



**Política de Prevenção e Combate à  
Lavagem de Dinheiro e ao Financiamento  
ao Terrorismo**

**ALTERAÇÕES**

<b>Documento:</b>	<b>Código de Ética e Conduta</b>
<b>Assunto:</b>	<b>Diretrizes Institucionais</b>
<b>Data da última alteração:</b>	<b>22/02/2023</b>
<b>Revisão:</b>	<b>Larissa Leal Ayrton Gomes Processos e Controles Internos</b>
<b>Aprovação:</b>	<b>Rafael Alves Quirino Presidente</b>
<b>Versão:</b>	<b>6.0</b>

## SUMÁRIO

1. OBJETIVOS .....	4
2. DEFINIÇÕES.....	4
2.1 LAVAGEM DE DINHEIRO .....	4
2.2 FINANCIAMENTO AO TERRORISMO .....	5
2.3 CONSELHO DE CONTROLE DE ATIVIDADES FINANCEIRAS (COAF) .....	5
2.4 ESTRATÉGIA NACIONAL DE COMBATE À CORRUPÇÃO E À LAVAGEM DE DINHEIRO (ENCCLA).....	6
2.5 GRUPO DE AÇÃO FINANCEIRA (GAFI) .....	6
3. DIRETRIZES .....	6
3.1 GESTORES E LÍDERES DE EQUIPES.....	7
3.2 ÁREA DE CONTROLES INTERNOS E COMPLIANCE.....	7
3.3 DIRETOR RESPONSÁVEL PELO COMPLIANCE .....	8
3.4 DEMAIS DIRETORES .....	9
3.5 RECURSOS HUMANOS .....	9
3.6 CADASTRO .....	9
3.7 FRONT- OFFICE (ATENDIMENTO, SUPORTE, CONSULTORES COMERCIAIS).....	9
3.8 AUDITORIA INTERNA (PRÓPRIA OU TERCEIRIZADA) .....	10
3.9 TECNOLOGIA DA INFORMAÇÃO .....	10
3.10 ANÁLISE DE RISCO DE NOVOS PRODUTOS OU SERVIÇOS .....	10
4. RECOMENDAÇÕES GERAIS A TODOS OS COLABORADORES DA EMPRESA.....	10
5. CUSTOMER DUE DILIGENCE.....	11
6. CATEGORIZAÇÃO DE RISCO DE CLIENTES .....	11
6.1 IDENTIFICAÇÃO DE CLIENTE .....	11
6.1.1 IDENTIFICAÇÃO SIMPLES .....	12
6.1.2 IDENTIFICAÇÃO JUNTO AO CLIENTE.....	12
6.1.3 IDENTIFICAÇÃO APRIMORADA.....	13
7. POLÍTICA CONHEÇA SEU FUNCIONÁRIO – KNOW YOUR EMPLOYEE .....	14
8. PESSOAS EXPOSTAS POLITICAMENTE – PEP .....	15
8.1 CONCEITO .....	15
8.2 IDENTIFICAÇÃO.....	16
8.3 APROVAÇÃO DE CADASTRO E CLIENT DUE DILIGENCE PARA PEP .....	17
8.4 MEDIDAS PARA DETERMINAR A ORIGEM DO PATRIMÔNIO E DILIGÊNCIA NAS OPERAÇÕES ..	17
8.5 PESSOAS DE MÍDIA.....	18
9. COMUNICAÇÃO DE INDÍCIOS AOS ORGÃOS COMPETENTES .....	19
10. INDISPONIBILIDADE DE ATIVOS.....	19
11. DISSEMINAÇÃO, QUALIFICAÇÃO, TREINAMENTO E ADERÊNCIA DOS PROFISSIONAIS.....	20
12. CONSIDERAÇÕES FINAIS .....	20

## 1. OBJETIVOS

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

- Estabelecer padrões de conduta, processos e procedimentos que devam ser seguidos por todos os colaboradores da empresa, principalmente os diretamente envolvidos nas operações, quanto à prevenção e combate à lavagem de dinheiro e ao financiamento ao terrorismo;
- Reforçar o compromisso da Kredit Bank no cumprimento das leis e regulamentos, nacionais e internacionais, relacionados à prevenção e combate à lavagem de dinheiro e ao financiamento ao 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 ao terrorismo;
- Promover uma cultura de controles e responsabilidades de forma a incentivar a aderência dos profissionais às regulamentações internas e externas, bem como às melhores práticas do mercado.
- Evitar que a Kredit Bank seja utilizada na prática de crime lavagem de dinheiro e de financiamento ao 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 ao Terrorismo).
- Definir programa de treinamento dos colaboradores para maior grau de conhecimento e identificação de possíveis indícios de ilícitos.

## 2. DEFINIÇÕES

### 2.1 LAVAGEM DE DINHEIRO

Regulamentado pela Lei 9.613 de 1998, o crime de lavagem de dinheiro caracteriza-se por um conjunto de operações comerciais ou financeiras que buscam a incorporação na economia, de modo transitório ou permanente, de recursos, bens e valores de origem ilícita e que se desenvolvem por meio de um processo dinâmico que envolve, teoricamente, três etapas independentes que, com frequência, ocorrem simultaneamente, quais sejam, a colocação, ocultação e integração dos ativos da economia regular.

Ainda, incorre no mesmo tipo penal quem, para ocultar ou dissimular a utilização de bens ou direitos, (i) os converte em ativos lícitos, (ii) os adquire, recebe, troca, negocia, dá ou recebe em garantia, guarda, tem em depósito, movimenta ou transfere, (iii) importa ou exporta bens com valores não correspondentes aos verdadeiros, (iv) utiliza, na atividade econômica ou financeira, bens, direitos ou valores provenientes de infração penal, (v) participa de grupo, associação ou escritório tendo conhecimento de que sua atividade principal ou secundária é dirigida à prática de crimes previstos na Lei 9.613/98.

O processo de lavagem de dinheiro envolve três etapas, são elas:

- **Colocação:** é a etapa em que o criminoso introduz o dinheiro obtido ilicitamente no sistema econômico mediante depósitos, compra de instrumentos negociáveis ou compra de bens. Trata da remoção do dinheiro do local que foi ilegalmente adquirido e sua inclusão, por exemplo, ao mercado financeiro.
- **Ocultação:** é o momento que o criminoso realiza transações suspeitas e caracterizadoras do crime de lavagem. Nesta fase, diversas transações complexas se configuram para desassociar a fonte ilegal do dinheiro, dificultando o rastreamento da origem do dinheiro por parte das autoridades. O objetivo é quebrar a cadeia de evidências ante a possibilidade da realização de investigações sobre a origem do dinheiro.
- **Integração:** os ativos são incorporados formalmente ao sistema econômico e financeiro. A partir deste momento, o dinheiro recebe aparência lícita.

## **2.2 FINANCIAMENTO AO TERRORISMO**

Financiamento ao terrorismo, disciplinado pela Lei 13.260 de 2016, se constitui através do apoio financeiro, por qualquer meio, ao terrorismo ou àqueles que incentivam, planejam ou cometem atos de terrorismo. O financiamento ao terrorismo tem como objetivo fornecer fundos ou capital para atividades terroristas. Essa arrecadação de fundos ou capital pode acontecer de diversas formas, entre elas de fontes legais, tais como contribuições associativas, doações ou lucros de atividades comerciais diversas bem como a partir de fontes criminosas como o tráfico de drogas, o contrabando de armas, prostituição, bens e serviços tomados indevidamente à base da força, crime organizado, fraude, sequestro, extorsão etc.

Consistem atos terroristas (i) usar ou ameaçar usar, transportar, guardar, portar ou trazer consigo explosivos, gases tóxicos, venenos, conteúdos biológicos, químicos, nucleares ou outros meios capazes de causar danos ou promover destruição em massa, (ii) sabotar o funcionamento ou apoderar-se, com violência, grave ameaça a pessoa ou servindo-se de mecanismos cibernéticos, do controle total ou parcial, ainda que de modo temporário, de meio de comunicação ou de transporte, de portos, aeroportos, estações ferroviárias ou rodoviárias, hospitais, casas de saúde, escolas, estádios esportivos, instalações públicas ou locais onde funcionem serviços públicos essenciais, instalações de geração ou transmissão de energia, instalações militares, instalações de exploração, refino e processamento de petróleo e gás e instituições bancárias e sua rede de atendimento, (iii) atentar contra a vida ou a integridade física de pessoa.

A luta contra o financiamento ao terrorismo está intimamente ligada com o combate à lavagem de dinheiro, já que as técnicas utilizadas para lavar o dinheiro são essencialmente as mesmas utilizadas para ocultar a origem e o destino final do financiamento terrorista, para que assim as fontes continuem a enviar dinheiro sem serem identificadas.

## **2.3 CONSELHO DE CONTROLE DE ATIVIDADES FINANCEIRAS (COAF)**

O Conselho de Controle de Atividades Financeiras (COAF), também instituído pela Lei 9.613/98, é um órgão ligado ao Banco Central do Brasil, que tem por finalidade auditoria e aplicação de penas administrativas relativas ao crime de Lavagem de Dinheiro.

O COAF, juntamente com o Banco Central, Polícia Federal, Corregedoria Geral da União e Ministério Público mantém engajamento e comunicação conjunta e complementar no combate contra os crimes de lavagem de dinheiro e ao financiamento ao terrorismo.

## **2.4 ESTRATÉGIA NACIONAL DE COMBATE À CORRUPÇÃO E À LAVAGEM DE DINHEIRO (ENCCLA)**

A ENCCLA foi instituída através da união dos poderes Executivo, Legislativo, Judiciário, Ministério Público e associações que atuam direta ou indiretamente na prevenção e combate à lavagem de dinheiro.

## **2.5 GRUPO DE AÇÃO FINANCEIRA (GAFI)**

O GAFI é uma entidade que define padrões e políticas com a finalidade de promover implementação de medidas legais, regulatórias e operacionais para combater a lavagem de dinheiro, o financiamento do terrorismo e o financiamento da proliferação, além de outras ameaças à integridade do sistema financeiro internacional relacionadas a esses crimes.

## **3. DIRETRIZES**

São princípios básicos esperados dos colaboradores da Kredit Bank:

- Usar os meios necessários e possíveis para realizar a verificação de identidade de todos os clientes que possuam relação com a Instituição Kredit Bank;
- 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 ao terrorismo, não realizar qualquer tipo de negócio e comunicar imediatamente a área de Controles Internos & Compliance;
- Havendo conhecimento de qualquer transação suspeita de um mesmo cliente que tenham sido propositadamente divididas, independentemente do valor, com objetivo não serem identificadas, comunicar imediatamente a área de Controles Internos & Compliance;
- 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 Controles Internos & Compliance;
- 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 Controles Internos & Compliance, 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 de Controles Internos & Compliance;
- 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 ao Terrorismo;
- Consultar um superior hierárquico em casos de dúvidas ou solicitar auxílio do departamento responsável quando da suspeita, dúvida ou desconfiança de atitudes de clientes, funcionários ou fornecedores.

Todos os colaborador e parceiros da empresa que violarem, mesmo que parcialmente, a regulamentação interna ou externa aplicável à prevenção e combate à lavagem de dinheiro e ao financiamento ao terrorismo, estarão sujeitos às sanções disciplinares cabíveis. Caso algum colaborador ou parceiro viole intencionalmente uma destas leis ou regulamentos, o fato será imediatamente notificado às autoridades competentes.

### **3.1 GESTORES E LÍDERES DE EQUIPES**

Cabe aos gestores e líderes da Kredit Bank aplicar seus melhores esforços quanto à disseminação dos conceitos deste documento aos seus respectivos colaboradores em suas atividades diárias, bem como verificar o cumprimento da mesma, 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 conduta ética, 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 Bank, 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.

### **3.2 ÁREA DE CONTROLES INTERNOS E COMPLIANCE**

Os colaboradores da área de Controles Internos & Compliance são os principais responsáveis pelo adequado funcionamento do processo de Prevenção e Combate à Lavagem de Dinheiro e ao Financiamento ao 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 ao 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 ao 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 ao 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. O sistema é atualizado em tempo real pelo autorizados. Todas as transações com valor maior de R\$15.000,00 são validas com o cliente, caso o cliente não reconheça, é feito o bloqueio imediato da conta.



- 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 cinco anos registro dos Relatórios de Transações Suspeitas;
- Informar sem demora os casos suspeitos de lavagem de dinheiro ou financiamento ao 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 ao terrorismo.

### 3.3 DIRETOR RESPONSÁVEL PELO COMPLIANCE

Patrocinador Executivo do processo de Prevenção e Combate à Lavagem de Dinheiro e ao Financiamento ao 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 ao 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 ao terrorismo, cumprir as determinações dos órgãos reguladores bem como aprovar a Política Interna que dispõe sobre esse assunto. O diretor é responsável por auditar, quinzenalmente, todos os relatórios e informações coletadas pela área de Controle Interno e Compliance e remeter ao COAF (SisCoaf), ou instituição transmissora e responsável, para análise sistêmica que distribuirá aos analistas competentes para as devidas comunicações e intercâmbios de informações.



### **3.4 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 ao terrorismo na empresa, bem como por divulgar a importância de seus conceitos a todos os seus subordinados.

### **3.5 RECURSOS HUMANOS**

A área de Recursos Humanos é responsável pelo suporte ao processo de prevenção e combate à lavagem de dinheiro e ao financiamento ao 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.

### **3.6 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 (Banco Central do Brasil), 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 à lavagem de dinheiro e ao financiamento ao terrorismo e suas principais atribuições podem ser verificadas no processo específico de cadastro.

### **3.7 FRONT- OFFICE (ATENDIMENTO, SUPORTE, CONSULTORES COMERCIAIS)**

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 ao 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.

### **3.8 AUDITORIA INTERNA (PRÓPRIA 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.

### **3.9 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 ao terrorismo.

### **3.10 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 BANK, será realizada análise e avaliação prévia acerca dos riscos operacionais e de fornecimento que possam contribuir com a lavagem de dinheiro e financiamento ao 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.

## **4. RECOMENDAÇÕES GERAIS A TODOS OS COLABORADORES DA EMPRESA**

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 ao 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 Controles Internos & Compliance 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.

## 5. CUSTOMER DUE DILIGENCE

O Customer Due Dilligence é uma pesquisa mais detalhada de diversas informações relacionadas aos clientes que demandam atenção diferenciada, quer seja pelas características do cliente, segmento de atuação, endereço residencial ou comercial, rede de relacionamentos, comunicação por colaboradores, órgãos reguladores ou pessoal externo, suspeitas de transações irregulares, informações na mídia ou qualquer outro motivo que justifique tal pesquisa. Por se tratar de um procedimento específico, com pesquisas criteriosas, inclusive sobre o país de origem do cliente e se o próprio cliente consta em alguma lista específicas de entidades competentes na prevenção e combate à lavagem de dinheiro e ao financiamento de terrorismo (COAF, GAFI, ONU e Transparência Internacional em relação ao país; e FBI e INTERPOL em relação ao cliente; mídia negativa) que demandam sigilo de informações e, principalmente, por se tratar e um procedimento confidencial e de conhecimento restrito às áreas de Cadastro e Controles Internos & Compliance, o conteúdo do procedimento adotado não é publicado neste ou em outro documento de acesso corporativo. Toda e qualquer comunicação aos órgãos reguladores competentes deve ser precedida do Customer Due Dilligence do cliente envolvido.

## 6. CATEGORIZAÇÃO DE RISCO DE CLIENTES



### 6.1 IDENTIFICAÇÃO DE CLIENTE

Verificação da identidade de um cliente através de documentos, para estabelecer se o cliente é quem ele diz ser. A prática de KYC é um elemento importante na luta contra a criminalidade financeira e lavagem de dinheiro, e com uma identificação do cliente mais minuciosa, o desempenho nas outras fases do processo será muito mais tranquilo, usando como base a régua de risco.

### 6.1.1 IDENTIFICAÇÃO SIMPLES

No caso de clientes que representem baixo risco a organização, como clientes Super Simples os passos que devem ser seguidos são:

<b>CLIENTES BAIXO RISCO</b>
<b>PASSO 1:</b> Verificar, através de documento oficial, a identidade do cliente (selfie com documento e apresentação).
<b>PASSO 2:</b> Validar contatos de email e telefone, deixando o cliente ciente que o contato principal se dará por meio destes.
<b>PASSO 3:</b> Realizar análise do comprovante de residência ou termo de Declaração de Residência e Domicílio.
<b>PASSO 4:</b> Conferência dos dados coletados com banco de dados.
<b>PASSO 5:</b> Acompanhamento de transações via BI (business intelligence) com notificação de risco em caso de transação atípica e comunicação via suporte.

### 6.1.2 IDENTIFICAÇÃO JUNTO AO CLIENTE

No caso de clientes que representem médio risco a organização, como clientes Silver os passos que devem ser seguidos são:

<b>CLIENTES MÉDIO RISCO</b>
<b>PASSO 1:</b> Verificar, através de documento oficial, a identidade do cliente (selfie com documento e apresentação).
<b>PASSO 2:</b> Validar contatos de email e telefone, deixando o cliente ciente que o contato principal se dará por meio destes.
<b>PASSO 3:</b> Realizar análise do comprovante de residência ou termo de Declaração de Residência e Domicílio.
<b>PASSO 4:</b> Conferência dos dados coletados com banco de dados.
<b>PASSO 5:</b> Solicitar certidão de casamento.
<b>PASSO 6:</b> Conferir última declaração de Imposto de Renda.
<b>PASSO 7:</b> Acompanhamento de transações via BI (business intelligence) com notificação de risco em caso de transação atípica e comunicação via suporte.

### 6.1.3 IDENTIFICAÇÃO APRIMORADA

No caso de clientes que representem alto risco a organização, como clientes Gold, Premium, Flex, Class e Empresarial os passos que devem ser seguidos são:

<b>CLIENTES ALTO RISCO – PESSOA FÍSICA</b>
<b>PASSO 1:</b> Verificar, através de documento oficial, a identidade do cliente (selfie com documento e apresentação).
<b>PASSO 2:</b> Validar contatos de email e telefone, deixando o cliente ciente que o contato principal se dará por meio destes.
<b>PASSO 3:</b> Realizar análise do comprovante de residência ou termo de Declaração de Residência e Domicílio.
<b>PASSO 4:</b> Conferência dos dados coletados com banco de dados.
<b>PASSO 5:</b> Solicitar certidão de casamento.
<b>PASSO 6:</b> Conferir última declaração de Imposto de Renda.
<b>PASSO 7:</b> Cadastrar e validar e-mail para acesso à Plataforma.
<b>PASSO 8:</b> Solicitar ao cliente pró-labore/ comprovante de renda.
<b>PASSO 9:</b> Conferir os dados, de forma comparativa, com os bancos de dados contratados e públicos.
<b>PASSO 10:</b> Acompanhamento de transações via BI (business intelligence) com notificação de risco em caso de transação atípica e comunicação via suporte.

<b>CLIENTES ALTO RISCO – PESSOA JURÍDICA</b>
<b>PASSO 1:</b> Coletar cartão CNPJ, contrato social, atos constitutivos e certidão simplificada da Junta Comercial;
<b>PASSO 2:</b> Solicitar balanço patrimonial ou documento de declaração do faturamento da empresa;
<b>PASSO 3:</b> Verificar, através de documento oficial, a identidade dos sócios (selfie com documento e apresentação).
<b>PASSO 4:</b> Validar contatos de email e telefone, deixando o cliente ciente que o contato principal se dará por meio destes.
<b>PASSO 5:</b> Realizar análise do comprovante de residência ou termo de Declaração de Residência e Domicílio dos sócios e sede da empresa.
<b>PASSO 6:</b> Solicitar certidão de casamento dos socios, se houver.
<b>PASSO 7:</b> Conferir última declaração de Imposto de Renda.
<b>PASSO 8:</b> Cadastrar e validar e-mail para acesso à Plataforma.
<b>PASSO 9:</b> Solicitar ao cliente pró-labore/ comprovante de renda.
<b>PASSO 10:</b> Conferir os dados de forma comparativa com os bancos de dados contratados e públicos.
<b>PASSO 11:</b> Remeter dados ao jurídico para conferência, caso haja demanda judicial envolvida.
<b>PASSO 12:</b> Acompanhamento de transações via BI (business intelligence) com notificação de risco em caso de transação atípica e comunicação via suporte.

## **7. POLÍTICA CONHEÇA SEU FUNCIONÁRIO – KNOW YOUR EMPLOYEE**

É bastante razoável supor que os controles de prevenção só possam funcionar adequadamente numa instituição financeira se todos os funcionários estiverem conscientes da importância e de como devem ser operacionalizados. Para isso, é fundamental que todos conheçam a política institucional, as normas externas e as normas internas existentes, bem como os demais Controles de Prevenção à Lavagem de Dinheiro e ao Financiamento ao Terrorismo implementados pela instituição. Os procedimentos “conheça-seu-funcionário” (Know Your Employee - KYE) são rotinas de trabalho, incluindo as respectivas ferramentas necessárias à sua execução, que visam propiciar à instituição um adequado conhecimento sobre seus funcionários. Geralmente as instituições financeiras procuram conhecer seus funcionários em virtude do receio de fraudes contra a instituição. As fraudes, além de trazerem um prejuízo imediato em função dos recursos desviados, podem trazer sérios danos à reputação da instituição. No entanto, o conhecimento do funcionário é importante também para a Prevenção à Lavagem de Dinheiro e ao Financiamento ao Terrorismo. Uma vez que os lavadores estão dispostos a arcar com custos significativos para lavar seus recursos, é de se esperar que eles tentem corromper os funcionários da instituição, como forma de obter auxílio para burlar os controles. A política conheça seu funcionário, estabelecida pela Kredit Bank, se baseia em dois elementos distintos:

- a) Procedimentos de contratação de funcionários;
- b) Procedimentos de monitoramento de funcionários.

Os procedimentos de contratação de funcionários foram estabelecidos em conjunto pela área de Controles Internos & Compliance e Recursos Humanos. Para toda e qualquer contratação deverá ser seguido procedimento de análise e coleta de documentação, sendo que, para certas áreas ou processos de atuação, consideradas como de maior vulnerabilidade, deverão ser efetuadas análises mais detalhadas do profissional a ser contratado. As análises, bem como seus resultados devem ficar sob a responsabilidade da área de Controles Internos & Compliance e deverão ser mantidos sob confidencialidade. Dessa forma, os documentos requeridos para a contratação do funcionário, tanto a coleta quanto a guarda, ficam a cargo da área de Recursos Humanos e a pesquisa de informações disponíveis no mercado fica sob a responsabilidade da área de Controles Internos & Compliance.

Como principais procedimentos, a política Conheça seu Funcionário, foca sua atuação nos seguintes aspectos:

- Foco não apenas na identificação de fraudes, mas também de convivência com a prática de crimes;
- Alteração inusitada nos padrões de vida e comportamento do empregado;
- Atenção especial com profissionais envolvidos em processos mais vulneráveis;
- Modificação inusitada do resultado operacional do empregado.

## **8. PESSOAS EXPOSTAS POLITICAMENTE – PEP**

### **8.1 CONCEITO**

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.

São também consideradas expostas politicamente as pessoas que, no exterior, sejam:

- I. Chefes de estado ou de governo;
- II. Políticos de escalões superiores;
- III. Ocupantes de cargos governamentais de escalões superiores;
- IV. Oficiais-generais e membros de escalões superiores do Poder Judiciário;
- V. Executivos de escalões superiores de empresas públicas; ou;
- VI. Dirigentes de partidos políticos.

Edição 2ª	Atualizado em 22/02/2023	<b>KREDIT BANK INSTITUICAO DE PAGAMENTOS S/A</b> <b>CNPJ: 34.678.263/0001-76</b>	Página 15 de 20
-----------	-----------------------------	-------------------------------------------------------------------------------------	-----------------

São também consideradas pessoas expostas politicamente os dirigentes de escalões superiores de entidades de direito internacional público ou privado.

No caso de clientes estrangeiros, devem ser adotadas as seguintes providências:

- I. Solicitar declaração expressa do cliente a respeito da sua classificação;
- II. Recorrer a informações publicamente disponíveis;
- III. Consultar bases de dados comerciais sobre PEP; e
- IV. 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.

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.

## **8.2 IDENTIFICAÇÃO**

A identificação de clientes Pessoa Exposta Politicamente na Kredit Bank 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.



Mesmo com a definição do conceito de PEP e a solicitação de identificação no momento do cadastro, clientes nessa condição podem passar despercebidos ou não se identificar como tal, para esses casos a Kredit Bank adota outros controles de identificação, a saber:

- a) Como passo obrigatório no procedimento de cadastramento de clientes é prevista consulta à base do ZAIG, 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 Auto Declaração como Pessoa Exposta Politicamente ou cancelada sua proposta;
- b) Em decorrência dos bancos de dados serem automatizados, 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 é confrontada com lista atualizada adquirida do ZAIG e SERASA e, identificado clientes na condição de PEP é solicitado ao mesmo que preencha e assine termo específico.

### **8.3 APROVAÇÃO DE CADASTRO E CLIENT DUE DILIGENCE PARA PEP**

Toda documentação cadastral de cliente Pessoa Exposta Politicamente deve ser aprovada por um diretor 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 Client Due Dilligence conforme descrito anteriormente neste documento.

### **8.4 MEDIDAS PARA DETERMINAR A ORIGEM DO PATRIMÔNIO E DILIGÊNCIA NAS OPERAÇÕES**

A tesouraria da instituição deverá informar a área de Controles Internos & Compliance toda vez que clientes PEP efetuarem movimentação financeira em suas contas na instituição. Caberá ao Compliance da instituição verificar a compatibilidade dos recursos envolvidos na transação, com a situação financeira patrimonial do cliente, bem como com a posição que o cliente PEP ocupa. Identificadas divergências ou discrepâncias de valores a área de Controles Internos & Compliance estará apta a tomar as ações necessárias.

Edição 2ª	Atualizado em 22/02/2023	<b>KREDIT BANK INSTITUICAO DE PAGAMENTOS S/A</b> <b>CNPJ: 34.678.263/0001-76</b>	Página 17 de 20
-----------	-----------------------------	-------------------------------------------------------------------------------------	-----------------

Ao efetuar operações para personalidades relacionadas à política, os colaboradores deverão estar atentos a qualquer indício, mesmo que potencial, de lavagem de dinheiro ou de financiamento ao terrorismo. A lista que segue abaixo não esgota todas as possibilidades, mas ilustra transações questionáveis ou suspeitas que, muitas vezes, ensejam maiores cuidados:

- Solicitação por um cliente PEP de associar alguma forma de sigilo com uma transação como, por exemplo, registrar a transação em nome de outra pessoa ou de uma empresa cujo favorecido não tenha sua identidade revelada;
- Direcionamento de transações envolvendo um cliente PEP por meio de várias jurisdições e/ou instituições financeiras, sem propósito evidente, exceto o de ocultar a natureza, fonte, detenção ou controle dos fundos;
- Rápido aumento ou redução dos recursos ou valor dos ativos na conta de uma personalidade política, que não seja atribuível a flutuações no valor de mercado dos instrumentos de investimento detidos na conta;
- Uso frequente ou excessivo de transferências de fundos ou transferências eletrônicas para a conta de um cliente PEP ou originando-se dela;
- Depósitos ou retiradas de alto valor que não sejam condizentes e proporcionais ao tipo de conta e patrimônio legítimo ou atividades do cliente PEP;
- Existência de um modelo segundo o qual, depois que um depósito ou transferência eletrônica é recebido pela conta de um cliente PEP, os fundos são rapidamente transferidos no mesmo valor para outra instituição financeira, especialmente se a transferência for efetuada para uma conta em uma instituição financeira offshore ou uma conta em "jurisdição sigilosa".

### **8.5 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 auto declaração do cliente.

## **9. COMUNICAÇÃO DE INDÍCIOS AOS ORGÃOS COMPETENTES**

Com base nos relatórios de análise mencionados no item 15 deste manual e nos demais controles definidos pela Kredit Bank para a identificação de suspeitas de crime de lavagem de dinheiro ou de financiamento ao terrorismo, a área de Controles Internos & Compliance, 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 diretor responsável pelo compliance, que deve confirmar a suspeita após análise e assinar a carta de comunicação aos órgãos reguladores. Kredit Bank se compromete a priorizar a comunicação de suspeita de crime de lavagem de dinheiro e de financiamento ao terrorismo aos órgãos reguladores, encaminhando a documentação comprobatória imediatamente após sua identificação.

As comunicações acima citadas serão efetivadas com a utilização, no que couber, de meio magnético dentre outros materiais e registros comprobatórios, havendo a postura de manter a informação em estrito sigilo, inclusive não sendo efetuada comunicação ou ciência de tais atos aos respectivos clientes.

## **10. 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 Bank, 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.

## **11. DISSEMINAÇÃO, QUALIFICAÇÃO, TREINAMENTO E ADERÊNCIA DOS PROFISSIONAIS**

A Kredit Bank 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 ao terrorismo. A eficácia do Programa de Treinamento relacionado à prevenção e combate à lavagem de dinheiro e ao financiamento ao terrorismo está condicionada à disciplina dos elementos relacionados a seguir:

- Todos os colaboradores da Instituição, inclusive sua Diretoria, especialmente aqueles que tenham contato com clientes ou que examinam as atividades de transação financeira ou operações devem receber treinamento adequado;
- O treinamento deve ser contínuo, incorporando eventos atuais e mudanças nas leis e regulamentos sobre a prevenção e combate à lavagem de dinheiro e ao financiamento ao terrorismo. O treinamento deve abranger esquemas de lavagem de dinheiro novos e diferentes, envolvendo clientes e instituições financeiras, bem como as instruções sobre como tais atividades poderiam ser detectadas e respectivas responsabilidades dos colaboradores;
- O treinamento se concentra nas consequências do descumprimento por parte de um colaborador da política e procedimentos estabelecidos (multa, suspensão ou encerramento do contrato de trabalho). Os programas deverão oferecer aos colaboradores instrução e orientação quanto às políticas da Instituição e recursos disponíveis;
- O programa de treinamento deve prever a guarda de registros de qualificação e cronogramas de atualização.

## **12. CONSIDERAÇÕES FINAIS**

O programa de treinamento consiste na leitura e ciência do Manual e do Procedimento de Prevenção e Combate à Lavagem de Dinheiro e ao Financiamento ao Terrorismo e no treinamento presencial e/ou E- Learning com duração mínima de uma hora e trinta minutos. Caso seja identificada a necessidade de novas formas de treinamento, seja pela função determinada para o profissional, pela distância que o profissional trabalha da sede ou qualquer outro motivo justificado a Área de Controles Internos & Compliance da Kredit Bank providenciará o desenvolvimento dos treinamentos ou contratação de serviço especializado. O treinamento presencial e/ou E- Learning será realizado a cada dois anos a todos os colaboradores da instituição, portanto, novos profissionais poderão ficar sem o treinamento presencial durante este período. Entretanto, a Instituição exige que no momento da contratação todo novo colaborador realize um treinamento E-Learning. Não obstante, o novo profissional deve ler com atenção o documento Manual de Prevenção e Combate à lavagem de Dinheiro e ao Financiamento ao Terrorismo, dando ciência de sua leitura por meio de termo específico.

Para aprovação e atestar o conhecimento, os colaboradores devem realizar prova com no mínimo de acerto de 70% (setenta por cento), caso contrário será exigido uma nova realização do treinamento. A área de Compliance da instituição possui por responsabilidade a manutenção dos registros de todos os colaboradores que receberam treinamento de prevenção e combate à lavagem de dinheiro e ao financiamento ao terrorismo, garantindo assim, que todos cumpram o requisito de treinamento obrigatório.

Os profissionais de Compliance deverão, como forma de aquisição de novos conhecimentos, participar de congressos e treinamentos externos direcionados para o tema e multiplicar o conteúdo as informações para os demais profissionais da instituição.

Edição 2ª	Atualizado em 22/02/2023	<b>KREDIT BANK INSTITUICAO DE PAGAMENTOS S/A</b> <b>CNPJ: 34.678.263/0001-76</b>	Página 20 de 20
-----------	-----------------------------	-------------------------------------------------------------------------------------	-----------------