

**POLÍTICA DE
PREVENÇÃO À
LAVAGEM DE
DINHEIRO,
FINANCIAMENTO AO
TERRORISMO E AO
FINANCIAMENTO DA
PROLIFERAÇÃO DE
ARMAS DE
DESTRUIÇÃO EM
MASSA**

ASA

MANEIRO

1. Aspectos Preliminares

A presente Política de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e ao Financiamento da Proliferação de Armas de Destrução em Massa (respectivamente, “Política” e “PLD.FTP”) se aplica ao ASA Sociedade de Crédito Financiamento e Investimento S.A. (“ASA”) e demais empresas do Grupo sob controle comum, e compreende uma gama de diretrizes e compromissos objetivando assegurar a licitude dos negócios realizados no âmbito das atividades desempenhadas pelo ASA e o cumprimento e conformidade à legislação e regulamentação em vigor atinentes a PLD.FTP.

Por meio desta Política, o ASA – incluindo seus sócios/acionistas, diretores, administradores e colaboradores – reafirma sua adesão às normas legais, regulatórias e autorregulatórias aplicáveis, notadamente a Lei nº 9.613, de 3 de março de 1998, Circular BCB nº 3.978, de 23 de janeiro de 2020 (“Circular nº 3.978”), a Carta-Circular BACEN nº 4.001, de 2020 (“Carta-Circular nº 4.001”), bem como demais normas e regulamentações em vigor pertinentes à atuação do ASA.

Todos os colaboradores do ASA, independentemente de sua área de atuação, têm a obrigação de reportar imediatamente à área de PLD.FTP qualquer situação que, de acordo com seu conhecimento, possa apresentar indícios de lavagem de dinheiro ou financiamento do terrorismo. Reportes sobre situações suspeitas relacionadas com Lavagem de Dinheiro ou Financiamento ao Terrorismo podem ser feitas na caixa de e-mail:

- PLD ASA <pld@asa.com.br>

A Diretoria do ASA reitera seu compromisso com a efetividade e com a melhoria contínua da Política, dos procedimentos e dos controles internos relacionados à prevenção à lavagem de dinheiro e ao financiamento do terrorismo.

2. DEFINIÇÕES

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

Financiamento ao Terrorismo e da proliferação de Armas de Destrução em Massa (“FTP”): consiste na reunião de fundos e/ou capital para a realização de atividades terroristas. Esses fundos podem ser provenientes de doações ou ganho de diversas atividades lícitas ou ilícitas, como crimes em geral.

Financiamento da Proliferação de Armas de Destrução em Massa:

Considera-se a provisão, movimentação ou disponibilização de recursos destinados ao desenvolvimento, produção, aquisição, posse, transporte ou utilização de armas nucleares,

químicas ou biológicas, ou de seus meios de lançamento, em desacordo com normas e tratados internacionais aplicáveis.

Corrupção: consiste em sugerir, oferecer, submeter, solicitar, aceitar ou receber, direta ou indireta, as pessoas do setor público, provado ou organizações do terceiro setor, vantagens indevidas.

Pessoa Exposta Politicamente (“PEP”): consideram-se pessoas expostas politicamente os agentes públicos que desempenham ou tenham desempenhado nos últimos 5 (cinco) anos, no Brasil ou em países, territórios e dependências estrangeiros, cargos, empregos ou funções públicas relevantes, assim como seus representantes, familiares e outras pessoas de seu relacionamento próximo. Além disso, são exemplos de situações que caracterizam relacionamento próximo e acarretam o enquadramento de cliente como pessoa politicamente exposta, como controle direto ou indireto, de cliente pessoa jurídica.

Clientes: pessoas físicas ou jurídicas que utilizam os produtos e serviços da instituição, sendo categorizados internamente – conforme suas características, porte, natureza e capacidade financeira.

Beneficiário Final: é a pessoa que em última instância, de forma direta ou indireta, possui, controla ou influencia significativamente a estrutura empresarial, em nome do qual uma transação esteja sendo conduzida ou dela se beneficie. É também considerado Beneficiário Final o representante, inclusive o procurador e o preposto, que exerça o comando de fato sobre as atividades da pessoa jurídica. Ainda, presume-se influência significativa quando a pessoa natural possui mais de 25% (vinte e cinco por cento) ou mais de participação societária. Excetuam-se do disposto as pessoas jurídicas constituídas sob forma de companhia aberta ou entidade sem fins lucrativos e as cooperativas, para as quais as informações coletadas devem abranger as informações das pessoas naturais autorizadas a representá-las, bem como controladores, administradores e diretores, se houver. Para os trusts, devem ser identificadas as figuras do settlor, protector (se houver), trustee e beneficiário do trust.

Banco de Fachada ou Shell Bank: banco constituído em uma jurisdição onde não há qualquer presença física e que não se encontra integrado em um grupo financeiro regulamentado.

Canal de Distribuição: meio pelo qual a instituição realiza a oferta de seus produtos e serviços. Para fins desta Política, entende-se como canais de distribuição: (i) canais digitais - por meio de um canal de distribuição mobile e versão internet desktop - responsáveis por expor uma interface de acesso pelos clientes aos produtos/serviços ofertados; e (ii) por canal interno denominado “Cockpit de Negócios”, voltado para o apoio das áreas comerciais da Instituição.

Ambiente de Negociação de Ativos: local (físico ou virtual) onde são negociados produtos de investimento. Para fins desta Política, entende-se como ambientes de negociação: a Bolsa de Valores e a Bolsa Balcão.

3. Governança e Responsabilidades de PLD.FTP

A governança para PLD.FTP é exercida de acordo com as responsabilidades dos seguintes componentes da estrutura organizacional:

Da Diretoria

- Designar, perante os órgãos reguladores, conforme o caso, um diretor responsável por PLD.FTP;
- Aprovar, em última Instância, a Política de PLD.FTP ;
- Prover recursos para que os procedimentos e controles internos relacionados à PLD.FTP cumpram seus objetivos;
- Tomar ciência da Avaliação Interna de Risco e da Avaliação de Efetividade, bem como do plano de ação destinado a solucionar as deficiências identificadas.

Do Diretor responsável por PLD.FTP (“Diretor de PLD.FTP”)

- Aprovar esta Política e os demais Manuais: Manual de Monitoramento de PLD.FTP e Manual Procedimental de PLD.FTP;
- Aprovar as diretrizes e procedimentos estabelecidos pela área de PLD.FTP;
- Deliberar comunicações órgãos competentes, notadamente o Conselho de Controle de Atividades Financeiras – COAF, na forma e prazos estabelecidos na forma da regulamentação aplicável;
- Aprovar e encaminhar à Diretoria os relatórios relativos à Avaliação Interna de Risco e a Avaliação de Efetividade, bem como acompanhar o plano de ação destinado a solucionar as eventuais deficiências identificadas.

Head de PLD.FTP:

- Estabelecer diretrizes e procedimentos a serem observados por todos os segmentos do ASA para aderência das atividades desempenhadas e dos produtos e serviços ofertados à legislação e regulamentação de PLD.FTP aplicáveis;
- Implementar e acompanhar o cumprimento desta Política e dos demais Manuais: Manual de Monitoramento de PLD.FTP e Manual Procedimental de PLD.FTP.
- Deliberar sobre situações consideradas de alto risco de Lavagem de Dinheiro, Financiamento ao Terrorismo e Financiamento da Proliferação de Armas de Destrução em Massa (“LD/FTP”), quando requerido pelo regime de alçadas vigente, relacionadas ao início ou manutenção de relacionamento com clientes, colaboradores, parceiros ou fornecedores/prestadores de serviços;
- Implementar processos e manter atualizadas as regras de monitoramento de operações de acordo com a legislação e regulamentação de PLD.FTP aplicáveis;
- Submeter à ciência do Diretor de PLD.FTP os alertas tratados e classificados como indícios de LD/FTP;
- Realizar as comunicações órgãos competentes, notadamente o Conselho de Controle de Atividades Financeiras – COAF, na forma e prazos estabelecidos na regulamentação aplicável, conforme deliberação do Diretor de PLD.FTP;
- Realizar as comunicações aos órgãos competentes, notadamente ao Conselho de Controle de Atividades Financeiras – COAF, na forma e prazos estabelecidos na regulamentação aplicável, após deliberação do Diretor de PLD.FTP;
- Conduzir os processos e preparar os relatórios de Avaliação Interna de Risco e

Avaliação de Efetividade do programa de PLD.FTP , bem como implementar e acompanhar o plano de ação destinado a solucionar as eventuais deficiências identificadas.

Equipe de PLD.FTP:

- Avaliar sob a ótica de PLD.FTP, os novos produtos ou serviços oferecidos pelo ASA;
- Analisar as situações consideradas de alto risco de LD/FTP relacionadas ao início ou manutenção de relacionamento com clientes, colaboradores, parceiros ou fornecedores/prestadores de serviços ou identificados no monitoramento e, caso identificado indício de LD.FTP , submeter à análise do Head de PLD.FTP;
- Conduzir os processos e auxiliar o Head de PLD.FTP na elaboração dos relatórios de Avaliação Interna de Risco e Avaliação de Efetividade do programa de PLD.FTP.

Equipe de RH:

- Avaliar sob a ótica de PLD.FTP, os candidatos que estão sendo considerados para contratação pelo ASA. Caso identifique situações consideradas de alto risco durante a análise deverá submeter à análise ao Head de PLD.FTP ou Compliance.

Equipe de Compliance:

- Avaliar a aderência regulatória das Políticas e Processos relacionados à PLD.FTP.

Auditoria Interna

- Fornecer aos órgãos de governança e à Alta Administração avaliações abrangentes, independentes e objetivas relativas aos riscos de PLD.FTP da Instituição.
- Revisar de modo sistemático a eficácia dos processos, contribuindo para o seu aprimoramento.

4. Diretrizes, Mecanismos e Ferramentas de PLD.FTP

Em linha com o disposto nas demais normas que regulam os procedimentos relacionados a PLD.FTP, a ASA estabeleceu diretrizes sobre:

- (i) Avaliação de Serviços e Produtos;
- (ii) Identificação, Qualificação e Classificação:
 - clientes;
 - funcionários (Colaboradores);
 - fornecedores;
- (iii) Prevenção ao financiamento do terrorismo;
- (iv) Registro de operações;
- (v) Monitoramento e Comunicação de Operações e Situações Suspeitas;
- (vi) Arquivamento de Informações;
- (vii) Treinamento e Divulgação;
- (viii) Teste de Efetividade;
- (ix) Avaliação Interna de Risco;
- (x) Sigilo e Arquivamento das Informações

Atualmente, o ASA utiliza ferramenta terceirizada para identificação de apontamentos diretos e indiretos em mídias negativas. Essa solução considera, além de menções explícitas ao próprio cliente, também aquelas relacionadas a familiares, sócios, ex-sócios e demais vínculos relevantes do indivíduo analisado. Como consequência, esses apontamentos são incorporados ao processo de classificação de risco, contribuindo para a elevação do número de clientes classificados como Alto Risco, conforme os critérios estabelecidos na abordagem baseada em risco adotada pela instituição.

Para tanto, o ASA conta com sistemas e ferramentas para auxiliar nos processos de Prevenção à Lavagem de Dinheiro, como AML Integrity, VADU, Risc Advice, conforme aplicável para cada tipo de relacionamento e/ou rotina; além de ferramentas proprietárias desenvolvidas internamente para monitoramento contínuo dos clientes.

Para fins de monitoramento e identificação de operações e situações potencialmente suspeitas, as regras e parâmetros estão configurados nas ferramentas terceirizadas contratadas, incluindo E-Guardian, conforme aplicável para cada tipo de relacionamento e/ou rotina.

A seguir, serão descritas as diretrizes que deverão ser observadas por completo pelos colaboradores, sob pena das responsabilizações previstas nesta Política e nas normas legais, regulatórias e autorregulatórias aplicáveis.

5. Processos de Identificação e Qualificação (KY's):

Para cumprimento do disposto na Circular BCB nº 3.978, o ASA, além da presente Política, dispõe de um Manual Procedimental de PLD.FTP que descreve, além de outros pontos, de forma detalhada, os processos de identificação, verificação e classificação de clientes (KYC), de colaboradores e terceiros (KYE), e de parceiros e prestadores de serviços (KYP).

Esses processos deverão garantir a realização de diligência prévia e contínua para todos os públicos citados, ao longo de todo o relacionamento, com vistas a identificar e mitigar riscos relacionados à LD.FTP.

O referido Manual contempla a coleta e a verificação das informações exigidas na Circular BCB nº 3.978, estabelecendo critérios de segmentação e classificação de risco dos clientes, de forma a permitir o monitoramento proporcional ao grau de exposição e risco identificados.

Com base nas informações recebidas no processo de identificação, em complemento à qualificação, o ASA estabelecerá metodologia própria de classificação de risco embasada pela regulamentação aplicável, para definição dos critérios adotados. A classificação de risco deverá ser realizada com base na alimentação das informações cadastrais.

Adicionalmente ao processo de classificação de risco de clientes, o ASA também realizará a classificação de riscos de seus funcionários, terceiros, parceiros e fornecedores.

Este processo deverá ser atualizado e revisado anualmente ou de acordo com atualizações

regulatórias, e a revisão do risco PLD.FTP dos clientes, funcionários, terceiros e fornecedores ocorrerá em períodos distintos conforme risco PLD.FTP anterior, podendo ser:

Classificação de risco PLD.FTP
Baixo
Médio
Alto

O ASA adota Abordagem Baseada em Risco. Para essa abordagem, o ASA considera as melhores práticas de mercado e adota diretrizes que incluem: a identificação e avaliação dos riscos inerentes, a definição do apetite de risco, a implementação de controles mitigadores, a avaliação do risco residual e a revisão periódica do *Risk Assessment*, sempre com foco na efetividade da prevenção aos crimes de LD.FTP.

Os demais controles relacionados à PLD.FTP, como diligências complementares realizadas ao longo do relacionamento e o monitoramento transacional, serão aplicados de forma proporcional ao perfil de risco do cliente e à natureza da relação de negócio estabelecida.

A descrição do processo de classificação para cada perfil e definição da Abordagem Baseada no Risco está disposta no Manual Procedimental de PLD.FTP, bem como na Avaliação Interna de Riscos.

4.1.1. Identificação e Qualificação de Clientes / Conheça seu Cliente (KYC)

Todo relacionamento comercial com potenciais clientes deve ser submetido a uma avaliação prévia de risco relacionada à PLD.FTP, seja por meio de uma análise individualizada ou por procedimentos que adotem perfis de relacionamento padronizados e previamente definidos.

O processo de cadastro de clientes do ASA está alinhado à regulamentação vigente, adotando procedimentos consistentes e robustos para coleta, registro e verificação de informações. Tais procedimentos garantem rigor na identificação, validação e qualificação cadastral dos clientes, permitindo, inclusive, a verificação da condição de Pessoa Exposta Politicamente (PEP), bem como a análise da cadeia de participação societária até a identificação do beneficiário final, nos termos da Circular BCB nº 3.978.

É realizada uma checagem do cliente na ferramenta AML Integrity, integrada com a Plataforma de cadastro, de tal sorte que, caso o risco atribuído a este potencial cliente, conforme Abordagem Baseada no Risco disposta no Manual Procedimental de PLD.FTP seja baixo, ou seja, não sejam identificados indícios de atipicidades e/ou apontamentos desabonadores, o cliente é aprovado automaticamente. Por outro lado, caso sejam identificados apontamentos que desabonem o potencial cliente, que elevem o risco do prospect para Médio ou Alto, a análise do relacionamento do cliente é derivada à equipe de PLD.FTP para análise e deliberação, conforme procedimentos e plano de alçadas

definidos no Manual Procedimental de PLD.FTP.

A manutenção da base cadastral deve permitir revisões periódicas e atualizações dinâmicas, de forma a acompanhar a evolução do relacionamento comercial e do perfil de risco do cliente, assegurando a aderência às exigências regulatórias e às melhores práticas de mercado.

Nenhuma relação de negócio poderá ser iniciada sem que os procedimentos de identificação e qualificação cadastral tenham sido realizados e compatíveis com o grau de risco identificado.

Os procedimentos de "Conheça Seu Cliente" (KYC) devem ser aplicados de forma proporcional ao nível de risco, tanto na abertura de novos relacionamentos comerciais quanto em situações que demandem a atualização de informações ou a obtenção de dados adicionais sobre o perfil do cliente, sua origem de recursos ou a natureza de sua atividade, sendo solicitadas informações adicionais que permitam esclarecer a situação do cliente..

Essa abordagem visa assegurar um conhecimento contextual adequado dos clientes, fortalecendo a capacidade institucional de identificar, monitorar e mitigar riscos associados às relações comerciais.

4.1.2. Conheça seu Colaborador (KYE)

O ASA compartilha a estrutura e unidades operacionais com as demais empresa sob controle comum do ASA. Essas unidades operacionais executam funções de apoio ao negócio e controle operacional, notadamente: administração predial, suprimentos, marketing, planejamento financeiro, contabilidade, desenvolvimento e manutenção de sistemas, jurídico, compliance, gestão de riscos, back office, middle office, recursos humanos, entre outras, observando as regras de segregação de funções e de ambientes físicos, de acordo com a regulamentação vigente.

Assim, o ASA possui processo de “Conheça seu Colaborador” (KYE), buscando contratar Colaboradores com perfis que condizem com os princípios e expectativas do ASA, principalmente em relação ao Código de Ética e Conduta e à presente Política. Para tanto, a Equipe de RH realiza o processo de análise e avaliação detalhada de informações sobre cada candidato, em momento prévio à admissão. Caso identifique situações consideradas de alto risco durante a análise deverá submeter à análise ao Head de PLD.FTP.

Para tanto, é utilizada ferramenta de background check, que consolida informações oriundas de listas restritivas internacionais, especialmente aquelas relacionadas à PLDFTP, listas de Pessoas Politicamente Expostas (PEPs) e outras bases públicas.

4.1.3. Conheça seus Produtos e Serviços

Os procedimentos de “Conheça seus Produtos e Serviços” asseguram a coleta de informações suficientes e adequadas sobre os produtos e serviços a serem oferecidos pelo ASA, antes de sua disponibilização ao mercado. O objetivo é subsidiar a análise de riscos associados ao uso indevido dessas soluções, possibilitando uma avaliação preventiva e fundamentada, conforme critérios de abordagem baseada em risco (ABR) definidos pela área de PLD.FTP, no Manual Procedimental de PLD.FTP e na Avaliação Interna de Riscos.

A área de PLD.FTP deve ser envolvida de forma prévia na avaliação de novos produtos, serviços e tecnologias aplicadas aos canais de relacionamento e comercialização. Essa atuação preventiva visa identificar e mitigar riscos regulatórios, bem como prevenir o uso indevido dessas soluções na prática de crimes de LD.FTP.

4.1.4. Conheça seu Parceiro e Conheça seu Fornecedor e Prestador de Serviço (KYP):

O ASA, realizará procedimentos de identificação e aceitação dos parceiros e prestadores de serviços relacionados aos serviços e produtos oferecidos para o estabelecimento de relações de parceria comercial.

A avaliação prévia do ASA, terá como objetivo prevenir a realização de negócios com parceiros inidôneos ou suspeitos de envolvimento em atividade ilícitas, bem como assegurar que tais parceiros também apresentem políticas de PLD.FTP consistentes e adequadas, conforme aplicável. O processo de avaliação também contempla verificação sistemática contra listas restritivas e fontes públicas.

Os parceiros e prestadores de serviço do ASA deverão admitir que a Instituição realize *due diligences* sempre que julgar necessário, além de responder, quando solicitado, questionários de diligências.

4.2. Pessoa Exposta Politicamente (PEP)

São considerados PEP Titulares os agentes públicos que desempenham ou tenham desempenhado, nos últimos cinco anos, no Brasil ou em países, territórios e dependências estrangeiras, cargos, empregos ou funções públicas relevantes, assim bem como a verificação da condição de representante, familiar ou estreito funcionário dessas pessoas (Relacionados).

Os procedimentos dispostos nesta Política, no Manual Procedimental de PLD.FTP compreendem a identificação e o tratamento diferenciado para as pessoas qualificadas como Pessoa Politicamente Exposta (PEP) no que tange à análise, avaliação de monitoramento para fins de PLD.FTP.

Para os clientes qualificados como pessoa exposta politicamente ou como representante, familiar ou estreito funcionário dessas pessoas, caso a caso deverão:

- (i) ser adotados procedimentos e controles internos compatíveis com essa qualificação;
- (ii) ser considerados essa qualificação na classificação do cliente nas categorias de risco; e
- (iii) ser avaliado o interesse no início ou na manutenção do relacionamento com o cliente ou terceiro. No processo de coleta das informações cadastrais os clientes e terceiros são obrigados a declarar se são ou não Pessoa Exposta Politicamente, sendo também submetido ao confronto das bases cadastrais que dados públicos e privados para identificação da condição de PEP. A aprovação dos clientes e terceiros que se encontram na condição de PEP, titular e relacionado, é realizada por detentor de cargo ou função de nível hierárquico superior ao do responsável pela autorização do relacionamento com o cliente ou terceiro, conforme critérios estabelecidos no Procedimento Operacional de Conheça seu Cliente (KYC). Os clientes e terceiros identificados como politicamente expostos (PEP Titular) são classificados de forma sistêmica com risco “alto”, e os relacionados são classificados com risco “médio”, sendo submetido a monitoramento de especial atenção, diligência reforçada, alinhada ao risco.

São aplicados nas bases cadastrais o confronto com bases de dados públicos e privados para identificação da condição de PEP, identificando se um cliente ou terceiro se tornou PEP, incluindo o representante, familiar e estreito funcionário, ou deixaram a condição PEP. Tal procedimento é de responsabilidade da área de cadastro, sendo os casos identificados submetidos ao processo de aprovação pelo Head de PLD.FTP, alinhado à avaliação interna de risco para revisão da classificação. A informação identificada deve ser armazenada na base cadastral e disponibilizada ao processo de monitoramento nas etapas de seleção e análise de operações atípicas. O sistema assegura a manutenção da informação de condição de PEP pelos cinco anos seguintes à data que a pessoa não mais atender aos requisitos para enquadramento como tal.

4.3. Identificação e qualificação do Beneficiário Final

Os procedimentos de qualificação do cliente pessoa jurídica incluem a análise da cadeia de participação societária até a identificação da pessoa natural caracterizada como seu Beneficiário Final, e serão aplicados à pessoa natural, no mínimo, os procedimentos de qualificação definidos para a categoria de risco do cliente ou terceiros pessoa jurídica na qual o Beneficiário Final detenha participação societária.

A informação identificada deve ser armazenada na base cadastral e disponibilizada ao processo de monitoramento nas etapas de seleção e análise de operações atípicas. O sistema assegura a manutenção da informação de condição de PEP pelos cinco anos seguintes à data que a pessoa não mais atender aos requisitos para enquadramento como tal.

Os Beneficiários Finais são submetidos ao confronto com bases de dados públicos e privados para identificação da condição de PEP, identificando se o mesmo tornou-se PEP, pelo período requerido na regulamentação em vigor e indicado nesta política.

5. Monitoramento e Comunicação de Operações Atípicas

O ASA deve empregar procedimentos e ferramentas adequadas à natureza, porte e complexidade de suas operações para o monitoramento contínuo das transações, de modo a possibilitar a identificação de operações atípicas, suspeitas ou inconsistentes com o perfil cadastral e transacional do cliente.

As áreas de negócio devem atuar observando atentamente os comportamentos e operações de seus clientes e comunicando prontamente a área de PLD.FTP quando identificadas situações atípicas, inconsistentes ou suspeitas.

Compete à área de PLD.FTP a análise e a comunicação tempestiva à autoridade competente, notadamente o COAF, de quaisquer indícios de LD.FTP, conforme os prazos e formas estabelecidos pela regulamentação em vigor.

Nesse sentido, o ASA editou Manual específico de monitoramento, seleção e análise de operações a fim de identificar e dispor de especial atenção especial às suspeitas de lavagem de dinheiro e financiamento do terrorismo (“Manual de Monitoramento de PLD.FTP”), incluindo:

- Situações descritas na Carta-Circular nº 4.001 aplicadas ao negócio do ASA;
- As operações realizadas incompatíveis com a capacidade financeira do cliente;
- Transações com envolvendo clientes PEPs, seus representantes, familiares ou pessoas de relacionamento próximo;
- Clientes e transações para as quais não é possível identificar o beneficiário final;
- As situações em que não é possível manter as informações cadastrais de clientes atualizadas;
- Operações e situações que podem indicar suspeitas de financiamento ao terrorismo e ou proliferação de armas de destruição em massa; e
- Operações realizadas por funcionários, prestadores de serviços e fornecedores.

As regras parametrizadas para monitoramento e seleção das operações suspeitas e os sistemas e procedimentos utilizados devem estar sujeitos à verificação quanto à sua adequação e eficácia, sendo revisados periodicamente ou de acordo com as exigências e atualizações regulatórias.

As movimentações análogas à Carta-Circular nº 4.001 ou ainda quaisquer outras situações que indiquem indícios de ilicitude, deverão ser avaliadas pela equipe de PLD.FTP, findando em decisão fundamentada quanto à baixa do alerta/investigação ou o reporte ao COAF e demais autoridades competentes, conforme aplicável, e submetidas à análise final do Head de PLD.FTP. e deliberação do Diretor de PLD.FTP.

De acordo com a abordagem baseada em risco, para clientes de maior exposição de LD/FTP deverá ser aplicado um conjunto de regras ou parâmetros mais rigorosos ou ainda um acompanhamento mais frequente ou aprofundado de suas atividades.

6. Cumprimento de Programas de Sanções

O cumprimento dos programas de sanções, conforme exigido pela regulamentação aplicável e vigente – incluindo a Circular BCB nº 3.978 e as diretrizes internacionais emitidas por órgãos como o Conselho de Segurança das Nações Unidas (ONU), o Office of Foreign Assets Control (OFAC) dos Estados Unidos e a União Europeia (UE) – compreende o conjunto de medidas e critérios que devem ser rigorosamente observados. Essas medidas incluem a implementação de políticas, procedimentos e controles internos destinados a evitar e prevenir o descumprimento de sanções econômicas e financeiras impostas por autoridades competentes, bem como o monitoramento contínuo das listas de sanções e a adoção de diligências apropriadas para assegurar a conformidade com tais exigências.

O ASA adota medidas que abrangem os processos e procedimentos a fim de cumprir com o programa de sanções, a fim de detectar vinculações com os países proibidos, pessoas e entidades sancionadas, assim, sendo identificadas quaisquer aplicações de sanções ou contramedidas financeiras nacionais ou internacionais. Após análise da equipe de PLD.FTP e deliberações das alçadas definidas, para o pleno atendimento a requisitos legais, será determinado o bloqueio ou congelamento de fundos ou recursos econômicos, tal como o bloqueio de operações financeiras submetidas a países e/ou pessoas e entidades sancionadas.

As consultas são realizadas para todos os Clientes, Colaboradores, Parceiros, Fornecedores e Prestadores de serviços, realizando a filtragem nas seguintes fontes:

- Organização das Nações Unidas (ONU) / CNSU: o Conselho de Segurança dessa instituição, mediante resoluções, estabelece restrições com capacidade vinculativa para seus membros;
- União Europeia (UE): Aplicação de medidas estabelecidas pelo direito comunitário através de distintos instrumentos (diretivas, regulamentos e decisões do Conselho da União, o Parlamento e a Comissão Europeia);
- Estados Unidos (EUA): através Office of Foreign Assets Control (OFAC);
- Financial Crimes Enforcement Network (FINCEN); e
- US Department of State (Cuba Restricted List).

6.1. Jurisdições Restritas ou Proibidas:

A Instituição adota procedimentos específicos e reforçados de prevenção à lavagem de dinheiro, ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa (PLD.FTP) em relação a jurisdições identificadas pelo Grupo de Ação Financeira Internacional (GAFI/FATF) como detentoras de deficiências estratégicas significativas em seus respectivos regimes de PLD.FTP.

Em conformidade com as recomendações do GAFI, a Instituição adotará as medidas a seguir:

- a) Aplicar medidas de Devida Diligência Reforçada (Enhanced Due Diligence – EDD) a clientes, operações e relacionamentos que envolvam, direta ou indiretamente, tais jurisdições;
- b) Avaliar a necessidade de adoção de contramedidas, nos casos considerados mais graves, com o objetivo de proteger a Instituição e o sistema financeiro dos riscos de PLD.FTP provenientes dessas jurisdições;
- c) Revisar e, se necessário, restringir ou encerrar relacionamentos comerciais, observando o apetite de risco da Instituição e a legislação aplicável;
- d) Intensificar o monitoramento transacional e reputacional, incluindo análise de beneficiários finais, estruturas societárias, origem e destino de recursos;
- e) Reportar operações suspeitas às autoridades competentes, quando aplicável, nos termos da regulamentação vigente.

As jurisdições enquadradas nessa categoria são comumente referidas, por agentes externos, como integrantes da chamada “lista negra” do GAFI, devendo sua classificação e atualização ser acompanhadas de forma contínua pela área de PLD.FTP.

7. Sigilo e Arquivamento de Informações

Toda e qualquer informação relacionada a clientes, suas propostas, operações ou comunicações realizadas junto aos órgãos reguladores está protegida por sigilo, devendo ser mantido acesso a essas informações restrito aos colaboradores diretamente envolvidos com a atividade de PLD.FTP.

As informações referentes a indícios ou suspeitas de LD/FTP possuem caráter estritamente confidencial e não devem, sob nenhuma circunstância, ser compartilhadas com as partes envolvidas ou terceiros não autorizados. As comunicações de operações suspeitas são de uso exclusivo das autoridades competentes, destinadas à análise e investigação no âmbito de suas atribuições legais.

As informações atinentes a esta Política, bem como os registros das operações e serviços prestados devem ser mantidos em sua forma original ou em arquivos eletrônicos, pelo prazo mínimo de 10 anos estabelecido pela legislação vigente.

8. Treinamento e Divulgação

Esta Política deverá ser conhecida e aplicada por todos os Colaboradores e mantida a sua versão atualizada no site do ASA.

A fim de garantir a capacitação de seus colaboradores sobre o tema da prevenção à lavagem de dinheiro e ao financiamento ao terrorismo, o ASA oferecerá contínuo programa de treinamento de PLD.FTP, visando aprofundar o conhecimento acerca dos requerimentos

normativos externos e internos de PLD.FTP, bem como capacitar os Colaboradores a identificar, prevenir, tratar e comunicar situações suspeitas ou relacionadas a PLD.FTP.

A aplicação do programa deve ocorrer no momento da admissão dos novos colaboradores e atualizada anualmente, por meio de ações institucionais e nas unidades de negócio, podendo contemplar cursos à distância (e-learning) e presencial, palestras, campanhas, comunicados, publicações, entre outras modalidades e formas.

As áreas de PLD.FTP, Compliance e Recursos Humanos devem acompanhar e garantir a efetividade desse programa de treinamento junto aos Colaboradores.

9. Avaliação Interna de Risco e Avaliação de Efetividade do programa de PLD.FTP:

9.1. Avaliação Interna de Risco

A Avaliação Interna de Risco será realizada pela área de PLD.FTP e tem como objetivo considerar os fatores de risco relevantes para os quais o ASA está exposta e considerar seus impactos, considerando os riscos dispostos no Capítulo IV da Circular BCB nº 3.978.

A Avaliação Interna de Risco deverá ser:

- Documentada e aprovada pelo Diretor responsável por PLD.FTP;
- Encaminhada para ciência à Diretoria do ASA;
- Revisada a cada dois anos, bem como quando ocorrerem alterações significativas nos perfis de risco identificados no relatório vigente.

9.2. Avaliação de Efetividade

O Head de PLD.FTP deve avaliar a efetividade da política, dos procedimentos e dos controles internos do programa e processos de PLD.FTP, conforme requerido disposto no caput XI da Circular 3.978/20.

A metodologia aplicada baseia-se na análise da política formalizada e vigente para o tema, bem como evidências documentais e entrevistas com a área responsável pela gestão de PLD/FT para ponderações sobre o grau de efetividade dos controles no decorrer do ano, com o intuito de identificar deficiências e/ou oportunidades de melhoria nos processos existentes.

Ao final, é elaborado um plano de ação com os ajustes necessários, com o acompanhamento periódico do status pelo Head de PLD.FTP .

A Avaliação de Efetividade deverá ser:

- Realizada anualmente com data-base de até 31 de dezembro do ano anterior;
- Documentada e aprovada pelo Diretor responsável por PLD.FTP; e
- Encaminhada para ciência da Diretoria da instituição ou do Comitê de Auditoria, seguindo os seguintes termos:

- Relatório: encaminhado, para ciência até 31/03 do ano seguinte ao da data-base; e
- O plano de ação e o respectivo relatório de acompanhamento: encaminhados para ciência e avaliação, até 30/06 do ano seguinte ao da data-base do relatório.

10. Registro das Operações

O ASA deve manter registros de todas as operações realizadas, produtos e serviços contratados, nos termos da Circular BCB nº 3.978.

11. Disposições Finais

Esta política deve ser revisada bianualmente, ou sempre que houver alterações na legislação ou regulamentação aplicável, visando assegurar a sua atualidade e aderência.

Essa Política foi aprovada pela Diretoria da ASA e sua versão atualizada ficará disponível no website da instituição.

São Paulo, 11 de Março de 2026.