

# Política de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo

## Política de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo

### HISTÓRICO DAS ALTERAÇÕES E REVISÕES

#### Elaboração

Data	Versão	Responsável
18/11/2019	000	Volnei Hillebrand - Área de Gestão de Riscos e Compliance

#### Revisão

Data	Versão	Responsável
18/05/2021	001	Sabrina Callegaro – Sconsulting Volnei Hillebrand - Área de Gestão de Riscos e Compliance
<b>Alteração</b> Revisão Geral		
Data	Versão	Responsável
11/04/2021	002	Deise Steffens - Área de Gestão de Riscos e Compliance Volnei Hillebrand - Área de Gestão de Riscos e Compliance
<b>Alteração</b> Atualização item 12. Avaliação da Efetividade		

#### DOCUMENTO DE ACESSO INSTITUCIONAL

Esta Política foi elaborada pela VIACERTA Banking, com finalidade única de ser meramente informativa. É proibida sua reprodução total ou parcial, de qualquer forma ou por qualquer meio.

# Política de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo

## SUMÁRIO

1.	ABRANGÊNCIA.....	5
2.	OBJETIVO.....	5
3.	DEFINIÇÕES .....	5
3.1	Coaf Conselho de Controle das Atividades Financeiras .....	5
3.2	Lavagem de Dinheiro.....	5
3.3	Financiamento ao Terrorismo.....	5
3.4	Cliente Permanente .....	6
4.	REGULAMENTAÇÃO .....	6
4.1	Externa .....	6
4.2	Interna .....	7
5.	RESPONSABILIDADES E ATRIBUIÇÕES .....	7
5.1	Diretoria .....	8
5.2	Diretor Responsável por PLD/FT .....	8
5.3	Auditoria Interna.....	8
5.4	Área de Análise de Crédito.....	8
5.5	Área de Fraudes de Crédito e Cobrança.....	9
5.6	Área de Gestão de Riscos e Compliance .....	9
5.7	Recursos Humanos.....	10
5.8	Tecnologia da Informação.....	10
5.9	Colaboradores .....	10
6.	ESTRUTURA RESPONSÁVEL .....	10
7.	DIRETRIZES .....	10
8.	PROCEDIMENTOS APLICÁVEIS.....	11
8.1	Conheça seu cliente (Know your client – KYC).....	11
8.1.1	Cadastro .....	12
8.1.2	Atualização Cadastral .....	12
8.2	Avaliação Interna de Riscos.....	12
8.3	Processo de Diligência Reforçada – Pessoas com Monitoramento Especial (PME)....	12
8.4	Pessoas Politicamente Expostas (PEPs).....	13
8.5	Conheça seu Funcionário (Know your employee – KYE).....	13
8.6	Conheça seu parceiro (Know your partner – KYP) .....	13

## Política de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo

8.7	Lançamento de Novos Produtos e Serviços .....	14
9.	OPERAÇÕES MONITORADAS .....	14
9.1	Dossiê de Operações Atípicas ou Suspeitas .....	15
9.1.1	Guarda dos Históricos de Dossiês .....	15
10.	SISTEMA DE MONITORAMENTO .....	16
11.	TRATAMENTO DAS OCORRÊNCIAS E COMUNICAÇÃO AOS ÓRGÃOS COMPETENTES .....	16
12.	AVALIAÇÃO DA EFETIVIDADE .....	18
13.	ASPECTOS OPERACIONAIS CSNU (CONSELHO DE SEGURANÇA DAS NAÇÕES UNIDAS) .....	18
14.	TREINAMENTO .....	19
15.	MANUTENÇÃO DE INFORMAÇÕES E REGISTROS .....	19
15.1	Ciência dos Colaboradores .....	19
15.2	Atualização da Política .....	19
15.3	Da Divulgação da Política de PLD/CFT .....	19
15.4	Infrações .....	20

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

### **1. ABRANGÊNCIA**

A presente Política dispõe sobre as normas e procedimentos a serem observados pela VIACERTA Banking, no que tange a atuação de todos os colaboradores e prestadores de serviços no Programa de Prevenção e Combate à Lavagem de Dinheiro e Ocultação de Bens, Direitos e Valores, e de Prevenção do Sistema Financeiro e financiamento do terrorismo para os ilícitos de que trata a Lei nº 9.613/1998 e demais normativos sobre o tema. É de responsabilidade de todos conhecer e cumprir todas as obrigações decorrentes da presente Política e regulamentações vigentes, bem como observar os mais altos padrões de conduta profissional ao conduzir suas atividades.

### **2. OBJETIVO**

Esta Política tem como objetivo estabelecer as orientações e procedimentos que devem ser adotados pela VIACERTA Banking na prevenção e combate dos crimes de lavagem de dinheiro e financiamento ao terrorismo.

### **3. DEFINIÇÕES**

#### **3.1 Coaf Conselho de Controle das Atividades Financeiras**

Trata-se de um Órgão Federal que atua em todo o território nacional na prevenção combate à lavagem de dinheiro e ao financiamento do terrorismo.

#### **3.2 Lavagem de Dinheiro**

Lavagem de Dinheiro é o processo pelo qual recursos originados de atividades ilegais são transformados em ativos de origem aparentemente legal. Essa prática geralmente envolve múltiplas transações, usadas para ocultar a origem dos recursos financeiros e permitir que eles sejam utilizados de forma a aparentar ter origem lícita. Os responsáveis por esta operação fazem com que os valores obtidos por meio das atividades ilícitas e criminosas (como o tráfico de drogas, corrupção, comércio de armas, prostituição, crimes de colarinho branco, terrorismo, extorsão, fraude fiscal, entre outros) sejam dissimulados ou escondidos, aparecendo como resultado de operações comerciais legais e que possam ser absorvidas pelo sistema financeiro, naturalmente.

#### **3.3 Financiamento ao Terrorismo**

O financiamento ao terrorismo consiste no processo de distribuição dissimulada de recursos a serem utilizados em atividades terroristas. Tais recursos são oriundos, geralmente, das atividades de outras organizações criminosas envolvidas com o tráfico de drogas, armas e munições e com o contrabando, ou podem ser derivados de atividades ilícitas, incluindo doações a instituições de caridade de “fachada”. Os métodos utilizados pelos terroristas para dissimular o vínculo entre eles e as fontes de financiamento são geralmente semelhantes aos utilizados na prática de crime de lavagem de dinheiro. Entretanto, normalmente, os terroristas utilizam recursos obtidos de forma legal, visando reduzir o risco de serem descobertos antes do ato terrorista.

## Política de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo

### 3.4 Cliente Permanente

Para fins da Circular nº 3.978 do Banco Central, a VIACERTA Banking considera todos os seus clientes como “Permanentes”, sendo qualquer pessoa natural ou jurídica com a qual seja mantido relacionamento destinado à prestação de serviço financeiro ou à realização de operação de crédito, que represente um risco maior, indiferente do valor da operação.

## 4. REGULAMENTAÇÃO

### 4.1 Externa

- a) Lei nº 13.974/20: Dispõe sobre o Conselho de Controle de Atividades Financeiras (Coaf), de que trata o art. 14 da Lei nº 9.613, de 3 de março de 1998.
- b) Decreto nº 9.825/19: Regulamenta a Lei nº 13.810, de 8 de março de 2019, para dispor sobre o cumprimento de sanções impostas por resoluções do Conselho de Segurança das Nações Unidas e por designações de seus comitês de sanções, incluída a indisponibilidade de ativos de pessoas naturais e jurídicas e de entidades, e a designação nacional de pessoas investigadas ou acusadas de terrorismo, de seu financiamento ou de atos a ele correlacionados.
- c) Lei nº 13.810/19: Dispõe sobre o cumprimento de sanções impostas por resoluções do Conselho de Segurança das Nações Unidas, incluída a indisponibilidade de ativos de pessoas naturais e jurídicas e de entidades, e a designação nacional de pessoas investigadas ou acusadas de terrorismo, de seu financiamento ou de atos a ele correlacionados; e revoga a Lei nº 13.170, de 16 de outubro de 2015.
- d) Lei nº 13.260/16: Regulamenta o disposto no inciso XLIII do art. 5º da Constituição Federal, disciplinando o terrorismo, tratando de disposições investigatórias e processuais e reformulando o conceito de organização terrorista; e altera as Leis nºs 7.960 de 21 de dezembro de 1989, e 12.850 de 2 de agosto de 2013.
- e) Lei 9.613/98 e alterações (Leis nº 10.467/02, 10.701/03, 12.683/12, 13.506/17, Lei Complementar nº 167/19 e Lei nº 13.974/20): Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras - COAF, e dá outras providências. BACEN Resolução nº 44/20: Estabelece procedimentos para a execução pelas instituições autorizadas a funcionar pelo Banco Central do Brasil das medidas determinadas pela Lei nº 13.810, de 8 de março de 2019, que dispõe sobre o cumprimento de sanções impostas por resoluções do Conselho de Segurança das Nações Unidas, incluída a indisponibilidade de ativos de pessoas naturais e jurídicas e de entidades, e a designação nacional de pessoas investigadas ou acusadas de terrorismo, de seu financiamento ou de atos a ele correlacionados;
- f) BACEN Carta-Circular nº 3.430/10: Esclarece aspectos relacionados à prevenção e combate às atividades relacionadas com os crimes previstos na Lei nº 9.613, de 3 de março de 1998, tratados na Circular nº 3.461, de 24 de julho de 2009 (substituída pela Circular 3.978/20);

## Política de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo

- g) BACEN Circular nº 3.858/17: Regulamenta os parâmetros para a aplicação das penalidades administrativas previstas na Lei nº 9.613, de 3 de março de 1998;
- h) BACEN Circular nº 3.942/19: Estabelece procedimentos para a execução pelas instituições autorizadas a funcionar pelo Banco Central do Brasil das medidas determinadas pela Lei nº 13.810, de 8 de março de 2019, que dispõe sobre o cumprimento de sanções impostas por resoluções do Conselho de Segurança das Nações Unidas, incluída a indisponibilidade de ativos de pessoas naturais e jurídicas e de entidades, e a designação nacional de pessoas investigadas ou acusadas de terrorismo, de seu financiamento ou de atos a ele correlacionados;
- i) BACEN Circular nº 3.978/20: Dispõe sobre a política, os procedimentos e os controles internos a serem adotados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil visando à prevenção da utilização do sistema financeiro para a prática dos crimes de “lavagem” ou ocultação de bens, direitos e valores, de que trata a Lei nº 9.613, de 3 de março de 1998, e de financiamento do terrorismo, previsto na Lei nº 13.260, de 16 de março de 2016;
- j) BACEN Carta Circular 4.001/20: Divulga relação de operações e situações que podem configurar indícios de ocorrência dos crimes de “lavagem” ou ocultação de bens, direitos e valores, de que trata a Lei nº 9.613, de 3 de março de 1998, e de financiamento ao terrorismo, previstos na Lei nº 13.260, de 16 de março de 2016, passíveis de comunicação ao Conselho de Controle de Atividades Financeiras (Coaf);
- k) BACEN Carta Circular 3.342/08: Dispõe sobre a comunicação de movimentações financeiras ligadas ao terrorismo e ao seu financiamento;
- l) BACEN Carta Circular 3.858/17: Dispõe sobre o processo administrativo sancionador na esfera de atuação do Banco Central do Brasil e da Comissão de Valores Mobiliários, e dá outras providências.
- m) Carta Circular nº 3.977, de 30 de setembro de 2019: Dispõe sobre o cumprimento das resoluções impostas pelo Conselho de Segurança das Nações Unidas.

### 4.2 Interna

- a) Manual de Conduta VIACERTA Financiadora;
- b) Política Conheça seu Funcionário;
- c) Política Conheça seu Lojista Parceiro;
- d) Manual Crédito PPE e PLDFT;
- e) Política Geral Crédito.

## 5. RESPONSABILIDADES E ATRIBUIÇÕES

Todos os Colaboradores notadamente dentro de suas correspondentes atividades têm funções e responsabilidade relacionadas ao Programa de PLDFT. As posições adiante apontadas são identificadas como tendo funções e responsabilidade diretas pelo Programa.

## Política de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo

### 5.1 Diretoria

- a) Aprovar a Política de PLD/FT considerando a compatibilidade com as operações executadas, o risco relacionado e a estrutura organizacional;
- b) Indicar o Diretor responsável por PLD/FT;
- c) Assegurar que o programa receba suporte adequado;
- d) Determinar as diretrizes institucionais com base em valores e princípios estabelecidos na presente Política, nas normas de controles internos da Instituição, nas normas emanadas dos órgãos e entidades de regulação e autorregulação, ademais das melhores práticas aplicáveis.

### 5.2 Diretor Responsável por PLD/FT

- a) Garantir a implantação do Programa de PLD/FT;
- b) Propor melhorias na Política e no Programa de PLD/FT;
- c) Avaliar a manutenção do relacionamento com clientes que requeiram especial atenção devido ao nível de risco de PLD/FT;
- d) Orientar os trabalhos da área de Gestão de Riscos;
- e) Vetar operações que possam gerar alto risco de PLD/FT.

### 5.3 Auditoria Interna

Executar o programa de auditoria interna para verificação do cumprimento da legislação vigente no que tange a verificação da efetiva implementação/aplicação dos instrumentos/rotinas destinados à PLD/FT.

### 5.4 Área de Análise de Crédito

Monitorar as situações relacionadas com a identificação e qualificação de clientes e com origem dos recursos suspeitos, conforme disposto na Carta Circular nº 4.001 do BACEN, tais como:

- a) Identificação e comprovação dos dados do cliente de Pessoa Física (nome, profissão, documento de identificação, endereço completo, telefone e fontes de referência, entre outros);
- b) Identificação e registro de sócios, diretores, representantes e beneficiários finais de operações de Pessoa Jurídica, e sua respectiva distribuição percentual (%) dentre à composição de sua estrutura acionária;
- c) Pesquisa sobre as atividades profissionais do cliente conforme diretrizes da Política de Crédito;
- d) Atualização do Cadastro sempre que ocorrer uma nova operação, e/ ou mediante demanda do cliente;
- e) Consultas aos superiores (Gestor, Comitê de Riscos ou Diretoria) quando do surgimento de indício de irregularidade;
- f) Comunicar à área de Gestão de Riscos e Compliance via email, as operações e situações suspeitas identificadas.



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

### **5.5 Área de Fraudes de Crédito e Cobrança**

Monitorar a ocorrência de liquidações de operações suspeitas, conforme definidas na Carta Circular nº 4.001 do BACEN, tais como:

- a) Operações de crédito no País liquidadas com recursos aparentemente incompatíveis com a situação financeira do cliente;
- b) Operações de crédito no País, simultâneas ou consecutivas, liquidadas antecipadamente ou em prazo muito curto;
- c) Operações de crédito no País liquidadas por terceiros sem demonstração da existência de relação familiar ou comercial;
- d) Comunicar à área de Compliance as operações e situações suspeitas identificadas.

### **5.6 Área de Gestão de Riscos e Compliance**

- a) Responsável por gerir e controlar os procedimentos desta Política;
- b) Promover a revisão desta Política, anualmente ou nos casos de inovações legais, regulamentares ou institucionais que venham afetá-la, submetendo-a à aprovação da Diretoria;
- c) Revisar periodicamente esta Política, ou sempre que ocorrerem fatos relevantes;
- d) Coordenar as atividades de monitoramento e identificação de operações e situações suspeitas;
- e) Realizar a análise, registro e decidir pela comunicação e realizar a comunicação ao COAF, quando cabível, das operações e situações suspeitas;
- f) Dar ciência à Diretoria de PLD/FT sobre as comunicações de operações suspeitas e ou atípicas;
- g) Providenciar a divulgação interna de informações e materiais referentes ao assunto PLD/FT;
- h) Controlar, avaliar e identificar a necessidade de realização dos Testes de Verificação Cadastral (Conceitual, Sistêmico e Físico), anuais ou extraordinários e coordenar sua execução;
- i) Coordenar a atualização cadastral;
- j) Monitorar o cumprimento desta Política pelas outras áreas;
- k) Avaliar a criação de novos produtos/ serviços sob a ótica de PLD;
- l) Manter registro de participação e das avaliações formais de todos que realizarem os treinamentos de Prevenção à Lavagem de Dinheiro e Combate ao Financiamento ao Terrorismo, na forma do item 16 desta Política;
- m) Controlar, avaliar e identificar a necessidade de realização dos treinamentos de Prevenção à Lavagem de Dinheiro e Combate ao Financiamento ao Terrorismo, anuais ou extraordinários;
- n) Apoiar o RH na elaboração de programas de treinamentos internos de PLD/FT;
- o) Disseminar a cultura de PLD dentro da Instituição;

## Política de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo

- p) Realizar a avaliação da efetividade desta Política, dos procedimentos e controles internos de PLD/FT.

### 5.7 Recursos Humanos

- a) Manter um controle dos registros funcionais de todos os seus colaboradores (Conheça seu Funcionário), a fim de acompanhar o desempenho funcional, o comportamento e o perfil socioeconômico;
- b) Implementar os programas de treinamento e respectivos registros funcionais.

### 5.8 Tecnologia da Informação

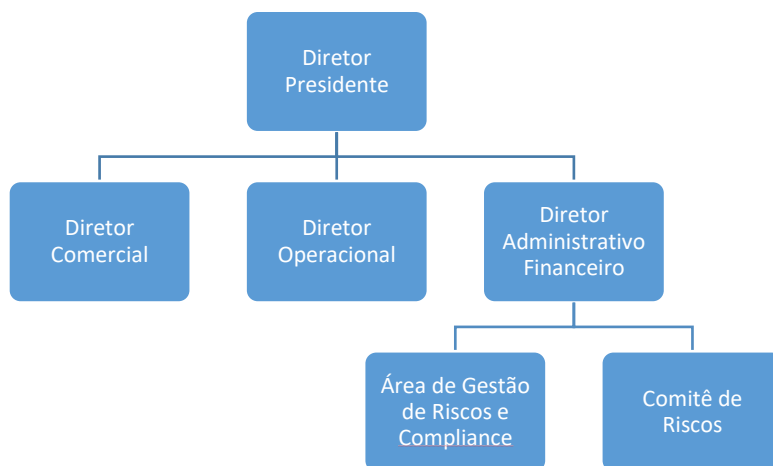
A TI tem papel fundamental para assegurar a integridade, segurança, armazenamento e disponibilidade dos dados e dos sistemas de informação utilizados.

### 5.9 Colaboradores

É dever dos Colaboradores informar e reportar inconsistências em procedimentos e práticas definidas no presente documento, seja para seu superior imediato e/ou para área de Gestão Integrada de Riscos.

## 6. ESTRUTURA RESPONSÁVEL

Objetivando afastar quaisquer possíveis conflito de interesses, a instituição segregou, em seu organograma institucional, área de Compliance, responsável pelas atividades e controles voltados à Prevenção à Lavagem de Dinheiro e Combate ao Financiamento ao Terrorismo, da área comercial, conforme indicado abaixo:



## 7. DIRETRIZES

As Diretrizes desta Política traçadas pela Diretoria estabelecem o compromisso da VIACERTA Banking quanto prevenção a lavagem de dinheiro e financiamento ao terrorismo, tais como:

- a) Manter controles e registros adequados desde o início do relacionamento com o cliente, que permitam identificá-lo adequadamente e verificar a compatibilidade

## Política de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo

- quanto a atividade econômica e a capacidade financeira, conforme determinado pela legislação vigente;
- b) Estabelecer os procedimentos de “Conheça Seu Cliente”, “Conheça Seu Funcionário” e “Conheça seu Parceiro” listados nesta Política;
  - c) Garantir investimento adequado em treinamento dos colaboradores com conteúdo adequado de acordo com as funções desempenhadas;
  - d) Investir em ferramentas de controle e monitoramento, que permitam a detecção de operações atípicas;
  - e) Manter sigilo quanto as situações analisadas sob a ótica de PLD/FT, bem como quanto as comunicações ao COAF;
  - f) Garantir o acesso hábil e irrestrito dos dados cadastrais de clientes, colaboradores e parceiros de negócios aos responsáveis pela análise e monitoramento das operações;
  - g) Garantir autonomia para área de Compliance executar as atividades de PLD/FT e estabelecer o risco das operações;
  - h) Estabelecer que todas as áreas da VIACERTA atendam as demandas da área de Compliance quanto as solicitações referentes a PLD/FT.

### 8. PROCEDIMENTOS APLICÁVEIS

#### 8.1 Conheça seu cliente (Know your client – KYC)

A VIACERTA Banking estabelece, no processo de aceitação do Cliente, não manter vínculo com pessoas que apresentem qualquer indício de relacionamento com atividades de natureza criminosa, especialmente aquelas supostamente vinculadas ao narcotráfico, terrorismo ou crime organizado, que tenham negócios cuja natureza impossibilite a verificação da legitimidade das atividades ou da procedência dos recursos movimentados ou recusam-se a fornecer informações ou documentos solicitados.

Conhecer o próprio cliente é um elemento crítico na administração de riscos, e a adequação de uma Política a respeito auxilia a proteger a reputação e a integridade das instituições e do mercado financeiro, sendo essencial que os Colaboradores da VIACERTA Banking envolvidos nas operações de Análises de Crédito obtenham conhecimento suficiente sobre os clientes, de forma a garantir a negociação transparente com pessoas físicas, jurídicas e quaisquer outras instituições de caráter idôneo, financeiras ou não financeiras.

Em conformidade com as boas práticas de mercado, e em atendimento aos regulamentos internos do mercado financeiro, a Instituição realiza diversos procedimentos relacionados ao processo de KYC, que contempla procedimentos e políticas internas relacionadas à aceitação e cadastramento de clientes que são praticados por todas as áreas geradoras de riscos da VIACERTA Banking. A seguir são descritos os procedimentos aplicados.

Antes de iniciar suas operações com a VIACERTA Banking, o Cliente deverá fornecer todas as informações cadastrais solicitadas, como:

## Política de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo

### 8.1.1 Cadastro

A aprovação do cadastro do cliente ocorre apenas mediante a checagem e validação dos dados relacionados abaixo, de forma eletrônica (sistemas customizados, birôs com fontes de enriquecimento) e manual (analistas de crédito validam os dados do cadastro e contatam com o cliente via telefone).

- a) Ficha Cadastral;
- b) Cópias de documentos cadastrais comprobatórios, tais quais, mas não se limitando a:
  - Identidade, CPF;
  - Comprovante de Residência;
  - Comprovante de Renda e;
  - Demais documentos pertinentes, a critério da Instituição.

Todos os clientes são submetidos a listas restritivas externas para identificar se são:

- a) Pessoas Politicamente Expostas;
- b) Pessoas ligadas ao Financiamento de Terrorismo e;
- c) Pessoas com objetivo de investir na Instituição com dinheiro ilícito (PLD).

A Auditoria Interna efetua verificações periódicas, por amostragem, para avaliar o cumprimento

As fichas cadastrais dos Clientes ativos devem ser atualizadas em períodos não superiores a 12 (doze) meses.

### 8.1.2 Atualização Cadastral

Atualização do Cadastro ocorre sempre que ocorrer uma nova operação, e/ ou mediante demanda do cliente.

### 8.2 Avaliação Interna de Riscos

A VIACERTA Banking adota um sistema interno para realizar a Classificação de Riscos de seus clientes, parceiros e prestadores de serviços, bem como fazer o monitoramento das operações, avaliando e identificando possíveis operações atípicas.

A Avaliação Interna de Riscos deve ser:

- a) Documentada e aprovada pelo Diretor Responsável por PLD/FT;
- b) Considerar os perfis de riscos estabelecidos na Circular 3.978 do BACEN;
- c) Revisada a cada dois anos ou sempre que ocorrerem alterações relacionadas aos perfis de riscos.

### 8.3 Processo de Diligência Reforçada – Pessoas com Monitoramento Especial (PME)

Os Colaboradores envolvidos nas análises de crédito e responsáveis pela captação de recursos junto a investidores devem dispensar atenção especial em relação aos clientes identificados como de alta sensibilidade, sendo estes classificados como:

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

- a) Pessoas Politicamente Expostas;
- b) Pessoas citadas em veículos de comunicação ou outras mídias por envolvimento em atividades criminais;
- c) Lotéricas, empresas de fomento mercantil, postos de gasolina, agências de turismo, igrejas, templos ou outras entidades religiosas, ONGs;
- d) Clientes que residam ou estejam sediados no exterior, em municípios brasileiros de fronteira e aeroportos.

### **8.4 Pessoas Politicamente Expostas (PEPs)**

São consideradas PEPs aquelas pessoas que desempenham ou tenham desempenhado, nos últimos 5 (cinco) anos, cargos, empregos ou funções públicas relevantes, no Brasil ou em outros países, territórios e dependências estrangeiros, assim como seus representantes, familiares e outras pessoas de relacionamento de primeiro grau.

O cliente, no início do relacionamento ou na atualização cadastral com a VIACERTA Banking, será identificado automaticamente no Fluxo do Cadastro do sistema interno (através de uma fonte enriquecimento externa), detalhando se é um cliente Politicamente Exposto.

No início do relacionamento com o cliente, quando inserida a proposta, são avaliadas automaticamente as Regras para realizar a Classificação de Risco.

Após o início do relacionamento, a cada 30 dias, é feita a reclassificação do Risco de cada cliente.

### **8.5 Conheça seu Funcionário (Know your employee – KYE)**

A VIACERTA Banking adota postura rígida e transparente na contratação de seus colaboradores, antes do ingresso na Instituição, todos os candidatos devem ser entrevistados pelo departamento de Recrutamento (Psicóloga, Gestor e Diretoria- quando aplicável). Requisitos ligados à reputação no mercado e perfil serão avaliados, bem como os antecedentes profissionais e criminais do candidato. Além destes procedimentos, a VIACERTA Banking promove treinamentos periódicos sobre os conceitos de seu Código de Ética e Conduta e da presente Política, possibilitando o conhecimento de seus colaboradores acerca de atividades vedadas e dos princípios da instituição.

### **8.6 Conheça seu parceiro (Know your partner – KYP)**

A VIACERTA Banking busca novas parcerias com lojistas correspondentes idôneos e de boa reputação, com qualificação técnica adequada e que se comprometam expressamente a adotar a mesma política de tolerância zero quanto à corrupção. Para isso, a VIACERTA Banking faz uma análise prévia de antecedentes, qualificações e reputação (Due Diligence) de seus parceiros e prestadores de serviços, buscando afastar quaisquer dúvidas quanto a seus valores éticos, idoneidade, honestidade e reputação, verificando cuidadosamente quaisquer indícios que possam indicar propensão ou tolerância do Terceiro quanto a atos de Lavagem de Dinheiro. Os procedimentos serão proporcionais aos riscos enfrentados pela VIACERTA Banking em cada contratação.

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

O processo de avaliação e contratação de novos parceiros e prestadores de serviço são atividades de suma importância na VIACERTA Banking, tanto para observância de questões regulatórias quanto para mitigação de riscos legais e reputacionais.

A VIACERTA Banking trabalha com parceiros e fornecedores com situação econômico-financeira saudável e que assumem suas responsabilidades legais, regulatórias, trabalhistas, sociais e ambientais, a fim de evitarmos risco de imagem. Novos prestadores de serviço deverão ser avaliados pela área solicitante e encaminhados para o departamento jurídico.

### **8.7 Lançamento de Novos Produtos e Serviços**

Todos os novos produtos e serviços serão analisados pelo Compliance a fim de identificar possíveis exposições a práticas de lavagem de dinheiro.

No estudo para o lançamento de produtos/serviços serão examinados aspectos relativos à:

- a) Natureza do mercado em que estejam inseridos;
- b) Histórico de relacionamento e avaliação do perfil dos clientes potenciais;
- c) Análise de histórico de relacionamento e perfil de parcerias comerciais e correspondentes que operem o produto/serviço;
- d) Estrutura de controles internos associados ao acompanhamento de sua performance, bem como a identificação das estruturas e colaboradores da instituição envolvidos com sua gestão.

Cabe à área de Gestão de Riscos e Compliance, fazer o estudo, e registrar o consentimento no documento, se este estiver de acordo. Quando cadastrar e ou lançar um novo produto, o mesmo só será liberado para lançamento após todas as áreas envolvidas realizarem as devidas análises, cadastramento e parametrização conforme consta no Check List de Novos Produtos e Planos.

### **9. OPERAÇÕES MONITORADAS**

Em conformidade com o estipulado na regulamentação anteriormente citada, é de suma importância que todos os Colaboradores envolvidos nas análises de Crédito e responsáveis pela captação de recursos junto a investidores tenham conhecimento das operações que configuram indícios de lavagem de dinheiro e financiamento ao terrorismo. Em conformidade com a Carta Circular Nº 4.001/20 do Banco Central do Brasil são considerados indícios de operações atípicas (Lavagem de Dinheiro e Financiamento ao Terrorismo) as propostas e operações cujos:

- i. Os valores solicitados ou recursos utilizados para realização da operação é incompatível com a ocupação profissional e situação financeira declarada;
- ii. Operações em que não seja possível identificar o beneficiário final;

## Política de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo

- iii. Situações em que clientes oferecem resistência no fornecimento informações pessoais, quer burlem a identificação dos efetivos envolvidos ou beneficiários;
- iv. Apresentação de diversas contas bancárias ou alteração com frequência das mesmas;
- v. Concessão de garantias por terceiros sem vínculo com o cliente;
- vi. Realização de operações simultâneas ou consecutivas, bem como liquidadas antecipadamente ou em prazo muito curto pelo cliente sem motivo justificado;
- vii. Operações cujas características ou desdobramentos evidenciem a atuação em nome de terceiros;

Sempre que identificada uma possível situação de lavagem de dinheiro (ainda que ainda não realizada pela Instituição), deve-se encaminhar a proposta ou operação para área de Compliance, juntamente com um Dossiê contendo todos os dados necessários para a tomada de decisão pela comunicação, ou não, ao COAF.

Propostas e operações de clientes atípicas, suspeitos de lavagem de dinheiro e financiamento ao terrorismo, NÃO serão levadas a conhecimento de terceiros e ao cliente envolvido.

### 9.1 Dossiê de Operações Atípicas ou Suspeitas

Nas situações em que for identificado algum indício de Operação Atípica ou Suspeita deverá ser formalizado o Dossiê do cliente, contendo de forma detalhada os seguintes dados:

- Número e data de inclusão da proposta;
- Data da efetivação ou reprovação da proposta;
- Nome completo do cliente;
- CPF;
- Endereço Completo;
- Dados profissionais;
- Renda;
- Valor da Operação;
- Finalidade do Valor da Operação;
- Motivo da Comunicação (Enquadramento conforme Carta Circular 4001/20);
- Relato dos dados identificados como divergentes; e
- Decisão da Comunicação (Sim ou Não).

#### 9.1.1 Guarda dos Históricos de Dossiês

A instituição deverá manter, pelo prazo de 05 (cinco) anos, os dossiês e documentos relativos às análises das operações (ou propostas de operações) selecionadas, que fundamentaram a decisão de efetuar ou não as comunicações ao COAF.

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

### **10. SISTEMA DE MONITORAMENTO**

O DTEC-Classificação de Risco (DTEC-CR) é um Sistema desenvolvido pela Softon Sistemas Inteligentes Ltda para classificação de risco em geral, entre eles a classificação do risco de lavagem de dinheiro (CR), reclassificação do risco (Batch) e monitoramento das transações (LD), de forma a atender a Circular 3.978 do BACEN. Seguem os módulos:

#### **1º Módulo: DTEC-CR On-line (Onboarding) - Início do Relacionamento do Cliente com a Instituição**

Neste módulo, ocorre Classificação de Risco (Regras que irão pontuar o CPF do cliente e informar se o cliente é de Risco Baixo, Médio, Alto e Crítico).

#### **2º Módulo: DTEC-CR Batch (Periódico) – Reclassificação de Risco**

Após o início do relacionamento, a cada 30 dias, é feita a reclassificação do Risco de cada cliente, baseado nas Regras de classificação de Risco.

#### **3º Módulo: DTEC-LD – Lavagem de Dinheiro**

Realiza o monitoramento de todas as transações dos clientes, seja cliente Digital ou Operação Normal, avaliando:

- Quitações antecipadas de Contratos.
- Movimentações e ou transações nas contas de pagamento, identificando possíveis movimentações ou operações atípicas, fora da realidade financeira do cliente (gerando alertas através de parametrização sistêmica).
- Gerar relatórios de Comunicações ao UIF (COAF).

### **11. TRATAMENTO DAS OCORRÊNCIAS E COMUNICAÇÃO AOS ÓRGÃOS COMPETENTES**

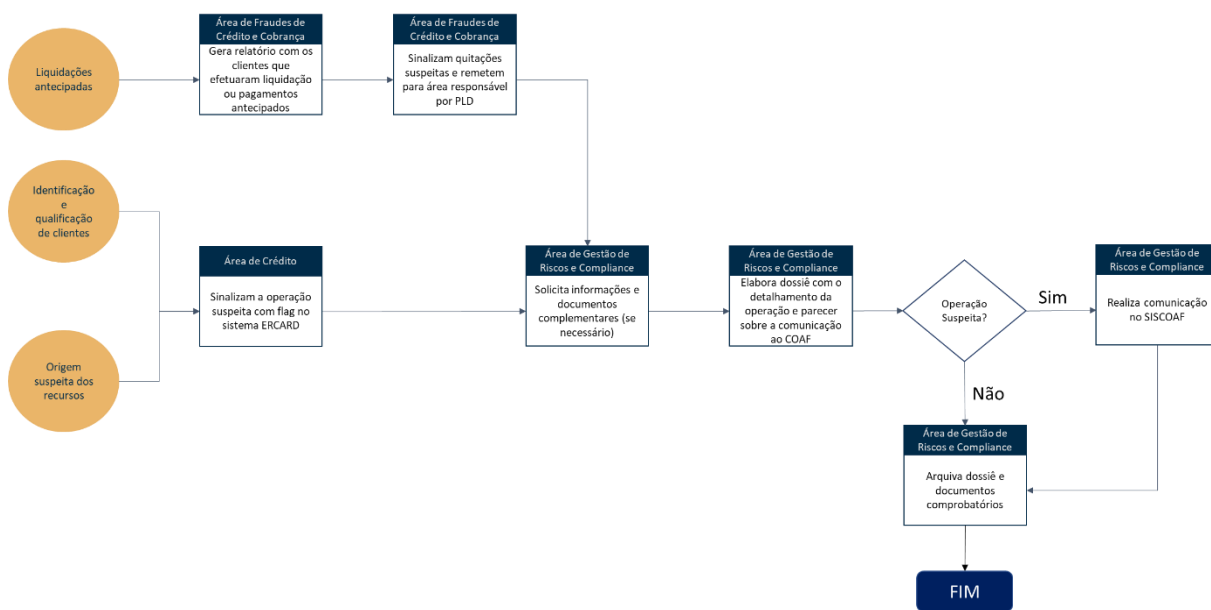
A Área de Gestão de Riscos e Compliance realiza a análise das operações e situações suspeitas, solicitando informações e documentos complementares às demais áreas e diretamente ao cliente, quando necessário.

Na falta de elementos que afastem a suspeita sobre a situação ou operação analisada, documentará a decisão de comunicação ao COAF, esclarecendo seus fundamentos de fato, de direito e econômicos.

Após a formalização da decisão de comunicação, a Área de Gestão de Riscos e Compliance realizará a comunicação no SISCOAF, esclarecendo os fundamentos da decisão de comunicação, acompanhada dos documentos cabíveis. E por fim, elaborará um dossiê com os documentos que embasaram a análise e decisão de comunicação para arquivar na instituição.



## Política de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo



Aquelas operações e situações analisadas pela Área de Gestão de Riscos e Compliance e que tiverem elementos que afastem a suspeita, não serão encaminhados ao Siscoaf e serão encerrados, sendo formalizada a decisão de NÃO comunicação, esclarecendo os fundamentos da referida decisão, acompanhada dos documentos cabíveis, formalizando também um dossiê para arquivar na instituição.

Todas as informações que tratam de indícios / suspeitas de lavagem de dinheiro e combate ao financiamento do terrorismo são de caráter confidencial, não devendo, em hipótese alguma, ser disponibilizadas a terceiros. As comunicações de casos suspeitos que tratam a Circular BACEN 3.978/20 NÃO devem ser levadas ao conhecimento do cliente envolvido, sendo de uso exclusivo dos Órgãos Reguladores para análise e investigação.

As comunicações ao COAF devem conter, dentre outros aspectos:

- a) Informações acerca do cliente e do processo de KYC que permitam identificar o comportamento deste; características da operação suspeita;
- b) Informações acerca da origem e destino dos recursos utilizados na operação, quando possível obtê-las;
- c) Relações da situação reportada com outras operações e movimentações suspeitas do mesmo cliente ou de outros clientes.

As comunicações ao COAF serão realizadas nos termos exigidos pela regulação do Banco Central do Brasil, atualmente em até 24 horas após a identificação da irregularidade. Os casos não considerados como críticos pela área de Gestão de Riscos e Compliance ou quando não confirmados os indícios de crime de lavagem de dinheiro são encerrados com o arquivamento da ocorrência.

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

### **12. AVALIAÇÃO DA EFETIVIDADE**

A Política de PLD/FT deve ser avaliada quanto a sua efetividade em relação aos procedimentos e controles internos.

A referida avaliação deve ser:

- a) Documentada em relatório específico;
- b) Elaborada anualmente, com data-base de 31 de dezembro; e
- c) Encaminhada, para ciência, até 31 de março do ano seguinte ao da data-base, à diretoria.

O relatório específico conterá as seguintes informações:

- a) A metodologia adotada na avaliação de efetividade;
- b) Os testes aplicados;
- c) A qualificação dos avaliadores;
- d) Dos procedimentos destinados a conhecer clientes, incluindo a verificação e a validação das informações dos clientes e a adequação dos dados cadastrais;
- e) Dos procedimentos de monitoramento, seleção, análise e comunicação ao Coaf, incluindo a avaliação de efetividade dos parâmetros de seleção de operações e de situações suspeitas;
- f) Da governança da política de PLD/CFT;
- g) Das medidas de desenvolvimento da cultura organizacional voltadas à prevenção da lavagem de dinheiro e ao financiamento do terrorismo;
- h) Dos programas de capacitação periódica de pessoal;
- i) Dos procedimentos destinados a conhecer os funcionários, parceiros e prestadores de serviços terceirizados;
- j) Das ações de regularização dos apontamentos oriundos da auditoria interna e da supervisão do Banco Central do Brasil.

A avaliação da efetividade deve conter plano de ação para as irregularidades identificadas e deve ser encaminhado para ciência e avaliação da Diretoria e auditoria interna até 30 de junho do ano seguinte ao da data-base.

### **13. ASPECTOS OPERACIONAIS CSNU (CONSELHO DE SEGURANÇA DAS NAÇÕES UNIDAS)**

Entre as diversas ferramentas e fontes de consulta utilizadas para PLD/FT serão também acessadas, por meio do sistema Softon, as informações do Conselho de Segurança das Nações Unidas - CSNU.

Listas restritivas utilizadas:

- a) LISTA – OFAC;
- b) LISTA - OFAC (NON SDN);
- c) LISTA – UN SECURITY COUNCIL SANCTIONS LIST.

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

### **14. TREINAMENTO**

Compete a Área de Gestão de Riscos Compliance da VIACERTA Banking, ao treinamento de seus Colaboradores envolvidos nas análises de Crédito e responsáveis pela captação de recursos junto a investidores de forma a que exerçam suas atividades de acordo com os princípios elementares adiante destacados.

A VIACERTA Banking dispõe de um programa anual de treinamento de Prevenção à Lavagem de Dinheiro, com a finalidade de estabelecer canal informativo aos Colaboradores sobre o tema e sobre a Política de PLD, que deverá ser conferido a todos os Colaboradores (exceto serviços gerais), desta Instituição, bem como dos prestadores de serviços, lojistas parceiros, e membros da Diretoria.

A sua realização é mandatória por parte de toda a Instituição. Deverá ser mantido registro de todos os Colaboradores e Diretores que receberam treinamento do Programa de PLDFT.

### **15. MANUTENÇÃO DE INFORMAÇÕES E REGISTROS**

Os documentos relativos às operações, incluindo as gravações de contato e documentos cadastrais devem ser arquivados pelo período mínimo de 5 (cinco) anos a partir do encerramento da operação realizada pelo cliente. As informações relacionadas a registro do repasse de recursos deverão ser arquivadas pelo prazo mínimo de 5 (cinco) anos.

#### **15.1 Ciência dos Colaboradores**

A Instituição dará ciência aos colaboradores de que poderá monitorar quaisquer atividades por eles desenvolvidas com o intuito de identificar casos suspeitos ou em desconformidade com a presente Política e demais documentos e normas aplicáveis.

#### **15.2 Atualização da Política**

A atualização da presente Política deverá ocorrer sempre que houver alterações substantivas em procedimentos ou regulamentações que afetem o tema, sendo de responsabilidade da área de Gestão de Riscos o acompanhamento das inovações legais e institucionais. Periodicamente, a VIACERTA Banking poderá publicar políticas e normas adicionais, complementares e/ou atualizações, devendo ser conferida a necessária divulgação aos Colaboradores.

#### **15.3 Da Divulgação da Política de PLD/CFT**

Cabe à Área de PLD/CFT dar ampla divulgação da implantação desta Política, bem como dos Manuais de PLD/CFT :

- a. Informativos;
- b. Disponibilização da política Institucional da PLD no site da Instituição;
- c. Divulgação dos Relatórios de Gestão da PLD/CFT;
- e. Treinamentos (treinamentos para colaboradores envolvidos diretamente na operação e colaboradores novos).

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

### **15.4 Infrações**

A infração da presente Política e demais normas dará ensejo à ação disciplinar, devendo a penalidade a ser aplicada observar a gravidade da infração, a hipótese de reincidência, podendo culminar em rescisão por justa causa do contrato de trabalho ou motivada em caso de contrato de outra natureza.