POLÍTICA DE PREVENÇÃO E COMBATE À LAVAGEM DE DINHEIRO, AO FINANCIAMENTO DO TERRORISMO E À CORRUPÇÃO

POLÍTICA DE PREVENÇÃO E COMBATE À LAVAGEM DE DINHEIRO, AO FINANCIAMENTO DO TERRORISMO E À CORRUPÇÃO

1. Para atender as disposições da Lei 9.613/98 e da Lei 12.846/13 e em consonância com as melhores práticas de mercado, a companhia elaborou proposta de política de prevenção e combate à lavagem de dinheiro, ao financiamento do terrorismo e à corrupção.

2. Além das diretrizes gerais da política voltada à prevenção e combate aos crimes acima enunciados, a norma proposta traz também a definição da Política "Conheça Seu Cliente" ("KYC"), da Política "Conheça Seu Parceiro" ("KYP") e do "Código de Ética e Conduta" de seus administradores e colaboradores em geral.

3. A minuta dessa norma consta das páginas a seguir.

4. Para implantação na companhia, submetemos a presente proposta à aprovação desse Conselho de Administração.

PC 01 - POLÍTICA CORPORATIVA DE PREVENÇÃO E COMBATE À LAVAGEM DE DINHEIRO, AO FINANCIAMENTO DO TERRORISMO E À CORRUPÇÃO (“PLDFT/PC”)

1. Objetivo

Este documento tem por objetivos (a) consolidar os princípios e as diretrizes do Grupo CIBRASEC para prevenção e combate à lavagem de dinheiro e ao financiamento do terrorismo e (b) estabelecer padrões mínimos de comportamento exigidos da CIBRASEC e de seus colaboradores frente a situações que possam envolver, aparentar ou caracterizar qualquer tipo de corrupção, como suborno e outros atos ilícitos ou lesivos à administração pública nacional, em consonância com as disposições da Lei nº 9.613/1998 (“Lei de Prevenção à Lavagem de Dinheiro e ao Financiamento ao Terrorismo”), da Lei nº 12.846/13 (“Lei Anticorrupção”) e com as melhores práticas de mercado.

2. Áreas de aplicação

Esta política se aplica a todos os administradores, funcionários, fornecedores, parceiros de negócios, assessores ou qualquer pessoa com a qual o Grupo CIBRASEC mantenha relacionamento comercial.

3. Compete

Ao **Conselho de Administração**, aprovar as políticas de prevenção e combate à lavagem de dinheiro, ao financiamento do terrorismo e à corrupção, e suas respectivas alterações.

Ao **Comitê de Risco e Tesouraria**, acompanhar a implementação e cumprimento dessas políticas, propor procedimentos e alterações e formular orientações relacionados a este assunto.

Aos **Administradores e funcionários da CIBRASEC**, conhecer e seguir as diretrizes dessas políticas e comunicar aos órgãos competentes, de forma tempestiva e objetiva, toda situação, operação ou proposta suspeita de envolvimento com algum ato ilícito, nos termos estabelecidos a seguir.

Ao **Comitê de Conformidade**, avaliar os eventos comunicados ou evidenciados sobre falhas na observância desta política e transgressões às regras aqui estipuladas e definir as ações a serem tomadas.

Ao **Diretor Executivo**, responsável pelas atividades de prevenção e combate à lavagem de dinheiro, ao financiamento do terrorismo e à corrupção, gerenciar os processos para atendimento dos requerimentos desta política, garantindo a sua operacionalização.

À **Gerência de Estruturação e Risco**, operacionalizar os processos requeridos por esta política.

4. PROGRAMA CORPORATIVO DE PREVENÇÃO A ATOS ILÍCITOS

Com o objetivo de prevenir e combater procedimentos e operações que viabilizem lavagem de dinheiro, financiamento ao terrorismo e atos de corrupção, o Grupo CIBRASEC, em consonância com a legislação e regulamentação vigentes, define as seguintes regras:

4.1. Programa de Prevenção e Combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo (“PLDFT”)

4.1.1. Conceitos:

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 pela estruturação de fontes de recursos financeiros (lícitos ou ilícitos), movimentados de forma oculta ou dissimulada, para permitir aos grupos terroristas realizarem suas atividades.

4.1.2. Aplicação:

Serão aplicados, em todas as operações realizadas pelo Grupo CIBRASEC, processos visando:

i. a identificação dos clientes, compreendendo a captura e armazenamento de informações cadastrais e sua atualização periódica; e
ii. a análise da estrutura das operações e a identificação dos beneficiários finais e de pessoas expostas politicamente.

Sua aplicação será efetuada conforme etapas a seguir:

4.1.2.1 Processo “Conheça seu Cliente”:

Trata-se de um conjunto de ações que devem ser adotadas para assegurar a identidade e a atividade dos clientes, bem como a origem e constituição de seu patrimônio e recursos financeiros. Para aqueles que apresentarem maior risco associado a atos ilícitos devem ser aplicados critérios de identificação e diligência mais rigorosos, com a aprovação do relacionamento por nível hierárquico superior.

Serão considerados “clientes”, para os fins desse processo: (a) os **cedentes, coobrigados e fiadores**, nas operações de cessão de créditos; e (b) os **investidores**, nas emissões de CRI realizadas sem participação de coordenador líder. Nas emissões de CRI com participação de coordenador líder, caberá a este a identificação dos investidores que irão subscrever os títulos emitidos.

É proibido o início ou a manutenção de relacionamento com indivíduos ou entidades mencionadas nas listas de sanções financeiras das Nações Unidas (ONU), US Office of Foreign Assets Control (OFAC) e União Europeia e que tenham indícios de práticas terroristas.

O processo “Conheça seu Cliente” (KYC) está descrito na Política “PC 02 – Conheça seu Cliente”.

4.1.2.2 Avaliação da Estrutura das Operações:

A estrutura das operações comerciais apresentadas ao Grupo CIBRASEC será avaliada não apenas no que se refere aos seus aspectos econômicos, mas também, quando possível, no que se refere à destinação dos recursos a serem captados, com o objetivo de tentar identificar situações que podem configurar indícios de ocorrência de lavagem de dinheiro ou financiamento ao terrorismo. Para os casos que requerem atenção especial, como o relacionamento com pessoas expostas politicamente e operações em que não seja possível identificar o beneficiário final, serão adotados procedimentos mais rigorosos de análise.

4.1.2.3 Monitoramento das Transações:

As transações e operações financeiras realizadas pelos clientes, devem ser monitoradas para apuração de situações que podem configurar indícios de ocorrência de lavagem de

dinheiro ou financiamento do terrorismo. Para os casos que requerem especial atenção, como o relacionamento com Pessoas Expostas Politicamente e operações em que não seja possível identificar o beneficiário final, são adotados procedimentos mais rigorosos de análise. O monitoramento considera o perfil, origem e destino dos recursos e a capacidade financeira dos clientes.

A CIBRASEC realiza periodicamente reuniões ("Comitê de Monitoramento") que monitoram as transações realizadas pelos clientes e avalia as situações que podem configurar indícios de ocorrência de lavagem de dinheiro ou financiamento do terrorismo e propõe medidas para aprimorar este monitoramento, caso necessário.

4.1.2.4 Comunicação de Transações Suspeitas aos Órgãos Reguladores:

As operações ou propostas de operações que contenham indícios de ocorrência de lavagem de dinheiro ou financiamento do terrorismo serão comunicadas pela Gerência Jurídica ao Conselho de Controle de Atividades Financeiras (COAF), por meio do "Segmento CVM", em cumprimento às determinações legais e regulamentares.

São exemplos de situações que podem configurar indícios da ocorrência dos crimes previstos na Lei nº 9.613/1998 e que, quando consideradas suspeitas pelo Comitê de Conformidade, devem ser comunicadas ao COAF:

- Realização de operações ou conjunto de operações de compra ou venda de ativos e valores mobiliários que apresentem atipicidade em relação à atividade econômica do cliente ou incompatibilidade com a sua capacidade econômico-financeira;
- Resistência ao fornecimento de informações necessárias para o início de relacionamento comercial ou para a atualização cadastral, oferecimento de informação falsa ou prestação de informação de difícil ou onerosa verificação;
- Apresentação de irregularidades relacionadas aos procedimentos de identificação e registro das operações exigidos pela regulamentação vigente;
- Informação do mesmo endereço comercial por diferentes pessoas jurídicas ou organizações, sem justificativa razoável para tal ocorrência;
- Informação do mesmo endereço residencial ou comercial por pessoas naturais, sem demonstração da existência de relação familiar ou comercial;
- Realização de operações por detentor de procuração ou de qualquer outro tipo de mandato, sem justificativa adequada;
- Representação de diferentes pessoas jurídicas ou organizações pelos mesmos

procuradores ou representantes legais, sem justificativa razoável para tal ocorrência;

- Operações onde o beneficiário final não possa ser identificado;
- Incompatibilidade entre a atividade econômica e o faturamento informados pelo cliente com o padrão apresentado por clientes com o mesmo perfil de risco;
- Indicação, nas operações, de contas que, por sua habitualidade, valor e forma, configurem artifício para burla da identificação da origem, do destino, dos responsáveis ou dos beneficiários finais;
- Operações ou conjunto de operações de compra e venda de títulos e valores mobiliários fora dos padrões praticados no mercado;
- Realização de operações que resultem em elevados ganhos para os agentes intermediários, em desproporção com a natureza dos serviços efetivamente prestados;
- Inclusão, como partes nas operações, de pessoas que reconhecidamente tenham cometido ou intentado cometer atos terroristas ou deles participado ou facilitado seu cometimento.

A legislação em vigor exige, para o caso de não haver sido efetuada nenhuma comunicação de operação suspeita em determinado ano civil, que seja comunicada ao COAF, até o fim de janeiro do ano subsequente, a não ocorrência no ano civil de transações ou propostas passíveis de comunicação (“Declaração Negativa”).

As comunicações de boa-fé não acarretam responsabilidade civil ou administrativa ao Grupo CIBRASEC, nem a seus administradores e demais colaboradores.

4.1.2.5 Manutenção e Guarda de Informações e Registros:

As informações e registros das operações realizadas e dos serviços nelas prestados serão mantidos em sua forma original ou em arquivos eletrônicos, conforme prazos e responsabilidades estabelecidos pela legislação vigente.

Nos termos do disposto no art. 7º, § 5º, da Instrução CVM nº 301/1999, os registros das conclusões acerca de operações ou propostas que fundamentaram a decisão de efetuar, ou não, as comunicações de operações suspeitas, devem ser mantidas pelo prazo de 05 anos ou por prazo superior por determinação expressa da CVM, em caso de processo administrativo.

4.2 Programa de Prevenção e Combate à Corrupção (“PPC”)

O Programa de Prevenção e Combate à Corrupção tem por objetivo estabelecer padrões mínimos de comportamento, exigidos dos administradores, funcionários e demais colaboradores do Grupo CIBRASEC, frente a situações que possam envolver, aparentar ou caracterizar atos de corrupção, como suborno ou outros atos ilícitos ou lesivos à Administração Pública, visando reduzir a exposição do Grupo CIBRASEC, de seus acionistas, administradores e funcionários aos riscos legais de imagem e de reputação decorrentes dessas ações.

Para cumprimento desse objetivo, todos os administradores, funcionários e demais colaboradores do Grupo CIBRASEC estão obrigados a observar, cumprir e fazer cumprir os termos e condições desta política, sem prejuízo do que mais dispuser a Lei nº 12.846/2013 ("Lei Anticorrupção") e demais regulamentos correlatos.

O descumprimento dessa política sujeita os infratores às ações disciplinares cabíveis, incluindo a rescisão do contrato de trabalho, sem prejuízo de outras penalidades ou medidas cabíveis, de acordo com a legislação em vigor.

4.2.1 Conceitos:

Corrupção refere-se à conduta de prometer, oferecer ou dar, direta ou indiretamente, vantagem indevida a agente público.

Suborno é uma forma de corrupção que se caracteriza pelo oferecimento ou aceitação de qualquer tipo de presentes, empréstimos, honorários ou qualquer outra vantagem, com a intenção de induzir determinada pessoa a realizar uma ação ou dela se omitir, de forma indevida, desonesta ou ilegal.

Vantagem indevida é não apenas dinheiro, mas também qualquer coisa de valor ou benefício oferecido a um agente público ou a pessoa a ele relacionada, que possa ser visto como contrapartida da obtenção de alguma forma de favorecimento indevido.

Agente público é qualquer pessoa que trabalhe ou exerça um cargo em um órgão público ou em uma empresa controlada pelo governo, ainda que de forma transitória ou sem remuneração.

4.2.2 Diretrizes gerais:

i. As relações comerciais da CIBRASEC e suas decisões de negócios devem sempre ser

pautadas por fatores comerciais legítimos, tais como preço, qualidade e níveis de serviço, dentre outros inerentes à livre concorrência.

ii. É proibido aos administradores, funcionários e demais colaboradores do Grupo CIBRASEC:

a. oferecer, prometer, fazer, autorizar ou proporcionar, direta ou indiretamente através de terceiros, qualquer vantagem indevida, pagamento, presente ou transferência de qualquer coisa de valor para qualquer pessoa, seja ela agente público ou não, com o objetivo de influenciar ou recompensar qualquer ação oficial ou decisão de tal pessoa em benefício da empresa; e/ou

b. aceitar tais benefícios ou vantagens por parte de pessoas, empresas, prestadores de serviços ou fornecedores com as quais o Grupo CIBRASEC se relacione comercialmente, com o objetivo de descumprir regras estabelecidas para contratação de operações ou serviços.

iii. Nenhum administrador, funcionário ou qualquer outro colaborador do Grupo CIBRASEC será penalizado por atraso ou perda de negócio, venda ou receita, porventura resultantes de sua recusa em oferecer vantagem indevida a agente público ou outra contraparte.

iv. No relacionamento com agentes públicos que atuem na fiscalização e/ou na supervisão das atividades da companhia, é vedado aos administradores, funcionários e demais colaboradores do Grupo CIBRASEC:

a. obstruir a atividade fiscalizatória de tais agentes, seja ocultando, segregando ou manipulando as informações requisitadas no âmbito de processos fiscalizatórios específicos ou ordinários; e/ou

b. buscar, mediante corrupção, promessa ou oferta de vantagem indevida ou qualquer outra forma de influência ou interferência indevidas, resultados artificiais para a fiscalização de que se trate.

v. Será considerada infração a esta política e ao Código de Ética e Conduta da CIBRASEC, o descumprimento destas diretrizes, independentemente de verificação da efetiva obtenção de vantagem ou do resultado pretendido com a conduta adotada.

a. Todo e qualquer descumprimento desta política deverá ser reportado via canal disponível na intranet (compliance@cibrasec.com.br) ou diretamente à administração da companhia;

b. A apuração das infrações à presente política e a imposição das respectivas sanções é de responsabilidade do Comitê de Conformidade da CIBRASEC.

vi. A Gerência Jurídica envidará seus melhores esforços no sentido de assegurar que, nos contratos corporativos relativos às operações da CIBRASEC e à contratação de prestadores de serviços, conste cláusula de adesão expressa da contraparte às diretrizes desta política.

4.2.3 Diretrizes específicas:

4.2.3.1 Pagamento de comissões:

Qualquer pagamento de comissão a terceiros, inclusive os decorrentes de operações contratadas pelo Grupo CIBRASEC, deverá constar dos documentos de aprovação da operação ou do negócio realizado, devendo-se cuidar para que o valor pago seja proporcional à atividade desenvolvida e de acordo com a legislação, quando houver.

4.2.3.2 Patrocínios:

Todas as ações de patrocínio realizadas pelo Grupo CIBRASEC devem ser transparentes, embasadas em contrato adequadamente formalizado, possuir uma finalidade de negócio lícito e ser adequado à compensação oferecida pelo patrocinado. É proibido prometer, oferecer ou efetivar patrocínios com a finalidade de garantir benefícios indevidos para o Grupo CIBRASEC, seus administradores, funcionários ou parceiros.

4.2.3.3 Doações a Partidos Políticos:

É proibido ao Grupo CIBRASEC efetuar doações a partidos ou agentes políticos.

4.2.3.4 Código de Ética e Conduta:

Todos os administradores, funcionários e estagiários do Grupo CIBRASEC estão sujeitos ao cumprimento do Código de Ética e Conduta, registrado como PC 04 “Código de Ética e Conduta”.

4.2.3.5 Processo “Conheça seu Parceiro”:

Trata-se de um conjunto de regras, procedimentos e controles que devem ser adotados para aceitação de parceiros comerciais, incluindo originadores de negócios (“brokers”) e prestadores de serviços, tais como assessores legais, empresas de engenharia e outros

fornecedores de serviços.

O processo “Conheça seu Parceiro” (KYP) está descrito na Política “PC 03 – Conheça seu Parceiro”.

4.2.4 Sinais de alerta e dever de reporte:

Os administradores, funcionários e demais colaboradores do Grupo CIBRASEC devem estar atentos a sinais de alerta, que podem indicar que práticas de corrupção estejam em andamento.

Alguns exemplos de sinais de alerta:

- A comissão ou remuneração da contraparte é incompatível com os serviços prestados, em comparação com o histórico de operações similares;
- Contraparte tem má reputação em relação ao recebimento ou oferecimento de suborno;
- Contraparte é controlada por agente público ou por seus familiares de primeiro grau, ou tem relacionamento próximo com o governo;
- Contraparte foi indicada por um agente público;
- Contraparte se recusa a incluir referência a medidas anticorrupção no contrato;
- Contraparte propõe esquema financeiro incomum, como a solicitação de pagamento em conta bancária em país diferente daquele em que o serviço esteja sendo prestado ou solicitação de pagamento em mais de uma conta bancária;
- Identificação de pagamentos realizados em espécie ou mediante uso de cheque ao portador, ou por meio de benefícios indiretos, identificados como vantagem indevida nessa política;
- Doação para instituição sem fins lucrativos, a pedido de um agente público;
- Um terceiro contratado para representar a companhia perante a administração pública requisita pagamento facilitador ou adiantamento em espécie para despesas não claramente identificadas.

O colaborador tem o dever de comunicar à administração da companhia, imediatamente, através do canal de comunicação mencionado no item 5, abaixo, quaisquer dos sinais de alerta mencionados ou ainda outros, igualmente relevantes, que venha a observar no dia a dia de suas atividades.

Os sinais de alerta não são, necessariamente, provas de corrupção, nem desqualificam

automaticamente a contraparte. Entretanto, levantam suspeitas que devem ser investigadas, assegurando a proteção dos padrões éticos adotados pela CIBRASEC, prevenindo atos de corrupção e preservando sua imagem no mercado.

5. CANAIS DE COMUNICAÇÕES E DENÚNCIAS

O administrador, funcionário ou estagiário do Grupo CIBRASEC que tiver conhecimento de qualquer violação ao Código de Ética e Conduta, aos princípios e diretrizes desta Política ou de qualquer norma interna, deverá comunicar o fato através do canal de comunicação disponível na intranet (compliance@cibrasec.com.br) ou diretamente à administração da companhia.

Administradores e colaboradores não podem praticar atos de retaliação contra aquele que, de boa-fé (i) denunciar ou manifestar queixa, suspeita, dúvida ou preocupação relativas a possíveis violações às diretrizes desta Política; e (ii) fornecer informações ou assistência nas apurações relativas a tais possíveis violações.

Os administradores e colaboradores devem preservar a confidencialidade das informações relativas às apurações de possíveis violações às diretrizes desta Política.
Manifestações anônimas devem ser aceitas pela administração e o anonimato deve ser preservado.

Sanções disciplinares serão aplicadas (i) a administradores ou colaboradores que tentarem ou praticarem retaliação contra quem, de boa-fé, comunicar possíveis violações às diretrizes desta Política; e (ii) a administradores ou colaboradores que, comprovadamente, utilizarem de má-fé ao comunicarem possíveis violações às diretrizes desta Política ou comunicarem fatos sabidamente falsos.

6. TREINAMENTO

O programa de treinamento PLDFT e PPC é contínuo e deve ser aplicado a todos os administradores e colaboradores do Grupo CIBRASEC.

PC 02 – POLÍTICA “CONHEÇA SEU CLIENTE” (KYC)

1. Objetivo

Esta política tem por objetivo orientar os colaboradores do Grupo Cibrasec quanto aos cuidados a serem tomados na identificação dos clientes envolvidos em suas operações, visando atender os princípios gerais estabelecidos na Política Corporativa de Prevenção e Combate à Lavagem de Dinheiro, ao Financiamento do Terrorismo e à Corrupção (“PLDFT/PC”).

2. Áreas de aplicação

Esta política se aplica a todas as operações comerciais que venham a ser contratadas pelo Grupo Cibrasec.

3. Definição

São considerados “clientes”, para os fins desta Política: (a) os cedentes, coobrigados e fiadores, nas operações de cessão de créditos; e (b) os investidores, nas emissões de CRI realizadas sem participação de coordenador líder.

Nas emissões de CRI com participação de coordenador líder, caberá a este a identificação dos investidores que irão subscrever os títulos emitidos.

4. Processo de consulta

O processo de identificação e de coleta de informações acerca dos clientes interessados em operar com o Grupo CIBRASEC será realizada, preponderantemente, por consulta aos setores de crédito e risco das instituições que participam do seu controle acionário.

O **Comitê de Risco e Tesouraria**, vinculado ao Conselho de Administração da CIBRASEC, indicará periodicamente as instituições acionistas que integrarão o grupo de consulta, para essa finalidade.

O objeto da consulta será centrado nos clientes e na existência, nas instituições consultadas, de eventuais restrições à contratação de operações comerciais com os mesmos, e não no mérito das operações propostas, cuja aprovação seguirá os ritos e alçadas estabelecidos nas políticas

operacionais em utilização no Grupo CIBRASEC.

A consulta aqui mencionada será de responsabilidade da Gerência de Estruturação e Risco da CIBRASEC e deverá preceder o início da análise de qualquer operação proposta.

5. Ficha Cadastral

Todos os clientes do Grupo CIBRASEC, com operações aprovadas, deverão ter ficha cadastral atualizada, contendo, no mínimo, as informações e os documentos indicados a seguir:

5.1 Pessoa Natural

a) nome completo, sexo, data de nascimento, naturalidade, nacionalidade, estado civil, filiação e nome do cônjuge ou companheiro;

b) natureza e número do documento de identificação, nome do órgão expedidor e data de expedição;

c) número de inscrição no Cadastro de Pessoas Físicas (CPF/MF);

d) endereço completo (logradouro, complemento, bairro, cidade, unidade da federação e CEP), número de telefone e endereço eletrônico para correspondência; e

e) ocupação profissional, entidade para a qual trabalha e informações sobre os rendimentos e situação patrimonial; **5.1.1.** O cadastro deverá conter (i) a assinatura do cliente; (ii) a data de sua atualização; e (iii) ser acompanhado dos seguintes documentos: RG, comprovante de residência ou domicílio; procuração e documento de identidade do procurador (se houver).

5.2 Pessoa Jurídica

a) denominação ou razão social;

b) nomes e CPF (ou razão social e inscrição no CNPJ) dos controladores diretos, administradores e procuradores;

c) número de identificação do registro empresarial (NIRE) e no Cadastro Nacional de Pessoa Jurídica (CNPJ);

d) endereço completo (logradouro, complemento, bairro, cidade, unidade da federação e CEP), número de telefone e endereço eletrônico para correspondência;

e) atividade principal desenvolvida;

f) informações acerca da situação patrimonial e financeira respectiva, com faturamento médio mensal dos últimos doze meses; e

g) denominação ou razão social de pessoas jurídicas controladoras, controladas ou coligadas.

5.2.1. O cadastro deverá conter (i) a assinatura do cliente; (ii) a data de sua atualização; e (iii) ser acompanhado dos seguintes documentos: CNPJ, documento de constituição da pessoa

jurídica devidamente atualizado e registrado no órgão competente; atos societários que indiquem os administradores da pessoa jurídica; e, quando for o caso, procuração e documento de identidade do procurador.

5.3 Nas demais hipóteses (Fundos de Investimentos, Sociedades Anônimas de Capital Aberto e Pulverizado, etc.)

a) identificação completa dos clientes e de seus representantes e/ou administradores; e
b) informações acerca da situação patrimonial e financeira respectiva.

5.3.1. O cadastro deverá conter (i) a assinatura do cliente e (ii) a data de sua atualização.

5.4. Investidores não residentes: para esses clientes, o cadastro deverá adicionalmente conter:

a) os nomes das pessoas naturais autorizadas a emitir ordens e, conforme o caso, dos administradores da instituição ou responsáveis pela administração da carteira; e
b) os nomes do representante legal e do responsável pela custódia dos seus valores mobiliários.

5.5. Em todos os casos: do cadastro deverá constar declaração, datada e assinada pelo cliente ou, se for o caso, por procurador legalmente constituído, de que:

a) são verdadeiras as informações fornecidas para o preenchimento do cadastro;
b) o cliente se compromete a informar, no prazo de 10 (dez) dias, quaisquer alterações que vierem a ocorrer nos seus dados cadastrais, inclusive eventual revogação de mandato, caso exista procurador; e
c) o cliente não está impedido de operar no mercado de valores mobiliários;

5.5.1. Do cadastro também deve constar declaração firmada e datada pelo cliente ou, se for o caso, por procurador legalmente constituído, sobre os propósitos e a natureza da relação de negócio com a instituição.

5.6. Manutenção dos dados da ficha cadastral

Os clientes deverão comunicar, de imediato, quaisquer alterações nos seus dados cadastrais. Os clientes com operações ativos devem atualizar seus dados cadastrais em períodos não superiores a 24 meses.

6. Identificação de pessoas consideradas expostas politicamente (PPE)

O Grupo CIBRASEC deve supervisionar, de maneira mais rigorosa, a relação de negócios mantida com pessoa exposta politicamente e dedicar especial atenção a propostas de início de relacionamento e a operações executadas com pessoas expostas politicamente oriundas de países com os quais o Brasil possua elevado número de transações financeiras e comerciais, fronteiras comuns ou proximidade étnica, linguística ou política.

O início de relacionamento e a realização de operações que envolvam pessoas expostas politicamente dependerão de prévia autorização do Comitê de Risco e Tesouraria. Essa autorização será necessária mesmo em caso de já existir operação anterior vigente com a pessoa objeto da solicitação.

6.1. Definição de Pessoas Expostas Politicamente:

I - Aquela que desempenha ou tenha desempenhado, nos últimos 5 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 seu relacionamento próximo.
II - Ocupantes de cargo, emprego ou função pública relevante, exercido por chefes de estado e de governo, políticos de alto nível, altos servidores dos poderes públicos, magistrados ou militares de alto nível.
III - Dirigentes de empresas públicas ou dirigentes de partidos políticos; e
IV - Familiares da pessoa exposta politicamente, seus parentes, na linha direta, até o primeiro grau, assim como o cônjuge, companheiro e enteado.

O prazo de 5 (cinco) anos referido no inciso I deve ser contado, retroativamente, a partir da data de início da relação de negócio ou da data em que o cliente passou a se enquadrar como pessoa exposta politicamente.

Sem prejuízo das definições anteriores são consideradas, no Brasil, pessoas expostas politicamente:

- Os detentores de mandatos eletivos dos Poderes Executivo e Legislativo da União;
- 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,

• Os ocupantes de cargo em empresas públicas ou sociedades de economia mista, do grupo de direção e assessoramento superiores -, nível 6, e equivalentes;

• Os membros do Conselho Nacional de Justiça, do Supremo Tribunal Federal e dos tribunais superiores;

• 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;

• Os membros do Tribunal de Contas da União e o Procurador-Geral do Ministério Público junto ao Tribunal de Contas da União;

• Os Governadores de Estado e do Distrito Federal, os Presidentes de Tribunal de Justiça, de Assembleia Legislativa e de Câmara Distrital e os Presidentes de Tribunal e de Conselho de Contas de Estados, de Municípios e do Distrito Federal; e

• Os Prefeitos e Presidentes de Câmara Municipal de capitais de Estados.

7. Guarda das informações

A guarda das informações dos clientes deve ser efetuada por período mínimo de 5 (cinco) anos, a contar da última transação realizada em nome do respectivo cliente, podendo este prazo ser estendido na hipótese de investigação comunicada formalmente pela CVM.

8. Monitoramento

O monitoramento do fiel cumprimento desta Política cabe à Gerência de Estruturação e Risco.

9. Atualização

A responsabilidade de atualização e revisão destas políticas é da Gerência de Estruturação e Risco.

PC 03 – POLÍTICA "CONHEÇA SEU PARCEIRO" (KYP)

1 Objetivo

Esta política tem por objetivo estabelecer um conjunto de regras, procedimentos e controles que devem ser adotados para identificação e aceitação de parceiros comerciais, incluindo originadores de negócios ("brokers") e prestadores de serviços, tais como assessores legais, empresas de engenharia e outros fornecedores de serviços, visando prevenir a realização de negócios com

contrapartes inidôneas ou suspeitas de envolvimento em atividades ilícitas.

Esta política objetiva, também, garantir que a relação da CIBRASEC com seus parceiros comerciais e fornecedores de bens e serviços obedeça aos princípios de legalidade, impessoalidade, moralidade, eficiência, isonomia, probidade administrativa e diretrizes estabelecidas em seu Código de Ética e Conduta, preservando a imagem e a reputação da empresa.

2 Abrangência

Esta política se aplica a todos os colaboradores da CIBRASEC.

3 Diretrizes

3.1 Cadastro: todos os parceiros comerciais e fornecedores da CIBRASEC deverão ter ficha cadastral atualizada, contendo no mínimo as seguintes informações:

i. Pessoas naturais:

a. Nome completo, sexo, data de nascimento, naturalidade, nacionalidade e estado civil.
b. Natureza e número do documento de identificação, órgão expedidor e data de expedição.
c. Endereço completo, número de telefone e endereço eletrônico para correspondência.
d. Ocupação profissional e entidade para a qual trabalha.
e. O cadastro deverá conter (i) assinatura do cadastrado; (ii) data de sua última atualização; e ser acompanhado de pelo menos um documento de identidade e comprovante de residência ou domicílio.

ii. Pessoas jurídicas:

a. Denominação ou razão social.
b. Nomes e CPF (ou razão social e inscrição no CNPJ) dos controladores diretos, administradores e procuradores.
c. Número de identificação do registro empresarial (NIRE) e do Cadastro Nacional de Pessoa Jurídica (CNPJ).
d. Endereço completo, número de telefone e endereço eletrônico para

correspondência.

e. Atividade principal desenvolvida.

f. O cadastro deverá conter (i) assinatura do representante legal do cadastrado; (ii) data de sua última atualização; e ser acompanhado de pelo menos (a) documento de constituição da pessoa jurídica, devidamente atualizado e registrado no órgão competente; (b) atos societários que indiquem os seus administradores; e (c) quando for o caso, procuração e documento de identidade do procurador.

3.2 Processo de certificação: para início do efetivo relacionamento comercial ou a cada renovação de contrato com o fornecedor, deverão ser adotadas as seguintes providências:

a. **Jurídico e área de Riscos** deverão efetuar levantamentos, via os meios legalmente autorizados, buscando identificar existência de indícios ou eventos que caracterizem atos de lavagem de dinheiro, corrupção ou tentativa de corrupção, entre outros atos criminosos, bem como situação creditícia inadequada, referentes ao parceiro comercial, fornecedor, administradores dessas organizações ou empresas ligadas.

b. Em se tratando de fornecedor, a **área técnica responsável pela contratação** deverá levantar informações sobre o desempenho desse fornecedor junto a outros clientes, bem como informações que permitam avaliar a qualidade dos serviços por ele prestados ou bens por ele fornecidos.

c. Todas as informações obtidas, assim como suas conclusões, devem fazer parte do cadastro do parceiro comercial / fornecedor.

d. Os fornecedores considerados **críticos para a atividade da CIBRASEC**, conforme definição de sua administração, devem ser acompanhados permanentemente pelas áreas de contratação, jurídica e riscos, de forma a verificar potenciais evoluções nas condições desses fornecedores que possam representar ameaça à CIBRASEC e/ou às operações gerenciadas pela companhia.

e. **O cadastro deve ser atualizado** anualmente ou (i) no caso de parceiros comerciais, a cada nova operação contratada; e (ii) no caso de fornecedores, a cada renovação do contrato de fornecimento de bens ou serviços. Considerando a criticidade e características do fornecedor, poderá ser definidas pela administração periodicidade inferior às aqui estabelecidas.

3.3 Contratação: do contrato firmado com o fornecedor, ou em seus anexos, deverá constar que

o mesmo tem e faz respeitar políticas e processos para:

a. Garantir em suas atividades o respeito às leis, ao comportamento ético com seus clientes e respeito ao meio ambiente.
b. Gerenciar os aspectos relativos à Prevenção à Lavagem de Dinheiro (Lei nº 9.613/98) e às práticas de Prevenção e Combate à Corrupção (Lei nº 12.846/13).
c. Repudiar, não tolerar e não utilizar trabalho infantil, escravo ou em condições degradantes, bem como práticas disciplinares abusivas em seus processos produtivos.
d. Garantir o cumprimento da legislação ambiental aplicável a suas atividades e serviços.
e. Garantir o respeito às leis trabalhistas.
f. Preservar as informações estratégicas e de caráter reservado, fornecidas pela CIBRASEC, exceto em caso de determinação judicial.
g. Garantir a segurança dos dados e informações da CIBRASEC, divulgando-as, em caso de necessidade, somente com expresso consentimento da área gestora do processo.

3.4 Gestão: todo fornecedor deverá ter uma área técnica da CIBRASEC responsável pelo acompanhamento de suas atividades.

O descumprimento comprovado dos princípios estabelecidos nessa política sujeitará o fornecedor à aplicação das sanções administrativas previstas nos instrumentos contratuais, sem prejuízo de eventuais sanções civis e criminais, legalmente estabelecidas.

PC 04 – CÓDIGO DE ÉTICA E CONDUTA

1 - Objetivo:

Este Código de Ética e Conduta (Código) orienta as relações dos administradores, funcionários e estagiários do Grupo CIBRASEC e os auxilia a tomar decisões e no modo de conduzir os negócios dentro e fora do Grupo (Instituição), com colegas, clientes, investidores, fornecedores, prestadores de serviços e competidores. Cada um dos funcionários e demais colaboradores tem a responsabilidade de zelar para que este Código seja sempre cumprido.

2 - Áreas de aplicação:

Todas as áreas, administradores, funcionários, estagiários e demais colaboradores do Grupo CIBRASEC.

3 - Regras e definições:

3.1 - Introdução

O Código deve ser rigorosamente seguido, sendo aplicável a todos os administradores, funcionários, estagiários e quaisquer outros colaboradores do Grupo CIBRASEC. A não observância a qualquer das previsões contidas no presente poderá resultar em ações disciplinares, incluindo a rescisão do contrato de trabalho ou de outro relacionamento com o Grupo CIBRASEC (ver capítulo 3.2 – Violações).

O Código não tem por objetivo cobrir todas as situações possíveis, tampouco todas as normas e políticas a elas aplicáveis. Os colaboradores devem utilizar seu bom senso como guia, sempre embasados nos princípios de conduta aqui relacionados. Em caso de situações não previstas nesta ocasião ou demais dúvidas, vide capítulo 3.12 – Contatos.

O Código de nenhuma forma constitui direito ou benefício adicional aos colaboradores, tampouco a garantia de continuidade de vínculo com a Instituição. Ademais, o presente instrumento não representa um contrato de trabalho ou de prestação de serviços.

Este Código poderá ser atualizado a qualquer tempo, com ou sem aviso prévio. A última versão do Código, assim como demais materiais de suporte e políticas a ele relacionadas, estará sempre disponível para consulta no Diretório “Normas e Políticas” da Instituição. O colaborador tem a obrigação de utilizar sempre a última versão deste Código para os fins necessários.

3.2 - Violações

Todos os colaboradores são obrigados e encorajados pela Instituição a reportar à Administração qualquer violação efetiva ou suspeita de violação ao Código ou a demais políticas internas e regulamentações aplicáveis. Tal comunicação será tratada com absoluta confidencialidade e poderá ser enviada através do canal de comunicação disponível na intranet (compliance@cibrasec.com.br) ou diretamente à administração da companhia, não sendo necessária a identificação do seu autor, caso este assim desejar. (ver capítulo 3.12 – Contatos).

Falhas na observação das regras estabelecidas neste Código e das demais regulamentações externas aplicáveis aos seus negócios dentro da Instituição serão levadas ao conhecimento do Comitê de Conformidade, podendo acarretar medidas disciplinares, que incluem a rescisão do contrato de trabalho ou de qualquer outro relacionamento com a Instituição.

As violações ao Código podem cumulativamente violar normas legais aplicáveis à matéria, caso em que os colaboradores e a própria Instituição estarão sujeitos a punições cíveis e/ou criminais.

A Instituição em nenhuma hipótese será conivente com qualquer ato que possa violar leis e demais normas em vigor por parte de seus colaboradores.

3.3 - Comitê de Conformidade

A Instituição mantém um Comitê de Conformidade ("Comitê"), que possui as seguintes responsabilidades:

- Deliberar, acompanhar e discutir as estratégias, políticas e medidas adotadas para difundir a cultura de conformidade e controles internos;
- Analisar e discutir efetivos e potenciais conflitos de interesses, assim como eventuais falhas nos controles internos;
- Discutir a exposição a riscos regulatórios e de imagem referentes a novos produtos, operações e clientes; e
- Deliberar sobre a aplicação de sanções às violações do Código.

São membros do Comitê de Conformidade (a) os Diretores Estatutários da Instituição; e (b) os Gerentes de Estruturação e Risco, Jurídico e Controladoria. Considerar-se-á impedido de participar o membro do Comitê em reunião destinada a examinar ato, direto ou indireto, de sua responsabilidade.

3.4 - Responsabilidade dos Gestores

Os gestores são responsáveis pelas suas ações e por supervisionar as ações de seus subordinados. Assim, estes têm maior responsabilidade no cumprimento dos padrões de conduta determinado no Código. É esperado que todos os gestores sirvam como modelo de conduta, em linha com os padrões morais e éticos da Instituição, para todos de sua equipe.

Em se tratando de situações conflituosas ou de condutas ilegais, ainda que em potencial, ou quando receber informação efetiva a respeito de possível conduta ilegal, o gestor deverá imediatamente analisar a conduta, informando a respectiva ocorrência ao Comitê de Conformidade, para que uma decisão possa ser tomada sobre a necessidade, ou não, de uma investigação interna formal e, em última instância, da aplicação de medidas disciplinares.

Os gestores também são responsáveis por evitar reincidências de violação, alterando os procedimentos estabelecidos das atividades sob sua responsabilidade, na medida do necessário.

A administração da Instituição prestará auxilio no desempenho das responsabilidades indicadas acima, inclusive no desenvolvimento dos procedimentos de supervisão necessários.

Os gestores devem garantir que os membros de sua equipe estejam atualizados em relação às exigências legais e regulamentares. Ademais, estes deverão monitorar e assegurar o comparecimento dos membros de sua equipe às sessões de treinamento de conformidade.

Além das responsabilidades acima, cumpre ao gestor:

- Assegurar a aderência de sua área e de seus colaboradores às normas externas e internas que lhe são aplicáveis;
- Fortalecer e divulgar a cultura de Controles Internos e Conformidade;
- Disseminar os conceitos éticos e morais da Instituição;
- Corretamente identificar, implantar procedimentos de controle, monitorar e mitigar todos os riscos das atividades de responsabilidade da área;
- Reportar ao Comitê de Conformidade, tempestivamente, ocorrências e/ou fatos relevantes relativos ao não cumprimento de normas internas ou externas, assim como dilemas éticos;
- Avaliar os impactos das normas dos órgãos reguladores;
- Garantir que os colaboradores tenham acesso tempestivo e oportuno à legislação e normativos internos;
- Acompanhar e cobrar a regularização das ocorrências apontadas em quaisquer processos internos; e
- Zelar pela integridade das barreiras de informação, garantindo a segregação física, lógica e de conduta entre as áreas e impedindo o fluxo indevido de informações confidenciais e privilegiadas.

3.5 - Confidencialidade de Informações

No exercício de suas atividades, a Instituição e seus colaboradores têm acesso a informações confidenciais e públicas. A confidencialidade pode decorrer de uma previsão legal ou contratual, ou ainda, de relações que a Instituição mantenha com seus clientes – sejam creditícias, societárias, de investimento ou de outra natureza. Todos os colaboradores, em qualquer nível hierárquico, são responsáveis por salvaguardar as informações confidenciais, independente da forma com que sejam adquiridas.

Informações confidenciais: todas e quaisquer informações cujo conhecimento irrestrito ou divulgação possa acarretar danos, independentemente do meio ou forma de transmissão.

Informações privilegiadas: são aquelas confidenciais e de natureza relevante, ainda não divulgadas ao mercado, capazes de propiciar ao seu detentor, ou terceiro, vantagem indevida na negociação de valores mobiliários. Essas informações podem, ainda, alterar ou influenciar a cotação de valores mobiliários ou a decisão de investidores. Incluem-se nesse conceito as informações relativas a operações de mercado de capitais, tais como emissão de valores mobiliários, de dívida ou de ações, bem como fusões e aquisições.

Aos colaboradores é vedado, mesmo após o término do contrato de trabalho ou outras formas de relacionamento com a Instituição, direta ou indiretamente, usar ou divulgar as informações confidenciais a que tenham acesso por seu vínculo com a Instituição, exceto se permitido pelo Código ou expressa e previamente autorizado.

3.5.1. Comunicações externas

É vedado aos colaboradores emitir qualquer tipo de declaração, comentário ou divulgação à imprensa, fóruns públicos e/ou qualquer meio de comunicação (incluindo, mas não se limitando a, *podcasts*, *webcasts*, salas de bate-papo, *blogs*, dentre outros), em nome próprio ou em nome da Instituição:

- que sejam obtidos pelo seu vínculo com a Instituição;
- sobre os negócios da Instituição;
- tocante às suas responsabilidades ou experiências dentro da Instituição; ou
- que possam ser associados à Instituição.

3.6. Conflitos de Interesse

Todo colaborador da Instituição deve basear suas decisões e ações visando o interesse desta, evitando, portanto, possíveis e potenciais conflitos de interesse. Estes conflitos surgem quando os interesses pessoais do colaborador interferem ou aparentam interferir, não importando a maneira, com os da Instituição, de seus clientes ou ainda com aqueles de colaboradores de outras áreas.

Os conflitos podem afetar nossos julgamentos e decisões como colaboradores da Instituição, podendo consequentemente ameaçar a reputação e negócios desta. Assim, todo conflito, ainda que aparente, deve ser refutado.

A título ilustrativo seguem os principais exemplos de conflitos:

Posição Corporativa: obter vantagens pessoais através do seu relacionamento com a Instituição ou se valer deste para obter tal vantagem. O colaborador também não poderá receber tratamento preferencial de fornecedores, prestadores de serviços ou clientes, sem antes se reportar ao Comitê de Conformidade, a não ser que tal tratamento preferencial esteja disponível nos mesmos termos a todas as pessoas em situação similar. (ex.: convênio com empresas aéreas, restaurantes, escolas, etc.).

Entre Colaboradores: os relacionamentos pessoais entre colaboradores não podem interferir na sua capacidade de buscar sempre o melhor para a Instituição e seus clientes. São vedados, sem a prévia autorização do Comitê de Conformidade, vínculos financeiros como a contratação de empréstimos ou prestação de garantias entre colaboradores e com familiares destes.

Atividade externa: as atividades externas dos colaboradores não podem interferir nas suas funções, performance e responsabilidades dentro da Instituição, tampouco conflitar, ainda que aparentemente ou potencialmente, com os interesses desta. O colaborador deve estar alerta para esses conflitos e estar ciente que poderá ser solicitado a descontinuar tal atividade, sem qualquer tipo de indenização ou reembolso. A regra vale ainda para atividades desempenhadas para Organizações Não Governamentais (ONGs), entre outras formas de associação, assim como outras atividades não remuneradas.

A Gerência de Controladoria deverá manter uma base de dados com registro das atividades externas dos colaboradores.

Assim, todos devem, ao iniciar suas funções na Instituição, informar a área via e-mail (compliance@cibrasec.com.br) sobre tais atividades. Qualquer início no exercício de uma atividade externa durante seu vínculo com a Instituição, ou alteração no status de uma já declarada, deverá ser prontamente informado ao Comitê de Conformidade pelo mesmo canal. Na comunicação, o colaborador deverá informar: entidade contratante ou para qual exerce a atividade; descrição das funções; horário de exercício das atividades e remuneração (se houver).

Não precisam ser declaradas as atividades beneficentes, não remuneradas e sem vínculo contratual, desde que não conflitantes com as atividades fins da Instituição.

3.7. Propriedade Intelectual

São de propriedade intelectual da Instituição quaisquer materiais, modelos, produtos ou serviços que sejam criados durante a jornada de trabalho, produzidos por seus colaboradores, por meio

dos recursos ou ativos da Instituição. Qualquer colaborador que se apropriar, copiar ou enviar a terceiros propriedade intelectual da Instituição, sem o consentimento formal do Comitê de Conformidade, pode responder civil e criminalmente por tal fato.

3.8. Tratamento Equitativo

A boa imagem da Instituição é pautada pela construção de bons relacionamentos, guiados pela honestidade, integridade e tratamento ético, assim como confiança mútua. Todos os colaboradores devem tratar com imparcialidade os clientes, fornecedores, concorrentes, assim como os demais colaboradores. Nenhum colaborador deve obter vantagem sobre os demais, seja para benefício próprio ou de terceiros, por meio de manipulação, encobrimento, abuso de informações confidenciais, distorção de fatos materiais ou outras práticas desonestas.

3.9. Operações com Valores Mobiliários de Emissão da Instituição

Em cumprimento ao que dispõe o art. 11, caput, e parágrafo 4º da Instrução CVM 358/02, os Diretores, os membros do Conselho de Administração e de quaisquer órgãos com funções técnicas e consultivas, criados por disposição estatutária, ficam obrigados a comunicar à Instituição a quantidade, as características e a forma de aquisição dos valores mobiliários de sua emissão, de que sejam titulares.

Incluem-se nessa obrigação todos os ocupantes dos cargos de Gerência, em razão de sua participação como membros do Comitê de Crédito da Instituição.

A comunicação deverá ser efetuada pelo canal de comunicação (compliance@cibrasec.com.br) no prazo de 5 (cinco) dias após a realização de cada negócio e/ou no primeiro dia útil após a investidura no cargo.

Consoante o disposto no parágrafo 2º do art. 11 da Instrução acima mencionada, a comunicação aqui tratada deve ser efetuada, inclusive, para valores mobiliários que sejam de propriedade do cônjuge do qual o informante não esteja separado judicialmente, de companheiro ou de qualquer dependente incluído em sua declaração anual de rendimentos.

3.9.1. Restrições às operações com valores mobiliários de emissão da Instituição:

Nenhum Colaborador poderá:

• realizar suas operações utilizando-se de informações confidenciais obtidas por meio de ou

sobre clientes, resultante do seu trabalho na Instituição, tampouco de informações privilegiadas, não importando a sua fonte;

• participar de qualquer transação que possa, de alguma forma, comprometer sua solvência e/ou credibilidade ou prejudicar a reputação da Instituição;

• usar sua posição dentro da Instituição ou o nome desta a fim de obter quaisquer benefícios pessoais;

• no caso de ordens concomitantes, executar ordem própria ou de outros colaboradores antes da ordem de um cliente.

3.9.2. Sanções legais pela negociação com informações privilegiadas:

Colaboradores de posse de informação material não-pública (*insider information*), referente aos negócios ou situação de uma companhia, não devem operar (*insider trading*) nem induzir outros a operarem valores mobiliários dessa companhia se tal negociação for violar uma obrigação ou se a informação tiver sido indevidamente apropriada. As informações privilegiadas precisam ser mantidas em sigilo por todos que a acessem, seja em função da prática da atividade profissional ou do relacionamento pessoal.

Os colaboradores que tiverem acesso a uma informação privilegiada, relacionada a cliente ou operação da Instituição, deverão transmiti-la ao Comitê de *Compliance* da Cibrasec, não podendo comunicá-la a ninguém, nem mesmo a outros membros da empresa, profissionais de mercado, amigos e parentes, e nem mesmo usá-la em seu próprio benefício ou de terceiros. Se não houver certeza quanto ao caráter privilegiado da informação, deve-se relatar o ocorrido ao Comitê de *Compliance*. Aquele que tiver acesso a uma informação privilegiada deverá reduzir ao máximo a circulação de documentos e arquivos com tal informação.

Uma informação é material se a abertura de tal informação for, aparentemente, causar impacto no preço do ativo ou se interessaria a investidores racionais ter conhecimento desta informação antes de efetuar uma decisão de investimento.

Uma informação é não-pública até que seja disseminada ao mercado em geral (em oposição a um seleto grupo de investidores) e investidores tenham a oportunidade de reagir à informação. Nesse sentido, analisar a Instrução CVM 358, artigo 11.

No Brasil, o "*insider trading*", como ilícito, está nitidamente caracterizado na legislação, especialmente no art. 155 da Lei nº 6.404/76. Além disto, porém, tendo em vista que o "*insider trading*" é ato ilícito, outros dispositivos genéricos de nossa legislação, que ora protegem o mercado de valores mobiliários em geral, visando proteção patrimonial dos indivíduos e

segurança social, são hábeis para enquadrar, e consequentemente penalizar, o "*insider trading*".

Insider trading é qualquer operação realizada por um "*insider*" com valores mobiliários de emissão da companhia, e em proveito próprio, pessoal.

A utilização de informação privilegiada na negociação de valores mobiliários é crime no Brasil, sujeito à pena de 1 (um) a 5 (cinco) anos de reclusão, cumulada com multa de até 3 (três) vezes a vantagem econômica obtida. A CVM (Comissão de Valores Mobiliários) poderá inabilitar o acusado para atuação no mercado por até 20 (vinte) anos. Além disto, quem negociar com base em informação privilegiada poderá ser condenado civilmente a indenizar as pessoas que com ele tiverem negociado de boa-fé, sem ter posse da informação.

A CVM pune terceiros (banqueiros de investimento, advogados, assessores, prestadores de serviços, etc.) que obtiveram informações no exercício de suas atividades e não se abstiveram de negociar valores mobiliários com base nestas. A CVM tem entendido que não existe presunção de intenção de obter ganho ilícito, ao contrário do que ocorre com os *insiders* (administradores e outras pessoas que trabalham na companhia). Mas a CVM tem considerado suficiente à condenação a presença de indícios de que a negociação visava ao aproveitamento da oportunidade gerada pela informação privilegiada.

3.10. Tecnologia de Informação

Telefones, correio eletrônico, sistemas de informática e demais equipamentos de comunicação eletrônica fornecidos pela Instituição para o exercício de suas funções, independentemente de onde se encontram, são de propriedade desta. Estes equipamentos devem ser usados para fins profissionais, não podendo infringir nenhuma regulamentação ou política interna aplicável a tal uso. É permitido o uso de tais equipamentos para fins pessoais, desde que em caráter eventual e limitado, devendo este uso ser consistente com as previsões do presente Código e demais políticas aplicáveis.

A Instituição considera que todos os dados e comunicações, transmitidos através de, recebidos por, ou contidos nos seus equipamentos eletrônicos de comunicação, são de sua propriedade.

Estes dados estão sujeitos às regulamentações e políticas internas aplicáveis e a Instituição se reserva o direito de monitorar, rever e torná-los públicos, se isso for necessário. Nenhum colaborador deve esperar privacidade ao se utilizar de tais meios de comunicação.