POLÍTICA DE PREVENÇÃO À LAVAGEM DE DINHEIRO E FINANCIAMENTO AO TERRORISMO

DOCUMENTO DE ACESSO PÚBLICO
Esta política foi elaborada pela LOGICS4U com fins meramente informativos.
É proibida a reprodução total ou parcial este documento, de qualquer forma ou por qualquer meio.

INFORMAÇÕES GERAIS

Dados	Política de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo
Número da Versão	V 1.5.00
Aprovador	Diretoria Executiva
Data da Aprovação	27/07/2026
Data da Revisão	07/07/2026

HISTÓRICO DAS VERSÕES

Versão	Motivo de Alteração	Data da Alteração	Autor	Área
1.0.00	Versão Inicial	21/01/2020	Thamires Oliveira	Jurídico e Compliance
1.2.00	Atualização dos procedimentos internos, revisão das definições e aperfeiçoamento da redação da política.	21/03/2022	Thamires Oliveira	Jurídico e Compliance
1.3.00	Revisão das responsabilidades das áreas, fortalecimento dos controles de prevenção e atualização dos procedimentos de KYC, KYP e KYE.	14/07/2022	Thamires Oliveira	Jurídico e Compliance
1.4.00	Adequação à regulamentação vigente, inclusão da Avaliação Interna de Risco (AIR), detalhamento das responsabilidades das áreas e revisão da estrutura da política.	19/11/2024	Thamires Oliveira	Jurídico e Compliance
1.5.00	Atualização da estrutura da política, adequação da governança de PLD/FT, revisão das responsabilidades das áreas, simplificação do documento e ajustes de redação, melhorias no procedimento de monitoramento, seleção e análise de operações e situações suspeitas e comunicação de operações e situações suspeitas.	27/07/2026	Thamires Oliveira	Jurídico e Compliance

DOCUMENTO DE ACESSO PÚBLICO
Esta política foi elaborada pela LOGICS4U com fins meramente informativos.
É proibida a reprodução total ou parcial este documento, de qualquer forma ou por qualquer meio.

APROVAÇÃO DIRETORIA EXECUTIVA

Diretor	Área	Data da Aprovação	Assinatura
Flávio Espuri	T.I	27/07/2026	
Marcelo Knoch	Relacionamento	27/07/2026	
Thamires Oliveira	Jurídico e Compliance	27/07/2026	
Vanderlei Silva	CEO	27/07/2026	

DOCUMENTO DE ACESSO PÚBLICO
Esta política foi elaborada pela LOGICS4U com fins meramente informativos.
É proibida a reprodução total ou parcial este documento, de qualquer forma ou por qualquer meio.

SUMÁRIO

1. OBJETIVO E ABRANGÊNCIA 5
1. VIGÊNCIA 5
2. DEFINIÇÕES 5
2.1. Lavagem de Dinheiro 5
2.2. Etapas do Crime de Lavagem de Dinheiro 5
2.3. Financiamento ao Terrorismo 6
2.4. Pessoa Exposta Politicamente (“PEP”) 6
2.5. Análise de Operações ou Situações Suspeita 6
3. AVALIAÇÃO INTERNA DE RISCO 7
4. REPONSABILIDADES E ATRIBUIÇÕES 7
4.1. Diretoria Executiva 7
4.2. Responsável por Compliance e PLD/FT 8
4.3. Área Comercial 8
4.4. Área Jurídica 9
4.5. Área de Produtos 9
4.6. Área de Operações/Relacionamento 9
4.7. Diretoria Executiva 9
4.8. Área de Tecnologia da Informação (“T.I”) 10
4.9. Colaboradores 10
5. AÇÕES DE PREVENÇÃO 11
5.1. Procedimentos Destinados a Conheça seu Cliente – “*KNOW YOUR CLIENT*” (“KYC”) 11
5.2. Procedimentos Destinados a Conheça seu Fornecedor/Parceiro – “*KNOW YOUR PARTNER*” (“KYP”) 11
5.3. Procedimentos Destinados a Conheça seu Funcionário – “*KNOW YOUR EMPLOYEE*” (“KYE”) 12
5.4. Registro de Operações 12
5.5. Monitoramento, Seleção e Análise de Operações e Situações Suspeitas 12
5.6. COMUNICAÇÃO DE OPERAÇÕES E SITUAÇÕES SUSPEITAS 13
6. CANAL DE COMUNICAÇÃO 13
7. NORMAS RELACIONADAS 13
8. DISPOSIÇÕES GERAIS 14

DOCUMENTO DE ACESSO PÚBLICO
Esta política foi elaborada pela LOGICS4U com fins meramente informativos.
É proibida a reprodução total ou parcial este documento, de qualquer forma ou por qualquer meio.

1. OBJETIVO E ABRANGÊNCIA

A presente Política de Prevenção à Lavagem de Dinheiro e de Financiamento do Terrorismo ("Política") visa estabelecer as diretrizes, regras e os procedimentos relacionadas à prevenção da utilização dos sistemas e serviços da Logics4u para a prática dos crimes de lavagem ou ocultação de bens, direitos e valores e de financiamento do terrorismo, conforme previsto na regulamentação do Banco Central do Brasil ("Bacen"), regras dos instituidores de arranjo de pagamento ("Bandeiras"), Lei n° 9.613/1998, Lei nº 13.260/2016, e demais legislações e regulações vigentes aplicáveis à matéria.

Esta Política é aplicável a todos os sócios, administradores, colaboradores, parceiros, fornecedores, clientes e prestadores de serviços internos e externos que mantenham qualquer relação com a Logics4u. É responsabilidade de todos os envolvidos conhecer e cumprir as obrigações estabelecidas nesta Política e nas regulamentações vigentes, bem como aderir aos mais elevados padrões de conduta ética e profissional ao desempenhar suas atividades, contribuindo de forma ativa para a prevenção de lavagem de dinheiro e do financiamento do terrorismo.

Ainda, é dever de todos informar e reportar à área de Compliance e PLD/FT qualquer inconsistência identificada nos procedimentos e práticas estabelecidas nesta Política.

1. VIGÊNCIA

Esta Política entra em vigor imediatamente após sua publicação, e encontra-se disponível na rede interna da empresa e em seu website https://logics4u.com.br/. A revisão do documento ocorrerá anualmente ou sempre que for necessário, seja em razão de alterações nas políticas internas da empresa ou em decorrência de mudanças nas legislações ou regulamentações aplicáveis ao tema.

2. DEFINIÇÕES

2.1. Lavagem de Dinheiro

Lavagem de Dinheiro é o processo pelo qual recursos originados de atividades ilegais são transformados em ativos de origem aparentemente legal. Essa prática geralmente envolve múltiplas transações, usadas para ocultar a origem dos recursos financeiros e permitir que eles sejam utilizados de forma a aparentar ter origem lícita.

Os responsáveis por esta operação fazem com que os valores obtidos por meio das atividades ilícitas e criminosas (como o tráfico de drogas, corrupção, comércio de armas, prostituição, terrorismo, extorsão, fraude, sonegação, suborno, estelionato, apropriação indébita, crime cibernético, entre outros) sejam dissimulados ou escondidos, aparecendo como resultado de operações comerciais legais e que possam ser absorvidas pelo sistema financeiro, naturalmente.

2.2. Etapas do Crime de Lavagem de Dinheiro

O processo de lavagem de dinheiro envolve três etapas, são elas: colocação, ocultação e integração.

(i) Colocação: É a etapa em que o criminoso introduz os valores obtidos ilicitamente no sistema econômico mediante depósitos, compra de instrumentos negociáveis, compra de bens, compra de criptomoedas, entre outros meios.

(ii) Ocultação: A ocultação é o momento que o agente realiza transações suspeitas e caracterizadoras do crime de lavagem de dinheiro. Nesta fase, diversas transações complexas se configuram para desassociar a fonte ilegal do dinheiro; e

(iii) Integração: O recurso ilegal integra-se definitivamente ao sistema econômico e financeiro. A partir deste momento, o dinheiro recebe aparência lícita.

2.3. Financiamento ao Terrorismo

O financiamento ao terrorismo consiste no processo de distribuição dissimulada de recursos a serem utilizados em atividades terroristas.

Tais recursos são oriundos, geralmente, das atividades de outras organizações criminosas envolvidas com o tráfico de drogas, armas e munições e com o contrabando, ou podem ser derivados de atividades ilícitas, incluindo doações a instituições de caridade de "fachada".

Os métodos utilizados pelos terroristas para dissimular o vínculo entre eles e as fontes de financiamento são geralmente semelhantes aos utilizados na prática de crime de lavagem de dinheiro. Entretanto, normalmente, os terroristas utilizam recursos obtidos de forma legal, visando reduzir o risco de serem descobertos antes do ato terrorista.

2.4. Pessoa Exposta Politicamente ("PEP")

Consideram-se pessoa politicamente exposta aquela que desempenha ou tenha desempenhado, nos 5 (cinco) anos seguintes à data em que a pessoa deixou de exercer cargos, empregos ou funções públicas relevantes no Brasil ou em outros países, territórios e dependências estrangeiras.

Os representantes, familiares e outras pessoas de seu relacionamento próximo também serão considerados PEP para fins desta Política.

2.5. Análise de Operações ou Situações Suspeita

Consiste na verificação da existência de indícios de utilização dos produtos e serviços da Logics4u para a prática dos crimes de Lavagem de Dinheiro e de Financiamento do Terrorismo ("PLD/FT"), baseada na movimentação, no comportamento ou nas características da operação.

Essa verificação é realizada em conformidade com os conceitos estabelecidos pela Circular nº 3978, de 23 de janeiro de 2020, e pela Circular nº 4001, de 29 de janeiro de 2020, ambas emitidas pelo Bacen.

DOCUMENTO DE ACESSO PÚBLICO
Esta política foi elaborada pela LOGICS4U com fins meramente informativos.
É proibida a reprodução total ou parcial este documento, de qualquer forma ou por qualquer meio.

3. AVALIAÇÃO INTERNA DE RISCO

Trata-se da implementação de um processo de Avaliação Interna de Risco em conformidade com as disposições desta Política. O objetivo é identificar possíveis riscos de uso dos serviços da Logics4u para práticas de Lavagem de Dinheiro e Financiamento ao Terrorismo. Esse processo permitirá mensurar os riscos identificados com base na probabilidade de ocorrência e à magnitude dos impactos financeiro, jurídico, reputacional e socioambiental para a Logics4u.

O processo de Avaliação Interna de Risco será previsto em documento específico apartado a esta Política, com a descrição da análise de risco a ser realizada para fins de PLD/FT, devendo constar minimamente:

(i) O perfil dos clientes;

(ii) O modelo de negócio e área geográfica de atuação da Logics4u;

(iii) As operações, transações, produtos e serviços, abrangendo todos os canais de distribuição e a utilização de novas tecnologias; e

(iv) As atividades exercidas pelos funcionários, parceiros e prestadores de serviços terceirizados.

Deverá ser definido categorias de risco que possibilitem a adoção de controles de gerenciamento e de mitigação reforçados para as situações de maior risco e a adoção de controles simplificados nas situações de menor risco.

4. REPONSABILIDADES E ATRIBUIÇÕES

A Logics4u está comprometida com a efetividade do disposto nesta política e com a promoção de cultura organizacional de prevenção à lavagem de dinheiro e de financiamento do terrorismo, contemplando, inclusive, os colaboradores, prestadores de serviços internos e externos e parceiros comerciais.

Será instituído mecanismos de acompanhamento e de controle de modo a assegurar a implementação e a adequação da política, dos procedimentos e dos controles internos determinados nesta Política.

As posições adiante apontadas são identificadas como tendo funções e responsabilidades diretas pela Política.

4.1. Diretoria Executiva

A Diretoria Executiva será responsável por:

(i) Deliberar sobre as diretrizes aplicáveis a esta Política;

(ii) Aprovar a Política de PLD/FT da empresa, e suas atualizações; e

DOCUMENTO DE ACESSO PÚBLICO
Esta política foi elaborada pela LOGICS4U com fins meramente informativos.
É proibida a reprodução total ou parcial este documento, de qualquer forma ou por qualquer meio.

(iii) Aprovar o processo/método utilizado para a Avaliação Interna de Risco.

4.2. Responsável por Compliance e PLD/FT

Considerando o porte, a estrutura organizacional e o modelo de negócios da LOGICS4U, as atividades relacionadas à Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo serão exercidas por responsável formalmente designado pela Diretoria Executiva, o qual poderá acumular outras funções na organização, sem prejuízo da autonomia necessária ao desempenho de suas atribuições.

Responsabilidades:

(i) Implementar e atualizar as Políticas em conformidade com as normas aplicáveis à PLD/FT, em especial aquelas que tratam sobre KYC, KYP e KYE, assegurando que a Logics4u atenda aos requisitos legislativos e regulatórios relacionados ao tema;

(ii) Analisar e fornecer suporte às áreas nas demandas regulatórias relacionadas à PLD/FT recebidas pela Logics4u;

(iii) Divulgar e dar treinamento aos colaboradores e prestadores de serviços internos quanto as normas e procedimentos relativos à esta Política;

(iv) Responsável por gerir e controlar os procedimentos, controles internos e manuais relacionados desta Política;

(v) Elaborar, documentar e manter a Avaliação Interna de Risco determinada nesta Política;

(vi) Identificar e analisar riscos operacionais e riscos relacionados a lavagem de dinheiro e de financiamento ao terrorismo;

(vii) Analisar e emitir parecer a ser submetido para deliberação de movimentações detectadas como operações suspeitas para fins de Lavagem de Dinheiro e de Financiamento ao Terrorismo; e

(viii) Gerar relatórios para acompanhamento das regulamentações e normas para PLD/FT.

(ix) Avaliar a efetividade da Política, dos procedimentos e dos controles internos de que trata esta Política.

4.3. Área Comercial

A área Comercial será responsável por:

(i) Solicitar os documentos necessários para realização de diligências em novos clientes e parceiros, bem como formulário cadastral e acompanhar essa demanda até que ela seja concluída pelas demais áreas envolvidas;

DOCUMENTO DE ACESSO PÚBLICO
Esta política foi elaborada pela LOGICS4U com fins meramente informativos.
É proibida a reprodução total ou parcial este documento, de qualquer forma ou por qualquer meio.

(ii) Encaminhar para áreas responsáveis todos os documentos necessários para a execução do processo de KYC/KYP; e

(iii) Reportar informações sobre clientes e parceiros à área de Compliance e PLD/FT, quando solicitados.

4.4. Área Jurídica

A área Jurídica será responsável por:

(i) Dar ciência aos prestadores de serviços externos e parceiros de negócios quanto as normas e procedimentos relativos à esta Política; e

(ii) Fornecer suporte à área de Compliance e PLD/FT nas investigações sobre suspeita de lavagem de dinheiro e de financiamento ao terrorismo.

4.5. Área de Produtos

A área de Produtos será responsável por:

(i) Dar ciência a Compliance e PLD/FT sobre novos produtos e serviços, para que sejam analisados os riscos sob a perspectiva de PLD/FT e que sejam atendidos os requisitos regulatórios necessários; e

(ii) Dar ciência a Compliance e PLD/FT sobre alteração/evolução de produtos e serviços e adoção de novas tecnologias, para que sejam analisados os riscos sob a perspectiva de Compliance e PLD/FT e que sejam atendidos os requisitos regulatórios necessários.

4.6. Área de Operações/Relacionamento

A área de Operações/Relacionamento será responsável por:

(i) Monitorar e selecionar operações e situações suspeitas realizadas no sistema de pagamento da Logics4u; e

(ii) Reportar à Compliance e PLD/FT as informações e relatórios relacionados à PLD/FT;

4.7. Diretoria Executiva

Compete a Diretoria Executiva assegurar que sejam adotadas as seguintes medidas:

(i) Adotar as recomendações para a seleção e a contratação de funcionários, prestadores de serviços e demais pessoas que atuem em nome da Logics4u, tendo em vista o risco de lavagem de dinheiro e de financiamento do terrorismo;

DOCUMENTO DE ACESSO PÚBLICO
Esta política foi elaborada pela LOGICS4U com fins meramente informativos.
É proibida a reprodução total ou parcial este documento, de qualquer forma ou por qualquer meio.

(ii) Divulgar aos colaboradores, prestadores de serviços e demais pessoas que atuem em nome da Logics4u os treinamentos, políticas e demais materiais relacionados ao tema de PLD/FT, conforme as recomendações de Compliance e PLD/FT;

(iii) Documentar todos os treinamentos realizados, bem como as políticas e demais materiais compartilhados sobre o tema de PLD/FT; e

(iv) Compartilhar com Compliance e PLD/FT um relatório contendo o registro dos treinamentos realizados, além das políticas e demais materiais compartilhados relacionados ao tema de PLD/FT.

4.8. Área de Tecnologia da Informação ("T.I")

A área de T.I será responsável por:

(i) Adotar as recomendações dispostas na Resolução BCB nº 85, de 08 de abril de 2021, que dispõe sobre segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

4.9. Colaboradores

São responsabilidades dos colaboradores, prestadores de serviços, administradores e demais pessoas que atuem em nome da LOGICS4U.

(i) Reportar imediatamente e diretamente à Compliance e PLD/FT qualquer indício ou suspeita de atividades ilícitas, incluindo Lavagem de Dinheiro e Financiamento ao Terrorismo, assegurando a confidencialidade das informações reportadas;

(ii) Conhecer, compreender e zelar pelo integral cumprimento desta Política e reportar imediatamente quaisquer irregularidades, falhas ou vulnerabilidades identificadas no processo de PDL/FT;

(iii) Atuar com probidade, boa-fé e ética profissional, adotando no desempenho de suas funções o máximo de cuidado, diligência e responsabilidade esperados de sua posição, e promovendo a integridade e a confiança nas práticas empresariais da Logics4u;

(iv) Participar de forma ativa em treinamentos e capacitações oferecidos pela empresa sobre PLD/FT, a fim de manter-se atualizado quanto às melhores práticas, legislações e normativos vigentes, fortalecendo o compromisso com a prevenção de atividades ilícitas; e

(v) Quando aplicável, colaborar com as investigações internas e externas sempre que solicitado, fornecendo informações precisas e completas, de acordo com as diretrizes estabelecidas pela empresa e pelas autoridades competentes.

DOCUMENTO DE ACESSO PÚBLICO
Esta política foi elaborada pela LOGICS4U com fins meramente informativos.
É proibida a reprodução total ou parcial este documento, de qualquer forma ou por qualquer meio.

5. AÇÕES DE PREVENÇÃO

Dentre as medidas adotadas para combater e prevenir a utilização dos produtos e serviços da Logics4u para a prática de crimes de lavagem de dinheiro e de financiamento ao terrorismo destaca-se:

(i) Procedimentos de "Conheça seu Cliente", "Conheça seu Fornecedor/Parceiro" e "Conheça seu Funcionário" listados nesta Política;

(ii) Investimentos em Treinamento de Pessoal;

(iii) Investimentos em ferramentas de controle e monitoramento, que permitam a detecção de operações e situações atípicas/suspeitas; e

(iv) Sistema de gestão de transações que registra e possibilita o monitoramento de todas as transações realizadas, com regras de parametrização para identificar casos que apresentem indícios de lavagem de dinheiro, financiamento ao terrorismo e corrupção, dentre outros comportamentos atípicos/suspeitos.

A Logics4u não estabelece negócios com pessoas físicas e/ou jurídicas que tenham comprovado envolvimento em fraudes e crimes financeiros, nem com pessoas físicas ou jurídicas cuja identificação não possa ser confirmada, ou que forneçam informações incompletas, falsas ou inconsistentes.

As ferramentas de monitoramento oferecem à Logics4u pleno controle de suas atividades, permitindo que quaisquer operações suspeitas possam ser prontamente analisadas para a devida comunicação aos órgãos competentes e atendimento da legislação em vigor.

5.1. Procedimentos Destinados a Conheça seu Cliente – "*KNOW YOUR CLIENT*" ("KYC")

Trata-se de um conjunto de ações destinadas a estabelecer mecanismos para identificação, qualificação e classificação dos clientes, identificação e qualificação do(s) beneficiário(s) final(is) e a identificação de Pessoa Exposta Politicamente ("PEP").

Os procedimentos deverão ser compatíveis com o perfil de risco do cliente, identificado no processo de KYC, e aderentes a esta Política. As informações obtidas durante o processo de KYC deverão ser armazenadas em sistemas informatizados apropriados e mantidas atualizadas durante toda a relação comercial e pelo período mínimo de 10 (dez) anos a contar do primeiro dia do ano seguinte ao encerramento da relação contratual.

O processo de KYC será detalhado em um documento específico, complementar a esta Política, contemplando, minimamente, os requisitos estabelecidos neste documento, devendo ser mantido atualizado.

5.2. Procedimentos Destinados a Conheça seu Fornecedor/Parceiro – "*KNOW YOUR PARTNER*" ("KYP")

Trata-se de um conjunto de ações destinadas a estabelecer mecanismos para identificação, qualificação e classificação dos fornecedores e parceiros comerciais da Logics4u. O objetivo é prevenir relações

Esta política foi elaborada pela LOGICS4U com fins meramente informativos.
É proibida a reprodução total ou parcial este documento, de qualquer forma ou por qualquer meio.

comerciais com partes inidôneas ou suspeitas em atividades ilícitas, garantindo que as relações de negócios sejam estabelecidas exclusivamente com partes em conformidade com esta Política.

O processo de KYP será detalhado em um documento específico e deverá contemplar os requisitos estabelecidos nesta Política, devendo ser mantido atualizado, considerando inclusive eventuais alterações que impliquem mudança de classificação nas categorias de risco.

As informações obtidas durante o processo de KYP deverão ser armazenadas em sistemas informatizados apropriados durante toda a relação comercial e pelo período mínimo de 10 (dez) anos a contar do encerramento da relação contratual.

5.3. Procedimentos Destinados a Conheça seu Funcionário – "*KNOW YOUR EMPLOYEE*" ("KYE")

Trata-se de um conjunto de ações destinadas a estabelecer mecanismos para identificação e qualificação de colaboradores, administradores, prestadores de serviços e demais pessoas que atuem em nome da Logics4u, com o objetivo de verificar a veracidade das informações fornecidas. A finalidade do processo é assegurar que as relações de trabalho sejam estabelecidas exclusivamente com pessoas que estejam em conformidade com esta Política.

O processo de KYE será detalhado em um documento específico, devendo as informações ser mantidas atualizadas e armazenadas em sistemas informatizados apropriados durante toda a relação de trabalho, e pelo período mínimo de 10 (dez) anos após o encerramento da relação contratual.

5.4. Registro de Operações

A Logics4u adotará procedimentos para manter registros de todas as operações realizadas, produtos e serviços contratados, devendo conter no mínimo o tipo de operação, o valor (quando aplicável), a data da realização, o nome e o número de inscrição do CPF ou CNPJ do titular e do beneficiário da operação e o canal utilizado.

O registro de operações relativas a transferências de recursos, deverão conter as informações necessárias à identificação da origem e do destino dos recursos.

5.5. Monitoramento, Seleção e Análise de Operações e Situações Suspeitas

A Logics4u implementará procedimentos de monitoramento, seleção e análise de operações e situações com o objetivo de identificar suspeitas de lavagem de dinheiro e de financiamento do terrorismo. Esses procedimentos serão previstos em documento específico apartado a esta Política.

O período para a execução dos procedimentos de monitoramento e de seleção das operações e situações suspeitas não poderá exceder o prazo de 45 (quarenta e cinco) dias, contados a partir da data de ocorrência da operação ou da situação.

A análise de operações e situações suspeitas deverá ser realizada diretamente pelo responsável por Compliance e PLD/FT ou por pessoa formalmente designada pela Diretoria Executiva para essa finalidade.

DOCUMENTO DE ACESSO PÚBLICO
Esta política foi elaborada pela LOGICS4U com fins meramente informativos.
É proibida a reprodução total ou parcial este documento, de qualquer forma ou por qualquer meio.

Adicionalmente, a LOGICS4U deverá contemplar, no âmbito do monitoramento de operações e situações suspeitas, mecanismos destinados à identificação de correspondências com pessoas, entidades ou ativos sujeitos a medidas de indisponibilidade de bens, direitos e valores previstas na Lei nº 13.810/2019 e na regulamentação aplicável. Identificada correspondência positiva, deverão ser adotadas imediatamente as medidas de indisponibilidade de bens, direitos e valores e demais providências previstas na regulamentação vigente, observados os procedimentos internos específicos.

5.6. Comunicação de Operações e Situações Suspeitas

Identificada operação ou situação com indícios de Lavagem de Dinheiro ou Financiamento ao Terrorismo, será instaurado procedimento interno de análise, conduzido pelo Responsável por Compliance e PLD/FT ou por pessoa formalmente designada pela Diretoria Executiva, observando o prazo máximo de análise previsto na Circular BCB nº 3978/2020.

Concluindo-se pela existência de operação ou situação suspeita de lavagem de dinheiro ou financiamento ao terrorismo, a comunicação ao Conselho de Controle de Atividades Financeiras (COAF) será realizada pelo Responsável por Compliance e PLD/FT, ou por profissional formalmente designado para essa finalidade, observados os prazos e requisitos estabelecidos na regulamentação vigente.

Todas as análises realizadas, bem como a decisão pela comunicação ou pelo arquivamento do caso, deverão ser formalmente fundamentadas, documentadas e mantidas pelo prazo mínimo de 10 (dez) anos, observado o disposto na regulamentação vigente, assegurando-se a rastreabilidade da decisão e o sigilo das informações.

O fluxo operacional, os critérios de análise, as responsabilidades e os procedimentos para comunicação ao COAF serão disciplinados em procedimento específico complementar a esta Política.

6. CANAL DE COMUNICAÇÃO

Qualquer desvio às diretrizes desta Política deverá ser relatado ao canal abaixo, ficando a critério da pessoa se identificar ou não.

✉ compliance@logics4u.com.br

7. NORMAS RELACIONADAS

Lei Federal nº 9.613/1998: Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras - COAF, e dá outras providências.

Lei Federal nº 13.260/2016: Regulamenta o disposto no inciso XLIII do art. 5º da Constituição Federal, disciplinando o terrorismo, tratando de disposições investigatórias e processuais e reformulando o conceito de organização terrorista; e altera as Leis nº 7.960, de 21 de dezembro de 1989, e 12.850, de 2 de agosto de 2013.

É proibida a reprodução total ou parcial este documento, de qualquer forma ou por qualquer meio.

Lei Federal nº 13.810/2019: Dispõe sobre o cumprimento de sanções impostas por resoluções do Conselho de Segurança das Nações Unidas, incluída a indisponibilidade de ativos de pessoas naturais e jurídicas e de entidades, e a designação nacional de pessoas investigadas ou acusadas de terrorismo, de seu financiamento ou de atos a ele correlacionados; e revoga a Lei nº 13.170, de 16 de outubro de 2015.

Circular nº 3.978/2020: Dispõe sobre a política, os procedimentos e os controles internos a serem adotados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil visando à prevenção da utilização do sistema financeiro para a prática dos crimes de "lavagem" ou ocultação de bens, direitos e valores, de que trata a Lei nº 9.613, de 3 de março de 1998, e de financiamento do terrorismo, previsto na Lei nº 13.260, de 16 de março de 2016.

Carta Circular nº 4.001/2020: Divulga relação de operações e situações que podem configurar indícios de ocorrência dos crimes de "lavagem" ou ocultação de bens, direitos e valores, de que trata a Lei nº 9.613, de 3 de março de 1998, e de financiamento ao terrorismo, previstos na Lei nº 13.260, de 16 de março de 2016, passíveis de comunicação ao Conselho de Controle de Atividades Financeiras (Coaf).

Resolução COAF nº 40/2021: Dispõe sobre procedimentos a serem observados, em relação a pessoas expostas politicamente, por aqueles que se sujeitam à supervisão do Conselho de Controle de Atividades Financeiras (Coaf) na forma do § 1º do art. 14 da Lei nº 9.613, de 3 de março de 1998. Após a entrada em vigor desta resolução, fica revogada a Resolução nº 29, de 7 de dezembro de 2017, do Coaf.

8. DISPOSIÇÕES GERAIS

Todas as informações relacionadas a dados de indícios/suspeitas de lavagem de dinheiro e combate ao financiamento do terrorismo são de caráter confidencial.

Esta Política entra em vigor na data de sua aprovação e revoga quaisquer documentos em contrário.

DOCUMENTO DE ACESSO PÚBLICO
Esta política foi elaborada pela LOGICS4U com fins meramente informativos.
É proibida a reprodução total ou parcial este documento, de qualquer forma ou por qualquer meio.