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

CONTROLE DE DOCUMENTO

INFORMAÇÕES DO DOCUMENTO

DOCUMENTO	
Título	Política de Prevenção à Lavagem de Dinheiro e o Combate do Financiamento ao Terrorismo - Versão Site
Código	PLD-001
Número da Versão	00
Data	27/11/2023
Departamento	PLD e Riscos
Responsável	Joana Puls Martines

REVISÃO

HISTÓRICO DA REVISÃO			
Data	Assunto	Responsável	Nº Rev.
27/11/2023	Elaboração da Política de Prevenção à Lavagem de Dinheiro e o Combate do Financiamento ao Terrorismo.	Joana Puls Martines	00

APROVAÇÃO

Nº Revisão.	Diretoria Executiva	
	Data	Responsável
00		Joana Puls Martines

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

I. Abreviações e Definições

Merchant: Clientes com contrato com a Sterbey, processando transações pela OKP.
Usuário: Todos os usuários/clientes do Merchant que compram online via meio de pagamento OKP.
OKP: One Key Payments
PLD/CFT: Prevenção à Lavagem de Dinheiro/Combate ao Financiamento ao Terrorismo
CDD: Customer Due Diligence (Devida Diligência do Cliente)
EDD: Enhanced Due Diligence (Devida Diligência Aprimorada)
GAFI: Grupo de Ação Financeira Internacional
PEP: Pessoa Exposta Politicamente
RBA: Risk-Based Approach (Abordagem Baseada em Risco)
SDD: Simplified Customer Due Diligence (Devida Diligência Simplificada do Cliente)
MLRO: Money Laundering Reporting Officer
KYC: Know Your Customer (Conheça Seu Cliente)

II. Políticas Abordadas

Este documento abrange as políticas e procedimentos da OKP para Prevenção à Lavagem de Dinheiro e Combate ao Financiamento ao Terrorismo.

III. Objetivo

Definir diretrizes, procedimentos e controles para funcionários, parceiros e terceirizados, promovendo a conformidade com as exigências legais e regulamentares.

IV. Escopo da Política

Aplicada a todos os funcionários, representantes e diretores da OKP. Deve ser entregue digitalmente, com confirmação de leitura.

V. DA LEGISLAÇÃO

A legislação a seguir caracteriza os crimes de "lavagem de dinheiro" e define as responsabilidades das Instituições perante os respectivos órgãos fiscalizadores:

Lei no 9.613 de 03/03/1998:

Dispõe sobre lavagem de dinheiro, cria o COAF, e trata da prevenção de ilícitos no sistema financeiro.

Lei no 12.863 de 09/07/2012:

Altera a Lei no 9.613 para melhorar a persecução penal dos crimes de lavagem de

dinheiro.

Lei no 13.260 de 16/03/2016:

Regulamenta o terrorismo, disposições investigatórias, processuais e reformula o conceito de organização terrorista; altera outras leis.

Lei no 13.506 de 13/11/2017:

Trata do processo administrativo sancionador no âmbito do Banco Central do Brasil e da Comissão de Valores Mobiliários.

Lei no 13.810 de 08/03/2019:

Dispõe sobre o cumprimento de sanções do Conselho de Segurança da ONU, incluindo indisponibilidade de ativos.

Circular Bacen no 3.978 de 23/01/2020:

Define políticas, procedimentos e controles internos para prevenir crimes financeiros.

Carta Circular Bacen no 4.001 de 29/01/2020:

Divulga operações e situações configurando indícios de crimes de lavagem de dinheiro e financiamento ao terrorismo.

Resolução BCB no 44 de 24/11/2020:

Estabelece procedimentos para execução de medidas relacionadas às sanções do Conselho de Segurança da ONU.

Resolução BCB no 96 de 19/05/2021:

Dispõe sobre a abertura, manutenção e encerramento de contas de pagamento.

Resolução BCB no 150 de 06/10/2021:

Consolida normas sobre arranjos de pagamento e aprova regulamento para serviços de pagamento.

Resolução BCB no 278 de 31/12/2022:

Regulamenta a Lei no 14.286 em relação ao capital estrangeiro no País, operações de crédito externo e investimento estrangeiro direto.

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

Comunicado no 40.390 de 10/07/2023:
Divulga comunicado do Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo (GAFI/FATF).

VI. DA POLÍTICA

1. **Introdução**

Como resposta à crescente preocupação mundial das autoridades em coibir a lavagem de dinheiro e o financiamento ao terrorismo, a OneKey Payments reforça seu compromisso e suas políticas internas, visando combater com eficácia tais condutas.

A OneKey Payments alinhada às normas emanadas pelas autoridades que lutam contra a lavagem de dinheiro e o financiamento ao terrorismo, manifesta sua solidariedade e máxima colaboração com asautoridades competentes, atuando para trazer segurança em todos os processos e procedimentos constantes de suas atividades. Cumprindo o compromisso de estabelecer de normas e procedimentos internos eficazes, a Onekey Payments visa desenvolver a atividade financeira conforme regras e regulamentos vigentes;

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

A OneKey Payments estabelece diretrizes rigorosas para prevenir a lavagem de dinheiro (LD) e o financiamento do terrorismo (FT). É vital que todas as áreas da empresa sigam essas diretrizes para garantir conformidade com as leis e regulamentações nacionais e internacionais. A Área de Monitoramento, juntamente com outros colaboradores, desempenha um papel fundamental na identificação e comunicação de operações suspeitas.

A lavagem de dinheiro é descrita como o processo de disfarçar a origem criminosa de recursos, podendo envolver estágios como colocação, diversificação e integração. A luta contra o financiamento do terrorismo está intrinsicamente vinculada à batalha contra a lavagem de dinheiro.

Os processos de lavagem de dinheiro podem abranger vários estágios, sendo o financiamento do terrorismo (FT) quando há tentativas de canalizar fundos para locais onde possam ser utilizados ilegalmente. Embora lavagem de dinheiro (LD) e FT compartilhem semelhanças, são crimes distintos. Ambos são desafios internacionais sérios, ameaçando a indústria de pagamentos e economias globais. Dada a natureza das operações da OneKey Payments, é crucial adotar medidas apropriadas para identificar e prevenir tais atividades criminosas, em conformidade com padrões internacionais.

VII. DIRETRIZES

A OneKey Payments (OKP) adota uma abordagem baseada em risco para enfrentar os desafios de lavagem de dinheiro (LD) e financiamento do terrorismo (FT). Suas diretrizes, revisadas regularmente, têm como foco:

Conhecimento Abrangente dos Clientes:

Estabelecimento de regras e controles internos para garantir a verificação completa dos clientes, prevenindo transações com identidades não verificadas ou informações falsas.
Governança Específica para LD/FT:

Estrutura de governança dedicada ao cumprimento das obrigações de prevenção à LD/FT, com comunicação de operações suspeitas ao Banco Central do Brasil.

Procedimentos para Produtos e Serviços:

Procedimentos para análise prévia de novos produtos e serviços, detecção de atividades suspeitas e ações correspondentes.
Avaliação Periódica de Riscos:

Avaliação interna periódica para identificação e mensuração de riscos relacionados a produtos, serviços, clientes, instituição e operações.

Revisão Regular da Efetividade:

Avaliação regular da efetividade da política, procedimentos e controles internos, promovendo uma cultura organizacional de prevenção à LD/FT.

Cultura Organizacional e Treinamento:

Práticas de promoção da cultura organizacional de prevenção e treinamento específico para funcionários, parceiros e prestadores de serviços terceirizados.

Medidas Preventivas na Contratação:

Estabelecimento de medidas preventivas no processo de contratação de funcionários, parceiros e prestadores de serviços.

Procedimentos de Identificação:

Procedimentos e mecanismos para identificação de clientes, funcionários, parceiros e prestadores de serviços, incluindo a verificação de beneficiários finais e presença em listas restritivas.

Registro Detalhado de Operações:

Registro detalhado de todas as operações, produtos e serviços, com procedimentos específicos para identificação de origem e destino dos recursos.

Monitoramento de Operações Suspeitas:

Implementação de métodos de monitoramento, seleção, análise e controle para examinar operações suspeitas de LD/FT.

Comunicação ao COAF:

Comunicação ao COAF com informações detalhadas sobre clientes, processo KYC, movimentação financeira ou operação suspeita, e origem e destino dos recursos utilizados.
Relatório Anual de Avaliação:

Elaboração anual de relatório de avaliação de efetividade da política, procedimentos e controles internos, destacando deficiências identificadas e plano de ação para solucioná-las.

VIII. ABORDAGEM BASEADA EM RISCO

A OneKey Payments (OKP) utiliza uma Abordagem Baseada em Risco (ABR) para aplicar os requisitos de Due Diligence do Cliente (CDD), adaptando-se sensivelmente ao risco associado a cada cliente, relacionamento comercial, produto ou transação. Esse processo envolve a identificação, mitigação e monitoramento contínuo de riscos de lavagem de dinheiro e financiamento do terrorismo, com armazenamento digital de informações obtidas durante o CDD. O Comitê de Riscos e Conformidade (CRCO) revisa e aprova regularmente os controles para garantir a eficácia das medidas de mitigação de risco. A aplicação da ABR visa gerenciar eficientemente os riscos, não proibir transações específicas, enquanto o CDD é realizado em todos os casos, independentemente da abordagem baseada em risco.

XIX. RISCO

A OneKey Payments (OKP) categoriza os riscos ao lidar com comerciantes com base em critérios como risco do comerciante, risco do produto/serviço, risco de interface e risco geográfico, resultando em grupos de Baixo, Médio e Alto risco. Após essa identificação, a OKP utiliza uma tabela de avaliação para conduzir a devida diligência correspondente. A empresa avalia se o cliente está alinhado com seu apetite de risco, determinando a aceitação ou rejeição, com o envolvimento dos times comercial, responsável pelo contato inicial, e Compliance, que realiza análise de risco e Know Your Customer (KYC). Clientes de alto risco estão sujeitos a medidas reforçadas de due diligence, como Pessoas Expostas Politicamente (PEPs) e clientes não presenciais. A avaliação inicial é seguida pelo acompanhamento contínuo das transações e revisões das atividades do cliente, sendo elementos cruciais da abordagem baseada em risco da OKP.

1. **Gestão e Mitigação de Riscos**

   A OneKey Payments (OKP) implementou controles abrangentes para gerenciar e mitigar riscos após a identificação e avaliação. Esses controles incluem programa de identificação e verificação do cliente, padrões de qualidade documental, obtenção de informações adicionais quando necessário e monitoramento de transações/atividades com base na avaliação de risco. A OKP monitora continuamente esses controles, ajustando-os conforme necessário diante de mudanças nas circunstâncias do cliente. Avaliações periódicas garantem a adequação dos riscos, controles internos e disposições de conformidade, assegurando a eficácia dos controles em todos os departamentos da instituição.

2. **Aceitação de Riscos**

   A OneKey Payments (OKP) proíbe explicitamente que seus clientes (Merchant)

realizem transações relacionadas à venda de itens como medicamentos prescritos, drogas ilícitas, armas de fogo, pornografia infantil, entre outros.

Além disso, a OKP não permite transações com comerciantes não licenciados quando a licença é exigida pela lei aplicável ao escopo específico do negócio do comerciante. A empresa também veta bens ou serviços que violem os direitos de propriedade intelectual de terceiros.

3. **Padrões internacionais**

A OneKey Payments (OKP) adota medidas rigorosas para mitigar riscos, recusando iniciar ou manter relações comerciais com indivíduos ou entidades cuja legitimidade esteja em dúvida. A empresa evita conexões com terroristas identificados por organizações como a ONU, OFAC, União Europeia, GAFI e World-Check, realizando verificações de listas internacionais durante a due diligence de novos clientes. Em caso de correspondência, o processo é interrompido e comunicado ao CRCO para ação. O nível de risco atribuído a um cliente influencia a intensidade da due diligence e monitoramento contínuo de suas atividades. A OKP mantém uma política de evitar jurisdições consideradas proibidas.

XX. DUE DILIGENCE

1. PROCEDIMENTOS DE USUÁRIOS FINAIS

O Merchant realiza uma Due Diligence abrangente dos usuários que operam em seu site online. Para efetuarem transações com a OneKey Payments, os usuários devem fornecer um número de documento de identificação, validado por verificações em bureaus por meio de API. As operações dos clientes e usuários são monitoradas, incluindo o acompanhamento de transações, controles de lista restrita (contendo pessoas envolvidas em fraudes ou proibidas de transações), e controles de limite de usuários, ajustados conforme o mercado estabelecido pelo cliente (Merchant).

2. Due Diligence Aprimorada (EDD)

A OneKey Payments (OKP) emprega a Due Diligence Aprimorada (EDD) com foco em riscos mais elevados de Lavagem de Dinheiro e Financiamento do Terrorismo (LD/FT). Conforme os padrões de Prevenção à Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo (PLD/FTC), a OKP requer medidas EDD em casos como transações sem presença física do comerciante, relações com Pessoas Politicamente Expostas (PEP), operações transfronteiriças e identificação de "sinais de alerta" durante a Due Diligence. Essas situações são classificadas como Risco Elevado na matriz de risco.

Para comerciantes de alto e muito alto risco, a OKP implementa medidas adicionais de Due Diligence, como rastreamento da origem dos fundos, monitoramento contínuo aprimorado, exigência de políticas PLD/FTC e solicitação de documentos adicionais em casos de bandeira vermelha. A aprovação do Diretor de Compliance e do CEO é necessária para comerciantes de risco muito alto.

A OKP realiza EDD para relações comerciais ou transações vinculadas a jurisdições listadas pelo Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do

Terrorismo (GAFI).

A definição de Pessoas Politicamente Expostas (PEP) abrange diversos cargos políticos e posições em entidades públicas ou privadas internacionalmente. A condição de PEP se aplica por cinco anos após a pessoa deixar de se enquadrar nas categorias especificadas. A OKP verifica diretamente com o comerciante ou beneficiário efetivo durante o processo de Due Diligence.

3. **Monitoramento contínuo e atualizações KYC do relacionamento comercial:**

Após o estabelecimento de um relacionamento comercial, a OneKey Payments (OKP) implementa procedimentos de monitoramento contínuo para garantir a conformidade com o perfil de risco e as informações detidas. Esse monitoramento abrange verificações de antecedentes, adversidades na mídia e acompanhamento contínuo de transações para identificar comportamentos incomuns. A equipe de compliance define limites para transações, rejeitando aquelas que ultrapassam esses limites para mitigar riscos. A OKP utiliza ferramentas automatizadas para monitoramento, verificações de antecedentes e atualizações regulares do KYC, variando a frequência com base no perfil de risco do cliente: anual para alto risco, a cada dois anos para médio risco e a cada três anos para baixo risco. A OKP reporta discrepâncias materiais nas informações da propriedade beneficiária ao registrador durante o monitoramento, garantindo registros atualizados e em conformidade com as regulamentações.

XXI. DAS RESPONSABILIDADES

A OneKey Payments estabeleceu uma estrutura interna de prevenção e controle para lidar com lavagem de dinheiro e financiamento ao terrorismo. Liderada pelo Diretor Executivo, essa estrutura abrange diversas áreas, incluindo Compliance, Comercial, Recursos Humanos, Auditoria Interna, Tecnologia, Produtos e demais colaboradores.

O Comitê Diretivo tem papel fundamental na aprovação/revisão de políticas, deliberação sobre procedimentos, recomendação de ações mitigatórias, análise de relatórios regulatórios e auditorias. O Diretor Executivo é responsável pela implementação e monitoramento do cumprimento da política.

Todos os profissionais da Instituição têm responsabilidades específicas na prevenção e controle, e para a área de PLD a identificação e monitoramento de operações suspeitas, avaliação de riscos, garantia de conformidade com leis e regulamentos, implementação de treinamentos e manutenção de registros.

XXII. REVISÃO E APROVAÇÃO

Esta política resumida será aprovada em conjunto com a política completa de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo após aprovada entrará automaticamente em vigor devendo ser divulgada no site da empresa.