

**POLÍTICA DE PREVENÇÃO À LAVAGEM DE DINHEIRO E
DO FINANCIAMENTO AO TERRORISMO – PLDFT**

SISPAY INSTITUIÇÃO DE PAGAMENTO LTDA.

Data 01.07.2025

Versão.01

SUMÁRIO

1. DEFINIÇÕES	3
2. NORMAS APLICÁVEIS.....	5
3. OBJETIVO DA POLÍTICA.....	7
4. ABRANGÊNCIA DA POLÍTICA.....	9
5. ATRIBUIÇÕES DA ÁREA DE <i>COMPLIANCE</i>	9
6. CONHEÇA O SEU CLIENTE (KYC), CONHEÇA SEU PARCEIRO E FORNECEDOR (KYP) E CONHEÇA SEU EMPREGADO (KYE).....	10
A. CONHEÇA O SEU CLIENTE (KYC)	11
B. CONHEÇA O SEU PARCEIRO (KYP)	12
C. CONHEÇA O SEU EMPREGADO (KYE)	13
7. PESSOAS EXPOSTAS POLITICAMENTE (PEP).....	14
8. PROCEDIMENTO DE REGISTRO DAS OPERAÇÕES.....	14
9. MONITORAMENTO E ANÁLISE DE OPERAÇÕES E SITUAÇÕES SUSPEITAS.....	15
10. PROCEDIMENTO DE COMUNICAÇÃO AO COAF	17
11. BLOQUEIO DE ATIVOS	18
12. COMUNICAÇÃO E TREINAMENTO	18
13. DISPOSIÇÕES GERAIS	19
ANEXO 1	21
ANEXO 2	22
ANEXO 3	23

1. DEFINIÇÕES

As palavras e expressões indicadas pela primeira ou todas as letras maiúsculas terão as definições abaixo, sem prejuízo de outras definições indicadas nesta Política:

- **ADMINISTRADORES:** sócios, administradores e diretores da SISPAY INSTITUIÇÃO DE PAGAMENTO LTDA (“SISPAY”)
- **ALTA ADMINISTRAÇÃO:** Diretores da SISPAY.
- **ÁREA DE COMPLIANCE:** área específica da SISPAY, responsável por garantir que sejam cumpridos todos os procedimentos internos e a Legislação Aplicável, estabelecendo um programa compatível com natureza, estrutura, perfil de risco e modelo de negócio da SISPAY, de modo a assegurar o gerenciamento dos riscos relacionados com a Lavagem de Dinheiro e o Financiamento do Terrorismo.
- **ARRANJO DE PAGAMENTO:** conjunto de regras e procedimentos que disciplina a prestação de determinado serviço de pagamento ao público pela Lei nº 12.865/2013.
- **BACEN:** Banco Central do Brasil.
- **CANAL DE COMUNICAÇÃO:** canais de comunicação disponibilizados pela SISPAY, para o recebimento de denúncias referentes às atividades que possam se caracterizar como Lavagem de Dinheiro ou Financiamento do Terrorismo.
- **CARTÃO:** instrumentos físicos ou eletrônicos com funções de pagamento disponibilizado pelos Emissores em forma de cartão plástico ou outro meio físico ou digital, para uso pessoal e intransferível dos Portadores, aceitos nos Sistemas SISPAY para a realização de Transações.
- **CHARGEBACK:** contestação de uma Transação realizada perante o Cliente, por parte dos Emissores ou Portadores dos Cartões.
- **CLIENTES:** aqueles que contratam e utilizam produtos e/ou serviços da SISPAY.
- **COLABORADORES:** funcionários, prestadores de serviços sem vínculo empregatício, trainees e estagiários da SISPAY.
- **COAF:** Conselho de Controle de Atividades Financeiras, que atua na prevenção e combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo ou órgão que o suceda com a mesma finalidade.
- **CREDENCIADORA:** Instituição de Pagamento que, sem gerenciar conta de pagamento, habilita estabelecimentos para a aceitação de Cartão emitido pelos Emissores participantes de um mesmo Arranjo de Pagamento e participa do processo de liquidação das transações de pagamento como credor perante o Emissor, de acordo com as regras do Arranjo de Pagamento.

- **FINANCIAMENTO DO TERRORISMO:** apoio financeiro, por qualquer meio, ao terrorismo ou àqueles que incentivam, planejam ou cometem atos de terrorismo.
- **FORNECEDORES:** toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividades de comercialização de produtos ou prestação de serviços para a SISPAY.
- **INSTITUIÇÃO DE PAGAMENTO:** para fins desta Política, é a SISPAY como emissora de moeda eletrônica, cuja atividade consiste em gerenciar a Conta de Pagamento de Clientes, utilizada para o pagamento de transações pré-pagas.
- **KNOW YOUR CUSTOMER (KYC):** é o processo pelo qual a SISPAY obtém informações dos Clientes, e que poderão ser indicados pelos Parceiros de Negócio, com a finalidade de, mediante diligência prévia, conferir sua reputação, idoneidade e veracidade dos dados cadastrais informados; buscando evitar a prática de Lavagem de Dinheiro e Financiamento do Terrorismo.
- **KNOW YOUR PARTNER (KYP):** é o processo pelo qual a SISPAY obtém informações dos seus Parceiros de Negócio e Fornecedores, com a finalidade de, mediante diligência prévia, conferir sua reputação, idoneidade e veracidade dos dados cadastrais informados; buscando evitar a prática de Lavagem de Dinheiro e Financiamento do Terrorismo.
- **KNOW YOUR EMPLOYEE (KYE):** é processo pelo qual a SISPAY obtém informações de seus Colaboradores, com a finalidade de conferir a sua reputação, idoneidade e veracidade dos dados cadastrais informados; buscando evitar a prática de Lavagem de Dinheiro e Financiamento do Terrorismo.
- **LAVAGEM DE DINHEIRO:** ato ilícito com o objetivo de ocultar ou dissimular a natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente, de infração penal.
- **MERCHANT CATEGORY CODE (MCC):** código universal de quatro dígitos que identifica o ramo de atuação de cada Cliente dentro do mercado de meios eletrônicos de pagamento. Este código define o percentual da taxa de intercâmbio (*interchange fee*) aplicável a cada Cliente pelos Arranjos de Pagamentos.
- **OFAC:** *Office of Foreign Assets Controls*, que consiste no órgão do Departamento do Tesouro dos Estados Unidos da América, que administra e aplica sanções econômicas e comerciais contra países e regimes estrangeiros considerados terroristas, traficantes internacionais de drogas, envolvidos em atividades relacionadas à proliferação de armas de destruição em massa e outras ameaças à segurança nacional, à política externa ou à economia daquele país.

- **PARCEIROS DE NEGÓCIO:** toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, que celebra contratos com a SISPAY, com a finalidade de, mediante retribuição, colaborar com os negócios da SISPAY.
- **PEP:** Pessoa Exposta Politicamente, que consiste em agente público que desempenha ou tenha desempenhado, nos 05 (cinco) anos anteriores, no Brasil ou em países, territórios e dependências estrangeiras, cargos, empregos ou funções públicas relevantes, assim como seus representantes, familiares e estreitos colaboradores, tudo conforme o definido nos artigos 19 e 27 da Circular nº 3.978/2020.
- **POLÍTICA:** esta Política de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo – PLDFT.
- **PORTADOR:** pessoa física ou preposto de pessoa jurídica, portador de Cartão emitido pelos Emissores, e que poderão realizar Transações pelo Sistema SISPAY.
- **SUBCREDENCIADOR:** para fins desta política é a SISPAY, que, na qualidade de participante de arranjos de pagamento instituídos pelas Bandeiras, possui autorização de uma ou mais credenciadoras para credenciar os estabelecimentos e realizar a liquidação das Transações, habilitando-os para realizar Transações com Cartões.
- **TRANSAÇÕES:** para fins desta Política, consistem: (i) nas movimentações realizadas pelo Cliente de sua conta de pagamento, mediante o aporte, a transferência ou o resgate de recursos financeiros, por qualquer modalidade; e (ii), nas operações de Subcredenciador, nas movimentações que geram os créditos que os Clientes possuem em virtude da venda de seus produtos e/ou serviços pagas com Cartão de crédito ou débito pelos seus respectivos Portadores.

2. NORMAS APLICÁVEIS

Todos aqueles a quem esta Política for aplicável deverão observar as leis e normas abaixo indicadas (em conjunto "Legislação Aplicável"):

- **LEI Nº 9.613/1998:** dispõe sobre os crimes de Lavagem de Dinheiro e a prevenção da utilização do sistema financeiro para os atos ilícitos previstos nesta lei.
- **LEI Nº 12.865/2013:** dispõe sobre os Arranjos de Pagamento e as Instituições de Pagamento integrantes do Sistema de Pagamentos Brasileiro (SPB).
- **LEI Nº 13.260/2016:** disciplina o Financiamento do Terrorismo.
- **LEI Nº 13.810/2019:** dispõe sobre o cumprimento de sanções impostas por resoluções do Conselho de Segurança das Nações Unidas.
- **RESOLUÇÃO COAF Nº 40/2021:** dispõe sobre os procedimentos a serem observados pelas pessoas reguladas pelo COAF.
- **RESOLUÇÃO BCB Nº 96/2022:** dispõe sobre a abertura, a manutenção e o encerramento de contas de pagamento.

- **RESOLUÇÃO BCB Nº 150/2021:** Consolida normas sobre os arranjos de pagamento, aprova o regulamento que disciplina a prestação de serviço de pagamento no âmbito dos arranjos de pagamento integrantes do Sistema de Pagamentos Brasileiro (SPB).
- **RESOLUÇÃO BCB Nº 80/2021:** estabelece os requisitos e os procedimentos para constituição e funcionamento, e de pedido de autorização de funcionamento das Instituições de Pagamento, e dispõe sobre a prestação de serviços de pagamento por outras instituições autorizadas a funcionar pelo Bacen.
- **RESOLUÇÃO BCB Nº 44/2020:** estabelece procedimentos para execução das medidas determinadas pela Lei nº 13.810/2019.
- **CIRCULAR BACEN Nº 3.978/2020:** dispõe sobre a política, os procedimentos e os controles internos a serem adotados pelas instituições autorizadas a funcionar pelo Bacen, visando à prevenção da utilização do sistema financeiro para a prática dos crimes de Lavagem de Dinheiro e de Financiamento do Terrorismo.
- **CARTA CIRCULAR BACEN Nº 4.001/2020:** divulga relação de operações e situações que podem configurar indícios de ocorrência dos crimes de Lavagem de Dinheiro e de Financiamento do Terrorismo, passíveis de comunicação ao COAF.
- **INSTRUÇÃO NORMATIVA BCB Nº 262/2022:** especifica e esclarece aspectos operacionais dos procedimentos estabelecidos na Resolução BCB nº 44/2020, para a execução de medidas determinadas pela Lei nº 13.810/2019, que dispõe sobre o cumprimento de sanções impostas por resoluções do Conselho de Segurança das Nações Unidas.

As leis e normas são citadas de forma exemplificativa e contemplam apenas as diretrizes em vigor na data de elaboração desta Política, não esgotando toda a Legislação Aplicável às atividades da SISPAY.

O Diretor de PLDFT será responsável por verificar eventual atualização, revogação e a edição de novas normas.

Para melhor entendimento da Legislação Aplicável por todas as pessoas abrangidas por esta Política, a SISPAY esclarece:

O crime de Lavagem de Dinheiro tem por objetivo disfarçar a natureza, origem, localização, movimentação ou propriedade de bens (dinheiro, ativos, imóveis, móveis, dentre outros) obtidos com a prática de atos ilícitos. Por meio da Lavagem de Dinheiro, os bens ou recursos de origem “suja” ou ilegal voltam à economia formal com a aparência de “limpos” ou legais, o que dificulta a punição do agente pela prática criminosa realizada.

A Lavagem de Dinheiro caracteriza-se em 3 (três) fases: a Colocação, a Ocultação e a Integração:

- **COLOCAÇÃO:** tem por objetivo inserir os bens ou recursos ilícitos na economia formal, ou seja, em empresas ou negócios lícitos. Esta fase consiste na introdução do bem ou recurso ilícito no sistema financeiro, dificultando a identificação de sua procedência.
- **OCULTAÇÃO:** adoção de medidas que visam a dificultar o rastreamento dos bens ou recursos ilícitos. Nesta fase há a tentativa de camuflar as evidências e a conexão entre o bem e o crime praticado. Podem ser realizadas diversas movimentações financeiras de modo a acrescentar complexidade e dificultar um futuro rastreamento.
- **INTEGRAÇÃO:** depois de ocultados e “lavados”, em diferentes operações financeiras, os bens ou recursos retornam aos agentes por meio da simulação de negócios aparentemente lícitos.

Para a caracterização da Lavagem de Dinheiro não é necessário que estejam presentes as 3 (três) fases acima citadas, bastando apenas a existência de 1 (uma) delas para que o crime esteja configurado.

A Lavagem de Dinheiro é tipificada como crime na Lei nº 9.613/1998 e é punida com prisão de 03 (três) a 10 (dez) anos, multa e outras sanções.

O Financiamento do Terrorismo está relacionado com a distribuição dissimulada de bens ou recursos a serem utilizados em atos e/ou por organizações terroristas, assim como o financiamento da proliferação de armas de destruição em massa. Os métodos utilizados geralmente são semelhantes àqueles empregados na Lavagem de Dinheiro.

O Financiamento do Terrorismo é tipificado como crime na Lei nº 13.260/2016 e pode ser punido com prisão de 05 (cinco) a 30 (trinta) anos, multa e outras sanções.

3. OBJETIVO DA POLÍTICA

Esta Política tem por objetivo estabelecer as diretrizes relacionadas à prevenção e combate aos crimes de lavagem de dinheiro e financiamento ao terrorismo, além de demais crimes envolvendo simulação ou ocultação de recursos financeiros, conforme previsto na regulamentação do Banco Central do Brasil, nas regras das bandeiras, e na Lei nº 9.613 de 1998.

A SISPAY, por meio desta Política estabelece seus procedimentos a serem seguidos por seus Administradores, Colaboradores, Fornecedores, Clientes, Parceiros de Negócio, das seguintes formas:

A SISPAY é Instituição de Pagamento emissora de moeda eletrônica, nos termos da Lei nº 12.865/2013 e Resolução BCB nº 80/2021.

Dentre os serviços oferecidos, a SISPAY realiza a gestão e custódia de recursos financeiros dos Clientes, que poderão ser indicados por Parceiros Comerciais, possibilitando o recebimento e a realização de pagamentos por meio das Transações.

A SISPAY também é Subcredenciador, nos termos da Lei nº 12.865/2013 e do Regulamento Anexo da Resolução BCB nº 150/2021.

Dentre os serviços oferecidos, a SISPAY realiza: (a) habilitação dos Clientes para aceitar pagamentos por cartão de crédito, débito e benefícios, mediante a realização de Transações; (b) a gestão e coordenação de pagamentos aos Clientes que sejam decorrentes de Transações realizadas pela SISPAY; e (c) o fornecimento de tecnologia e serviços relacionados a meio de pagamentos, incluindo a venda ou locação, por si ou por terceiros homologados, dos equipamentos necessários para a captura das Transações.

Assim, os Clientes e Parceiros Comerciais poderão tentar utilizar os serviços prestados pela SISPAY para a prática de crimes relacionados com Lavagem de Dinheiro e Financiamento do Terrorismo, mediante a ocultação ou dissimulação da natureza, origem, localização e movimentação de recursos provenientes de infração penal, com a finalidade de incorporá-los ao sistema financeiro.

Portanto, esta Política tem por objetivo definir as diretrizes nas quais se baseia a prevenção à Lavagem de Dinheiro e do Financiamento do Terrorismo em razão das atividades da SISPAY, como Instituição de Pagamento e como Subcredenciador.

A SISPAY irá adotar, por meio de sua Área de *Compliance*, normas internas, padrões, procedimentos, treinamentos, comunicação corporativa e medidas preventivas, corretivas e punitivas, a fim tornar a SISPAY, em todas as áreas, aderente a esta Política.

Ainda, a SISPAY disponibiliza um Canal de Comunicação, que irá realizar o tratamento adequado das ocorrências encaminhadas pelo endereço **compliance@sispay.com.br**, por meio do(a): recebimento, análise preliminar, classificação, tratamento, monitoramento, investigação, tomada de decisão e reporte das denúncias ao(s) órgão(s) competente(s), até o devido encerramento das ocorrências.

A SISPAY receberá e atuará nas denúncias de Administradores, Colaboradores, Fornecedores, Clientes, Parceiros de Negócio ou quaisquer terceiros, sobre atividades atípicas ou suspeitas que possam se caracterizar como indícios de crimes relacionados com a Lavagem de Dinheiro e Financiamento ao Terrorismo.

As ocorrências e denúncias serão recebidas por profissionais capacitados e com autonomia necessária, sendo garantido o anonimato e sigilo das comunicações, bem como a preservação da integridade do denunciante.

4. ABRANGÊNCIA DA POLÍTICA

Esta Política abrange todas as áreas da SISPAY, seus Administradores, Clientes, Colaboradores, Fornecedores e Parceiros de Negócio, os quais deverão concordar, aderir e se obrigar a respeitar aquilo que seja aqui estabelecido.

Por meio da Área de *Compliance*, todos serão instruídos para que sejam capazes de identificar indícios de crimes relacionados com a Lavagem de Dinheiro e com o Financiamento do Terrorismo, bem como realizar denúncias de suspeitas de atividades ilícitas no Canal de Comunicação.

5. ATRIBUIÇÕES DA ÁREA DE COMPLIANCE

A Área de *Compliance* será responsável, através do Diretor de PLDFT, por garantir que todos os procedimentos internos da SISPAY sejam cumpridos.

É a Área de *Compliance* que deverá promover a cultura organizacional de prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo, contemplando os Administradores, Clientes, Colaboradores, Fornecedores e Parceiros de Negócio.

Por meio da Área de *Compliance*, a SISPAY atribuirá obrigações e ações específicas para as demais áreas de negócios, em especial:

- **COMERCIAL:** observar os processos de KYC e KYP para Clientes e Parceiros de Negócio.
- **COMPRAS:** observar o processo de KYP com relação aos Fornecedores, por meio de cadastro e verificação das informações fornecidas após a Solicitação de Proposta / *Request for Proposal* (“RFP”), Solicitação de Informações / *Request for Information* (“RFI”) ou Solicitação de Cotação / *Request For Quotation* (“RFQ”), ou outros processos de contratação conforme aplicável.
- **JURÍDICA:** estabelecer e assegurar o cumprimento, dentre outras atividades, desta Política e das exigências da Legislação Aplicável.
- **MARKETING:** observar o processo de KYP com relação aos Fornecedores, por meio de cadastro e verificação das informações fornecidas pela RFP, RFI ou RFQ, ou outros processos de cadastro e verificação das informações fornecidas conforme aplicável. Como também o processo de KYE com relação aos Colaboradores nas funções de ações e campanhas de marketing, brindes, premiações etc., conforme aplicável.
- **OPERAÇÕES:** observar os processos de KYC e KYP para Clientes, Fornecedores e Parceiros de Negócio, no que diz respeito aos processos operacionais, logísticos, de abertura de contas e habilitação de Clientes.
- **RECURSOS HUMANOS:** estabelecer critérios e processos de KYE para a seleção e contratação de Colaboradores que possuam perfil condizente com esta Política, e em observância do grau de responsabilidade de cada Colaborador quanto ao cumprimento das responsabilidades que lhe forem atribuídas no

procedimento de análise, registro, monitoramento e comunicação de atividades suspeitas.

- **TI:** atuar com diligência na autorização de acesso aos sistemas, segurança da informação, proteção e sigilo dos dados e para manutenção das ferramentas tecnológicas a serem utilizadas, a fim de coibir ações que tenham o objetivo de fomentar a prática da Lavagem de Dinheiro e do Financiamento ao Terrorismo.

Cada uma das áreas da SISPAY deverá, por meio dos respectivos Colaboradores, comunicar a Área de *Compliance* sobre atividades suspeitas relacionadas à Lavagem de Dinheiro e Financiamento do Terrorismo.

Caberá à Área de *Compliance*: (i) criar e gerenciar os mecanismos de controle voltados à prevenção à Lavagem de Dinheiro e do Financiamento ao Terrorismo; (ii) criar e coordenar a comunicação e treinamento dos Administradores e Colaboradores; (iii) assegurar o cumprimento dos mecanismos de atuação do Canal de Comunicação; (iv) monitorar as ocorrências sobre Transações atípicas ou suspeitas identificadas pelas ferramentas tecnológicas da SISPAY ou que sejam comunicadas pelos Colaboradores; (v) o enquadramento e monitoramento de PEP, quando houver necessidade; (vi) a análise de Clientes, Fornecedores e beneficiário final envolvidos em listas sancionadoras; e (vii) a comunicação com o COAF, Bacen, Ministério da Justiça e Segurança Pública.

Ainda, a Área de *Compliance* deverá assegurar a ampla divulgação desta Política aos Fornecedores e Parceiros de Negócio, assim como assegurar que suas condições estejam previstas nos contratos com os Clientes.

Também é atribuição da Área de *Compliance* analisar novos produtos e serviços da SISPAY, a fim de identificar vulnerabilidades diante da necessidade de prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo.

6. CONHEÇA O SEU CLIENTE (KYC), CONHEÇA SEU PARCEIRO E FORNECEDOR (KYP) E CONHEÇA SEU EMPREGADO (KYE)

Os procedimentos de KYC e KYP têm por finalidade impedir que as atividades da SISPAY sejam, de qualquer modo, utilizadas para a prática de algum dos crimes elencados nesta Política. Ainda, este processo tem o objetivo de manter a integridade e a imagem da SISPAY perante seus Administradores, Clientes, Colaboradores, Fornecedores, Parceiros de Negócio, perante a sociedade, e evitar o envolvimento com pessoas mencionadas em listas sancionadoras.

Os dados informados nos procedimentos de KYC e KYP serão confirmados por meio do envio de documentos e/ou mediante consulta em bancos de dados públicos ou privados, tais como *bureaux* de análises de crédito e risco, além de base de dados interna ou que seja compartilhada por outras empresas.

Haverá o armazenamento das informações obtidas nos procedimentos de KYC e KYP, as quais devem ser compatíveis com o perfil de risco definido pela Área de *Compliance*, de acordo com a natureza do negócio e o risco ao qual a SISPAY será exposta.

Os documentos com as informações cadastrais dos clientes e parceiros serão arquivados em meio físico ou digital e mantidos à disposição do Bacen.

Anualmente, a SISPAY deverá executar testes para a validação das informações cadastrais fornecidas. Caso existam inconsistências nestas informações, a SISPAY realizará as devidas tratativas, visando à regularização.

A. CONHEÇA O SEU CLIENTE (KYC)

O processo de KYC, de acordo com a atividade a ser exercida pela SISPAY, seja ela de Instituição de Pagamento ou de Subcredenciador, no que se aplicar, tem o objetivo de implementar procedimentos destinados a conhecer os respectivos Clientes, com a adoção de diligência prévia e periódica que assegure sua identificação, qualificação e classificação, prevenindo a ocorrência de Lavagem de Dinheiro e Financiamento do Terrorismo e evitando o envolvimento com pessoas mencionadas em listas sancionadoras.

A SISPAY apenas aceitará potenciais Clientes que desempenhem atividades lícitas e que não sejam contrárias a Legislação Aplicável.

No cadastro dos Clientes, a SISPAY deverá sempre observar os seguintes procedimentos:

- a. O cadastro dos Clientes será realizado de forma individualizada e padronizada, contendo todos os dados pessoais e informações exigidas pela Legislação Vigente;
- b. Será realizada a consulta sobre a veracidade, idoneidade e atualidade das informações;
- c. Haverá a consulta das informações disponíveis em sites especializados em prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo;
- d. Os Clientes que exercerem atividade empresária ou profissional serão classificados de acordo com seu ramo de atividade, e haverá a consulta em fontes públicas ou privadas para validação da informação;
- e. O Cliente será classificado de acordo com sua atividade, informações de cadastro e situação patrimonial;
- f. Haverá classificação específica para Clientes considerados como PEP;
- g. Não haverá a aprovação do cadastro de potenciais Clientes incluídos na lista da OFAC ou listas sancionadoras;

- h. A qualquer momento, inclusive após o cadastro, poderá ser solicitado o envio de informações complementares, declarações e documentos para validação das informações;
- i. As informações dos Clientes serão atualizadas periodicamente, por período não superior a 12 (doze) meses.

Os Clientes serão classificados de acordo com perfis de risco específicos para possibilitar o controle e monitoramento das Transações, sendo, os tipos mais comuns de classificação: (i) pessoa física, (ii) pessoa jurídica, (iii) cadastro simplificado, (iv) cadastro completo; (v) atividade empresarial ou profissional exercida; (vi) correlação de suas atividades empresariais aos respectivos *MCC* definidos pelos Arranjos de Pagamentos; (vii) PEP; e (viii) integrante da lista da OFAC ou lista do CSNU, sendo possível que, um mesmo Cliente, seja enquadrado em mais de um tipo de classificação.

Após a classificação e análise de risco, o Cliente poderá: (i) ter seu pedido de cadastro negado; (ii) sofrer medidas restritivas, mediante a indisponibilidade de determinados serviços ou a limitação do valor das Transações; (iii) ter o Monitoramento Reforçado (conforme abaixo definido), ou (iv) ter o bloqueio ou término de relacionamento. As normas internas da Área de *Compliance* detalharão quais restrições serão aplicáveis.

A SISPAY estabelecerá critérios de mitigação de riscos no credenciamento de Clientes que não comprovem o desenvolvimento de atividade empresária ou profissional, mediante a fixação de limite máximo para a realização das Transações em períodos determinados, de acordo com os critérios definidos pela Área de *Compliance* e com a Legislação Vigente, e com as regras da Credenciadora e dos Arranjos de Pagamentos, no que couberem.

Caso o Cliente desenvolva atividade empresária ou profissional em estabelecimento físico, a SISPAY ou um Parceiro Comercial (caso aplicável) poderá, de forma física ou remota (inclusive utilizando de tecnologias de geolocalização), verificar a efetiva existência do estabelecimento no local indicado.

B. CONHEÇA O SEU PARCEIRO (KYP)

O processo de KYP tem o objetivo de implementar procedimentos destinados a conhecer os Fornecedores e Parceiros de Negócio, com a adoção de diligência prévia e periódica que assegure sua identificação, qualificação e classificação, prevenindo a ocorrência de Lavagem de Dinheiro e Financiamento do Terrorismo, e evitando o envolvimento com pessoas mencionadas em listas sancionadoras.

No cadastro dos Fornecedores e Parceiros de Negócio, a SISPAY observará os seguintes procedimentos:

- a. Realizar o cadastro de forma individualizada e padronizada, contendo todas as informações exigidas no processo de RFP, RFI ou RFQ, ou outros processos de contratação definido pela SISPAY;
- b. Realizar a consulta sobre a veracidade, idoneidade e atualidade das informações;
- c. Consultar as informações disponíveis em sites especializados em prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo;
- d. Realizar a análise da situação de crédito e endividamento;
- e. Realizar pesquisas na mídia para verificação da existência de notícias negativas relacionadas à Lavagem de Dinheiro ou Financiamento do Terrorismo;
- f. A qualquer momento, inclusive após o cadastro, solicitar o envio de informações complementares, declarações e documentos para validação das informações.

O Fornecedor ou Parceiro de Negócio poderá ser classificado de acordo com sua atividade empresária ou profissional, caso se identifique um perfil de risco associado à sua atividade, conforme as normas internas da Área de *Compliance*.

Os seguintes procedimentos serão observados com relação aos Sócios, Administradores, Diretores e/ou representantes dos Fornecedores e Parceiros de Negócio: (i) consulta na lista de PEP e OFAC; (ii) verificação da documentação de identificação; e (iii) outros procedimentos previstos no item anterior, conforme aplicável.

Em razão do processo de KYP, poderá ser recusada a contratação com qualquer Fornecedor ou Parceiros de Negócio.

Caso a atividade empresarial ou profissional exercida pelo Fornecedor ou Parceiro de Negócio seja classificada como sendo de alto risco, haverá o Monitoramento Reforçado sobre os valores recebidos.

A remuneração a ser paga pela SISPAY, independentemente de sua natureza, deverá ser liquidada em conta de pagamento ou conta bancária de titularidade do respectivo Fornecedor ou Parceiro de Negócio.

Os contratos a serem celebrados com os Fornecedores e Parceiros de Negócio deverão necessariamente constar obrigações específicas relacionadas à prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo.

C. CONHEÇA O SEU EMPREGADO (KYE)

A seleção e contratação de Colaboradores, inclusive terceirizados, serão realizadas com o objetivo reduzir o risco de práticas ilícitas de qualquer natureza, incluindo, a prevenção à Lavagem de Dinheiro e o Financiamento ao Terrorismo, independentemente do cargo ou função.

Os gestores das respectivas áreas da SISPAY são responsáveis por identificar e comunicar a Área de *Compliance* sobre comportamentos contrários ao estabelecido nesta Política, ou outras políticas e procedimentos adotados pela área de Recursos Humanos da SISPAY.

A SISPAY, através de sua área de Recursos Humanos, estabelece critérios e processos para a seleção e contratação de Colaboradores que possuam perfil condizente com esta Política, visando o cumprimento das responsabilidades que lhe forem atribuídas no exercício de suas atividades.

O monitoramento dos Colaboradores será realizado nos termos da Lei nº 9.613/1998, em especial de seus artigos 9º, 10 e 11. Deve haver isonomia de tratamento nessa conduta, abrangendo todos os Colaboradores, sendo vedado o monitoramento com fins discriminatórios. A SISPAY deverá comunicar previamente ao Colaborador este monitoramento, mediante a entrega desta Política ou menção expressa em seu contrato de trabalho.

7. PESSOAS EXPOSTAS POLITICAMENTE (PEP)

A Área de *Compliance* indicará os procedimentos que deverão ser adotados para que se possa qualificar os Clientes, Fornecedores e Parceiros de Negócio (assim como seus Sócios, Administradores, Diretores e/ou Representantes) como PEP.

A qualificação de Clientes, Fornecedores e Parceiros de Negócio será realizada pela consulta às listas públicas e privadas disponíveis, e por meio de autodeclaração que constará do cadastro de cada um deles.

A aprovação do cadastro do Cliente, Fornecedor ou Parceiro de Negócio classificado como PEP deverá ser reportada à Área de *Compliance*, a quem caberá, com exclusividade, aprovar ou não o cadastro.

Caso haja a aprovação, as áreas respectivas deverão reportar à Área de *Compliance* todas as Transações realizadas pelos Clientes PEP.

8. PROCEDIMENTO DE REGISTRO DAS OPERAÇÕES

Cada área da SISPAY, será responsável por, em conjunto com a Área de *Compliance*, desenvolver os processos para manter os registros das Transações realizadas pelos Clientes.

Os registros deverão ser realizados de acordo com as seguintes modalidades:

- a. Transações de aporte, transferências ou resgate de recursos;
- b. Transações feitas pelo próprio Cliente ou de/para terceiros, considerando a inscrição no CPF ou CNPJ do Cliente;

- c. Modalidade das Transações, tais como, conforme aplicável, boleto bancário, cartão pré-pago, cartão pós-pago, transferência pelo sistema financeiro, transferência por outros arranjos de pagamento;
- d. Captação de Cliente;
- e. Captura, transmissão, processamento de dados e liquidação da Transação;
- f. Data de realização da Transação;
- g. Modalidades de soluções de captura da Transação;
- h. Modalidade das Transações, tais como, conforme aplicável, cartão presente, cartão não presente, link de pagamento, pagamentos recorrentes, assinatura em arquivo, token etc.

No registro das Transações também serão identificadas as informações necessárias sobre a origem, o destino e o beneficiário final dos recursos.

Para o monitoramento das Transações, a Área de *Compliance* deverá estipular, além dos registros acima citados, o valor das Transações e os critérios de monitoramento e seleção que permitam identificar Transações suspeitas.

A SISPAY manterá registros de todas as operações realizadas pelos Clientes, os quais serão arquivados em meio físico ou digital pelo período mínimo de 10 (dez) anos, contados a partir do primeiro dia do ano seguinte ao da conclusão da operação, bem como no caso de informações e registros de transferência de recursos.

9. MONITORAMENTO E ANÁLISE DE OPERAÇÕES E SITUAÇÕES SUSPEITAS

A Área de *Compliance* será responsável pelos procedimentos de monitoramento e seleção que permitam identificar Transações e situações que possam indicar suspeitas de Lavagem de Dinheiro e de Financiamento do Terrorismo, sejam elas em processos referentes à Instituição de Pagamento, ou processos do Subcredenciador, de acordo com suas atribuições, no que couber.

Para o monitoramento das Transações deverão ser utilizadas ferramentas tecnológicas de monitoramento e com alertas automáticos de atividades atípicas.

Poderão ser automaticamente reprovadas e canceladas as Transações em que, de acordo com os procedimentos de monitoramento instituídos pela Área de *Compliance*, se verifique indícios de Lavagem de Dinheiro ou de Financiamento do Terrorismo, em razão do(a):

- a. habitualidade, valor, periodicidade, forma ou histórico do Cliente com relação às Transações anteriores;
- b. intuito de gerar ganho, sem que haja benefício econômico fundamentado;
- c. omissão ou atraso injustificado no envio de informações e/ou documentos pelo Cliente;
- d. oscilação significativa em relação ao volume e/ou frequência das Transações;
- e. alteração repentina e injustificada da modalidade ou valor da Transação;

- f. incompatibilidade com a capacidade financeira do Cliente, diante de sua renda, faturamento ou patrimônio;
- g. repetição contínua de Transações entre o Cliente e o mesmo beneficiário;
- h. compensação de créditos e débitos entre o Cliente e o mesmo beneficiário;
- i. atuação do Cliente em nome de terceiros;
- j. suspeita de que o beneficiário, por interposta pessoa, é o próprio Cliente;
- k. dificuldade ou impossibilidade de identificação do beneficiário final;
- l. constatação de informações errôneas, inverídicas ou desatualizadas do Cliente;
- m. denúncias recebidas pelo Canal de Comunicação.

A Área de *Compliance* da SISPAY, de acordo com os critérios previstos nesta Política, deverá criar procedimento para monitoramento de Clientes ou Transações específicas (“Monitoramento Reforçado”).

Haverá o Monitoramento Reforçado, quando a Transação for realizada: (i) por Cliente considerado PEP; (ii) em valor superior ao limite estabelecido; (iii) por Cliente pessoa jurídica, que, em razão da atividade desenvolvida, for classificado como de alto risco; (iv) pelo mesmo valor, de forma repetida, no mesmo dia; (v) por valores de transação discrepantes do comportamento cotidiano do Cliente (horário, valor, modalidade de captura de transação etc.) ou (vi) por incremento de vendas no valor 50% (cinquenta por cento) superior ao volume total de Transações realizadas no mês anterior, de forma inexplicável ou sem ter havido a consolidação da operação do Cliente.

As Transações sujeitas a Monitoramento Reforçado deverão ser aprovadas manualmente pela área responsável. Havendo suspeita de irregularidade, o Colaborador da área: (i) não deverá aprovar a Transação; e (ii) deverá entrar em contato com o Cliente para solicitar informações complementares e documentos.

Para as Transações em valores acima do limite estabelecido, o Cliente deverá complementar suas informações de cadastro e encaminhar os documentos necessários.

Para a análise da licitude da Transação deverão ser solicitados documentos que comprovem sua regularidade e licitude, sendo admitidos, de forma cumulativa: (i) contratos de compra e venda das mercadorias ou prestação de serviços; (ii) nota fiscal; e (iii) comprovante de entrega das mercadorias ou serviços.

Os documentos deverão ser encaminhados à Área de *Compliance* para análise, a quem caberá aprovar ou não a Transação.

Durante o procedimento de análise, a Área de *Compliance* deverá adotar as seguintes medidas:

- a. bloqueio do acesso pelo Cliente à plataforma eletrônica da SISPAY e suspensão dos serviços;

- b. retenção dos valores até a averiguação da legalidade da Transação;
- c. orientação para a rescisão do contrato celebrado com o Cliente, em caso de não aprovação da Transação.

Caso a Transação não seja aprovada em razão de indícios de suspeita de fraude, os recursos deverão ser restituídos ao remetente, em conta bancária da mesma titularidade, e mediante a assinatura de recibo ou declaração pelo recebedor, dando plena quitação da restituição.

Caso ocorra a notificação pelas Credenciadoras ou Arranjos de Pagamento referente a transações de disputa de Chargeback ou com suspeita de fraude e de indícios de lavagem de dinheiro, a Área de *Compliance* deverá observar o procedimento estipulado pelos Arranjos de Pagamentos e Credenciadoras, de identificação da transação; notificação do Cliente e solicitação do envio de documentos de confirmação da transação; reter o valor da transação; iniciar o processo de disputa, se for o caso; concluir a ocorrência.

Nos casos de reincidência das ocorrências, caberá o descredenciamento do Cliente e respectiva inclusão na lista de restrições da SISPAY.

A Transação atípica sempre deverá ser reportada à Área de *Compliance* pelos Colaboradores, mesmo que haja contato com o Cliente e envio de documentos e informações.

10. PROCEDIMENTO DE COMUNICAÇÃO AO COAF

A SISPAY, por meio da Área de *Compliance*, é responsável por realizar as comunicações ao COAF das Transações consideradas suspeitas, nos termos desta Política e da Legislação Aplicável.

De acordo com a Legislação Aplicável, a SISPAY deverá abster-se de fornecer aos Clientes, informações sobre eventuais comunicações realizadas em decorrência de indícios de crime de Lavagem de Dinheiro ou Financiamento do Terrorismo.

A comunicação ao COAF será realizada no prazo legal e sem dar ciência aos envolvidos ou a terceiros. Em caso de inexistência de comunicações em determinado ano, a SISPAY providenciará o envio de declaração negativa, na forma da Legislação Aplicável.

As comunicações ao COAF devem conter minimamente:

- a data do início de relacionamento do comunicante com a pessoa autora ou envolvida na operação ou situação;
- a explicação fundamentada dos sinais de alerta identificados;
- a descrição e o detalhamento das características das operações realizadas;

- a apresentação das informações obtidas por meio das diligências internas realizadas, que qualifiquem os envolvidos, inclusive informando tratar-se, ou não, de PEP, e que detalhem o comportamento da pessoa comunicada; e
- a conclusão da análise, incluindo o relato fundamentado que caracterize os sinais de alerta identificados como uma situação suspeita a ser comunicada para o COAF.

A comunicação ao COAF deve ser efetuada no prazo de 24 (vinte e quatro) horas a contar da conclusão da análise que caracterizou a necessidade de reporte de atividades suspeitas de LDFT.

O Diretor de PLDFT atenderá qualquer demanda, solicitação ou pedido de esclarecimentos do COAF e do Bacen.

11. BLOQUEIO DE ATIVOS

Caso algum Fornecedor, Cliente ou beneficiário final esteja registrado em alguma lista de sanção imposta por resoluções do Conselho de Segurança das Nações Unidas, deverá ser realizado de imediato o bloqueio dos ativos nos termos da Lei nº 13.810/2019, bem como a realização da comunicação do fato ao COAF, ao Bacen, Ministério da Justiça e Segurança Pública e outros órgãos de registro público que forem aplicados.

12. COMUNICAÇÃO E TREINAMENTO

A responsabilidade pela comunicação e pelo treinamento dos Administradores e Colaboradores da SISPAY é da Área de *Compliance*, que deverá, em conjunto com o Marketing e o RH, elaborar toda a documentação adequada para a comunicação, o treinamento e a comprovação da ciência e participação dos envolvidos.

Os treinamentos serão realizados: (i) sempre que houver a admissão de novos Administradores e Colaboradores; (ii) periodicamente, em prazo não superior a 01 (um) ano, ou (iii) caso haja qualquer alteração desta Política ou dos procedimentos internos adotados pela Área de *Compliance*, ou em detrimento à Legislação vigente.

Os treinamentos serão realizados pelos responsáveis pela Área de *Compliance*, de forma presencial ou remota, e que poderá contar com o auxílio de assessores externos.

Ainda, a Área de *Compliance* deverá realizar a comunicação dos procedimentos previstos nesta Política para os Fornecedores e Parceiros de Negócio.

A divulgação desta Política tem o objetivo de realizar a disseminação de padrões de integridade e conduta ética como parte da cultura da SISPAY, e com a finalidade de assegurar o pleno cumprimento dos deveres legais.

13. DISPOSIÇÕES GERAIS

A Área de *Compliance* e o Diretor de PLDFT, são responsáveis pela revisão, alteração e atualização desta Política, sempre que necessário.

Esta Política deverá ser aprovada pela Alta Administração da SISPAY, de acordo com suas atribuições internas.

A SISPAY deverá avaliar a efetividade desta política, seus procedimentos e controles internos, e documentar em relatório específico que deve ser elaborado anualmente, com data-base de 31 de dezembro e encaminhado, para ciência, até 31 de março do ano seguinte ao da data-base aos Administradores da instituição.

O relatório deve conter informações que descrevam: a metodologia adotada na avaliação de efetividade; os testes aplicados; a qualificação dos avaliadores; e as deficiências identificadas. Como também, no mínimo, a avaliação: dos procedimentos destinados a conhecer clientes, incluindo a verificação e a validação das informações dos clientes e a adequação dos dados cadastrais; dos procedimentos de monitoramento, seleção, análise e comunicação ao COAF, incluindo a avaliação de efetividade dos parâmetros de seleção de operações e de situações suspeitas; da governança da política de PLDFT; das medidas de desenvolvimento da cultura organizacional voltadas à PLDFT; dos programas de capacitação periódica de pessoal; dos procedimentos destinados a KYE e KYP; e das ações de regularização dos apontamentos oriundos da auditoria interna e da supervisão do Banco Central do Brasil, no que couber.

A SISPAY deverá elaborar plano de ação destinado a solucionar as deficiências identificadas por meio da avaliação de efetividade acima descrita, documentada por meio de relatório de acompanhamento que será elaborado e encaminhado para ciência e avaliação dos Administradores, até 30 de junho do ano seguinte ao da data-base do relatório de avaliação da efetividade da Política, dos procedimentos e dos controles internos.

O Diretor de PLDFT, conforme aplicável, manterá à disposição da Alta Administração e do Bacen, documentos, atas, relatórios, avaliações de risco e manuais relacionados com a prevenção à Lavagem de Dinheiro e Prevenção do Terrorismo.

Esta Política tem vigência a partir da data de sua aprovação pela Alta Administração da SISPAY e vigorará por prazo indeterminado, devendo ser revisada sempre que necessário.

Esta Política está acompanhada de um Termo de Adesão a PLDFT e um Termo de Adesão as Alterações desta PLDFT.

ANEXO 1

TERMO DE ADESÃO À PLDFT

Eu, _____, inscrito no CPF sob o nº _____, declaro estar ciente de todos os termos dispostos nesta Política de Prevenção a Lavagem de Dinheiro e ao Financiamento do Terrorismo, bem como das diretrizes contidas nas demais políticas, nas normas e nos procedimentos internos da SISPAY.

Declaro, ainda, estar ciente das atividades da SISPAY e de que tais atividades podem ser utilizadas para a prática de crimes relacionados a Lavagem de Dinheiro e ao Financiamento do Terrorismo. Assim, dentro das minhas obrigações e atribuições, devo, sempre que necessário, utilizar o Canal de Comunicação para comunicar qualquer indício de atividade suspeita e/ou tratada como criminosa por esta Política e pela SISPAY.

_____/_____/_____

Data

Assinatura

ANEXO 2

TERMO DE ADESÃO ÀS ALTERAÇÕES DESTA PLDFT

Eu, _____, inscrito no CPF sob o nº _____, declaro estar ciente das alterações promovidas nesta Política de Prevenção a Lavagem de Dinheiro e ao Financiamento do Terrorismo, bem como das diretrizes contidas nas demais políticas, nas normas e nos procedimentos internos da SISPAY.

Declaro, ainda, ter ciência das atividades da SISPAY e de que tais atividades podem ser utilizadas para a prática de crimes relacionados a Lavagem de Dinheiro e ao Financiamento do Terrorismo. Assim, dentro das minhas obrigações e atribuições, devo, sempre que necessário, utilizar o Canal de Comunicação para comunicar qualquer indício de atividade suspeita e/ou tratada como criminosa por esta Política e pela SISPAY.

_____/_____/_____

Data

Assinatura

ANEXO 3

DECLARAÇÃO DE CONFORMIDADE COM AS RESOLUÇÕES DO CONSELHO DE SEGURANÇA DAS NAÇÕES UNIDAS

Todos os procedimentos desta Política devem ser realizados em conformidade com as diretrizes da Lei nº 13.810, de 8 de março 2019, que dispõe sobre o cumprimento de sanções impostas por resoluções do Conselho de Segurança das Nações Unidas (“ONU”).

A SISPAY adota processos de identificação e mapeamento de Clientes e Fornecedores incluídos nas listas de sanções impostas pelas resoluções da ONU, com o objetivo de cumprir com as seguintes obrigações:

- Garantia da comunicação imediata ao Diretor de PLDFT e de Compliance da SISPAY de qualquer fornecedor, cliente ou beneficiário (“Sancionado”) que conste em qualquer lista de sanções que seja aplicável à Lei nº 13.810/2019;
- Realização do imediato encerramento do relacionamento com o Sancionado, bem como do bloqueio para novas transações;
- Adoção das medidas necessárias para a realização da indisponibilidade de ativos de titularidade, direta ou indireta, do Sancionado, na forma e nas condições definidas pelo COAF ou outro órgão com finalidade semelhante;
- Comunicação do fato ao COAF ou outro órgão com finalidade semelhante, Bacen, Ministério da Justiça e Segurança Pública e demais órgãos competentes, conforme aplicável.

Caberá à SISPAY verificar se já foram adotadas as providências correspondentes e adotá-las, caso necessário.

O disposto nesta Política aplica-se às relações de negócio mantidas pela SISPAY e seus Clientes, e às relações que venham a ser iniciadas posteriormente com quaisquer Clientes alcançados pelas determinações de indisponibilidade.

Os procedimentos aqui listados estão integrados nos processos de mapeamento e monitoramento identificados nesta Política.

- Procedimentos a serem adotados pela SISPAY em caso de sanções impostas pelo CSNU

Para assegurar a efetividade desta Política, a instituição adotará os seguintes procedimentos no caso de sanções impostas pelo CSNU:

- Procedimentos de indisponibilidade de ativos de Pessoa Física, Pessoa jurídica e de entidades (proibição de transferir, converter, trasladar, disponibilizar ativos ou deles dispor, direta ou indiretamente);
- Comunicação tempestiva ao Bacen, ao Ministério Público e ao COAF referente as pessoas investigadas ou acusadas de terrorismo que aparecem nas listas sancionadoras da ONU;
- Acompanhamento de forma direta e atualizada, das informações divulgadas no site do CSNU, <https://lnkd.in/dgErmBjp> ;
- Na detecção de irregularidades, a SISPAY deve assegurar que se mantenham os ativos sob verificação, para efeito de colocá-los em regime de indisponibilidade;
- No caso de constatação de irregularidades, a instituição deverá cumprir imediatamente as medidas estabelecidas nas resoluções do CSNU no caso de comunicação por meio do sistema BC Correio, e dirigidas especificamente para pasta Deati/CSNU ;
- Ainda, a SISPAY deverá realizar as comunicações para o Ministério da Justiça e Segurança Pública (MJSP) devem ser dirigidas ao endereço institucional de e-mail csnu@mj.gov.br .

O monitoramento de informações abrange inclusões e exclusões de listas de pessoas naturais, pessoas jurídicas, entidades ou ativos sujeitos a medidas de indisponibilidade decorrentes de sanções ou determinações do CSNU ou de seus comitês de sanções.

Esta Política está disponível em local acessível a todos funcionários diretamente envolvidos no gerenciamento e no cumprimento de sanções impostas por resoluções do Conselho de Segurança das Nações Unidas. É possível acessá-la no site <https://sispay.com.br>

Marcelo Artur Motta Ramos Marques

Diretor

Vera Lucia Teixeira

Diretora