POLÍTICA DE PREVENÇÃO À LAVAGEM DE DINHEIRO E FINANCIAMENTO AO TERRORISMO

Dados da Empresa

Razão Social	POWERPAY SOLUCOES DE MEIOS DE PAGAMENTOS LTDA
CNPJ	29.991.788/0001-27
Nome Fantasia	Powerpay
Endereço	Av. Presidente Getúlio Vargas, 1605, LJ 013, Bairro Novo – Olinda / PE
CEP	53.030-010

Informações Gerais

Título	Política de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo (PLD/FT)
Número da Versão	V1.0.03
Aprovador	Diretoria Executiva
Data da Aprovação	19/02/2025
Departamento Responsável pela Política	Jurídico e Compliance
Classificação da Informação	Interna

Histórico das versões

Versão	Motivo da Alteração	Data da alteração	Autor	Departamento
1.0.02	Adequação	08/08/2025	Midian Michelle Santos da Silva	Compliance
1.0.03	Adequação	19/02/2026	Midian Michelle Santos da Silva	Compliance

SUMÁRIO

1. INTRODUÇÃO *4*

2. OBJETIVO *4*

3. APLICABILIDADE *4*

4. VIGÊNCIA, REVOGAÇÃO E CICLO DE REVISÃO *5*

5. DEFINIÇÕES, ETAPAS E INDICIOS DE LD/CT *5*

5.1 ETAPAS DO CRIME DE LAVAGEM DE DINHEIRO *5*

5.2 DIRETRIZES PARA IDENTIFICAÇÃO DE TRANSAÇÕES ATÍPICAS *6*

5.3 IDENTIFICAÇÃO E TRATAMENTO DE INDÍCIOS DE LAVAGEM DE DINHEIRO E FINANCIAMENTO AO TERRORISMO *7*

5.4 TREINAMENTOS *8*

5.5 AVALIAÇÃO INTERNA DE RISCOS *9*

5.6 METODOLOGIA *9*

6. RESPONSABILIDADES *10*

6.1 DIRETORIA EXECUTIVA *10*

6.2 COMITÊ DE RISCO E COMPLIANCE *11*

6.3 COMPLIANCE *11*

6.4 ÁREA COMERCIAL *12*

6.5 COLABORADORES *12*

6.6 TECNOLOGIA DA INFORMAÇÃO *12*

6.7 RECURSOS HUMANOS..... *12*

6.8 DIRETORIA DE PREVENÇÕ DE FRAUDE..... *12*

6.9 DEPARTAMENTO DE OPERAÇÕES/CREDENCIAMENTO *12*

7. PROCEDIMENTO DE COMUNICAÇÃO DE ATIVIDADES SUSPEITAS *13*

7.1 TREINAMENTO E CONSCIENTIZAÇÃO *13*

8. FLUXO DE TRATAMENTO DE CASOS SUSPEITOS DE FRAUDE DE LD/FT *14*

9. LISTAS RESTRITIVAS *15*

10. REGISTRO DE OPERAÇÕES E SERVIÇOS FINANCEIROS *16*

11. RELATÓRIO ANUAL *16*

12. PENALIDADES..... *16*

13. SIGILO DAS INFORMAÇÕES *16*

14. ADESÃO *17*

15. CONSIDERAÇÕES FINAIS *17*

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

1. INTRODUÇÃO

A Política de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (PLD/FT) da PowerPay estabelece as diretrizes e procedimentos destinados a assegurar que sua operação de meios de pagamento, realizada exclusivamente de forma presencial por meio de terminais POS, esteja em conformidade com a legislação e regulamentação aplicáveis.

A Política tem como finalidade prevenir a utilização da estrutura operacional da PowerPay para práticas ilícitas, incluindo ocultação ou dissimulação de origem de recursos, fraude, financiamento ao terrorismo e outros crimes correlatos.

Para tanto, a PowerPay adota controles proporcionais ao seu modelo de negócio, contemplando:

- Procedimentos de identificação e qualificação de clientes (KYC);
- Avaliação de risco cadastral e operacional;
- Monitoramento contínuo de comportamento transacional atípico em ambiente presencial;
- Análise reforçada para Pessoas Expostas Politicamente (PEP);
- Comunicação e reporte de operações suspeitas, quando aplicável;
- Adoção de medidas preventivas e corretivas sempre que identificadas inconsistências relevantes.
-

Considerando tratar-se de operação exclusivamente presencial, o monitoramento concentra-se na compatibilidade entre atividade declarada, porte do estabelecimento e volume transacionado, bem como na identificação de padrões que possam indicar desvio de finalidade.

Esta Política deve ser interpretada em conjunto com o Código de Conduta e Ética, a Política de Gestão de Riscos e demais normativos internos da PowerPay, compondo o seu sistema integrado de governança e compliance.

O compromisso da PowerPay é atuar de forma diligente, preventiva e colaborativa com autoridades e parceiros do ecossistema de pagamentos, preservando a integridade de sua operação e a confiança do mercado.

2. OBJETIVO

A **PowerPay** adota a Política de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (PLD/FT) como parte integrante de sua estrutura de governança e compliance, com o objetivo de conduzir suas atividades de forma íntegra, transparente e em conformidade com a legislação aplicável ao setor de meios de pagamento.

Esta Política estabelece diretrizes e procedimentos que devem ser observados

por colaboradores, administradores, sócios e prestadores de serviços, visando prevenir a utilização da estrutura operacional da companhia para práticas ilícitas.

Além da identificação e tratamento de situações suspeitas, a Política busca integrar os mecanismos de gestão de riscos da PowerPay aos princípios de ética, responsabilidade e conformidade que orientam suas operações.

3. APLICABILIDADE

Esta Política é aplicável a todas as pessoas vinculadas à POWERPAY, em especial aos administradores, colaboradores, estagiários, diretores terceirizados e operadores envolvidos com negócios e atividades da empresa.

4. VIGÊNCIA, REVOGAÇÃO E CICLO DE REVISÃO

Esta Política/manual possui vigência de 1 (um) ano e deve ser revisada e aprovada pelo Departamento de Compliance, anualmente ou em prazo inferior, se assim requerido pelo regulador local, no caso de alteração na legislação aplicável ou se houver alguma alteração das práticas de negócios da POWERPAY ou arranjo de pagamento que justifiquem, no entender do Compliance, a atualização desta Política. Após aprovada, esta Política será amplamente divulgada internamente.

5. DEFINIÇÕES, ETAPAS E INDICIOS DE LD/CT

Lavagem de Dinheiro - A expressão "lavagem de dinheiro" consiste na prática de atividades criminosas que visam tornar o dinheiro ilícito em lícito, ou seja, é o processo pelo qual o criminoso transforma recursos ganhos em atividades ilegais em recursos com uma origem aparentemente legal ao ocultar ou dissimular a natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente, de infração penal.

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 ganho de diversas atividades lícitas ou ilícitas tais como tráfico de drogas, prostituição, crime organizado, contrabando, extorsões, sequestros, fraudes etc.

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

Coligadas - As sociedades Corretoras de Valores Mobiliários, Corretoras de Seguros, Seguradora, Gestoras de Recursos de Terceiros em que a Companhia tenha influência significativa (art. 243, §1o, da Lei no 6.404/76).

5.1 ETAPAS DO CRIME DE LAVAGEM DE DINHEIRO

O processo de Lavagem de Dinheiro envolve algumas etapas que serão dispostas a seguir (i) colocação, (ii) ocultação e (iii) integração.

(i) **Colação:** momento em que o criminoso introduz valores obtidos ilicitamente no sistema econômico através da realização de depósitos, compra de bens, ou até mesmo, instrumentos negociáveis.

Basicamente, trata-se de remoção do dinheiro do local em que foi ilegalmente adquirido, com posterior inclusão no mercado financeiro.

(ii) **Ocultação:** é a etapa em que o agente realiza transações suspeitas e caracterizadoras do crime de Lavagem de Dinheiro, consistindo em segregação física entre o agente e o dinheiro ilícito, através de transações para desassociar a fonte ilegal do dinheiro.

(iii) **Integração:** momento em que o dinheiro recebe aparência lícita, integrando definitivamente no sistema econômico e financeiro.

5.2 DIRETRIZES PARA IDENTIFICAÇÃO DE TRANSAÇÕES ATÍPICAS

É diretriz da PowerPay assegurar que todos os colaboradores, sócios e parceiros envolvidos na operação estejam aptos a identificar situações que possam indicar indícios de lavagem de dinheiro ou financiamento ao terrorismo.

Considerando que a atuação da PowerPay é **exclusivamente presencial, por meio de terminais POS**, a companhia adota mecanismos de monitoramento compatíveis com seu modelo operacional, voltados à identificação de comportamentos transacionais atípicos e inconsistentes com o perfil do estabelecimento credenciado.

Para esse fim, a PowerPay utiliza sistemas internos de acompanhamento e regras automatizadas de monitoramento, aliados à análise humana realizada pela área de Risco e Compliance. Esses mecanismos incluem:

Diretrizes Gerais de Monitoramento

1. Monitoramento contínuo das transações realizadas nos terminais POS, com geração de alertas para movimentações atípicas ou incompatíveis com o perfil do estabelecimento;
2. Análise de padrões transacionais com base em critérios comportamentais, financeiros e operacionais;
3. Revisões periódicas da base de clientes e do comportamento transacional;
4. Capacitação periódica dos colaboradores para identificação de sinais de alerta no contexto da operação presencial.

Regras de Monitoramento – Ambiente Presencial (POS)

Financeiros

1. Comparação entre valor da transação e modo de captura utilizado (chip, tarja ou NFC), para identificar operações fora do padrão esperado para cada modalidade presencial;
2. Variação incomum do ticket médio por estabelecimento;
3. Transações com valores incompatíveis com o porte, segmento ou perfil cadastral do estabelecimento comercial;
4. Crescimento abrupto e não justificado de volume transacionado.

Temporais

5. Operações realizadas em horários incompatíveis com o funcionamento declarado do estabelecimento;
6. Mudanças relevantes e súbitas no padrão de dias e horários de operação.

Operacionais

7. Volume excessivo de transações com o mesmo cartão no mesmo estabelecimento, podendo indicar autofinanciamento ou circularidade de recursos;
8. Alta incidência de cancelamentos ou transações negadas;
9. Padrões repetitivos de captura incompatíveis com a prática usual do segmento;
10. Inconsistência entre atividade declarada e comportamento transacional observado.

Análise Complementar

Além das métricas automatizadas, a empresa mantém uma **lista de sinais adicionais de alerta**, que podem indicar operações suspeitas quando observadas isoladamente ou em conjunto:

6. Transações repetidas entre as mesmas partes com ganhos ou perdas incomuns, salvo em operações recorrentes.
7. Mudanças repentinas nas práticas operacionais do EC (volume, frequência, horário ou modo de entrada).
8. Dificuldade ou resistência no fornecimento de informações básicas de identificação ou documentação.
9. Impossibilidade de identificar o beneficiário final da operação.
10. Propostas ou operações incompatíveis com o perfil socioeconômico ou a capacidade técnica e financeira declarada.
11. Participação de pessoas físicas ou jurídicas vinculadas a países **não cooperantes com as diretrizes do Grupo de Ação Financeira Internacional (GAFI)** ou constantes em listas de sanções internacionais, como OFAC, União Europeia ou ONU, especialmente quando envolvem transações de alto valor, envio de recursos para o exterior ou uso de instituições financeiras off-shore.

5.3 IDENTIFICAÇÃO E TRATAMENTO DE INDÍCIOS DE LAVAGEM DE DINHEIRO E FINANCIAMENTO AO TERRORISMO

Existem alguns meios de identificação e tratamento de Indícios de Lavagem de Dinheiro e Financiamento ao Terrorismo que devem ser explorados, sendo estes:

(i) Processo de Identificação "Conheça Seu Cliente" e Diretrizes para EC's.

A política denominada Know Your Client ("KYC") é parte integrante da Política de Prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo, conhecida como "PLDFT". Além de estabelecer limites de padrão de prevenção de atividades ilícitas, a política KYC implementa diretrizes específicas para assegurar um eficaz conhecimento dos clientes e das atividades que os integram. Essas diretrizes incluem:

1. **Identificação e Verificação:** Exigir que todos os clientes forneçam documentação oficial de identificação, como passaporte, RG ou CPF, selfie do cliente, além de comprovante de endereço. A autenticidade desses documentos é verificada e as informações fornecidas são validadas. Também utilizamos ferramentas especializadas de parceiros para apoiar a análise, incluindo consultas a bases públicas e privadas, a fim de identificar possíveis processos legais ou presenças em listas restritivas.
2. **Due Diligence Contínua:** Manter um monitoramento contínuo das transações e atividades dos clientes, identificando padrões suspeitos ou incomuns que possam indicar atividades ilícitas. Revisar periodicamente os perfis dos clientes para garantir que as informações estejam atualizadas.

3. **Classificação de Risco:** Avaliar o nível de risco de cada cliente com base em fatores como histórico de transações, país de origem, natureza dos negócios e outras informações relevantes. Clientes de alto risco deve ser submetidos a uma due diligence aprimorada.
4. **Treinamento de Colaboradores:** Garantir que todos os colaboradores recebam treinamento adequado sobre a política KYC e estejam cientes das suas responsabilidades na identificação e prevenção de atividades ilícitas.
5. **Registros e Relatórios:** Manter registros detalhados de todas as interações e transações dos clientes por um período mínimo exigido pela legislação. Relatar qualquer atividade suspeita às autoridades competentes de acordo com as obrigações legais.

Cumpre informar que a política supracitada se assemelha a uma medida de segurança utilizada pelas organizações através de políticas de compliance, tendo como principal foco a busca de meios para proteger a empresa contra procedimentos de suborno e corrupção. Além disso, o adequado conhecimento do cliente minimiza a possibilidade de entrada de capital decorrente de atividade criminosa ou ilícita na POWERPAY, assegurando o escopo e a cultura da empresa.

(ii) Processo "Conheça seu Funcionário"

A política denominada Know Your Employee ("KYE") é parte integrante da Política de Prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo, conhecida como "PLDFT". Ademais, estabelece limites de padrão de prevenção de atividades consideradas ilícitas, efetuando monitoramentos contínuos e obtendo informações do dia a dia de todos os seus colaboradores.

Cumpre informar que a política supracitada se assemelha a uma medida de segurança utilizada pelas organizações através de políticas de compliance, tendo como principal foco, a garantia da segurança na relação entre colaboradores e empresas, desde os primórdios da fase de recrutamento e seleção.

Dessa forma, a política visará o controle e formalização de procedimentos, levando a organização e o bem-estar empresarial e dos colaboradores como prioridade.

(iii) Processo "Conheça Seu Fornecedor"

Trata-se de um conjunto de regras e procedimentos que devem ser adotados para identificação e aceitação de fornecedores e prestadores de serviços, prevenindo a contratação de empresas inidôneas ou suspeitas de envolvimento em atividades ilícitas.

Cumpre informar que para aqueles que representarem maior risco, devem ser adotados procedimentos complementares e diligências aprofundadas de avaliação e alçadas específicas de aprovação, de acordo com a criticidade dos apontamentos ou exceções.

Sendo assim, o processo de investigação assegura a relação com todas as entidades que a organização se relaciona para que haja um controle maior perante fornecedores e prestadores de serviço.

(iv) Processo "Conheça seu Parceiro"

Tem como principal objetivo estabelecer diretrizes e procedimentos destinados a conhecer os clientes, parceiros e prestadores de serviço terceirizados, bem como colaboradores, assegurando a diligência na identificação, qualificação e classificação de risco de LDFT nestes relacionamentos.

O conjunto de regras, procedimentos e controles que devem ser adotados para identificar negócios com contrapartes idôneas ou suspeitas de envolvimento com atividades

ilícitas, com relação aos parceiros comerciais da empresa.

5.4 TREINAMENTOS

A área de Compliance da POWERPAY é responsável por revisar regularmente os conceitos contidos na Política de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo (PLDFT) e promover a adoção de medidas apropriadas em casos de suspeita de atividades ilícitas.

Para garantir a eficácia dessas medidas, são conduzidos treinamentos que abrangem uma parte conceitual detalhada e uma avaliação dos conhecimentos adquiridos. É requerido que colaboradores, sócios e agentes autônomos alcancem um mínimo de 70% de acertos na avaliação para aprovação. Aqueles que não atingirem esse padrão deverão realizar um novo treinamento, garantindo assim a competência na detecção de operações suspeitas de lavagem de dinheiro e financiamento ao terrorismo.

Diretrizes para Treinamento:

1. **Abrangência dos Treinamentos:** Os treinamentos cobrem aspectos essenciais da PLDFT, incluindo reconhecimento de sinais de alerta, procedimentos de reporte e responsabilidades individuais.
2. **Participação Obrigatória:** Todos os funcionários, incluindo dirigentes, devem participar dos treinamentos iniciais e de reciclagem conforme exigido pela área de Compliance.
3. **Plataforma de Treinamento:** Utilização de plataforma online de terceiros para realizar os treinamentos, garantindo acesso fácil e documentação dos resultados.
4. **Avaliação de Conhecimento:** Além da parte conceitual, os treinamentos incluem avaliações que devem ser passadas com sucesso para demonstrar compreensão adequada das políticas e procedimentos.
5. **Reforço da Importância da Conformidade:** Os treinamentos destacam a importância estratégica da conformidade com as leis e regulamentos aplicáveis, protegendo assim a integridade e reputação da empresa.

Além disso, durante o processo de contratação, todos os novos colaboradores, sócios ou agentes autônomos devem completar este treinamento. A POWERPAY está associada à Associação PAGOS, que oferece treinamentos especializados em compliance, transações e subadquirentes, enriquecendo ainda mais a capacitação de nossos colaboradores para enfrentar os desafios regulatórios e éticos do setor.

5.5 AVALIAÇÃO INTERNA DE RISCO

Para identificação dos riscos de que trata o caput, a avaliação interna deve considerar, no mínimo, os perfis de risco:

1. Dos clientes;

2. Do próprio supervisionado, levando em conta seus modelos de negócio e áreas de atuação;

3. Das operações, independentemente do modo como possam ser formalmente designadas no âmbito da entidade supervisionada, levando em conta suas características, notadamente no que se refere a forma e meio de pagamento, bens, valores, ativos, produtos ou serviços envolvidos e instrumentos, tecnologias ou canais utilizados em sua realização; e

4. Dos funcionários, prestadores de serviços terceirizados e colaboradores de um modo geral,

bem como dos parceiros com atuação relevante em modelos de negócio adotados pelo supervisionado, levando em conta as atividades correspondentes.

Diante disso, os riscos identificados devem ser avaliados quanto à probabilidade de ocorrência e magnitude dos impactos associados, bem como, devem ser definidas categorias de risco que possibilitem a adoção de procedimentos reforçados.

Tal avaliação deve ser documentada e aprovada, bem como divulgada a todos os prestadores de serviço.

A política não tem por objetivo elencar as exigências mínimas para a avaliação interna de risco. Seguem alguns critérios que podem ser utilizados na avaliação interna de riscos:

1. Clientes que têm histórico de investigação com atividades criminosas podem receber pontuações mais altas, assim como figuras políticas, PEP, ou pessoas que fazem parte de organizações políticas ou organizações sem fins lucrativos.

2. Companhias abertas, que na maioria das vezes contam com mais informações disponíveis publicamente e auditoria independente, podem receber pontuação mais baixa do que empresas de capital fechado que não disponibilizem essas mesmas informações ou não tenham essa mesma condição.

3. Especial atenção pode ser requerida para estruturas societárias como trusts ou outras nas quais seja difícil identificar o Beneficiário Final, bem como para sociedades localizadas em países com regras inadequadas de PLDFT ou proteção rigorosa de sigilo societário.

5.6 METODOLOGIA

A **POWERPAY** adota a **Abordagem Baseada em Risco (ABR)** para o gerenciamento e mitigação de riscos, ajustando os controles conforme o nível de exposição identificado. Essa abordagem tem como base a **Avaliação Interna de Riscos**, que considera:

- Perfis de risco de clientes e da instituição;
- Tipologia de operações, transações, produtos e serviços;
- Canais de distribuição utilizados, incluindo novas tecnologias.

A Avaliação é revisada **anualmente ou sempre que necessário**, garantindo constante aprimoramento dos processos.

A empresa adota uma abordagem estruturada e contínua para garantir a efetividade de sua Política de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (PLDFT). Para isso, são realizados programas permanentes de capacitação, direcionados a colaboradores, parceiros e prestadores de serviços, sempre alinhados aos riscos identificados.

O monitoramento das operações é conduzido de forma sistemática, com base em procedimentos rigorosos de registro e rastreabilidade das transações, assegurando a identificação da origem e do destino dos recursos. Para apoiar esse processo, são utilizados modelos analíticos e estatísticos capazes de identificar comportamentos atípicos e detectar operações suspeitas.

As comunicações de operações consideradas suspeitas seguem um fluxo estruturado, garantindo que os casos sejam devidamente analisados e, quando cabível, comunicados ao COAF dentro dos prazos legais estabelecidos. Todo o tratamento das informações é realizado com a devida confidencialidade e em conformidade com os normativos internos.

Além disso, qualquer lançamento de novos produtos, serviços ou canais passa por análise

prévia sob a ótica da PLDFT, assegurando a adoção de medidas mitigatórias compatíveis com os riscos envolvidos.

6. RESPONSABILIDADES

Toda a estrutura organizacional da POWERPAY tem atribuições específicas no processo de combate à Lavagem de Dinheiro e ao Financiamento ao Terrorismo.

6.1 DIRETORIA EXECUTIVA

A Diretoria Executiva será responsável por:

(i). Revisar e aprovar as diretrizes aplicáveis às questões de PLD e CFT;

(ii). Supervisionar o cumprimento e aderências das práticas com o auxílio da área de compliance;

(iii). Prover recursos para que toda equipe atuante no processo possa alcançar seus objetivos;

(iv). Zelar pela prevenção aos crimes de Lavagem de Dinheiro e Financiamento ao Terrorismo descritos nesta política.

6.2 COMITÊ DE RISCO E COMPLIANCE

É de responsabilidade deste comitê:

(i). Validar as manutenções das normas pertinentes a essa política;

(ii). Aprovar os manuais de procedimentos que envolvem a prevenção e o combate aos crimes de Lavagem de Dinheiro e Financiamento ao Terrorismo;

(iii). Assegurar a conformidade com a legislação e os regulamentos internos que disciplinam a prevenção e combate à Lavagem de Dinheiro e ao Financiamento ao Terrorismo;

(iv). Zelar pelos manuais que envolvem a prevenção à Lavagem de Dinheiro e Combate ao Financiamento ao Terrorismo, descritos neste documento;

(v). Apreciar os relatórios e comunicações emitidos pelos órgãos reguladores, autorreguladores, pela auditoria interna e auditoria externa, determinando as ações e providências necessárias para atendimento das demandas.

6.3 COMPLIANCE

Essa área é a principal responsável pelo programa e tem por funções:

(i). Divulgar e dar conhecimento aos colaboradores quanto as normas e procedimentos relativos à prevenção aos crimes de Lavagem de Dinheiro e Combate ao Terrorismo;

(ii). Efetuar manutenção aos controles internos e manuais relativos a essa política;

(iii). Prover treinamento aos colaboradores;

(iv). Monitorar e analisar as transações suspeitas ou de não conformidade identificadas através das ferramentas disponíveis;

(v). Informar ao UIF os casos considerados suspeitos após ter passado pelo Comitê de Compliance, conforme procedimentos descritos neste manual;

(vi). Registrar e fornecer parecer conclusivo com relação à análise realizada dos suspeitos;

(vii). Informar aos colaboradores da POWERPAY, eventos e tendências no que tange à prevenção e combate à Lavagem de Dinheiro, contemplando inclusive mudanças nas políticas e procedimentos, através de e-mails enviados e/ou treinamentos;

(viii). Em decorrência de qualquer identificação de indícios de Lavagem de Dinheiro, corrupção ou Financiamento ao Terrorismo por parte dos clientes, a POWERPAY, deve seguir com o bloqueio do cadastro suspeito até que o processo seja avaliado e caso seja comprovado iniciar o processo de término do relacionamento com o cliente.

6.4 ÁREA COMERCIAL

É de responsabilidade do departamento comercial:

Aplicar as melhores práticas no que tange o "(KYC - Know Your Customer)", comunicando o compliance da POWERPAY, ou seu superior sempre que suspeitar de alguma atividade que vá de encontro às diretrizes aqui descritas.

6.5 COLABORADORES

Todos os colaboradores da POWERPAY, têm as responsabilidades relacionadas ao programa de prevenção e combate à Lavagem de Dinheiro e ao combate do financiamento ao terrorismo.

Estas funções e responsabilidades variam de acordo com a área e função do colaborador na POWERPAY Em comum, todos são responsáveis por comunicar à área de Compliance, qualquer situação de atipicidade ou suspeição com que se depararem no desempenho de suas atividades.

6.6 TECNOLOGIA DA INFORMAÇÃO

Responsável por garantir a confidencialidade, a integridade e a disponibilidade da informação e dos sistemas utilizados pela POWERPAY, solucionando quaisquer problemas decorrentes de falhas que possam colocar em risco as diretrizes dessa política.

6.7 RECURSOS HUMANOS

Responsável por viabilizar programas de treinamento periódicos garantindo com isso que todos os colaboradores estejam aptos e atualizados quanto às suas obrigações e responsabilidades de acordo com a regulamentação aplicável pela POWERPAY

Certificar-se de que todos os colaboradores fizeram o treinamento anual do Programa de PLD e disponibilizá-los sempre que for solicitado.

6.8 DIRETORIA E PREVENÇÃO DE FRAUDE

É de responsabilidade da Prevenção a Fraude:

1. Monitorar o risco operacional e reportar ao Compliance caso seja identificada alguma atipicidade;

2. Implementar controles visando à mitigação do risco transacional onde essas transações e as liquidações possam ser utilizadas para o Financiamento ao Terrorismo ou para a Lavagem de Dinheiro.

6.9 DEPARTAMENTO DE OPERAÇÕES / CREDENCIAMENTO

É responsabilidade do departamento:

1. Verificar com o time de risco/compliance quando houver surgimento de indício de irregularidade ou dúvida sobre o procedimento a ser adotado para o devido encaminhamento do processo;

2. Consultas ao risco/compliance quanto a identificação de clientes PEP/OFAC/BLACKLIST/COAF/CADIN e demais listas restritivas, que seguem procedimento particular com a efetivação do processo de cadastro, com periodicidade mensal além do onboarding;

3. Efetuar o cumprimento de todos os requisitos contidos na Política de credenciamento (Cadastro) e informar ao responsável por compliance caso haja alguma alteração nas regras de credenciamento.

7. PROCEDIMENTO DE COMUNICAÇÃO DE ATIVIDADES SUSPEITAS

A Política deve prever a obrigatoriedade de que os Colaboradores relatem qualquer indício de situação atípica de à área de PLDFT, compliance, Controles Internos, Gerenciamento de Riscos ou outra área equivalente responsável para esse fim.

O objetivo deste procedimento é estabelecer diretrizes claras para a identificação, documentação e comunicação de atividades suspeitas relacionadas a lavagem de dinheiro e financiamento ao terrorismo ao COAF (no Brasil) ou ao Credenciador, conforme aplicável. Este procedimento visa garantir a conformidade legal e a integridade das operações financeiras da empresa.

Transações que apresentem qualquer um dos critérios estabelecidos, conforme descrito no documento " Prevenção de Fraudes POWERPAY," devem ser consideradas como atividades suspeitas.

A área responsável deverá promover a imediata análise da operação atípica, de forma a averiguar a materialidade dos indícios existentes, devendo comunicar ao COAF, no prazo de **24 (vinte e quatro) horas** da conclusão da análise, as transações ou propostas de transação que constituam ou possam constituir sérios indícios de crime de lavagem de dinheiro ou ocultação de bens, direitos ou valores provenientes direta ou indiretamente de infração penal.

As comunicações realizadas têm caráter confidencial e devem ser restritas aos Colaboradores envolvidos no processo de análise. Todos os registros que fundamentem a comunicação ou a decisão pela sua não realização deverá ser arquivados pelo prazo de 5 (cinco) anos.

Na hipótese de inexistência de operações de comunicação ao COAF durante o ano civil, a Instituição deverá atestar a inocorrência de tais operações na periodicidade e forma estabelecida

pelos órgãos reguladores e fiscalizadores.

7.2 Treinamento e Conscientização:

Todos os colaboradores, sócios e agentes autônomos devem ser treinados e conscientizados sobre a importância da identificação e comunicação de atividades suspeitas. Eles devem estar cientes dos critérios estabelecidos e das etapas deste procedimento.

Este procedimento deve ser revisado periodicamente para garantir sua eficácia e conformidade contínuas com as regulamentações.

8. FLUXO DE TRATAMENTO DE CASOS SUSPEITOS DE FRAUDE DE LD/FT

(i) **Detecção Inicial:**

- A detecção inicial de casos suspeitos pode ocorrer por meio do monitoramento contínuo, revisão de transações, denúncias internas ou externas, ou qualquer outra atividade de prevenção de fraudes.

(ii) **Triagem Inicial:**

- Quando um caso suspeito é detectado, ele é encaminhado para a equipe de triagem inicial, que avalia a credibilidade das suspeitas. Casos com alta probabilidade de serem fraudulentos ou relacionados a LD/FT são priorizados para investigação.

(iii) **Investigação Preliminar:**

- A equipe de investigação preliminar realiza uma análise mais aprofundada do caso. Isso inclui revisão de documentos, registros de transações, entrevistas com envolvidos e qualquer outra atividade necessária para determinar a gravidade da suspeita.

(iv) **Avaliação de Risco:**

- Com base na investigação preliminar, o caso é avaliado em termos de risco. Isso envolve determinar o impacto potencial sobre a empresa e sua conformidade com regulamentações.

(v) **Comunicação Interna:**

- Caso o caso seja considerado de alto risco ou envolva atividades claramente fraudulentas ou relacionadas a LD/FT, ele é comunicado internamente às autoridades apropriadas, como o departamento de compliance, o jurídico e a alta administração da POWERPAY.

(vi) **Comunicação Externa:**

- Caso as suspeitas se confirmem após a investigação detalhada e haja evidências suficientes para acreditar que o caso está relacionado a fraudes ou LD/FT, a POWERPAY tomará as medidas necessárias para comunicar prontamente as autoridades competentes, incluindo o Credenciador, a polícia e outras agências reguladoras pertinentes (vii) **Monitoramento Contínuo:**

- Após a resolução do caso, continuaremos monitorando atentamente a atividade dos nossos clientes e transações relacionadas para garantir que não haja reincidência.

(viii) **Indisponibilidade de Bens e Ativos em Caso de Vínculo com Terrorismo**

- Conforme o Art. 11 da Lei Federal 13.813/19, em situações onde seja identificada a ligação de clientes ou beneficiários com atividades terroristas, será implementada a indisponibilidade imediata de seus bens, direitos e ativos, tanto no território nacional quanto no exterior. A POWERPAY colaborará com as autoridades competentes para assegurar o cumprimento das sanções aplicáveis, tomando as medidas cabíveis para bloquear os recursos financeiros e bens que possam estar envolvidos.

Este fluxo de tratamento de casos suspeitos é essencial para manter a conformidade legal, proteger a integridade da empresa e mitigar riscos relacionados a fraudes e LD/FT. É importante adaptar o processo às necessidades específicas de sua organização e à legislação aplicável em sua jurisdição.

9. LISTAS RESTRITIVAS

Serão realizadas revisões periódicas (no momento do cadastro, no decorrer da operação/mensalmente e em situações pontuais) para que haja a devida atualização de dados e pesquisas, e os pareceres se dividirão em:

(i) **Aprovado**, em que o contrato poderá ser firmado com o cliente;

(ii) **Aprovado com ressalvas**, no caso de clientes ou pessoas relacionadas à condição de PPE, clientes com restrições leves que não sejam ligadas a crimes de lavagem de dinheiro ou condutas corruptas, e portanto, será remetido ao Comitê de Compliance para emissão de parecer final.

Assim, quando classificado como "Aprovado com Ressalvas" e/ou Alto Risco, ele também deverá ser classificado conforme a lista abaixo no sistema de acompanhamento e monitoramento de PLDFT:

I. Pessoa Politicamente Exposta (PPE);

II. Listas Restritivas;

III. Listas de Sanções;

IV. Especial Atenção (para todos os clientes Aprovados com Ressalvas);

V. Não residente no Brasil;

VI. Apontado na Lei Anticorrupção;

VII. Apontado em Mídia;

VIII. Grandes Fortunas.

(iii) **Em processo de aprovação**, no aguardo de justificativa ou documento complementar; ou

(iv) **Rejeitado**, quando este possui ligação com crimes de lavagem de dinheiro, financiamento ao terrorismo, corrupção ou condutas em desacordo com os procedimentos, códigos e manuais de políticas da POWERPAY Em consequência disso, não terá contrato firmado.

A pesquisa em listas restritivas se constitui como um procedimento preventivo que procura sinalizar, se o cliente figurou em situações PLDFT. Essas rotinas têm o propósito de identificar se os clientes e terceiros são pessoas expostas politicamente, se figuram em alguma lista restritiva externa nacionais e internacionais, exercem profissão de risco (lista interna), se residem em cidade de fronteira e se possuem processos judiciais.

Durante o preenchimento do cadastro, os clientes devem declarar se são considerados Pessoas Politicamente Expostas (PPE), conforme exigido pela Instrução CVM nº 463/08, Resolução COAF nº 29/17, Circular BACEN nº 3.978/20 e Carta Circular BACEN nº 3430/10. As PPEs exigem atenção especial, uma vez que se enquadram em um grupo de alto risco. Além disso, de acordo com o Art. 67 da Circular BACEN nº 3.978/20, é necessário manter a guarda do cadastro e das informações do cliente por um período mínimo de **10 anos.**

Caso o cliente faça parte de PPE e não informe a POWERPAY, será considerada nas análises de indícios de lavagem de dinheiro.

Importante ressaltar que os clientes que sejam representantes, família ou pessoas de relacionamento próximo, devem igualmente ser consideradas, e diante disso, monitoradas de forma especial.

Informa-se que as revisões das análises deverão ocorrer de acordo com o nível de risco observado, e as fichas cadastrais devem apresentar a assinatura do gestor responsável e do Diretor de Risco, Compliance e PLDFT, de acordo com o Artigo 64 da Lei 8.383/91.

Apenas no momento em que todas as informações e documentos forem validados e aprovados, os clientes serão aceitos. Entretanto, mesmo em caso de não aceitação, serão informados.

Em decorrência de qualquer identificação de indícios de Lavagem de Dinheiro, corrupção, Financiamento ao Terrorismo, ou registro em listas de sanções impostas por resoluções do Conselho de Segurança das Nações Unidas (CSNU), a POWERPAY pode deliberar pelo término do relacionamento.

Ademais, todas as situações em que um colaborador da POWERPAY entender que tenha relação com indícios de condutas ilícitas, deverá reportar imediatamente à Diretoria de Risco, Compliance e PLDFT.

10. REGISTRO DE OPERAÇÕES E SERVIÇOS FINANCEIROS

A POWERPAY assegura que possui mecanismos efetivos para o registro de todas as operações e serviços financeiros realizados, conforme estabelecido pela Seção I, Capítulo VI da Circular BACEN nº 3.978. Esses registros, efetuados via CERC, incluem as informações mínimas exigidas, como a identificação dos clientes, a natureza das operações, valores transacionados, e demais dados relevantes para garantir a rastreabilidade e a conformidade com a regulamentação vigente.

A POWERPAY mantém sistemas de controle e acompanhamento contínuo dessas operações, permitindo que os registros sejam acessíveis às autoridades competentes e preservados de acordo com o prazo regulamentar.

11. RELATÓRIO ANUAL

Para devida verificação dos procedimentos contidos na regulamentação que rege a PLD/CFT, são realizados testes anuais, que posteriormente deverão constar em relatório formalizado de responsabilidade da Diretoria de Compliance e PLDFT. Ao ser ratificado pelo Comitê Executivo, será encaminhado à Administração anualmente.

Este relatório é de extrema importância para o acompanhamento das políticas da empresa.

12. PENALIDADES

Em caso de violação às regras estabelecidas desta Política, será realizada investigação pela área de compliance e aplicação das medidas disciplinares cabíveis, podendo inclusive, haver rescisão contratual de trabalho ou serviço e comunicação às autoridades competentes.

Ademais, em casos de exceção ao cumprimento das regras previstas na política, o solicitante deverá apresentar pedido de exceção à Diretoria com as razões que o fundamentam para que este entre em análise.

As penalidades podem ocorrer administrativamente, podendo chegar em penalidade de caráter criminal.

13. SIGILO DAS INFORMAÇÕES

Cumpre informar que toda e qualquer relacionada a dados de indícios ou suspeita de lavagem de dinheiro e combate ao financiamento de terrorismo são de caráter confidencial, não devendo ser disponibilizadas de forma alguma as partes envolvidas.

As comunicações de casos suspeitos, conforme previsto na Circular BACEN nº 3.978/20, são de uso exclusivo dos Órgãos Reguladores, não sendo compartilhadas com outras partes. Além disso, reforça-se que os dados dos clientes devem ser mantidos pela instituição por um período mínimo de 10 anos, conforme exigido pela regulamentação

14. ADESÃO

Todos os colaboradores deverão assinar um termo comprovando o recebimento deste documento, bem como ciência de todo o seu conteúdo, obrigando-se a respeitá-lo de forma integral.

Todos os colaboradores, ainda, deverão aderir aos treinamentos dispostos neste documento.

A política referida no caput deve ser divulgada aos funcionários, prestadores de serviços terceirizados e colaboradores de um modo geral, bem como aos parceiros com atuação relevante em modelos de negócio adotados pelo supervisionado, mediante linguagem clara e acessível, em nível de detalhamento compatível com os papéis que desempenhem e com a sensibilidade das informações.

15. CONSIDERAÇÕES FINAIS

Em casos de dúvidas ou esclarecimentos sobre o conteúdo desta política, ou em relação a algum assunto específico, o colaborador da deverá enviar um e-mail para contato@PowerPay.com