatórios à área de Legal, Risk & Compliance sobre a eficácia dos processos de PLD/FTP. A equipe de Controles Internos da Localpayment é responsável por analisar esses relatórios e elaborar planos de ação para criar controles eficazes para mitigar os riscos de PLD/FTP.

Todos os colaboradores devem estar atentos a esta Política e buscar prevenir e detectar ações, operações ou transações que apresentem características atípicas, a fim de combater a Lavagem de Dinheiro e o Financiamento do Terrorismo.

Para estar em conformidade com esta Política, os colaboradores são instruídos a:

- Reportar toda e qualquer situação considerada atípica ou suspeita por meio dos canais apropriados estabelecidos pela empresa, incluindo o Canal de Denúncias, quando aplicável.

- Atuar com diligência e probidade no apoio ao processo de PLD/FTP assegurando a precisão das informações fornecidas e colaborando ativamente em investigações internas relacionadas a solicitações de produtos, serviços e operações;
- Divulgar a cultura de Prevenção e Combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo;
- Participar de seminários de treinamento e atualização sobre Prevenção à Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo garantindo a aplicação prática dos conhecimentos adquiridos.

4.2 Riscos

A Localpayment adota uma abordagem baseada em riscos a fim de avaliar a maneira mais efetiva e proporcional de prevenir, gerir e mitigar riscos de lavagem de dinheiro e financiamento do terrorismo. Os passos que a Localpayment dá para atingir esse objetivo são:

- Identificar os riscos de lavagem de dinheiro relevantes;
- Avaliar os riscos presentes nos clientes, produtos, serviços, transações, canais de entrega, parceiros e prestadores de serviço, colaboradores e áreas geográficas de operação da Localpayment;
- Monitorar continuamente utilizando ferramentas tecnológicas avançadas, análises manuais e revisões periódicas, quando aplicável, para identificar, avaliar e mitigar riscos emergentes de lavagem de dinheiro e financiamento do terrorismo.

Os riscos identificados devem ser classificados por níveis de criticidade (baixo, médio, alto), com controles desenhados para mitigá-los proporcionalmente ao nível de risco avaliado. Os clientes, parceiros, prestadores de serviço e colaboradores serão classificados em categorias de risco – alto, médio ou baixo. Aqueles classificados como “alto risco” deverão passar por processo de Enhanced Due Diligence (EDD).

4.3 Devida Diligência (Due Diligence)

Um cliente é todo empresa (Merchant) a quem a Localpayment ofereça, tenha a intenção de oferecer ou tenha oferecido no passado um serviço e/ou um produto. Assim, também estão incluídos nesse conceito os clientes em potencial.

Um partner é todo indivíduo ou empresa (fornecedor, provedor, instituição financeira, agente, referral, freelancer) que forneça produtos e/ou serviços ou que tenha algum tipo de relacionamento comercial e/ou estratégico com a Localpayment.

Antes de realizar o onboarding de qualquer novo Merchant, usuário, partner ou colaborador, a Localpayment deve executar o processo de Devida Diligência. Para fins desta Política, Merchants, usuários e parceiros serão considerados terceiros. Alguns terceiros oferecerão risco maior que outros. Para que o nível de risco oferecido por um terceiro possa ser determinado, todos eles passarão por um processo de Diligência Simplificada e terão seu risco definido por pelo de Avaliação de Risco.

As Devidas Diligências são realizadas de acordo com a abordagem de risco de cada unidade de negócio. Terceiros avaliados como "médio risco", passarão por processo de Devida Diligência Padrão. Os avaliados como "high risk", de Devida Diligência Reforçada.

4.3.1 Devida Diligência Simplificada

Devida Diligência Simplificada envolve reunir informações e documentos que permitam:

- Identificar o terceiro e verificar sua identidade;
- Estabelecer a natureza da relação de negócios;
- Executar verificação para identificar se o terceiro é pessoa exposta politicamente (PEP) e/ou se é sujeito a sanções;
- Assegurar que qualquer pessoa agindo em nome do terceiro está autorizada para tanto, além de identificar e verificar essa pessoa.
- Realizar verificações de notícias adversas e mídia negativa para todas as categorias de risco. Essas verificações são repetidas durante as revisões periódicas, com os ciclos de revisão determinados com base no perfil de risco.

Uma vez que esse processo seja concluído, a Avaliação de Risco será executada, a fim de se determinar o nível de due diligence necessário.

4.3.2 Devida Diligência Padrão

Além das verificações realizadas no processo de Devida Diligência Simplificada, terceiros cujo nível de risco seja médio devem passar pelo processo de Diligência Devida Padrão, que envolve:

- Identificação e verificação completa de qualquer beneficiário que detenham 25% ou mais da empresa (no caso do beneficiário final ser outra empresa, a verificação deve ser feita apenas em relação à empresa acionista, e não de seus diretores);
- Realização de verificações de notícias adversas e mídia negativa para todas as categorias de risco. Essas verificações são repetidas durante as revisões periódicas, com os ciclos de revisão determinados com base no perfil de risco.

Todos os colaboradores e candidatos selecionados para vagas de qualquer nível hierárquico passarão pelo processo Devida Diligência Padrão, podendo ocorrer a necessidade de Diligência reforçada se encontrado fator de risco que eleve sua classificação de risco.

4.3.3 Devida Diligência Reforçada

Além das verificações realizadas nos processos de Diligência Simplificada e Diligência Padrão,, terceiros classificados como alto risco devem passar pelas seguintes verificações

- Identificação e verificação completas de todos os beneficiários, incluindo verificação dos diretores da empresa;
- Identificação e verificação completa de eventuais empresas constituídas em nome de colaborador;
- Identificação do beneficiário final, quando relevante, verificando sua identidade e procurando compreender a estrutura de controle da empresa, quando aplicável.
- Realização de verificações de notícias adversas e mídia negativa para todas as categorias de risco. Essas verificações são repetidas durante as revisões periódicas, com os ciclos de revisão determinados com base no perfil de risco.

As medidas de Diligência Reforçada também incluem:

- Aumento da frequência de revisão, a fim de verificar se a Localpayment permanece apta a gerir o risco associado com a relação de negócios ou com o cargo ocupado pelo colaborador e de ajudar a identificar quaisquer transações que demandem revisão posterior;
- Aumento da frequência de revisão da relação de negócios, a fim de verificar se o perfil de risco do terceiro foi alterado e se o risco permanece gerenciável;
- Obtenção da aprovação da Coordenação e/ou Gerência da área para dar início ou continuar a relação de negócios, a fim de assegurar que a alta administração está ciente dos riscos que a Localpayment está exposta e lhes permitir tomar decisões embasadas acerca de quanto estamos aptos a gerenciar esses riscos;

- Casos em que a exposição a Risco esteja alta e/ou em casos em que a área entenda, após análise, que o caso possui severidade, poderão ser escalados ao Comitê de Risco para uma deliberação sobre a entrada de um cliente/parceiro/fornecedor/colaborador, através de um processo formal de Risk Acceptance.
- Condução de monitoramento de transações com maior frequência ou com maior profundidade, a fim de identificar quaisquer transações incomuns ou inesperadas que possam levantar suspeitas de lavagem de dinheiro ou de financiamento do terrorismo. Isso pode incluir o estabelecimento da destinação dos fundos do terceiro ou a definição da razão de certas transações.

O processo de Due diligence também deve ser executado a qualquer momento em que a Localpayment suspeite ou tenha razões para suspeitar de lavagem de dinheiro ou em que se acredite que quaisquer documentos ou informações expirados ou imprecisos tenham sido fornecidos. Qualquer relação de negócios com um Merchant, usuário, parceiro, prestador de serviço ou colaborador estará sujeita a monitoramento constante,.

Relações de negócios, transações e demais comportamentos devem ser consistentes com o conhecimento que a Localpayment possui acerca do Merchant, do usuário, partner ou colaborador, assim como acerca de seus negócios, perfis de risco, origem da riqueza e origem dos fundos (documentos como extratos bancários, declarações fiscais ou acordos de acionistas são revisados para verificar a origem da riqueza e a origem dos fundos).

Quando o risco exceder o apetite do negócio, o terceiro ou colaborador não será integrado ou contratado pela Localpayment. Caso a área requisitante acredite que a oportunidade é importante o suficiente e que controles alternativos podem reduzir o risco identificado, exceções formais podem ser aplicadas.

4.3.4 A Localpayment não fará negócio com:

- Indivíduos ou empresas suspeitos de lavagem de dinheiro e/ou financiamento do terrorismo;
- Shell banks;
- Indivíduos ou empresas para os quais o nível necessário de Due Diligence NÃO tenha sido executado;
- Usuários listados como não aceitáveis pelas Políticas da Localpayment;

- Empresas baseadas em países sancionados;

Além disso, a Localpayment não fará negócios com qualquer terceiro que envolva atividades ou comportamentos que possam representar um risco significativo à reputação ou à conformidade regulatória da empresa. Para mais informações sobre os produtos proibidos, acessar a base pública da Localpayment.

Avaliação de Novos Produtos, Serviços e Tecnologias

A instituição deverá realizar avaliação prévia de risco de lavagem de dinheiro e de financiamento do terrorismo antes do lançamento de novos produtos, serviços, canais de distribuição, modelos operacionais ou da implementação de novas tecnologias que possam impactar sua exposição a riscos regulatórios.

Essa avaliação deverá considerar, no mínimo, o público-alvo, a natureza das operações, os fluxos financeiros envolvidos, as jurisdições relacionadas, o uso de intermediários, a complexidade da estrutura operacional e eventuais riscos inerentes à tecnologia utilizada.

A área de Compliance deverá participar obrigatoriamente do processo de aprovação, emitindo parecer quanto aos riscos identificados e às medidas mitigadoras necessárias, podendo recomendar ajustes, controles adicionais ou restrições operacionais.

A implementação de novos produtos, serviços ou tecnologias somente poderá ocorrer após a conclusão da análise de risco e a definição dos controles internos compatíveis com o nível de risco identificado. As avaliações realizadas deverão ser formalizadas e mantidas arquivadas para fins de evidência regulatória.

4.3.5. Sanções

A Localpayment deve bloquear Merchants, usuários e/ou entidades originadas de países que desrespeitem programas de sanções, a fim de garantir que a empresa não faça negócios com pessoas e organizações sancionadas, combatendo, assim, o financiamento e a proliferação de armas de destruição em massa.

Algumas jurisdições representam risco excepcional em relação a lavagem de dinheiro e a crimes financeiros. Essas jurisdições são identificadas pelo FATF como possuindo controles fracos ou

demandando ações ou são regimes sancionados pelos Estados Unidos da América, pelo Reino Unido e/ou por outras nações. Além disso, qualquer jurisdição ou região que possua políticas de compliance deficientes ou que esteja sujeita a embargos comerciais será considerada de alto risco. O risco geográfico será monitorado e atualizado diariamente.

A verificação e monitoramento de Merchants, usuários e partners quanto a sanções é efetuada por meio de um banco de dados global com acesso a centenas de listas de sanções buscadas em diversas fontes mundiais de informação. Esse processo é atualizado em tempo real para garantir que qualquer alteração nas listas de sanções seja imediatamente incorporada ao monitoramento.

4.3.6 Revisão de Compliance

Todo Merchant registrado em nossas bases de dados passam por revisões periódicas de suas informações de Identificação e Qualificação, bem como dos dados de Integração - tais como website e/ou aplicativo, entre outros.

Essa revisão periódica é realizada levando em consideração o Nível de Risco (Risk Score) apontado no momento do Onboarding do mesmo na Localpayment, sendo:

- 1 ano para Alto Risco
- 3 anos para Médio Risco
- 5 anos para Baixo Risco

Independente de revisão realizada dentro dos períodos supracitados, qualquer alteração significativa quanto a pessoa jurídica de um Merchant deve provocar uma revisão de Compliance nesse Merchant. É responsabilidade do Merchant notificar a Localpayment sempre que houver alterações em relação a:

- Estrutura societária e controle da empresa (diretores e beneficiários finais);
- Controlador da empresa;
- Outras pessoas autorizadas a assinar pela empresa;
- Mídias negativas, no momento em que forem divulgadas ou conhecidas pelo Merchant ou qualquer informação relevante.

Adicionalmente, qualquer alteração solicitada pelo Merchant relacionada a integração do mesmo junto a Localpayment - alteração ou inclusão de URL, aplicativo ou qualquer outro dado relevante para a operação - também acarreta em revisão do mesmo por parte do time de Compliance. Além disso, a Localpayment se reserva o direito de revisar periodicamente os dados dos Merchants,

mesmo que não haja alterações, caso haja modificações significativas no ambiente regulatório ou no perfil de risco do Merchant.

4.4 Armazenamento de dados

A Localpayment deve armazenar os dados de todos os detalhes obtidos com o propósito de identificar Merchants, usuários e partners, assim como seus documentos, de acordo com as regulações. A Localpayment vai armazenar:

4.4.1 Atualização cadastral

No intuito de manter as informações atualizadas, a Localpayment poderá conduzir revisão documental considerando a seguinte periodicidade:

- Alto Risco - Anual
- Médio Risco – 3 anos
- Baixo Risco - 5 anos

4.4.2 Informações de transações

- As transações financeiras executadas pela Localpayment com ou para cada cliente;
- Reportes de atividades suspeitas internos e externos ou razões para não reportar. Esses documentos devem ser mantidos por, no mínimo, 10 (dez) anos após a realização do reporte, ou conforme exigido pelas regulamentações locais aplicáveis, o que for mais longo.

4.4.3 Treinamentos

- Materiais e testes utilizados nos treinamentos;
- Resultados dos testes e avaliações realizadas;
- Datas dos treinamentos;
- Natureza dos treinamentos, incluindo tópicos abordados e objetivos de aprendizagem;
- Identificação pessoal de quem participou do treinamento, incluindo função e cargo.

4.4.4 Tomada de decisões

Os dados e informações podem ser armazenados das seguintes formas:

1. Documentos originais;

2. Cópias de documentos originais;
3. Cópias digitalizadas;
4. Formatos eletrônicos;

Quando do fim do prazo de 10 (dez) anos, a Localpayment deve apagar quaisquer dados pessoais, a não ser que a empresa seja obrigada a manter dados que contenham dados pessoais por razões legais ou devido a processo judicial ou que o indivíduo a quem os dados pertencem tenha dado consentimento expresso para que sejam mantidos

Proteção de dados: os países em que a Localpayment opera possuem diversos requisitos e obrigações que são respeitados ao realizarmos atividades de tratamentos de dados pessoais. Cumprimos com as legislações de proteção à privacidade de dados pessoais, como por exemplo, a General Data Protection Regulation (GDPR) de 2017 e a Lei Geral de Proteção de Dados (LGPD) de 2018, que regulam o uso de dados pessoais, essencialmente de qualquer informação sobre indivíduos identificáveis. A Localpayment possui o time de Cyber Security, que é responsável pela coordenação operacional e estratégica, assim como toda a proteção de dados e os controles do programa de privacidade de dados da empresa. Para mais informações, consultar a Política de Segurança da Informação.

4.5 Monitoramento

A Localpayment deve executar monitoramento regular de clientes e de transações de acordo com sua Avaliação de Risco. O monitoramento também deve ser executado a fim de assegurar que as Políticas, normas e procedimentos estejam sendo corretamente implementados.

Comportamentos de clientes ou problemas com negócios de clientes que possam identificar a necessidade de uma investigação mais profunda pela Localpayment serão considerados “Red Flags”. Exemplos de red flags incluem, mas não limitam-se a:

- Cliente é relutante ou evasivo ao fornecer informações;
- A estrutura de negócio do cliente é desnecessariamente complicada;
- Há envolvimento de terceiros sem razão válida;
- Alterações sucessivas de conta bancária sem razão válida;
- Cliente aparenta desinteresse em preços, comissões, custos, etc.;
- Transações diferentes das esperadas do cliente;
- Transferências inexplicáveis de fundos;
- Volume de transações incompatível com o modelo de negócio;

- Concentração de vendas em uma determinada região;
- Volume alto de pedidos de reembolso e/ou chargeback.

Se uma red flag for identificada nos processos de Due Diligence ou de monitoramento do cliente, os responsáveis devem notificar o Compliance Officer imediatamente.

A Localpayment utiliza ferramentas de monitoramento transacional para identificar quaisquer comportamentos incomuns ou inesperados que possam provocar suspeita de lavagem de dinheiro ou de financiamento do terrorismo.

Com base no conhecimento da Localpayment acerca do cliente, o monitoramento vai buscar:

- Comportamento incomum: alterações abruptas ou significantes nas atividades de transações, quanto a valor, volume ou natureza, como por exemplo mudança de beneficiário ou de destino do dinheiro;
- Relações conectadas: beneficiários e remetentes comuns em contas e/ou clientes em que aparentemente não há relação;
- Países, regiões e entidades de alto risco geográfico: aumentos significativos de atividade ou altos níveis constantes de atividade com países, regiões ou entidades de alto risco geográfico;
- Outros comportamentos típicos de lavagem de dinheiro: transações abaixo dos limites reportados, em números redondos, estruturadas, sequenciais e/ou extremamente complexas;
- Relações correntes: a Localpayment executará revisões retroativas em clientes para assegurar que o negócio em curso seja consistente com o que foi acordado quando da entrada do cliente.

A Localpayment conduzirá o monitoramento das transações, verificando seus valores, volumes e velocidade. Alertas mais intensivos serão gerados para àqueles que representem maior risco. Alertas serão disparados para garantir que as transações sejam monitoradas adequadamente e que operações suspeitas sejam reportadas.

Todos os novos produtos propostos pela Localpayment devem passar por análise de Compliance. A análise visa identificar processos que precisam ser analisados para que os riscos apontados sejam mitigados.

4.6 Encerramento de Relacionamento

A Localpayment pode decidir encerrar uma relação de negócios após identificar atividade suspeita. Mesmo na ausência de atividades suspeitas, o Compliance Officer pode recomendar o encerramento de relações com Merchants, parceiros ou outros terceiros, caso o risco associado a essas partes seja considerado excessivo ou incompatível com o apetite de risco da Localpayment.

4.7 Treinamentos e Capacitações

A Localpayment vai assegurar que todos os colaboradores e empregados sejam devidamente treinados para compreender suas obrigações quanto a esta Política e quanto aos requisitos para identificação de terceiros. Treinamentos específicos serão oferecidos a diferentes áreas, levando em consideração suas responsabilidades e níveis de exposição ao risco de Lavagem de Dinheiro e Financiamento ao Terrorismo.

Todos os colaboradores e empregados devem estar cientes de que o não cumprimento de suas responsabilidades pode resultar em medidas disciplinares internas e, em casos mais graves, em sanções criminais.

A instituição deverá manter programa contínuo de capacitação em prevenção à lavagem de dinheiro e ao financiamento do terrorismo, compatível com o porte, a complexidade, o perfil de risco e o modelo de negócios da organização.

O programa de treinamento deverá abranger todos os colaboradores, administradores e profissionais que atuem em atividades relacionadas à identificação de clientes, monitoramento de operações, prevenção a fraudes e demais funções relevantes para a gestão de riscos de PLD-FT.

A capacitação deverá ocorrer de forma periódica, bem como sempre que houver alterações regulatórias relevantes, mudanças nos produtos, serviços ou processos internos que impactem o risco de lavagem de dinheiro e financiamento do terrorismo.

Quando aplicável, os funcionários de correspondentes no País que atuem em nome da instituição deverão receber orientação adequada sobre as obrigações relacionadas à prevenção à lavagem de dinheiro e ao financiamento do terrorismo, de modo compatível com as atividades desempenhadas.

A instituição deverá manter registros que evidenciem a realização dos treinamentos, o conteúdo ministrado e a participação dos envolvidos.

4.8 Auditoria Interna

O programa de Prevenção à Lavagem de Dinheiro e Combate ao Financiamento ao Terrorismo da Localpayment será auditado anualmente. A auditoria interna reportará a alta administração o status dos controles e das áreas que precisem ser remediadas. Esse processo garante a identificação e mitigação de lacunas nos controles. Caso solicitado, os relatórios resultantes poderão ser encaminhados às autoridades reguladoras. A área de Legal, Risk & Compliance será responsável por receber e monitorar os relatórios de auditoria, assegurando a implementação de medidas corretivas e a manutenção da conformidade com os requisitos legais e regulatórios aplicáveis.

4.9 Medidas disciplinares

Qualquer colaborador que viole as diretrizes desta Política estará sujeito a medidas disciplinares, as quais serão aplicadas de acordo com a gravidade da violação. As violações serão devidamente investigadas de acordo com os procedimentos do Comitê de Ética, garantindo anonimato aos envolvidos, preservando a confidencialidade e a integridade das partes. Todos os colaboradores têm obrigação de cooperar integralmente com investigações em curso.

4.10 Reporte de atividades suspeitas

Todas as transações de clientes estão sujeitas a monitoramento e revisão constantes e passíveis de comunicação ao Conselho de Controle de Atividades Financeiras (COAF). Quando o Compliance Officer determina que um cliente ou transação em particular requer investigação adicional, os analistas de Compliance devem executá-la, fornecendo informações completas e realizando as análises necessárias.

Os procedimentos, prazos e critérios para comunicação de operações suspeitas ao COAF encontram-se detalhados no Manual de Monitoramento, Seleção, Análise e Comunicação (MSAC).

Qualquer diretor ou colaborador que suspeite de lavagem de dinheiro deve imediatamente reportar suas suspeitas através do Canal de Denúncias ou ao Compliance Officer por escrito, incluindo detalhes completos. Todos os sinais de suspeita de lavagem de dinheiro são reportáveis, mesmo que cheguem ao conhecimento do colaborador após a transação ter ocorrido, de o registro ter sido fechado ou que a transação tenha sido conduzida por outra pessoa. Ao realizar o reporte, o diretor ou colaborador terá cumprido com suas obrigações legais.

Revelar a uma pessoa suspeita ou a um terceiro que um reporte foi feito ao Compliance Officer ou às autoridades, ou que uma investigação está em curso é uma violação de conduta, uma vez que pode prejudicar as apurações. Questionar um cliente quanto a uma transação específica, a fim de saber

sua identidade ou definir sua fonte de renda não configura violação. No caso de um reporte de atividade suspeita ter sido realizado, deve-se ter muita cautela para que o cliente ou o indivíduo citado não fique ciente disso.

Caso sinais suspeitos de lavagem de dinheiro sejam identificados, a transação deve ser bloqueada e não deve ter continuidade sem a autorização do Compliance Officer. O Compliance Officer receberá reportes relacionados a qualquer suspeita de lavagem de dinheiro ou efetiva lavagem de dinheiro e irá registrar, investigar e reportar a suspeita às autoridades competentes, se necessário. O reporte de suspeita de lavagem de dinheiro às autoridades não configura quebra da obrigação de confidencialidade para com o cliente e fornece importantes salvaguardas à Localpayment.

No caso de os reportes não serem encaminhados às autoridades, todos os detalhes da tomada dessa decisão devem ficar registrados. Todas as notificações realizadas serão processadas com extrema confidencialidade. No entanto, poderá haver circunstâncias em que a Localpayment será obrigada a revelar a identidade dos envolvidos na suspeita, como, por exemplo, quando compelido pela lei. Nesse caso específico, o anonimato não pode ser garantido.

Exemplos de transações que podem provocar suspeita de lavagem de dinheiro estão listadas abaixo, mas, por si só, não necessariamente geram suspeita suficiente para realização de um reporte:

- Transações de compra e venda sem propósito claro ou em circunstâncias incomuns;
- Instruções para direcionar valores a uma conta corrente diferente daquela acordada previamente ou em nome de terceiro;
- Qualquer transação em que uma das partes não seja conhecida ou que tenha volume ou frequência incomum;
- Transações em que o investidor seja por pessoa estrangeira e ambos estejam baseados em países com altas taxas de produção ou tráfico de drogas.

Não é esperado dos colaboradores que saibam ou que estabeleçam a exata natureza de qualquer crime ou que fundos ou propriedades específicos definitivamente sejam frutos de um crime ou de financiamento do terrorismo.

5. VERIFICAÇÃO E EFETIVIDADE DA POLÍTICA PLD-FT

A instituição deverá manter processo contínuo de verificação do cumprimento desta Política, dos procedimentos internos de PLD-FT e dos controles implementados, com o objetivo de avaliar sua efetividade e aderência à regulamentação vigente.

A área de Compliance será responsável por realizar revisões periódicas dos processos de cadastro, monitoramento de operações, comunicação ao COAF, retenção de documentos e demais controles relacionados à prevenção à lavagem de dinheiro e ao financiamento do terrorismo.

As deficiências identificadas deverão ser formalmente registradas, avaliadas quanto à sua criticidade e submetidas à definição de plano de ação com responsáveis e prazos para regularização. A implementação das medidas corretivas deverá ser acompanhada até sua conclusão, sendo mantidos registros que evidenciem a adoção das providências necessárias.

Quando aplicável, a auditoria interna ou função equivalente deverá avaliar de forma independente a efetividade da estrutura de PLD-FT, reportando suas conclusões à alta administração.

5.1 Avaliação Interna de Risco

- Define o objetivo: identificar, mensurar e compreender os riscos por atividades, produtos, clientes e geografias
- Estabelece periodicidade mínima anual (ou quando houver mudanças significativas no negócio)
- Determina que os resultados subsidiam a calibragem dos controles e são reportados à Alta Administração

5.2 Avaliação de Efetividade

- Define o objetivo: verificar se políticas, procedimentos e controles são adequados e funcionam efetivamente
- Lista os elementos cobertos: cadastro/due diligence, monitoramento, comunicações ao COAF, treinamentos
- Incorpora os parágrafos já existentes sobre deficiências e plano de ação
- Inclui o papel da Auditoria Interna e conecta os resultados ao ciclo de revisão anual da Política

6. PUBLICAÇÃO E DISTRIBUIÇÃO DE POLÍTICAS

Qualquer nova política ou modificação de documento existente deve ser disponibilizada a todas as partes interessadas. Documentos públicos podem ser encontrados nos websites da Localpayment.

HISTÓRICO DE REVISÃO E APROVAÇÃO	
13/03/2026	Revisão
18/03/2026	Aprovação pelo Comitê de Compliance