

Prevenção à Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo

PRINCIPAIS PONTOS DA POLÍTICA



Sumário

1 Introdução	3
1.1 Visão Geral	3
1.2 Objetivo	3
1.3 Escopo	3
1.4 Cumprimento	3
1.5 Reporte de suspeita de violação à política	3
1.6 Exceções	3
1.7 Divulgação Da Política	3
2 Definições	4
3. Programa De PLD/CFT	4
3.1. Avaliação Interna de Risco	4
3.2. Abordagem Baseada em Risco	5
3.3. Avaliação De Efetividade	5
3.4. Produtos, Serviços e Novas Tecnologias	5
3.5. Conheça seu Cliente, Funcionários, Parceiros e Terceiros	5
3.5.1. Conheça seu Cliente - KYC	6
3.5.2. Conheça seu Funcionário e Conheça seu Parceiro e Terceiro	6
3.6. Monitoramento, Seleção, Análise de Operações e Situações Suspeitas	6
3.7. Comunicação de Operações ou Situações Suspeitas ao COAF	7
3.8. Quality Assurance	7
3.9. Bloqueio de Ativos (Lista sancionadora CSNU)	7
3.10. Treinamento	7
4. Mecanismos de Acompanhamento e de Controle	7
5. Guarda e Manutenção das Informações e Documentos	8
6. Sigilo	8
7. Canais de Comunicação e denúncias de PLD/CFT	8

SumUp Brasil	Versão: 6.2
Principais pontos da Política PLD-CFT	Data: 7 de abril de 2026

1 INTRODUÇÃO

1.1 VISÃO GERAL

A SumUp está comprometida com a criação, manutenção e execução de um efetivo programa de PLD/CFTP cumprindo as melhores práticas nacionais e internacionais, além das leis aplicáveis.

1.2 OBJETIVO

Estabelecer diretrizes para à Prevenção de Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo, com base no porte, volume das transações, natureza e complexidade dos produtos, serviços, atividades, processos e canais de distribuição, bem como estabelecer uma abordagem baseada em risco.

1.3 ESCOPO

Esta Política de Prevenção à Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo (“Política”) é aplicada a todos os produtos, serviços, operações, canais de distribuição, funcionários, clientes, parceiros e terceiros da SumUp Brasil, que envolve a Instituição de Pagamento e a Sociedade de Crédito Direto.

1.4 CUMPRIMENTO

A adesão e o cumprimento desta Política são obrigatórios, e suas violações podem resultar em procedimentos disciplinares, sanções administrativas e até penalidades criminais, por lavagem de dinheiro e financiamento ao terrorismo. A negligência e a falha voluntária são consideradas descumprimento desta política.

1.5 REPORTE DE SUSPEITA DE VIOLAÇÃO À POLÍTICA

Funcionários e terceiros com informações sobre possíveis descumprimento a esta Política devem imediatamente reportar a situação.

1.6 EXCEÇÕES

Exceções a esta política devem ser aprovadas pelo proprietário da política e formalmente documentadas. As exceções de política serão revisadas periodicamente para verificar sua adequação.

1.7 DIVULGAÇÃO DA POLÍTICA

Esta Política é amplamente divulgada dentro da organização através de seus canais corporativos de comunicação.

Sendo também divulgada aos parceiros e prestadores de serviços terceirizados, conforme sua relevância, através de comunicações por e-mail e, quando aplicável através de treinamento dedicado a este público.

2 DEFINIÇÕES

A lavagem de dinheiro consiste na ocultação ou dissimulação da natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente, de infração penal.

As etapas do processo de lavagem de dinheiro podem desenvolver-se ao longo de determinado espaço de tempo ou simultaneamente e podem ser definidas da seguinte maneira:

- I. **Colocação:** a colocação se realiza por meio da aplicação dos recursos obtidos de forma ilícita em depósitos, compra de instrumentos negociáveis ou de bens no comércio ou em operações nas quais se admite dinheiro em espécie.
- II. **Ocultação:** a segunda etapa do processo consiste em dificultar a recomposição do ciclo das operações e o rastreamento contábil dos recursos. Nessa etapa o criminoso busca quebrar a cadeia de evidências da origem dos recursos movimentados.
- III. **Integração:** nesta última etapa, os recursos ilícitos são incorporados formalmente ao sistema econômico.

O financiamento do terrorismo se configura quando alguém, direta ou indiretamente, por qualquer meio, prestar apoio financeiro, fornecer ou reunir fundos com a intenção de serem utilizados ou sabendo que serão utilizados, total ou parcialmente, por grupos terroristas para a prática de atos terroristas.

3. PROGRAMA DE PLD/CFTP

O programa de PLD/CFTP visa mitigar de forma eficaz e robusta as ameaças de LD/FTP, evitando que os produtos e serviços oferecidos pela SumUp sejam utilizados para tais atividades ilícitas. Este programa é regido por políticas e procedimentos que estabelecem diretrizes claras.

É composto também pelos elementos descritos a seguir:

3.1. **AVALIAÇÃO INTERNA DE RISCO**

A SumUp elabora a cada dois anos sua Avaliação Interna de Risco (AIR), documento que identifica, mensura e mitiga o risco de utilização de seus produtos e serviços na prática de lavagem de dinheiro e financiamento ao terrorismo levando em consideração as suas características específicas, e prevê critérios específicos relativos:

- I. Aos clientes.
- II. Instituição, incluindo o modelo de negócio e a área geográfica de atuação.

SumUp Brasil	Versão: 6.2
Principais pontos da Política PLD-CFT	Data: 7 de abril de 2026

- III. Das operações, transações, produtos e serviços, abrangendo todos os canais de distribuição.
- IV. Das atividades exercidas pelos funcionários, parceiros e prestadores de serviços terceirizados.

O risco identificado deve ser avaliado quanto à sua probabilidade de ocorrência e à magnitude dos impactos financeiro, jurídico, reputacional e socioambiental para a instituição. Deve utilizar a Avaliação Nacional de Riscos (ANR) como subsídio.

3.2. ABORDAGEM BASEADA EM RISCO

A SumUp utiliza a Avaliação Interna de Risco para definir uma abordagem proporcional aos riscos identificados de LD/FT, sendo assim, medidas de diligências aprofundadas em riscos mais altos e diligências simplificadas quando os riscos forem menores.

3.3. AVALIAÇÃO DE EFETIVIDADE

A SumUp elabora anualmente a Avaliação de Efetividade, de modo a avaliar a efetividade das políticas, procedimentos e controles internos de PLD/CFTP. Os planos de ação endereçados a solucionar as deficiências identificadas, por meio da referida avaliação, devem ser acompanhados pelo time de PLD/CFTP e Controles Internos.

A SumUp deve elaborar um plano de ação destinado a solucionar as deficiências identificadas por meio da avaliação de efetividade, o acompanhamento da implementação do plano de ação deve ser documentado por meio de relatório de acompanhamento.

A data-base da avaliação será de 31 de dezembro, e deve ser encaminhada para ciência da diretoria executiva até 31 de março do ano seguinte da data-base. O plano de ação e o respectivo relatório de acompanhamento devem ser encaminhados para ciência e avaliação, até 30 de junho do ano seguinte ao da data-base do relatório à Diretoria Executiva.

3.4. PRODUTOS, SERVIÇOS E NOVAS TECNOLOGIAS

Novos produtos e serviços, incluindo a utilização de novas tecnologias, bem como alterações significantes, devem ser avaliados e analisados de forma prévia, sob a óptica de PLD/CFTP, para a identificação, mitigação dos riscos e a realização de seu monitoramento.

Após avaliação, as recomendações e pareceres serão documentados. Deve dispensar especial atenção a produtos, serviços e novas tecnologias com classificação de maior risco.

3.5. CONHEÇA SEU CLIENTE, FUNCIONÁRIOS, PARCEIROS E TERCEIROS

A SumUp possui procedimentos de coleta, verificação, validação e atualização cadastral visando conhecer seus funcionários, parceiros e terceiros, além da devida diligência (Due Diligence) a fim de garantir que os mesmos sejam avaliados, qualificados e classificados quanto ao perfil de risco de

SumUp Brasil	Versão: 6.2
Principais pontos da Política PLD-CFT	Data: 7 de abril de 2026

PLD/CFTP, que deve ser mantido atualizado e contemplando medidas reforçadas para as classificações de maior risco.

3.5.1. CONHEÇA SEU CLIENTE - KYC

A SumUp definiu procedimentos descritos em documento específico para o processo de Conheça seu Cliente com um conjunto de ações que são adotadas pela área de Onboarding e KYC para assegurar a identidade e a idoneidade das atividades exercidas por todos seus clientes.

A base desse programa é composta pelas exigências regulatórias de coleta, verificação, validação e atualização das informações necessárias à identificação de clientes e verificação da qualidade das informações prestadas. Após a devida diligência, o cliente poderá ser classificado de acordo com seu perfil de risco.

Para os perfis de alto risco, são realizadas pesquisas complementares, com a solicitação de documentação adicional e uma diligência aprofundada (*Enhanced Due Diligence*), incluindo a aprovação de um membro da área de PLD/CFTP com nível hierárquico superior quando necessário.

Além disso, a SumUp realiza revisões periódicas e atualização de dados de acordo com o nível de risco dos clientes, e a classificação é revista sempre que houver alteração em seu perfil de risco e na natureza da relação de negócio.

3.5.2. CONHEÇA SEU FUNCIONÁRIO E CONHEÇA SEU PARCEIRO E TERCEIRO

Os processos de Conheça seu Funcionário e Conheça seu Terceiro são um conjunto de regras, controles e processos, estabelecidos e adotados com a finalidade de preservar o alto padrão de integridade e evitar o vínculo com pessoas relacionadas à prática de LD/FT e crimes antecedentes.

Devem ser classificados de acordo com as atividades exercidas e compatíveis com a avaliação interna de riscos. As informações relativas aos funcionários, parceiros e terceiros devem passar por uma atualização periódica, considerando inclusive eventuais alterações que impliquem mudança de classificação nas categorias de risco.

3.6. MONITORAMENTO, SELEÇÃO, ANÁLISE DE OPERAÇÕES E SITUAÇÕES SUSPEITAS

Todas as movimentações e operações financeiras, além de propostas, realizadas por seus clientes são monitoradas de forma tempestiva, englobando todos os produtos e serviços disponibilizados pela instituição, bem como por meio de convênio de participação.

3.7. COMUNICAÇÃO DE OPERAÇÕES OU SITUAÇÕES SUSPEITAS AO COAF

As operações, situações e/ou propostas com indícios de LD/FT são comunicadas ao órgão regulador competente - COAF, de forma tempestiva, não ultrapassando o prazo máximo de 24 horas após a

Público	SumUp Brasil	Página 6 de 8
---------	--------------	---------------

SumUp Brasil	Versão: 6.2
Principais pontos da Política PLD-CFT	Data: 7 de abril de 2026

decisão. As comunicações realizadas têm caráter confidencial e devem ser restritas aos colaboradores envolvidos no processo de análise.

3.8. QUALITY ASSURANCE

O QA em PLD/CFTP é uma função estratégica de segunda linha de defesa que monitora continuamente a efetividade dos processos e controles, combinando análises quantitativas e qualitativas. De forma independente e amostral, identifica lacunas sistêmicas, erros operacionais e alterações de processo não aprovadas por GRC, avaliando a aderência às normas internas e regulatórias, bem como a qualidade das análises e decisões tomadas. É aplicado aos processos de Monitoramento de Transações, KYC, KYE, KYS/KYP e PEP.

3.9. BLOQUEIO DE ATIVOS (LISTA SANCIONADORA CSNU)

Caso seja identificado qualquer cliente sancionado por Resoluções do CSNU, a SumUp realizará os procedimentos necessários para que os ativos sejam imediatamente indisponibilizados e prontamente realizará as comunicações dos ativos indisponibilizados e/ou tentativas de transferências.

3.10. TREINAMENTO

A Alta Administração da SumUp é comprometida em garantir uma cultura organizacional orientada a práticas de PLD/CFTP. Neste sentido, a SumUp promove a capacitação contínua e disseminação dessa cultura por meio de um programa de treinamento, visando o desenvolvimento, aprofundamento e a reciclagem do conhecimento sobre o tema e sua relevância..

O treinamento é direcionado à diretoria executiva, a todos os colaboradores, bem como a terceiros e parceiros relevantes. O programa tem como objetivo conscientizar sobre responsabilidades legais e regulamentares, bem como promover a cultura organizacional e disseminar as diretrizes definidas pela SumUp relacionadas ao tema.

4. MECANISMOS DE ACOMPANHAMENTO E DE CONTROLE

A área de PLD/CFTP mantém o controle e acompanhamento, incluindo a manutenção do conteúdo das Políticas e Procedimentos à disposição do Banco Central do Brasil, auditoria, membros da diretoria, entre outros.

5. GUARDA E MANUTENÇÃO DAS INFORMAÇÕES E DOCUMENTOS

A SumUp registra e armazena as informações de todas as operações realizadas e serviços financeiros, em seus produtos e serviços, inclusive saques, depósitos, aportes, pagamentos, recebimentos e transferências de recursos. Também registra e armazena os dossiês das operações/situações que fundamentaram a decisão de efetuar ou não as comunicações ao COAF.

SumUp Brasil	Versão: 6.2
Principais pontos da Política PLD-CFT	Data: 7 de abril de 2026

Os documentos referentes às operações, incluindo gravações e documentos cadastrais, são arquivados pelo período mínimo de 10 anos a partir do encerramento da conta ou da conclusão da última transação realizada pelo cliente.

Todas as informações relacionadas a dados de indícios / suspeitas de lavagem de dinheiro e financiamento do terrorismo são confidenciais, e não é permitida a disponibilização às partes envolvidas. As comunicações de casos suspeitos são de uso exclusivo dos Órgãos Reguladores para análise e investigação.

6. SIGILO

É proibido por lei o compartilhamento com o cliente ou com terceiros de qualquer informação referente a um caso que está sob investigação de LD/FT ou referente à uma comunicação de operação suspeita (SAR ou STR) que será enviada ao COAF.

Qualquer violação da lei será endereçada ao Comitê de Ética e as medidas disciplinares serão tomadas de acordo com a decisão dos mesmos.

7. CANAIS DE COMUNICAÇÃO E DENÚNCIAS DE PLD/CFTP

A SumUp dedica canais de comunicação para denúncia de indícios e / ou suspeitas de PLD/CFTP para seus Funcionários, Clientes, Terceiros e Parceiros, que observarem quaisquer desvios às diretrizes desta Política por meio dos canais eletrônicos:

- I. Canal de denúncias - A abertura de denúncias deve ser realizada conforme Política do Canal de Denúncias.

As situações comunicadas são totalmente sigilosas e mantém a confidencialidade do conteúdo e também do comunicante.