

**POLÍTICA DE PREVENÇÃO E
COMBATE À LAVAGEM DE
DINHEIRO E AO FINANCIAMENTO
DO TERRORISMO – PLD/FT**



DOCUMENTO: POLÍTICA DE PREVENÇÃO E COMBATE À LAVAGEM DE DINHEIRO
E AO FINANCIAMENTO DO TERRORISMO – PLD/FT

CLASSIFICAÇÃO: #PÚBLICO

TIPO DE DOCUMENTO: PO – POLÍTICA

DATA DA ÚLTIMA ALTERAÇÃO: 22/06/2026

ELABORAÇÃO:

Ayrton Gomes – Gerência de Operações

REVISÃO:

Ayrton Gomes – Gerência de Operações

Guilherme Medeiros – Risco e Compliance

Elyaquim Mendes – Processo, Fluxos e Controles Internos

APROVAÇÃO:

Rafael Alves Quirino – Diretoria Executiva

VERSÃO: 006

ALTERAÇÕES

22/06/2026 – Versão 006:

- Alteração do nome do arquivo, cabeçalho e “Documento:” da presente página para: POLÍTICA DE PREVENÇÃO E COMBATE À LAVAGEM DE DINHEIRO E AO FINANCIAMENTO DO TERRORISMO – PLD/FT.
- Alteração dos textos para Política de Prevenção e Combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo (adição de Combate e alteração para “do Terrorismo”), para adequação aos documentos oficiais governamentais.

VIGÊNCIA

A partir de sua publicação

SUMÁRIO

1.	OBJETIVO	5
1.1.	Abrangência.....	5
2.	AVALIAÇÃO DE EFETIVIDADE	6
3.	REGULAMENTAÇÃO BASE	6
3.1.	Normas e Diretrizes Internacionais	6
3.2.	Legislação Nacional Sobre Crimes Financeiros	7
3.3.	Regulamentação do Banco Central do Brasil (BCB), COAF e Conselho Monetário Nacional (CMN)	7
3.3.1.	Normas Sobre PLD/FT	7
3.3.2.	Gestão De Riscos e Compliance	7
3.3.3.	Indisponibilidade de Bens e Ativos.....	8
3.4.	Normas Sobre Contas De Pagamento e Meios de Pagamento	8
4.	DEFINIÇÕES	8
5.	DIRETRIZES.....	10
5.1.	Gestores e Líderes de Equipes	12
5.2.	Área de Controles Internos e Compliance.....	12
5.3.	Diretor Responsável pelo Compliance	14
5.4.	Demais Diretores.....	14
5.5.	Recursos Humanos.....	14
5.6.	Cadastro.....	15
5.7.	Front- Office (Atendimento, Suporte, Executivos De Negócios).....	15
5.8.	Auditoria – Interna ou Terceirizada	16
5.9.	Tecnologia da Informação	16
5.10.	Análise de Risco de Novos Produtos ou Serviços	16
6.	RECOMENDAÇÕES GERAIS	16
7.	AVALIAÇÃO INTERNA DE RISCO.....	17
7.1.	Identificação dos Clientes	17

7.2.	Qualificação dos Clientes	18
7.2.1.	Pessoas Expostas Politicamente	19
7.2.2.	Identificação	21
7.2.3.	Aprovação de Cadastro e Due Dilingence para PEP	22
7.2.4.	Pessoas de Mídia	22
7.2.5.	Beneficiário Final	23
8.	COMUNICAÇÃO DE INDÍCIOS AOS ORGÃOS COMPETENTES	23
9.	INDISPONIBILIDADE DE ATIVOS	23
10.	QUALIFICAÇÃO E TREINAMENTO.....	24
11.	GUARDA DE DOCUMENTOS E INFORMAÇÕES	25

1. OBJETIVO

A Política de Prevenção e Combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo tem por objetivos:

- Estabelecer padrões de conduta, processos e procedimentos que deveram ser seguidos por todos os colaboradores, parceiros e prestadores de serviço do grupo Kredit, principalmente os diretamente envolvidos nas operações, quanto à prevenção e combate à lavagem de dinheiro e ao financiamento do terrorismo;
- Reforçar o compromisso da Kredit no cumprimento das leis e regulamentos, nacionais e internacionais, relacionados à prevenção e combate à lavagem de dinheiro e ao financiamento do terrorismo;
- Identificar produtos, serviços e processos que possam representar riscos e estabelecer controle adequado para prevenir e combater a lavagem de dinheiro e o financiamento do terrorismo;
- Promover uma cultura de controles e responsabilidades de forma a incentivar a aderência dos profissionais às regulamentações internas e legislação vigente, bem como às melhores práticas do mercado.
- Evitar que a Kredit seja utilizada na prática de crime lavagem de dinheiro e de financiamento do terrorismo, reduzindo os riscos que desabonem sua reputação e imagem;
- Promover o conhecimento, verificação e obediência à legislação vigente, em especial as Leis 9.613 de 1998 (Lavagem de Dinheiro) e 13.260 de 2016 (Financiamento do Terrorismo).
- Definir programa de treinamento dos colaboradores para maior grau de conhecimento e identificação de possíveis indícios de ilícitos.

1.1. Abrangência

Esta Política de Prevenção e Combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo - PLD/FT aplica-se integralmente a todas as empresas do grupo Kredit, incluindo suas subsidiárias, filiais, parceiros comerciais e prestadores de serviço que, direta ou indiretamente, desempenham atividades relacionadas aos seus objetos sociais.

A política deve ser observada por todos os colaboradores, executivos, conselheiros, representantes e terceiros que atuem em nome da instituição, independentemente do nível hierárquico ou da natureza de sua relação contratual.

Além disso, sua aplicabilidade estende-se a clientes, fornecedores e demais partes envolvidas em operações financeiras ou comerciais, no que couber, garantindo que todos os agentes vinculados à instituição adotem práticas compatíveis com as regulamentações nacionais e internacionais de prevenção e combate à lavagem de dinheiro e ao financiamento do terrorismo.

Esta política deve ser incorporada às diretrizes internas da instituição e respeitada de forma irrestrita, garantindo a conformidade com a legislação vigente e promovendo um ambiente de negócios íntegro e seguro. A não observância das diretrizes estabelecidas poderá resultar em sanções disciplinares, contratuais e legais, conforme a gravidade da infração e a legislação aplicável.

2. AVALIAÇÃO DE EFETIVIDADE

A efetividade das políticas, normas, procedimentos e controles internos de PLD/FT deve ser avaliada anualmente, para garantir o cumprimento das responsabilidades do grupo Kredit. Após a emissão, a revisão e a validação dos pontos de aprimoramento identificados na Avaliação de Efetividade, a Diretoria do Jurídica, Controles Internos & Compliance desenvolverá plano de ação para acompanhar, junto às áreas de negócio, ou de governança, a implementação dos pontos de melhoria para correção das deficiências apontadas no relatório. O plano de ação deverá ser encaminhado para ciência e validação pela Alta Administração.

3. REGULAMENTAÇÃO BASE

A presente política está alinhada às normativas nacionais e internacionais de prevenção e combate à lavagem de dinheiro e ao financiamento do terrorismo, conforme detalhado a seguir:

3.1. Normas e Diretrizes Internacionais

Recomendações do Grupo de Ação Financeira (GAFI) – Define padrões internacionais para PLD/FT, incluindo medidas de *due diligence*, monitoramento de transações e reporte de operações suspeitas.

3.2. Legislação Nacional Sobre Crimes Financeiros

- Lei nº 9.613/1998 – Dispõe sobre os crimes de lavagem de dinheiro, estabelece penalidades e cria mecanismos de controle financeiro.
- Lei nº 13.260/2016 – Define crimes de terrorismo e medidas para seu combate, incluindo financiamento ilícito.
- Lei nº 13.810/2019 – Trata da indisponibilidade de bens, direitos e valores de pessoas investigadas por terrorismo ou corrupção internacional.

3.3. Regulamentação do Banco Central do Brasil (BCB), COAF e Conselho Monetário Nacional (CMN)

3.3.1. Normas Sobre PLD/FT

- Circular BCB nº 3.978/2020 – Regula a Política de PLD/FT para instituições financeiras, estabelecendo diretrizes sobre monitoramento, comunicação de operações suspeitas e governança.
- Carta Circular BCB nº 4.001/2020 – Especifica situações suspeitas passíveis de comunicação ao COAF, determinando critérios objetivos para identificação de transações atípicas.
- Resolução Nº 29, de 7 de dezembro de 2017 - Dispõe sobre os procedimentos a serem observados pelas pessoas reguladas pelo COAF, na forma do § 1º do artigo 14 da Lei nº 9.613, de 3 de março de 1998, relativamente a pessoas expostas politicamente.

3.3.2. Gestão De Riscos e Compliance

- Resolução CMN nº 4.557/2017 – Dispõe sobre a Gestão Integrada de Riscos (GIR) e a estrutura de gerenciamento de riscos em instituições financeiras.
- Resolução BCB nº 65/2021 – Estabelece a política de conformidade (compliance) nas instituições de pagamento, determinando padrões para mitigação de riscos regulatórios.
- Resolução BCB nº 93/2021 – Regulamenta auditoria interna nas instituições de pagamento, garantindo avaliação independente da aderência às normas de PLD/FT.

3.3.3. Indisponibilidade de Bens e Ativos

Resolução BCB nº 44/2020 – Define os procedimentos para cumprimento de ordens de indisponibilidade de bens relacionadas a atividades ilícitas e terrorismo.

3.4. Normas Sobre Contas De Pagamento e Meios de Pagamento

- Resolução BCB nº 1/2020 – Institui e regulamenta o arranjo de pagamento PIX, determinando controles para mitigação de riscos de PLD/FT nas transações instantâneas.
- Resolução BCB nº 96/2021 – Dispõe sobre abertura, manutenção e encerramento de contas de pagamento, exigindo critérios de identificação e monitoramento de clientes.

4. DEFINIÇÕES

- **Lavagem de Dinheiro:** Crime previsto na Lei 9.613/1998, caracterizado pela incorporação de recursos ilícitos ao sistema econômico. O processo ocorre em três etapas: colocação, quando os valores são inseridos na economia formal; ocultação, quando transações complexas dificultam o rastreamento da origem dos recursos; e integração, quando os ativos são legalizados e passam a circular com aparência lícita.
- **Financiamento do Terrorismo:** Regulamentado pela Lei 13.260/2016, refere-se ao fornecimento de recursos financeiros para atos terroristas. Os fundos podem ser obtidos de forma lícita (doações, lucros comerciais) ou ilícita (tráfico de drogas, extorsão, contrabando). As ações terroristas incluem o uso de explosivos e armas químicas, sabotagem de infraestruturas essenciais e atentados contra pessoas.
- **COAF (Conselho de Controle de Atividades Financeiras):** Criado pela Lei 9.613/1998, é o órgão vinculado ao Banco Central responsável pela supervisão e aplicação de penalidades em casos de lavagem de dinheiro. Atua em conjunto com órgãos como a Polícia Federal e o Ministério Público, fortalecendo o combate a crimes financeiros.
- **ENCCLA (Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro):** Iniciativa que reúne Poderes Executivo, Legislativo, Judiciário e Ministério Público, além de entidades especializadas, para desenvolver e

aprimorar políticas de combate à lavagem de dinheiro e ao financiamento do terrorismo.

- **GAFI (Grupo de Ação Financeira):** Organização internacional responsável por definir padrões globais para a prevenção de crimes financeiros. Suas recomendações são referência para a criação de políticas nacionais e regulatórias voltadas ao combate à lavagem de dinheiro, financiamento do terrorismo e proliferação de armas ilegais.
- **Pessoa Exposta Politicamente (PEP):** Indivíduo que ocupa ou ocupou, nos últimos cinco anos, cargo, emprego ou função pública relevante no Brasil ou no exterior. Devido ao alto risco de envolvimento em corrupção, transações envolvendo PEPs exigem monitoramento reforçado e medidas adicionais de *due diligence*.
- **Beneficiário Final:** Pessoa natural que, em última instância, possui, controla ou influencia significativamente uma entidade jurídica. A identificação do beneficiário final é essencial para evitar que empresas sejam usadas para ocultar operações ilícitas.
- **Devida Diligência do Cliente (DDC):** Processo de verificação da identidade do cliente e da origem de seus recursos, visando mitigar riscos de envolvimento com atividades ilícitas. Inclui análise documental, avaliação de perfil e monitoramento contínuo de transações.
- **Know Your Customer (KYC):** Conjunto de procedimentos adotados pelas instituições financeiras para verificar a identidade dos clientes, compreender suas atividades e avaliar o risco de envolvimento em crimes financeiros. O KYC é um dos pilares da política de prevenção à lavagem de dinheiro.
- **Know Your Employee (KYE):** Processo de análise e monitoramento de funcionários para prevenir riscos internos relacionados a fraudes, corrupção e vazamento de informações sensíveis. Inclui verificações cadastrais, histórico profissional e avaliação contínua de conduta.
- **Know Your Supplier (KYS):** Procedimento aplicado para garantir que fornecedores e parceiros comerciais não estejam envolvidos em atividades ilícitas. Engloba análise de registros financeiros, estrutura societária e possíveis conexões com crimes financeiros.

- **Know Your Partner (KYP):** Processo de análise e monitoramento de parceiros, diretos ou indiretos, para prevenir riscos internos relacionados a fraudes, corrupção e vazamento de informações sensíveis. Inclui verificações cadastrais, histórico profissional, das empresas coligadas ou com que mantém negócios e avaliação contínua de conduta.
- **Transação Suspeita:** Qualquer operação financeira que apresente indícios de irregularidade ou desvio de finalidade, como movimentações incompatíveis com o perfil do cliente, transações fracionadas para evitar detecção e operações envolvendo países com alto risco de lavagem de dinheiro ou financiamento do terrorismo.
- **Sanções Econômicas e Lista Restritiva:** Medidas impostas por organismos nacionais e internacionais que restringem transações com determinados indivíduos, empresas ou países envolvidos em atividades ilícitas. Instituições financeiras devem consultar listas como OFAC, ONU e Banco Central antes de realizar operações.
- **Monitoramento Contínuo:** Processo de acompanhamento sistemático das atividades financeiras dos clientes para identificar padrões suspeitos, alterações de comportamento ou operações incompatíveis com a origem declarada dos recursos.
- **Relatório de Operação Suspeita (ROS):** Documento enviado ao COAF quando uma transação apresenta indícios de lavagem de dinheiro ou financiamento do terrorismo. Sua comunicação é obrigatória e não depende da confirmação da irregularidade.
- **Regime de Colaboração Internacional:** Conjunto de acordos entre países e organismos reguladores para facilitar a troca de informações e o rastreamento de ativos ilícitos. Inclui cooperação com o GAFI, Interpol, ONU e órgãos nacionais de fiscalização.

5. DIRETRIZES

São princípios básicos esperados dos colaboradores, parceiros e prestadores de serviço da Kredit:

- Usar os meios necessários e possíveis para realizar a verificação de identidade de todos os clientes que possuam relação com o grupo Kredit;

- Havendo conhecimento ou suspeita de quaisquer irregularidades relacionadas ao cliente ou às operações por ele solicitadas, independentemente do valor, inclusive em relação à suspeita de lavagem de dinheiro ou de financiamento do terrorismo, não realizar qualquer tipo de negócio e comunicar imediatamente a área de PLD/FT;
- Havendo conhecimento de qualquer transação suspeita de um mesmo cliente que tenham sido propositadamente divididas, independentemente do valor, com objetivo de não serem identificadas, comunicar imediatamente a área de PLD/FT;
- Havendo conhecimento ou suspeita de lavagem de dinheiro ou de financiamento de terrorismo, mesmo nos casos em que não haja transações, comunicar imediatamente a área de PLD/FT;
- Atentar aos indícios de recursos que possam vir a ser originários de atividades ilegais;
- Caso venham à tona fatos que possam levar a uma suposição de que os recursos do cliente ou por ele mantidos originam-se de atividades ilegais, ou, detectadas finalidades estranhas às transações, deve-se comunicar, imediatamente, à Área de PLD/FT, para que sejam apurados os fatos e tomadas as providências cabíveis;
- Havendo percepção ou suspeita de informações falsas, alteradas ou incompletas, ou ainda ocultação de informações, não oferecer suporte ou assistência ao cliente, comunicando imediatamente a Área PLD/FT;
- Manter-se atualizado por meio de treinamentos, leitura de materiais e estudo de assuntos relacionados à Prevenção e Combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo;
- Consultar um superior hierárquico em casos de dúvidas ou solicitar auxílio à área de PLD/FT ou ao departamento responsável quando da suspeita, dúvida ou desconfiança de atitudes de clientes, funcionários, prestadores, parceiros ou fornecedores.

Todos os colaboradores, prestadores de serviço, parceiros (diretos ou indiretos) e fornecedores da Kreidt que violarem, mesmo que parcialmente, a regulamentação interna, a presente política ou às normas vigentes, ainda que aqui não explicitadas, estarão sujeitos às sanções disciplinares cabíveis.

5.1. Gestores e Líderes de Equipes

Cabe aos gestores e líderes do grupo Kredit aplicar seus melhores esforços quanto à disseminação dos conceitos deste documento aos seus respectivos colaboradores em suas atividades diárias, bem como verificar o integral cumprimento, sempre evitando o desconhecimento, negligência e, principalmente, a má-fé. Os gestores e líderes possuem também sob sua responsabilidade, o desenvolvimento e o fomento junto à sua equipe, de uma cultura de controles e condutas éticas, esclarecendo eventuais dúvidas, e atualizando seu pessoal nas melhores práticas de mercado e da responsabilidade de cada um no exercício correto de suas funções.

A referida atuação destes será ainda pautada pelo Código de Ética e Conduta da Kredit, obedecendo, inclusive, as previsões acerca de relacionamento com clientes e demais parceiros, também pautado no combate de qualquer medida que tenha por escopo final a dissimulação de procedimentos para disseminação de fraude ou crimes.

5.2. Área de Controles Internos e Compliance

Os colaboradores da área de Controles Internos & Compliance são os principais, mas não únicos, responsáveis pelo adequado funcionamento do processo de Prevenção e Combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo, cabendo a estes as seguintes atribuições:

- Realiza aprovação de proposta de abertura de conta com verificação acerca de vida pregressa, situação patrimonial e jurídica do propenso cliente;
- Desenvolver, implementar, avaliar e aprimorar o processo de prevenção e combate à lavagem de dinheiro e ao financiamento do terrorismo, disseminando seus conceitos aos colaboradores da empresa a fim de garantir a aderência às políticas e procedimentos;
- Garantir, através de treinamentos, que o processo de prevenção e combate à lavagem de dinheiro e ao financiamento do terrorismo seja claro, consistente, atualizado e seguido por todos os colaboradores;
- Desenvolver as políticas e padrões utilizados pela empresa, bem como as estratégias e requisitos de funcionamento do processo, criando e incentivando o fluxo adequado de informações em toda a empresa;

- Identificar os pontos de inconsistências e recomendando eventuais planos de ação e melhorias do processo de prevenção e combate à lavagem de dinheiro e ao financiamento do terrorismo, transmitindo à Diretoria tais informações;
- Monitorar transações de clientes e detalhar em relatório transações suspeitas após a análise de informações relevantes tais como: identificação do cliente, padrão de transações recorrentes, beneficiário final e propósito das transações;
- Monitoramento ocorre através do sistema de BI (Business Intelligence). No sistema, é possível identificar todas as transações suspeitas e analisar a rotina de transações de cada cliente.
- Monitorar operações de clientes e apontar em relatório aquelas que demonstrem incompatibilidade com a respectiva situação financeira patrimonial ou qualquer suspeita de irregularidade entre parte e contraparte, operações diretas, transferências de custódia, entre outras;
- Informar em relatório operações sobre as quais recaiam suspeitas de lavagem de dinheiro ou de financiamento de terrorismo, mesmo que não haja nenhum indício de atividade ilegal ou ilegalidade na origem dos recursos, ou casos em que os clientes se recusem a fornecer maiores informações quando solicitadas e quando suas transações forem suspeitas de serem inapropriadas após a análise.
- Preparar e manter, por 10 (dez) anos, registro dos Relatórios de Transações Suspeitas;
- Informar, após análise, montagem do dossiê e aprovação junto ao Comitê de risco, os casos suspeitos de lavagem de dinheiro ou financiamento do terrorismo aos organismos competentes, quando forem assim considerados;
- Manter o registro e controle das comunicações feitas aos órgãos reguladores; e
- Preparar informações relevantes acerca dos controles adotados pela empresa, atualização de regulamentação publicada no mercado, alteração em documentação interna, eventuais operações de clientes para análise e definição de ações, entre outras.
- Realizar o acompanhamento da ENCCLA, a fim de realizar implantação de medidas porventura disponibilizadas para aumentar o potencial de

enfrentamento aos crimes de lavagem de dinheiro e financiamento do terrorismo.

5.3. Diretor Responsável pelo Compliance

Patrocinador Executivo do processo de Prevenção e Combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo, sendo responsável por garantir a independência e autonomia do processo em relação às áreas de negócios e por assegurar que o assunto receba suporte adequado. O Diretor Responsável pelo Compliance é o principal interessado no sucesso e total aderência de toda empresa ao processo de Prevenção e Combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo. É o profissional que responde diretamente aos órgãos reguladores ou instituição competente em casos de suspeitas de irregularidades ou qualquer outra demanda relacionada à Lavagem de Dinheiro.

Cabe ao diretor responsável pelo Compliance desenvolver, implementar, avaliar e aprimorar o processo de prevenção e combate à lavagem de dinheiro e ao financiamento do terrorismo, cumprir as determinações dos órgãos reguladores bem como aprovar a Política Interna que dispõe sobre esse assunto. O diretor é responsável por auditar todos os relatórios e informações coletadas pela área de Controle Interno e Compliance e remeter ao COAF (SisCoaf).

5.4. Demais Diretores

As demais diretorias se responsabilizam por apoiar e dar suporte ao processo de prevenção e combate à lavagem de dinheiro e ao financiamento do terrorismo na empresa, bem como por divulgar a importância de seus conceitos a todos os seus subordinados.

5.5. Recursos Humanos

A área de Recursos Humanos é responsável pelo suporte ao processo de prevenção e combate à lavagem de dinheiro e ao financiamento do terrorismo na empresa, especialmente quanto ao processo de “Conheça seu funcionário (Know Your Employee)”. Possui ainda um importante papel na divulgação da documentação relacionada, na guarda de registros de treinamentos e ciência em documentação específica.

5.6. Cadastro

Aos colaboradores da área de Cadastro, além das atribuições inerentes a todos os colaboradores da empresa, cabe o atendimento completo do processo de cadastro que, dentre outros pontos, prevê a adequada identificação dos clientes e o atendimento a uma série de regulamentações do BACEN, e traz conceitos de conhecimento adequado do cliente, verificação de patrimônio, pesquisa do histórico do cliente, entre outros. A área de Cadastro possui papel importante no processo de prevenção e combate à lavagem de dinheiro e ao financiamento do terrorismo e suas principais atribuições podem ser verificadas no processo específico de cadastro.

5.7. Front- Office (Atendimento, Suporte, Executivos De Negócios)

Aos colaboradores do front-office, ou seja, colaboradores que possuem maior contato com os clientes, ficam estabelecido o dever de conhecer e cumprir integralmente todas as leis e regulamentos de prevenção e combate à lavagem de dinheiro e ao financiamento do terrorismo, além das políticas e procedimentos internos relacionados ao tema. Cabe aos colaboradores de front-office o auxílio à correta identificação dos clientes, enviando as informações cadastrais relevantes corretamente para uma adequada classificação do perfil.

Toda e qualquer atividade suspeita deverá ser imediatamente comunicada à área de Controles Internos & Compliance.

Quanto ao acompanhamento das operações e aos procedimentos de “Conheça seu Cliente (Know Your Customer)”, os colaboradores de front-office, bem como o diretor responsável pela área comercial, devem:

- Atualizar as áreas de Cadastro, Controles Internos & Compliance e Risco com dados relevantes dos clientes, em especial aqueles que trazem informações financeiras, para uma adequada identificação dos clientes e eventual atualização de limites operacionais;
- Informar aos clientes sobre a utilização, guarda e compartilhamento de dados, em total adequação à Lei Geral de Proteção de Dados;
- Analisar previamente se a contratação condiz com as condições informadas e comprovadas pelos clientes, principalmente em caso de desenvolvimento de atividade comercial.

5.8. Auditoria – Interna ou Terceirizada

Faz parte do processo de auditoria interna a realização de relatórios anuais que atestem a efetividade da política implantada, nos termos da CBC nº 3978/2020, com a descrição da metodologia, testes, avaliadores, identificação de possíveis deficiências e correções, bem como avaliação e monitoramento de transações, governança e cultura organizacional dessa política com a devida capacitação de pessoal. O relatório de efetividade é composto ainda pelas políticas de conhecimento (cliente, funcionários, parceiros e terceirizados) e procedimento de análise e comunicação ao COAF.

5.9. Tecnologia da Informação

Responsável pela garantia da perfeita operacionalidade dos sistemas utilizados pela empresa, em especial pela área de Controles Internos & Compliance, provendo de forma tempestiva os serviços de manutenção aos sistemas e a priorização na recuperação de informações quando solicitadas pelo Compliance. Garantir a proteção dos dados com um plano de Back-up seguro e confiável, de forma a recuperar as informações em tempo razoável para execução de atividades relacionadas a controle, em particular à prevenção e combate à lavagem de dinheiro e ao financiamento do terrorismo.

5.10. Análise de Risco de Novos Produtos ou Serviços

Sempre que houver desenvolvimento ou parceria que tenha projeção de novos produtos ou serviços a serem oferecidos pela Kredit, será realizada análise e avaliação prévia acerca dos riscos operacionais e de fornecimento que possam contribuir com a lavagem de dinheiro e financiamento do terrorismo. A análise envolve a viabilidade de ocorrência de LD/FT através do levantamento do risco inerente à atividade ou produto, bem como as tecnologias e formas de prevenção destes nas operações.

6. RECOMENDAÇÕES GERAIS

A identificação e conhecimento de clientes é um processo contínuo, sendo intensificado no início do relacionamento com a empresa e melhorado a cada transação, atendimento e relacionamento pessoal ou eletrônico. É de suma importância que todos os colaboradores da empresa conheçam os principais conceitos do mercado e indicações dos organismos reguladores relacionados à identificação de clientes e a

prevenção e combate à lavagem de dinheiro e ao financiamento do terrorismo, para tanto seguem em destaque algumas recomendações de extrema relevância:

- Identificar o cliente através de documentos, dados e informações de origem acreditável e independente, de preferência a identificação pessoal do cliente;
- Manter vigilância contínua sobre a relação de negócios e examinar atentamente as operações realizadas no decurso dessa relação, verificando se são condizentes com o conhecimento que a instituição possui do cliente, de seus negócios e de seu perfil de risco, incluindo, se necessários, a origem dos valores transacionados;
- Examinar com particular atenção todas as transações de montantes significativamente elevados e todos os tipos não habituais;
- Comunicar a área de PLD/FT todo e qualquer indício de informações falsas, operações divergentes à situação financeira do cliente, operações divergentes do perfil da conta ou qualquer situação atípica que gere suspeita de irregularidade.

7. AVALIAÇÃO INTERNA DE RISCO

Para os clientes da Kredit, incluindo aqueles prospectados por empresas parceiras, os critérios destinados à identificação, qualificação e classificação dos clientes estão previstos no Manual Específico KYC/KYP. Esses critérios seguem as diretrizes e orientações desta Política, compatíveis com o perfil de risco do cliente e com a Avaliação Interna de Risco da Kredit.

A Avaliação Interna de Risco sempre deve considerar a aderências dos clientes aos produtos e serviços da Kredit, levando em consideração o grau de risco de cada cliente.

Toda e qualquer comunicação aos órgãos reguladores competentes deve ser precedida do *Customer Due Dilligence* do cliente envolvido.

7.1. Identificação dos Clientes

A Kredit adota uma política de análise criteriosa para identificar e validar a identidade do cliente, garantindo a obtenção, verificação e validação da autenticidade das informações fornecidas. Essas informações são confrontadas com listas disponíveis em bancos de dados públicos e privados, conforme a classificação de risco do cliente.

No mínimo, são coletados os seguintes dados:

- **Pessoa Física:** Nome completo, CPF, data de nascimento e domicílio;
- **Pessoa Jurídica:** Razão social e número de registro no CNPJ, Contrato social ou estatuto social e última alteração registrada, bem como Composição societária e identificação de sócios, administradores e beneficiários finais (conforme a Resolução nº 50 da CGSIM).

Adicionalmente, podem ser solicitados outros dados e informações que reforcem o processo de identificação e classificação de risco do cliente. Os números de CPF e CNPJ são checados junto à Receita Federal do Brasil (RFB), sendo vedado o início de relacionamento com clientes que apresentem status de inabilitação perante a RFB, como cadastros suspensos, cancelados, baixados, inaptos ou nulos.

As informações e dados obtidos são periodicamente atualizados, conforme os níveis de risco dos clientes cadastrados, em conformidade com o Manual Específico.

7.2. Qualificação dos Clientes

A Kredit adota procedimentos para qualificar seus clientes por meio da coleta, verificação e validação de informações, sempre em alinhamento com a classificação de risco e a natureza da relação de negócios. Durante esse processo, são identificados:

- **Pessoa Física:** Local de residência e capacidade financeira (renda);
- **Pessoa Jurídica:** Local da sede ou filial e capacidade financeira (faturamento).

A qualificação do cliente é reavaliada continuamente, de acordo com a evolução da relação de negócios e do perfil de risco, garantindo que as informações permaneçam atualizadas. Nenhuma relação comercial é iniciada sem a conclusão dos procedimentos de identificação e qualificação, salvo exceções aprovadas pela área de Controles Internos & Compliance, por um período máximo de 30 dias, desde que se mantenha a integridade dos processos de monitoramento, seleção e análise de operações suspeitas.

Durante a qualificação, são analisados aspectos comportamentais e reputacionais do cliente, com consultas a bancos de dados públicos e privados que contenham listas restritivas globais e domésticas, mídias negativas, sanções socioambientais, processos judiciais, entre outros.

7.2.1. Pessoas Expostas Politicamente

Conforme os Artigos 18 e seguintes, da Circular nº 3.978, de 23 de janeiro de 2020, do Banco Central do Brasil, consideram-se pessoas politicamente expostas os agentes públicos que desempenham ou tenham desempenhado, nos últimos cinco anos, contado, retroativamente, a partir da data de início da relação de negócio ou da data em que o cliente passou a se enquadrar como PEP, no Brasil ou em países, territórios e dependências estrangeiros, cargos, empregos ou funções públicas relevantes, assim como seus representantes, familiares e estreito colaborador.

Por estreito colaborador é compreendida qualquer pessoa natural que tenha participação societária, de fato ou de direito, conjunta com PEP, seja como sócio, mandatário ou criadas para benefício destes. São considerados familiares os parentes, na linha reta, até o primeiro grau, o cônjuge, o companheiro, a companheira, o enteado e a enteada.

No caso de clientes brasileiros, conforme o Artigo 27, da Circular 3.978/2020, devem ser abrangidos:

- I. Os detentores de mandatos eletivos dos Poderes Executivo e Legislativo da União;
- II. Os ocupantes de cargo, no Poder Executivo da União:
 - a) De ministro de estado ou equiparado;
 - b) De natureza especial ou equivalente;
 - c) De presidente, vice-presidente e diretor, ou equivalentes, de autarquias, fundações públicas, empresas públicas ou sociedades de economia mista; do Grupo Direção e Assessoramento Superiores - DAS, nível 6, ou equivalentes;
- III. Os membros do Conselho Nacional de Justiça, do Supremo Tribunal Federal, dos tribunais superiores;
- IV. Os membros do Conselho Nacional do Ministério Público, o Procurador-Geral da República, o Vice- Procurador-Geral da República, o Procurador-Geral do Trabalho, o Procurador-Geral da Justiça Militar, os Subprocuradores-Gerais da República e os Procuradores-Gerais de Justiça dos estados e do Distrito Federal;

- V. Os membros do Tribunal de Contas da União e o Procurador-Geral do Ministério Público junto ao Tribunal de Contas da União;
- VI. Os presidentes e os tesoureiros nacionais, ou equivalentes, de partidos políticos;
- VII. Os governadores e os Secretários de Estado e do Distrito Federal, os presidentes de tribunal de justiça, de assembleia e câmara legislativa, os presidentes de tribunal de contas, tribunais militares de Estado, do Distrito Federal e de Município, e de conselho de contas dos Municípios;
- VIII. Os prefeitos, vereadores, secretários municipais, presidentes, ou equivalentes, de entidades da administração pública indireta municipal e os presidentes dos tribunais de contas ou equivalentes dos municípios.
- IX. São também consideradas expostas politicamente as pessoas que, no exterior, sejam:
- X. Chefes de estado ou de governo;
- XI. Políticos de escalões superiores;
- XII. Ocupantes de cargos governamentais de escalões superiores;
- XIII. Oficiais-generais e membros de escalões superiores do Poder Judiciário;
- XIV. Executivos de escalões superiores de empresas públicas; ou;
- XV. Dirigentes de partidos políticos.
- XVI. São também consideradas pessoas expostas politicamente os dirigentes de escalões superiores de entidades de direito internacional público ou privado.
- XVII. No caso de clientes estrangeiros, devem ser adotadas as seguintes providências:
- XVIII. Solicitar declaração expressa do cliente a respeito da sua classificação;
- XIX. Recorrer a informações publicamente disponíveis;
- XX. Consultar bases de dados comerciais sobre PEP; e
- XXI. Considerar como PEP a pessoa que exerce ou exerceu funções públicas proeminentes em um país estrangeiro, tais como chefes de estado ou de governo, políticos de alto nível, altos servidores governamentais, judiciais, do

legislativo ou militar, dirigente de empresas públicas ou dirigentes de partidos políticos.

XXII. No caso de relação de negócio com cliente estrangeiro que também seja cliente de instituição estrangeira fiscalizada por entidade governamental assemelhada ao Banco Central do Brasil, admite-se que as providências em relação a PEP sejam adotadas pela instituição estrangeira, desde que assegurado ao Banco Central do Brasil o acesso aos respectivos dados e procedimentos adotados. Também se aplica a pessoa que exerce ou exerceu função de alta administração em uma organização internacional de qualquer natureza, assim considerados diretores, subdiretores, membros de conselho ou funções equivalentes. As operações ou propostas de operações que possuam PEP como parte envolvida será sempre considerada como merecedoras de especial atenção.

7.2.2. Identificação

A identificação de clientes Pessoa Exposta Politicamente na Kredit é efetuada em duas situações distintas, e visam assegurar que nenhum cliente nessa condição seja cadastrado, ou efetue suas operações, sem os controles adotados pela instituição para clientes PEP (direto ou indireto). No momento do cadastramento, todos os clientes são questionados sobre a condição de Pessoa Exposta Politicamente e, caso o cliente se identifique nessa condição, após verificação sobre o titular, é solicitado ao mesmo que preencha e assine um termo se intitulando Pessoa Exposta Politicamente.

Para identificação de clientes PEP, além da consulta a fontes de dados públicas, a Kredit adota outros controles de identificação, a saber:

- a) Como passo obrigatório no procedimento de cadastramento de clientes é prevista consulta à base do ZAIG – QI Tech CaaS, que, dentre outras informações, identifica clientes na condição de Pessoa Exposta Politicamente segundo os critérios descritos anteriormente. Verificado que o cliente se encontra na condição de PEP, é encaminhado ao mesmo o modelo de Termo de Autodeclaração como Pessoa Exposta Politicamente ou cancelada sua proposta;
- b) Em decorrência dos bancos de dados serem automatizados, como no caso da utilização do BackOffice, em caso de suspeita por quaisquer apontamentos dos bancos de dados, é realizada busca e análise humana para melhor verificação.

Além disso, todas as transações são acompanhadas pelo Compliance de maneira periódica, tendo em vista que o conceito é temporário;

- c) Como o conceito prevê prazos para enquadramento na condição de Pessoa Exposta Politicamente, a lista de clientes nessas condições varia periodicamente, especialmente após a ocorrência de eleições e épocas de troca de cargos políticos. Para garantir a confiabilidade do processo de identificação, semestralmente toda a base de clientes cadastrada no SINACOR e Portal da Transparência é confrontada com lista atualizada adquirida do ZAIG – QI Tech e SERASA e, identificado clientes na condição de PEP é solicitado ao mesmo que preencha e assine termo específico.

7.2.3. Aprovação de Cadastro e Due Dilligence para PEP

Toda documentação cadastral de cliente Pessoa Exposta Politicamente deve ser aprovada pelo Comitê de Risco e PLD/FT da instituição e encaminhado para conhecimento da área de Controles Internos & Compliance. De posse da documentação cadastral do cliente PEP a área de Controles Internos & Compliance efetua análise de *Due Dilligence*.

7.2.4. Pessoas de Mídia

São consideradas “Pessoas da Mídia” as seguintes pessoas:

- Pessoas que estejam em voga na mídia, artistas, esportistas, jornalistas, incluindo membros de suas “famílias imediatas” (pais, irmãos, cônjuge, filhos e parentes por afinidade) e “associados próximos” (uma personalidade da mídia é uma pessoa ampla e publicamente conhecida por manter relacionamento extraordinariamente próximo com a personalidade da mídia, incluindo uma pessoa que está em condições de realizar transações financeiras, em âmbito nacional e internacional, em nome desta).
- Sociedades, empresas, ou outras pessoas jurídicas que tenham sido formadas por uma personalidade da mídia ou em seu benefício. Quando um colaborador, especialmente da área de cadastro, identificar uma Pessoa da Mídia, este comunicar imediatamente a área de Controles Internos & Compliance. No caso de comprovação de Pessoa da Mídia

os mesmos procedimentos adotados para Pessoas Politicamente Expostas deverão ser cumpridos, exceto a autodeclaração do cliente.

7.2.5. Beneficiário Final

Nos procedimentos de qualificação do cliente pessoa jurídica, a Kredit realiza uma análise aprofundada da cadeia de participação societária para identificar a pessoa natural caracterizada como beneficiário final. Essa pessoa está sujeita, no mínimo, aos mesmos procedimentos de qualificação aplicáveis ao cliente pessoa jurídica em questão.

A Kredit considera como beneficiário final também representantes, procuradores e prepostos que exerçam o comando de fato sobre as atividades da empresa. O valor mínimo de participação societária para a identificação do beneficiário final é estabelecido de forma documental e justificada no Manual Específico KYC Integrado, respeitando um limite máximo de 25% (vinte e cinco por cento) da participação societária, incluindo participações diretas e indiretas.

A identificação e qualificação do beneficiário final são etapas essenciais para mitigar riscos associados a lavagem de dinheiro e financiamento do terrorismo, reforçando o compromisso da Kredit com a transparência e a conformidade regulatória.

8. COMUNICAÇÃO DE INDÍCIOS AOS ORGÃOS COMPETENTES

Para a identificação de suspeitas de crime de lavagem de dinheiro ou de financiamento do terrorismo, a área de PLD/FT, caso identifique a intenção de prática irregular, elabora material detalhando os motivos pelo qual houve a suspeita do crime. O dossiê elaborado com as evidências colhidas e o histórico das operações, bem como a documentação cadastral do cliente deve ser analisado pelo Comitê de PLD/FT, que deve confirmar a suspeita após análise e assinar a carta de comunicação aos órgãos reguladores.

9. INDISPONIBILIDADE DE ATIVOS

A indisponibilidade de ativos é uma medida adotada por ordem superior que tem por finalidade a retirada do direito de propriedade de ativos por transações atípicas ou que contenham indícios de ilícito.

A Kredit, imediatamente, ao tomar conhecimento, e através da Área de Compliance determinará aos setores responsáveis o cumprimento, e sem aviso prévio

aos sancionados, das medidas determinadas nas resoluções sancionatórias do CSNU (Conselho de Segurança das Nações Unidas) inclusive de seus comitês de sanções, que determinem a indisponibilidade de ativos, de quaisquer valores, de titularidade, direta ou indireta, de pessoas naturais, de pessoas jurídicas ou de entidades, nos termos da Lei nº 13.810, de 2019 e art. 27 e 28 da ICVM 617/19. Também em consonância com a CBC nº 44 e Lei 9.613 de 1998, sempre que necessário será realizada a comunicação com o Banco Central, Ministério de Justiça e Segurança Pública e COAF, no devido prazo e condições de confidencialidade que a informação demanda.

10. QUALIFICAÇÃO E TREINAMENTO

A Kredit estabelece a seus colaboradores a obrigatoriedade de adequação à qualificação mínima referente às demandas de órgãos reguladores, bem como às políticas e procedimentos da instituição desenvolvidos para prevenção e combate à lavagem de dinheiro e ao financiamento do terrorismo. A eficácia do Programa de Treinamento relacionado à prevenção e combate à lavagem de dinheiro e ao financiamento do terrorismo está condicionada à disciplina dos elementos relacionados a seguir:

Público	Frequência	Observações
Todos os colaboradores	Anual	Treinamento geral sobre conceitos básicos e atualizações regulatórias.
Equipes de alto risco	Semestral ou trimestral	Foco em áreas como Compliance, Operações e Atendimento ao Cliente.
Novos colaboradores	Durante o <i>onboarding</i>	Treinamento básico obrigatório.
Mudanças regulatórias	Imediatamente após a mudança	Treinamento emergencial para todas as áreas impactadas.
Gestores e Compliance	Semestral	Treinamentos avançados e específicos.

11. GUARDA DE DOCUMENTOS E INFORMAÇÕES

Tipo de Documento/Informação	Prazo de Guarda	Meio de Armazenamento	Controle de Acesso	Observações
Dados cadastrais de clientes	10 anos, contados a partir do 1º dia do ano seguinte ao término do relacionamento	Digital (criptografado) ou físico (em ambiente seguro com controle de umidade e temperatura)	Acesso restrito a equipes de Compliance, Auditoria e Jurídico	Inclui KYC, registros de due diligence e atualizações cadastrais.
Registros de funcionários, parceiros e terceirizados	10 anos, contados a partir do encerramento da relação contratual	Digital (sistema de gestão com backup em nuvem)	Acesso limitado a RH, Compliance e gestores diretos	Dados de due diligence, histórico de cargos e treinamentos em PLDFT.
Registros de operações e transações	10 anos, contados a partir do 1º dia do ano seguinte à realização da operação	Digital (banco de dados auditável e com timestamp)	Acesso monitorado por sistemas de log (ex: equipes de Risco e Compliance)	Inclui operações suspeitas, transações acima de R\$ 10 mil e relatórios de CTR/STR.
Dossiê de perfil de risco do cliente	10 anos, contados a partir da última atualização do dossiê	Digital (sistema integrado de gestão de riscos)	Acesso exclusivo à área de Compliance e autoridades regulatórias	Deve incluir análise de risco, movimentação atípica e medidas mitigadoras.
Comunicações ao COAF	10 anos, contados a partir do envio da comunicação	Digital (com assinatura eletrônica qualificada)	Acesso restrito à equipe de Compliance e COAF	Backup físico opcional, desde que em envelope lacrado e armazenado em cofre.
Registros de treinamentos em PLDFT	5 anos, contados a partir da data do treinamento	Digital (plataforma de gestão de aprendizagem)	Acesso ao RH, Compliance e Auditores Internos/Externos	Inclui lista de participantes, conteúdo programático e resultados de avaliações.