

**POLÍTICA CORPORATIVA DE PREVENÇÃO E COMBATE A
ATOS ILÍCITOS**

SUMÁRIO

- 1. OBJETIVO**
- 2. TERMOS E DEFINIÇÕES**
- 3. PAPEIS E ATRIBUIÇÕES**
 - 3.1. Corpo Administrativo CONTOBANK**
 - 3.2. Compliance Office**
 - 3.3. Squad de Risco, Modelagem e Prevenção à Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo (SRPLD)**
 - 3.4. Squad Comerciais e BackOffice**
 - 3.5. Departamento Jurídico**
- 4. PROGRAMA INTERNO CORPORATIVO DE PREVENÇÃO E COMBATE A ATOS ILÍCITOS**
 - 4.1. Conheça Seu Cliente - KYC**
 - 4.2. Conheça Seu Parceiro - KYP**
 - 4.3. Conheça Seu Fornecedor - KYS**
 - 4.4. Conheça Seu Funcionário - KYE**
 - 4.5. Avaliação de Novos Produtos e Serviços e Aquisição de Clientes**
 - 4.6. Monitoramento de Transações**
 - 4.7. Comunicação de Transações Suspeitas aos Órgãos Reguladores**
 - 4.8. Treinamento**
- 5. PREVENÇÃO E COMBATE A FRAUDES E SINISTROS**
- 6. MODELO DE ATUAÇÃO NA PREVENÇÃO E COMBATE A FRAUDES E SINISTROS**
- 7. MANUTENÇÃO E GUARDA DE INFORMAÇÕES E REGISTROS**
- 8. TRANSPARÊNCIA NO RELACIONAMENTO COM OS CLIENTES**
- 9. CANAIS DE DÚVIDAS E DENÚNCIAS**
- 10. DECLARAÇÃO DE CIÊNCIA E COMPROMISSO**
- 11. INFORMAÇÕES DE CONTROLE**

1. OBJETIVO

Esta Política de Prevenção e Combate a Atos Ilícitos objetiva consolidar os princípios e diretrizes para a prevenção e combate à lavagem de dinheiro, ao financiamento do terrorismo, às fraudes e aos sinistros, em consonância com a legislação e regulamentação vigentes e com as melhores práticas de mercado nacionais e internacionais, tendo em vista que as plataformas eletrônicas dos serviços financeiros desempenham papel fundamental na prevenção de atos ilícitos voltados ao Mercado Financeiro.

O grande desafio é identificar e coibir operações cada vez mais sofisticadas que procuram ocultar ou dissimular a natureza, a autoria, origem, localização, disposição, movimentação ou a propriedade de bens, direitos e/ou valores provenientes direta ou indiretamente de atividades ilegais.

O CONTOBANK estabelece a presente Política com o intuito de evitar a sua intermediação em atividades ilícitas, de zelar e proteger seu nome, sua reputação e imagem perante os colaboradores, clientes, parceiros estratégicos, fornecedores, prestadores de serviços, reguladores e sociedade, por meio de uma estrutura de governança orientada para a transparência, o rigoroso cumprimento de normas e regulamentos e a cooperação com as autoridades policial e judiciária.

Também busca alinhar-se continuamente às melhores práticas nacionais e internacionais para prevenção e combate a atos ilícitos, por meio de investimentos e contínua capacitação de seus colaboradores.

2. TERMOS E DEFINIÇÕES

A Lavagem De Dinheiro consiste na ocultação ou dissimulação da natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente, de infração penal.

O Financiamento Do Terrorismo se configura quando alguém, direta ou indiretamente, por qualquer meio, prestar apoio financeiro, fornecer ou reunir fundos com a intenção

de serem utilizados ou sabendo que serão utilizados, total ou parcialmente, por grupos terroristas para a prática de atos terroristas.

A Corrupção consiste em sugerir, oferecer, prometer, conceder, solicitar, exigir, aceitar, receber, direta ou indiretamente, mediante exigência ou não, de pessoas ou empresas dos setores público, privado e organizações do terceiro setor, bem como entre pessoas, empresas e organizações de diferentes países, vantagens indevidas de qualquer natureza (financeira ou não) em troca de realização ou omissão de atos inerentes às suas atribuições, operações ou atividades, visando a benefícios para si ou para terceiros.

Fraude refere-se a quaisquer atividades, atitudes ou ações ilícitas que têm o propósito de enganar ou iludir alguém, utilizando-se de má-fé para benefício próprio ou de terceiros, quer dizer, a omissão e/ou manipulação de informação, apropriação de valores, adulteração de documentos, registros e demonstrações contábeis.

Sinistro refere-se a eventos atípicos que resultem em prejuízos ou desastres a empresa, tais como, extorsão mediante sequestro, furtos, acidentes, arrombamentos, entre outros.

Embargo é a proibição total ou parcial de realizar operações comerciais com determinado local e país, estabelecido por uma jurisdição ou por um órgão internacional em represália a determinadas ações, adotadas pela jurisdição embargada, de caráter econômico, político, social ou bélico. Ações essas que contrariam os princípios estabelecidos pela jurisdição ou organismo internacional que impõe o embargo. Algumas jurisdições ou organismos internacionais também estabelecem restrições a determinadas pessoas ou companhias que atuam em atividades ilícitas.

3. PAPÉIS E ATRIBUIÇÕES

3.1. Corpo Administrativo do CONTOBANK

Os líderes administrativos aprovam as diretrizes de prevenção a atos ilícitos da Instituição formuladas pelo Compliance Office e suas respectivas alterações.

3.2. Compliance Office

Supervisiona o Programa Corporativo de Prevenção a Atos Ilícitos a partir de informações compiladas e apresentadas pelas áreas, bem como de outros mecanismos de que dispõe.

Como terceira linha de defesa, avalia anualmente a efetividade do Programa de Prevenção e Combate a Atos Ilícitos e propõe medidas para aprimorá-lo.

- Define e propõe ao Corpo administrativo da empresa as diretrizes de prevenção a atos ilícitos da Instituição;
- Analisa os resultados dos processos e atividades do programa de prevenção a atos ilícitos;
- Delibera sobre situações não previstas nesta Política.

3.3. Squad de Risco, Modelagem e Prevenção à Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo (SRPLD)

- Gerencia o Programa de Prevenção à Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo do CONTOBANK no Brasil e no exterior;
- Aprimora a qualidade e efetividade de seus processos e as responsabilidades sobre os processos de Prevenção à Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo da empresa;
- Realiza a avaliação prévia dos riscos de lavagem de dinheiro e financiamento do terrorismo em produtos e serviços;
- Define as diretrizes e os critérios mínimos de classificação de riscos de lavagem de dinheiro e financiamento do terrorismo dos clientes, colaboradores, parceiros comerciais, fornecedores e prestadores de serviços;
- Acompanha e classifica as diferentes tipologias de atos ilícitos, no sentido de antecipar tendências e propor soluções preventivas e de combate;
- Valida os procedimentos de Prevenção à Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo do CONTOBANK;
- Reporta periodicamente ao Comitê de Auditoria fatos relevantes de Prevenção à Lavagem de Dinheiro, Atos Ilícitos e Combate ao Financiamento do Terrorismo;

- Aprimora a qualidade e efetividade de seus processos, assegurando a integridade, disponibilidade e confidencialidade das informações; a segurança patrimonial e física dos colaboradores, dos clientes e dos executivos e as responsabilidades sobre os processos de Prevenção a Atos Ilícitos;
- Realiza a avaliação prévia dos riscos de fraudes em produtos e serviços;
- Define as diretrizes e os critérios mínimos de classificação de riscos de fraudes dos clientes, colaboradores, parceiros comerciais, fornecedores e prestadores de serviços;
- Valida os procedimentos de Prevenção a Atos Ilícitos mencionados nos documentos;
- Gerencia eventos extremos, únicos e raros que ameacem a estratégia, o objetivo e a viabilidade da organização, sua imagem e/ou reputação.

3.4. Squad Comercial e BackOffice

Como primeira defesa, definem e implementam procedimentos e controles aderentes a esta política com a orientação da (SRPLD), considerando a avaliação dos riscos no início e manutenção do relacionamento com pessoas físicas e jurídicas, naqueles processos que são executados e estão sob sua responsabilidade direta.

Asseguram que os colaboradores realizem o treinamento de prevenção e combate à lavagem de dinheiro, ao financiamento do terrorismo, fraudes e sinistros, bem como reciclagem anualmente.

3.5. Departamento Jurídico

Analisa os requerimentos legais e regulatórios de Prevenção à Lavagem de Dinheiro (PLD) e Combate ao Financiamento do Terrorismo (CFT) e seus respectivos impactos aos negócios. Como também auxiliam os gestores de negócio e colaboradores na elaboração de planos de ação para implantação de controles de PLD/CFT, apoiando a avaliação dos riscos e providências necessárias para tratamento de ocorrências de transações ou operações suspeitas de lavagem de dinheiro, fraudes e sinistros, sob a ótica jurídica.

4. PROGRAMA INTERNO CORPORATIVO DE PREVENÇÃO E COMBATE A ATOS ILÍCITOS

4.1. Conheça Seu Cliente - KYC

Trata-se de um conjunto de ações que devem ser adotadas para assegurar e confirmar a identidade e a atividade econômica dos clientes, bem como a origem e a constituição de seu patrimônio e seus recursos financeiros.

Quanto mais precisas forem as informações coletadas e registradas no início do relacionamento, maior será a capacidade de identificação de atos ilícitos.

Para os casos que requerem Especial Atenção, como o relacionamento com Pessoas Expostas Politicamente (PEPs) e clientes onde não foi possível identificar o beneficiário final, são adotados procedimentos rigorosos específicos de análise.

É obrigatória a autorização do responsável administrativo do CONTOBANK 4 U para o início do relacionamento com pessoas físicas ou pessoas jurídicas classificadas como PEPs e para a manutenção do relacionamento já existente quando o cliente passar a se enquadrar nesta situação, conforme definido em política interna.

4.2. Conheça Seu Parceiro - KYP

Conheça Seu Parceiro trata-se de um conjunto de regras, procedimentos e controles que devem ser adotados para identificação e aceitação de parceiros comerciais, incluindo correspondentes no país e no exterior. 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 em documento interno.

São consideradas Parceiros as Pessoas Jurídicas que realizam acordos comerciais ou associações com o CONTOBANK e que atendem aos requisitos estabelecidos em Política Interna.

O CONTOBANK não admite o relacionamento com empresas que estejam na lista de apontamentos do Conselho de Controle de Atividades Financeiras (COAF) ou da

Organização das Nações Unidas (ONU), podendo abranger outros. Contribuindo assim para o relacionamento positivo e fomento de combate aos negócios com contrapartes inidôneas ou suspeitas de envolvimento em atividades ilícitas.

4.3. Conheça Seu Fornecedor - KYS

Trata-se de um conjunto de regras, procedimentos e controles que devem ser adotados para identificação e aceitação de fornecedores e prestadores de serviços, visando proporcionar um adequado conhecimento dos colaboradores de modo a prevenir a contratação de empresas inidôneas ou suspeitas de envolvimento em atividades ilícitas.

Para clientes, parceiros, fornecedores e prestadores de serviços que apresentarem maior risco associado a atos ilícitos são aplicados critérios de identificação e diligência mais rigorosos, com a aprovação do relacionamento por nível hierárquico superior.

4.4. Conheça Seu Funcionário - KYE

Trata-se de um conjunto de regras, procedimentos e controles que devem ser adotados para seleção, contratação e acompanhamento de 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.

4.5. Avaliação de Novos Produtos e Serviços e Aquisição de Clientes

Os novos produtos e serviços devem ser avaliados de forma prévia, sob a ótica de PLD/CFT, conforme diretrizes estabelecidas na **Política de Clientes**.

4.6. Monitoramento de Transações

As transações e operações financeiras realizadas pelos clientes, devem ser monitoradas por amostra, dentro da análise de logs da ferramenta ELK, para apuração de situações que podem configurar indícios de ocorrência de lavagem de dinheiro ou financiamento

do terrorismo. O monitoramento considera o perfil, origem e destino dos recursos e a capacidade financeira dos clientes.

4.7. Comunicação de Transações Suspeitas aos Órgãos Reguladores

As operações, situações ou propostas que contêm indícios de ilicitude devem ser comunicadas às instituições financeiras intermediadoras e parceiras, para que estas avaliem e se julgarem, comuniquem aos reguladores competentes, quando aplicável, em cumprimento às determinações legais e regulamentares. As comunicações de boa-fé não acarretam responsabilidade civil ou administrativa, nem a seus administradores e colaboradores. Informações sobre essas comunicações são restritas, não devendo ser divulgadas a clientes e/ou terceiros.

4.8. Treinamento

O programa de treinamento de PLD/CFT é contínuo e deve ser aplicado a todos os colaboradores elegíveis, visando:

- (i) Aprofundar o conhecimento que os administradores e colaboradores têm das exigências e responsabilidades legais e regulamentares, bem como das diretrizes corporativas de PLD/CFT;
- (ii) Capacitar administradores e colaboradores a identificar, prevenir, tratar e comunicar situações de risco ou com indícios de ocorrência de lavagem de dinheiro ou financiamento do terrorismo nos negócios realizados.

A aplicação do programa deve ocorrer por meio de ações institucionais e nas unidades de negócios, podendo contemplar cursos presenciais ou à distância (e-learning), palestras, teleconferências, comunicados, publicações, entre outras modalidades e formas.

5. PREVENÇÃO E COMBATE A FRAUDES E SINISTROS

A prevenção e combate a fraudes é responsabilidade de todos. As Fraudes podem ser classificadas como:

(i) Violações ao Código de Ética e Descumprimento do Contrato, cometidas em grupo ou isoladamente:

- Adoção de práticas não autorizadas pela empresa;
- Desvios de comportamento;
- Quebra de sigilo e conflito de interesse.

(ii) Inobservância de Normas Legais e Regulamentares:

São todas as situações identificadas por descumprimento de normas legais e regulamentares, que coloquem em risco a imagem, o patrimônio ou a continuidade da Organização.

(iii) Atos Ilícitos de Qualquer Natureza:

São todas as modalidades de atos ilícitos (crimes ou contravenções penais) previstos na Legislação Penal Brasileira e que possam ocasionar prejuízos, diretos ou indiretos, ao Banco, seus colaboradores, a clientes ou terceiros. Alguns exemplos são a Falsificação; Adulteração; Estelionato (em todas as suas formas); Abertura fraudulenta de conta (contas frias) ou de contratação de produtos; Apropriação indébita; Furto; Roubo; Assalto; Arrombamento; Extorsão mediante sequestro; Fraudes por meio dos canais eletrônicos e não eletrônicos; entre outros.

6. MODELO DE ATUAÇÃO NA PREVENÇÃO E COMBATE A FRAUDES E SINISTROS

(i) Avaliação de Riscos no Início do Relacionamento

Os processos de contratação de serviços e produtos devem contemplar procedimentos para prevenir e mitigar o risco de fraude no início do relacionamento com proponentes.

(ii) Prevenção e Combate à Fraude Interna

O CONTOBANK adota medidas específicas para evitar a ocorrência de fraudes envolvendo seus colaboradores, por meio de diretrizes e procedimentos de controle para prevenção e detecção de atividades irregulares.

(iii) Prevenção e Combate à Fraude Contábil

O CONTOBANK adota medidas para resguardar a qualidade e a integridade de suas demonstrações financeiras, por meio de controles internos, da atuação das Auditorias Interna e Externa e da supervisão pelo Comitê de Auditoria.

(iv) Avaliação de Riscos em Novos Produtos e Serviços

Os novos produtos e serviços devem ser avaliados de forma prévia, sob a ótica de prevenção a fraudes, conforme as diretrizes estabelecidas em Política de Clientes.

(v) Monitoramento de Transações

Os produtos e serviços contratados pelos clientes devem ser monitorados para detecção e apuração de situações atípicas ou suspeitas de ocorrência de fraude ou outros atos ilícitos.

(vi) Tratamento de Ocorrências

As situações sob suspeita ou confirmadas devem ser tratadas para apuração de responsabilidades e providências necessárias.

Os procedimentos e decisões tomados durante o tratamento das ocorrências devem ser formalizados visando à geração de subsídios a processos judiciais.

(vii) Treinamento e Conscientização

O programa de treinamento de Prevenção a Fraudes e Sinistros é contínuo e deve ser aplicado a todos os colaboradores elegíveis, visando:

- Aprofundar o conhecimento que os administradores e colaboradores têm dos requerimentos normativos externos e internos de prevenção e combate a fraudes e sinistros;
- Capacitar administradores e colaboradores a identificar, prevenir, tratar e comunicar situações suspeitas ou relacionadas com fraudes e outros atos ilícitos.

A aplicação do programa deve ocorrer por meio de ações institucionais, podendo contemplar cursos à distância (e-learning) e presencial, palestras, teleconferências, comunicados, publicações, entre outras modalidades e formas.

7. MANUTENÇÃO E GUARDA DE INFORMAÇÕES E REGISTROS

As informações e registros das operações e serviços prestados devem ser mantidos em sua forma original ou em arquivos eletrônicos, conforme prazos e responsabilidades estabelecidos pela legislação vigente, em foco, a Lei Geral de Proteção de Dados.

8. TRANSPARÊNCIA NO RELACIONAMENTO COM OS CLIENTES

Os clientes do CONTOBANK possuem acesso, por intermédio de diversos canais, às suas informações financeiras, incluindo os recursos investidos, produtos contratados e transações em sua conta. Com isso, o próprio cliente é um parceiro forte e atuante na prevenção e no combate a Atos Ilícitos.

O CONTOBANK também alerta continuamente seus clientes, por meio dos canais de relacionamento, sobre as possibilidades de ocorrência de Atos Ilícitos e as ações e os cuidados que devem ser tomados para preveni-los.

9. CANAIS DE DÚVIDAS E DENÚNCIAS

Todos no CONTOBANK devem comunicar imediatamente as situações com indícios ou evidências de atos ilícitos, identificadas na prospecção, negociação ou durante o relacionamento utilizando-se de e-mail anônimo para atendimento@contobank.com.br e/ou para dpo@contobank.com.br

Estes canais também podem ser utilizados pelos clientes, prestadores de serviços e público em geral.

(i) Proteção ao Denunciante:

São vedados atos de Retaliação contra aquele que, de boa-fé, denunciar ou manifestar queixa, suspeita, dúvida ou preocupação relativas a possíveis violações às diretrizes desta Política, preservada a confidencialidade das informações relativas às apurações.

10. DECLARAÇÃO DE CIÊNCIA E COMPROMISSO

Você está recebendo a Política de Prevenção Contra Atos Ilícitos para parceiros, funcionário e/ou colaboradores do CONTOBANK, ele contém princípios de conduta a serem cuidados por todos que tem relacionamento com o CONTOBANK. As diretrizes e valores precisam ser considerados em todas as suas relações com o CONTOBANK e em sua representação. Assinando essa Declaração você manifesta seu compromisso em cumpri-lo integralmente.

Declaro que tenho ciência das regras e boas práticas desta política e da sua importância na condução das minhas atividades e dia a dia.

Local e Data

Nome Completo

CPF

Assinatura

11. INFORMAÇÕES DE CONTROLE

VERSÃO	MOTIVO	DATA	ELABORADOR	RESUMO DAS ALTERAÇÕES
1.0	Criação da Política	22/01/2026	Dejur Contobank	Criação da Política