



GREEN NET INSTITUIÇÃO DE PAGAMENTO LTDA.

**POLÍTICA DE PREVENÇÃO À LAVAGEM DE DINHEIRO  
E FINANCIAMENTO AO TERRORISMO**

ESTE DOCUMENTO PODE CONTER INFORMAÇÕES PRIVADAS E NÃO DEVE SER DISTRIBUÍDO SEM  
PRÉVIA AUTORIZAÇÃO.

## Sumário

<b>1. Apresentação</b> .....	4
<b>1.1. Objetivo:</b> .....	4
<b>1.2. Público-alvo:</b> .....	4
<b>1.3. Revisão e Controle da Política</b> .....	4
<b>2. Introdução</b> .....	4
<b>2.1. Conceito de Lavagem de Dinheiro e de Financiamento do Terrorismo</b> .....	5
<b>2.1.1. Fases da Lavagem de Dinheiro</b> .....	5
<b>2.1.2. Financiamento do Terrorismo:</b> .....	6
<b>3. Atribuições e Responsabilidades:</b> .....	6
<b>3.1. Diretoria Executiva:</b> .....	6
<b>3.2. Diretoria Financeira:</b> .....	7
<b>3.4. Compliance/ PLDFT:</b> .....	7
<b>3.5. Recursos Humanos:</b> .....	8
<b>3.6. Gestores e Funcionários:</b> .....	8
<b>3.7. Auditoria Interna:</b> .....	9
<b>4. Programa de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo</b> .....	9
<b>4.1. Políticas e Procedimentos</b> .....	9
<b>4.2. Procedimento de Conheça Seu Cliente – CSC (KYC)</b> .....	9
<b>4.2.1. Identificação do Cliente</b> .....	10
<b>4.2.2. Qualificação do Clientes</b> .....	10
<b>4.2.3. Classificação do Cliente</b> .....	10
<b>4.2.4. Identificação e Qualificação dos Beneficiário Final</b> .....	11
<b>4.2.5. Qualificação como Pessoa Exposta Politicamente – PEP</b> .....	11
<b>4.2.6. Registro de Operações e Guarda de Documentos</b> .....	12
<b>4.3. Monitoramento, Seleção e Análise de Operações e Situações Suspeitas</b> .....	12

<b>4.4. Comunicações de Operações e Situações Suspeitas ao COAF .....</b>	<b>12</b>
<b>4.5. Procedimentos destinados a conhecer o Funcionário (CSF – KYE), parceiros e Prestadores de Serviços Terceirizados (CSP – KYP) .....</b>	<b>13</b>
<b>5. Treinamentos.....</b>	<b>13</b>
<b>6. Auditoria .....</b>	<b>14</b>
<b>7. Avaliação Interna de Risco.....</b>	<b>14</b>
<b>8. Avaliação de Efetividade (do que?) .....</b>	<b>14</b>
<b>9. Avaliação de Novos Produtos e Serviços .....</b>	<b>15</b>
<b>10. Leis e Normativos Relacionados.....</b>	<b>15</b>

## 1. APRESENTAÇÃO

### 1.1. Objetivo:

Esta Política tem como objetivo estabelecer as diretrizes mais importantes para a Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (PLDFT) e minimizar os riscos de utilização indevida dos negócios da GREEN NET INSTITUIÇÃO DE PAGAMENTO LTDA. (GREEN NET), disciplinando a ação gerencial, mantendo a ordem administrativa e fundamentando a eficácia dos processos operacionais, tendo como premissas:

- Orientar e disciplinar ações pessoais ou corporativas de todos os colaboradores, parceiros e prestadores de serviço da Instituição;
- Dotar os Gestores com ferramentas para supervisionar, treinar e avaliar os colaboradores, sempre apoiados nas determinações e orientações das políticas vigentes.

### 1.2. Público-alvo:

Este documento contém informações indispensáveis para todos os funcionários e parceiros da GREEN NET INSTITUIÇÃO DE PAGAMENTO LTDA.

### 1.3. Revisão e Controle da Política

A responsabilidade pela manutenção e atualização desta Política é da Área de Compliance.

Este documento estará disponível na intranet com o título de Política de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo, e o original em meio físico arquivado na Área de Compliance.

## 2. INTRODUÇÃO

Esta Política tem por finalidade reiterar a atenção da Green Net sobre as atribuições e responsabilidades que compartilham seus diretores, funcionários e parceiros, relativos à Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo.

A Lei Federal nº 9.613/98, alterada pela Lei 12.683/2012 e regulamentada pela Circular BACEN nº 3.978/20 e normativos complementares, dispõem sobre os crimes de lavagem ou de ocultação de bens, direitos e valores, e financiamento ao terrorismo, bem como sobre a prevenção da utilização do sistema financeiro contra os ilícitos.

A referida Lei define sanções às pessoas físicas e jurídicas que deixem de cumprir as obrigações previstas, e àquelas que, tendo conhecimento da prática do fato, deixarem de comunicar às autoridades competentes.

A imagem de uma instituição é o seu ativo mais valioso e pode ser seriamente afetada se, de alguma maneira, for envolvida, mesmo que involuntariamente, em operações que impliquem em lavagem de dinheiro e financiamento ao terrorismo (LDFT).

Neste contexto a Green Net, dentro dos seus valores e princípios éticos, repudia a prática do crime de lavagem de dinheiro e o financiamento ao terrorismo e, visando impedir o uso indevido da instituição para fins ilícitos, desenvolveu a presente Política e os necessários procedimentos de prevenção estabelecidos pela Circular BACEN 3.978/20.

## 2.1. Conceito de Lavagem de Dinheiro e de Financiamento do Terrorismo

A Lavagem de Dinheiro (LD) é o processo pelo qual o criminoso transforma recursos oriundos de atividades ilegais em ativos com uma origem aparentemente legal. Essa prática geralmente envolve múltiplas transações usadas para ocultar a origem dos ativos financeiros, e permitir que eles sejam utilizados sem comprometer os criminosos. A dissimulação é, portanto, a base para toda operação de lavagem que envolva dinheiro proveniente de um crime antecedente.

A LD, bem como as atividades criminosas subjacentes (ex.: corrupção, tráfico de narcóticos, organização criminosa, crimes financeiros e de sonegação fiscal etc.), enfraquecem a reputação e a sustentação de qualquer instituição que, frente a acusações de lavagem de dinheiro e financiamento ao terrorismo por promotores, agentes executores legais ou pela imprensa, poderá enfrentar sérios prejuízos à sua reputação e afetar a continuidade de suas operações.

### 2.1.1. Fases da Lavagem de Dinheiro

O processo de lavagem de dinheiro apresenta três fases, cada qual envolvendo a interação com uma instituição:

- a. **Colocação:** nessa fase os criminosos buscam desembaraçar-se do dinheiro em espécie obtido com sua atividade ilícita. Ele é removido para algum lugar (cidade, estado, país etc.) que o considera legal e o depositam em algum estabelecimento bancário. É nessa fase que o dinheiro "sujo" deve ter sua origem identificada, o que pode ser feito através da aplicação de medidas que a legislação impõe.
- b. **Ocultação:** o propósito perseguido nessa fase é desviar os fundos ilícitos de sua origem, de maneira a gerar um sistema completo de encadeamento de transações financeiras, dirigidas a apagar os vestígios contábeis de tais fundos ilícitos. Alguns dos métodos utilizados são:

- Conversão do dinheiro em espécie em outros meios de pagamentos (cheque bancário, cheques de viagens, títulos ao portador, moeda estrangeira etc.);
  - Revenda de bens adquiridos com dinheiro em espécie; e
  - Transferência eletrônica de fundos.
- c. Integração:** essa fase presta-se a conferir uma aparência de legalidade a um patrimônio de origem criminoso.
- d. Legitimação:** superada a fase anterior, o criminoso necessita legitimar seu patrimônio integrando-o ao sistema econômico. Alguns de seus métodos são: compra de imóveis, empresas de fachada, empréstimos simulados/fictícios, duplicatas/faturas falsas, entre outros.

### **2.1.2. Financiamento do Terrorismo:**

Em decorrência, principalmente, dos eventos perpetrados em 11 de setembro de 2001, os organismos internacionais reconheceram a importância de se adotarem medidas para reforçar o combate ao financiamento do terrorismo, publicando assim as chamadas “Recomendações Especiais”, as quais formam a estrutura básica para detectar, prevenir e suprimir o financiamento ao terrorismo e de atos terroristas.

Importante observar que em virtude de conter características específicas, comumente o crime de terrorismo é abordado como assunto correlato à lavagem de dinheiro. Contudo, no caso do terrorismo, a origem do dinheiro não precisa ser necessariamente ilícita contrariando assim a definição clássica de lavagem de dinheiro.

São exemplos de atividades utilizadas no financiamento do terrorismo: as doações de pessoas físicas e jurídicas, a pirataria e o contrabando de produtos, o tráfico de drogas, tráfico de pessoas e fraudes em cartões de crédito.

## **3. ATRIBUIÇÕES E RESPONSABILIDADES:**

Os agentes envolvidos nas atividades de PLDFT no âmbito da Green Net têm a responsabilidade de cumprir com essa política e demais diretrizes e procedimentos relacionados, cabendo-lhes os seguintes papéis e responsabilidades:

### **3.1. Diretoria Executiva:**

- 3.1.1.** Aprova as diretrizes e políticas de prevenção à lavagem de dinheiro e ao financiamento do terrorismo e, por meio de patrocínio, autoriza os investimentos necessários, incentiva o comprometimento, a efetividade e a melhoria contínua do processo;
- 3.1.2.** Toma ciência dos resultados da Avaliação Interna de Risco e do Relatório de Avaliação de Efetividade, bem como os planos de ação elaborados para solucionar deficiências, e seu respectivo relatório de acompanhamento.

### **3.2. Diretoria Financeira:**

- 3.2.1.** Responsável pela supervisão do programa de prevenção à lavagem de dinheiro e ao financiamento do terrorismo;
- 3.2.2.** Responsável pela aprovação da Avaliação Interna de Risco;
- 3.2.3.** Define as diretrizes e os critérios da classificação de riscos de lavagem de dinheiro e financiamento do terrorismo dos clientes, colaboradores, parceiros comerciais, fornecedores e prestadores de serviços terceirizados;
- 3.2.4.** Responsável pela comunicação ao COAF dos reportes de transações suspeitas, operações e/ou situações com indícios de PLDFT;

### **3.3. Diretoria Operacional:**

- 3.3.1.** As equipes responsáveis pelo relacionamento comercial direto com os clientes ficam encarregadas, na fase inicial, pela coleta de documentos e informações necessárias para a identificação e qualificação dos clientes e seus representantes.
- 3.3.2.** Responsável pela aprovação dos clientes, concomitantemente à celebração de contratos de prestação de serviços.

### **3.4. Compliance/ PLDFT:**

- 3.4.1.** Assegurar a conformidade com a legislação, normas, regulamentos e políticas internas que disciplinam a prevenção e combate à LDFT;
- 3.4.2.** Desenvolver e implementa ferramentas e processos de apoio às estratégias e programa de prevenção à LDFT;
- 3.4.3.** Estabelecer o programa de treinamento e de conscientização ao quadro de colaboradores, em conjunto com o Departamento de Recursos Humanos;
- 3.4.4.** Interagir com os órgãos reguladores;
- 3.4.5.** Confirmar a integridade das informações cadastrais dos clientes, inclusive na identificação de Pessoas Expostas Politicamente e os beneficiários finais;

- 3.4.6.** Monitorar, identificar e registrar as operações efetuadas pelos clientes, no intuito de minimizar riscos operacionais, legais e de imagem da Green Net;
- 3.4.7.** Realiza checagem de listas restritivas que possam envolver os clientes e providenciar o bloqueio de ativos, quando for o caso;
- 3.4.8.** Monitora periodicamente as notícias divulgadas na mídia relacionadas à prevenção à lavagem de dinheiro e verificar os impactos na lista de clientes ativos;
- 3.4.9.** Mantém lista de clientes com impedimentos, suspeitos ou comunicados em listas de Atenção e Restrição;
- 3.4.10.** Analisar e proceder as comunicações ao COAF de qualquer operação ou situação que possa configurar indício de crime de LDFT, mantendo a confidencialidade sobre o processo, medida esta que deve ser praticada por todos os colaboradores;
- 3.4.11.** Realiza a avaliação prévia de riscos de lavagem de dinheiro e financiamento do terrorismo em novos produtos e serviços, incluindo a utilização de novas tecnologias.

### **3.5. Recursos Humanos:**

- 3.5.1.** Viabilizar, em conjunto com o Compliance /APLDFT, o programa de treinamento para assegurar que todos os colaboradores estejam devidamente orientados e atualizados quanto às suas obrigações e responsabilidades perante a regulamentação;
- 3.5.2.** Adotar, nos processos de admissão de funcionários, os procedimentos necessários para assegurar a contratação de pessoas idôneas, assim como acompanhar situações que possam caracterizar algum tipo de risco ou desvio, para fins de prevenção à lavagem de dinheiro, financiamento ao terrorismo e demais atos ilícitos.

### **3.6. Gestores e Funcionários:**

- 3.6.1.** Os gestores e demais funcionários são os principais responsáveis pelo cumprimento e aplicação desta Política, devendo estar comprometidos com a participação em atividades de capacitação sobre o tema prevenção à lavagem de dinheiro e ao financiamento do terrorismo;
- 3.6.2.** Adicionalmente, tem o dever de acompanhar as transações e comportamentos de clientes, reportando prontamente, ao Compliance, operações ou situações que possam configurar indícios da prática de ilícitos passíveis de comunicação ao COAF.



### **3.7. Auditoria Interna:**

- 3.7.1.** responsável por verificar o cumprimento e a aderência aos termos desta Política e às demais normas internas e externas aplicáveis ao assunto;

## **4. PROGRAMA DE PREVENÇÃO À LAVAGEM DE DINHEIRO E AO FINANCIAMENTO DO TERRORISMO**

Com o objetivo de viabilizar o cumprimento das diretrizes desta Política e evitar o uso indevido de que seus produtos e serviços sejam usados em atividades ilícitas, a Green Net definiu um Programa de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo, nos termos previstos na Circular BACEN nº 3.978/20, cuja aplicação ficará centralizada na estrutura da área de Compliance/PLDFT e deverá contemplar, no mínimo, as seguintes atividades:

### **4.1. Políticas e Procedimentos**

- 4.1.1.** A Green Net implementou políticas e procedimentos formulados com base nos princípios e diretrizes da empresa e em conformidade com as leis e regulamentos que tratam da prevenção à lavagem de dinheiro e ao financiamento do terrorismo. Referidos documentos devem ser aprovados pela diretoria e revisados periodicamente, e contemplam dispositivos sobre os perfis de risco dos clientes; da instituição; das operações, transações, produtos e serviços; e dos funcionários, parceiros e prestadores de serviços terceirizados.

### **4.2. Procedimento de Conheça Seu Cliente – CSC (KYC)**

Inicialmente, é importante reafirmar a posição de que a imagem da Green Net deve ser preservada a partir da adoção de procedimentos bem estruturados, de modo a evitar graves danos à instituição e à sociedade indiretamente.

Conhecendo bem seus clientes e colaboradores, a Green Net terá sua reputação protegida e, conseqüentemente, reduzidos os riscos de seus serviços e produtos serem utilizados para legitimar recursos provenientes de atividades ilícitas.

No processo de Avaliação Interna de Risco é aplicada a abordagem baseada em risco, cuja metodologia possibilita que as medidas de prevenção e mitigação da lavagem de dinheiro e do financiamento do terrorismo guardem proporcionalidade com os níveis de riscos identificados, ou seja, aonde os riscos forem mais altos, serão adotadas medidas reforçadas

para administrar e mitigar tais riscos e, onde os riscos forem menores, serão utilizadas medidas simplificadas.

Assim, os procedimentos necessários para permitir o conhecimento pleno dos clientes deverão constar formalmente de manual específico, com a necessária aprovação da Diretoria da Instituição e mantido atualizado. Na definição dos procedimentos deve ser observada a compatibilidade com os perfis de risco dos clientes, com as diretrizes da Política de PLDFT e considerando os resultados da Avaliação Interna de Risco.

O detalhamento dos procedimentos exigidos pela regulamentação e definidos em conformidade com a avaliação de riscos, devem contemplar as seguintes fases de verificação e análise:

#### **4.2.1. Identificação do Cliente**

Devem ser capturados e mantidos atualizados os dados cadastrais obrigatórios dos clientes e de pessoas relacionados (sócios, representantes, procuradores e beneficiários finais), conforme exigido pelas regulamentações vigentes, diretrizes internas e decorrente da avaliação interna dos produtos e serviços.

No caso de cliente pessoa jurídica, deve ser conduzida análise da cadeia de participação societária até a identificação da pessoa física caracterizada como seu beneficiário final.

#### **4.2.2. Qualificação do Clientes**

A qualificação dos clientes deve ser realizada por meio de procedimentos que permitam identificar seus clientes por meio da coleta, verificação e validação de informações, compatíveis com o perfil de risco do cliente e com a natureza da relação de negócio.

As informações coletadas na qualificação do cliente devem ser mantidas atualizadas e devem incluir a verificação da condição do cliente como pessoa exposta politicamente, bem como a verificação da condição de representante, familiar ou estreito colaborador dessas pessoas. Com base nas informações coletadas, deve ser avaliada, também, a capacidade financeira do cliente, incluindo a renda, no caso de pessoa física, ou o faturamento para a pessoa jurídica.

#### **4.2.3. Classificação do Cliente**

A classificação de risco deve ser conduzida em conformidade com as categorias definidas na avaliação interna de risco, com base no perfil de risco do cliente e na natureza da relação de negócio, que devem ser revisadas sempre que houver alterações.

#### **4.2.4. Identificação e Qualificação dos Beneficiário Final**

A Green Net adota procedimentos para identificar a pessoa física que detém, em última instância, o controle societário dos clientes pessoa jurídica, sendo analisada a cadeia de participação societária, com o estabelecimento de referência mínima de 25% (vinte e cinco por cento) da participação de cada sócio/acionista.

Deve também ser considerado beneficiário final o representante, inclusive o procurador e o preposto, que exerçam o comando de fato sobre as atividades do cliente pessoa jurídica.

Os procedimentos definidos na regulamentação para a identificação do beneficiário final não se aplicam às pessoas jurídicas constituídas sob a forma e companhia aberta ou entidades sem fins lucrativos e cooperativas. Nesses casos, as informações coletadas devem alcançar as pessoas físicas autorizadas a representá-las, seus controladores e administradores.

#### **4.2.5. Qualificação como Pessoa Exposta Politicamente – PEP**

Os procedimentos de qualificação previstos na regulamentação de PLDFT devem incluir a verificação da condição dos clientes como pessoa exposta politicamente, bem como prever a adoção de medidas mais rigorosas de controles internos, classificação de risco e alçada superior de aprovação, tanto no início ou na manutenção do relacionamento com o cliente.

São caracterizados como clientes PEP: os agentes públicos que desempenham ou tenham desempenhado, nos últimos cinco anos, no Brasil ou em países, territórios e dependências estrangeiras, cargos, empregos ou funções públicas relevantes, assim como seus representantes, familiares diretos ou colaterais até o segundo grau, o cônjuge, companheiro, companheira, enteado, enteada, bem como os estreitos colaboradores. Também são considerados nessa condição as pessoas jurídicas cujos representantes ou controladores, direto ou indireto, sejam classificados como PEP.

#### **4.2.6. Registro de Operações e Guarda de Documentos**

Deve ser mantido o de registro de todas as operações realizadas, produtos e serviços contratados, contendo todas as informações obrigatórias previstas na regulamentação. Da mesma forma, devem ser mantido um processo rigoroso de guarda física ou sistêmica de documentos que atendem aos processos desta Política, obedecidos os prazos mínimos estabelecidos nas disposições normativas.

#### **4.3. Monitoramento, Seleção e Análise de Operações e Situações Suspeitas**

As instituições autorizadas a funcionar pelo Banco Central devem instituir procedimentos de monitoramento, seleção e análise de operações e situações, com o objetivo de identificar e dar tratamento para os indícios de suspeita de lavagem de dinheiro e de financiamento do terrorismo.

A Green Net definiu procedimentos relacionados com as atividades de monitoramento, seleção e análise de operações e situações atípicas, bem como o atendimento dos prazos estabelecidos para a execução dos trabalhos, os quais encontram-se detalhados em manual específico, sob a responsabilidade da área de Compliance/PLDFT.

As informações cadastrais e as transações e operações financeiras, inclusive as propostas realizadas pelos clientes, devem ser monitoradas para apuração de situações que podem configurar indícios de ocorrência de lavagem de dinheiro ou financiamento do terrorismo.

A ferramenta de monitoramento considera o perfil, origem e destino dos recursos e a capacidade financeira dos clientes. Tomando como referência o resultado da avaliação interna de risco, o conjunto de regras é aplicado conforme a exposição do risco e mediante a adoção de parâmetros mais rigorosos ou ainda um acompanhamento mais aprofundado.

A Green Net realiza, também, por meio de ferramenta sistêmica, a detecção de nomes de pessoas ou operações que não cumpram com os programas de sanções divulgadas por organismos internacionais. Também são mantidos procedimentos com vistas a possibilitar o bloqueio de ativos e/ou fundos das pessoas, entidades ou grupos identificados no Conselho de Segurança das Nações Unidas (CSNU) e comunicar as autoridades, quando necessário.

#### **4.4. Comunicações de Operações e Situações Suspeitas ao COAF**

A legislação brasileira determina a comunicação ao COAF, no prazo de 24 horas, de todas as operações suspeitas de lavagem de dinheiro, sem dar ciência dos fatos aos envolvidos ou a terceiros.

A área de Compliance/PLDFT é responsável pelo tratamento de situações atípicas identificadas nas atividades de monitoramento, por meio de dossiê específico, com a devida análise e alçada para decidir sobre o arquivamento ou a comunicação dos fatos ao COAF.

Em complemento, a Green Net estabelece que todas as áreas envolvidas devem comunicar imediatamente à área de Compliance/PLDFT, por meio de canal próprio, quaisquer situações ou operações que possam ter indícios de envolvimento com lavagem de dinheiro, bem como qualquer circunstância relacionada com as mencionadas operações, que seja produzida posteriormente.

As comunicações terão caráter estritamente confidencial, assim como a identidade dos funcionários que tenham realizado e nenhuma informação será dada ao cliente ou a terceiros.

Nos períodos em que não tiverem sido efetuadas comunicações ao COAF em cada ano civil, deverá ser prestada declaração, até dez dias úteis após o encerramento do respectivo ano, atestando a não ocorrência de operações ou situações passíveis de comunicação.

O conjunto dos procedimentos relacionados com as comunicações do COAF encontram-se descritos em manual específico, sob o controle da área de Compliance/PLDFT.

#### **4.5. Procedimentos destinados a conhecer o Funcionário (CSF – KYE), parceiros e Prestadores de Serviços Terceirizados (CSP – KYP)**

Em conformidade com as diretrizes desta Política e utilizando-se dos resultados dos riscos apurados na realização da avaliação interna de risco dos produtos e serviços da instituição, a Green Net instituiu os procedimentos cabíveis para conhecer os seus funcionários, parceiros e prestadores de serviços terceirizados, os quais se encontram formalizados em documento específico e devidamente aprovado pela Diretoria.

De forma geral, os procedimentos contemplam um conjunto de regras, procedimentos e controles que devem ser adotados para identificar e qualificar adequadamente, tanto os funcionários quanto os parceiros e prestadores de serviços terceirizados, para os fins de evitar participações em crimes de lavagem de dinheiro e financiamento do terrorismo.

O objetivo é prevenir a realização de negócios com contrapartes inidôneas ou suspeitas de envolvimento em atividades ilícitas, bem como assegurar que eles possuam procedimentos adequados de PLD/CFT, conforme definido nas normas internas.

## **5. TREINAMENTOS**

Tendo como objetivo alcançar a melhor forma de capacitar os funcionários para a identificação, tratamento e comunicação de situações com indícios de lavagem de dinheiro e de financiamento do terrorismo, assim como aprofundar o conhecimento das exigências e

responsabilidades legais e regulamentares, a Green Net definiu um programa de treinamento periódico de todos os colaboradores e parceiros, contemplando os módulos específicos e o cronograma de aplicação, contando com a participação de gestores e da área de Recursos Humanos.

## **6. AUDITORIA**

As auditorias são conduzidas permanentemente com o objetivo de verificar o cumprimento de políticas e procedimentos de diligência obrigatória por parte de cada área.

As auditorias internas e externas avaliam periodicamente a conformidade e veracidade dos dados cadastrais e revisam os relatórios de visitas. Portanto, é imprescindível que estes estejam atualizados e consistentes.

## **7. AVALIAÇÃO INTERNA DE RISCO**

A Green Net elaborará a sua Avaliação Interna de Risco em períodos de 2 (dois) anos ou quando ocorrerem alterações significativas nos perfis de risco, e cujos resultados deverão ser submetidos à aprovação do Diretor Responsável pelas atividades de PLDFT e levado para ciência de instâncias superiores, quando houver.

A referida avaliação tem por objetivo identificar, mensurar e mitigar o risco de utilização de seus produtos e serviços na prática de lavagem de dinheiro e do financiamento ao terrorismo, sendo aplicados os conceitos de abordagem baseada em risco, com vistas a garantir que as medidas de prevenção e mitigação da lavagem de dinheiro e do financiamento do terrorismo sejam proporcionais aos riscos identificados, ou seja, medidas reforçadas para administrar e mitigar os riscos mais altos e medidas simplificadas onde os riscos forem menores.

O detalhamento das diretrizes que fundamenta a abordagem baseada em risco será formalizado em documento específico.

## **8. AVALIAÇÃO DE EFETIVIDADE DA POLÍTICA**

A GREEN NET deve avaliar anualmente a efetividade desta Política, dos procedimentos e dos controles internos relacionados à PLD, visando garantir o cumprimento das suas responsabilidades, bem como elaborar e acompanhar plano de ação destinado a solucionar eventuais deficiências identificadas.

Os resultados da Avaliação de Efetividade devem ser formalizados em relatório específico, devendo ser levado ao conhecimento da Diretoria da Green Net.

## 9. AVALIAÇÃO DE NOVOS PRODUTOS E SERVIÇOS

Os novos produtos e serviços, incluindo a utilização de novas tecnologias, quando aplicável, devem ser avaliados de forma prévia, sob a ótica de PLD/CFT, conforme as diretrizes estabelecidas em política interna.

## 10. LEIS E NORMATIVOS RELACIONADOS

Esta Política deve ser aplicada, primordialmente, em função das disposições emanadas dos seguintes documentos legais e regulamentares:

**10.1. Lei Federal nº 9.613/1998 e alterações decorrentes da Lei nº 12.683/2012** - 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.

**10.2. Lei Federal nº 13.260/16** - regulamenta o inciso XLIII do art. 5º da Constituição Federal, disciplinando o terrorismo, tratando de disposições investigatórias e processuais e reformulando o conceito de organização terrorista.

**10.3. Lei Federal 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.

**10.4. Circular BACEN 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 de dinheiro e ao financiamento do terrorismo.

**10.5. Carta Circular BACEN nº** - 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).