

# Manual de Operações

---

Código de Ética, Manual de Compliance,  
Plano de Continuidade de Negócios e  
Políticas aplicáveis a todos colaboradores  
da Moat Capital

**Versão Atualizada**

**29 – JAN - 19**

## Índice

CÓDIGO DE ÉTICA.....	2
DIRETORIA DE COMPLIANCE .....	6
PROCEDIMENTOS DISCIPLINARES (ENFORCEMENT).....	10
POLÍTICA DE COMBATE E PREVENÇÃO A LAVAGEM DE DINHEIRO E FINANCIAMENTO AO TERRORISMO (PLDFT).....	11
POLÍTICAS DE SEGREGAÇÃO DE ATIVIDADES .....	16
POLÍTICA DE CONFIDENCIALIDADE .....	17
POLÍTICA DE TREINAMENTO E CERTIFICAÇÕES.....	20
DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO .....	22
PLANO DE CONTINGÊNCIA E CONTINUIDADE DOS NEGÓCIOS.....	30
POLÍTICA DE INVESTIMENTOS PESSOAIS .....	44
TERMO DE RESPONSABILIDADE E ADESÃO AO MANUAL DE OPERAÇÕES (ANEXO I).....	48
DECLARAÇÃO ANUAL DE INVESTIMENTOS (ANEXO II) .....	50

## CÓDIGO DE ÉTICA

### Princípios à conduta do Colaborador

- I. Agir com integridade, competência, diligência, respeito e de maneira ética com o público, clientes, possíveis clientes, empregadores, funcionários, colegas de profissão, como também outros participantes dos mercados globais de capitais. Colocar a integridade da categoria de profissionais da área de investimentos e os interesses dos clientes acima dos seus interesses pessoais.
- II. Agir com cautela razoável e exercer discernimento profissional independente ao conduzir análises de investimentos, fazer recomendações sobre investimentos, tomar decisões de investimento e envolver-se em outras atividades profissionais.
- III. Exercer a profissão e incentivar outras pessoas a fazer o mesmo de maneira ética e profissional, que nos trará crédito pessoal e profissionalmente.
- IV. Promover a integridade e defender as regras que regem os mercados de capitais.
- V. Manter e aprimorar a competência profissional e empenhar-se para manter e aprimorar a competência de outros profissionais da área de investimentos.

### Padrões de Conduta

#### I. PROFISSIONALISMO

- a. Conhecimento da legislação. Os colaboradores devem entender e estar em conformidade com todas as leis, regras e regulamentos vigentes de qualquer governo, organização normativa, órgão de licenciamento ou associação profissional que possa controlar as suas respectivas atividades profissionais. Em caso de conflito, os colaboradores devem cumprir as mais rigorosas leis, regras ou regulamentos. Os colaboradores não devem, conscientemente, participar, auxiliar e devem-se desassociar de qualquer violação de tais leis, regras ou regulamentos.
- b. Independência e objetividade. Os colaboradores devem usar cautela e discernimento razoáveis para atingir e manter a independência e a objetividade de suas respectivas atividades profissionais. Os colaboradores não devem oferecer, solicitar, nem aceitar nenhum presente, benefício, remuneração ou pagamento que, de maneira razoável, possa comprometer as suas independência e objetividade ou as de outra pessoa.
- c. Apresentação incorreta. Os colaboradores não devem fazer, conscientemente, nenhuma apresentação incorreta relacionada com a análise de investimentos, recomendações, ações ou outras atividades profissionais.
- d. Conduta inadequada. Os colaboradores não devem se envolver em nenhuma conduta profissional que envolva desonestidade, fraude, enganar terceiros ou cometer qualquer ato que reflita de maneira contrária à sua reputação, integridade ou competência profissional.

## II. INTEGRIDADE DOS MERCADOS DE CAPITAIS

### a. Informações relevantes não divulgadas ao público.

Os colaboradores que possuem informações relevantes não divulgadas ao público, que poderiam afetar o valor de um investimento (“informação privilegiada”), não devem agir nem fazer com que outros indivíduos ajam com base nessas informações.

### b. Manipulação do mercado.

Os colaboradores não devem se envolver em práticas que alterem preços ou aumentem artificialmente o volume de negócios com a intenção de enganar os participantes do mercado.

## III. DEVERES PARA COM OS CLIENTES

a. A distribuição de quotas dos fundos de investimento sob gestão da MOAT será realizada por instituições devidamente habilitadas, que também serão responsáveis pela aplicação da política de Conheça seu Cliente (KYC) aos Clientes.

b. Lealdade, prudência e zelo. Os colaboradores têm um dever de lealdade para com seus clientes: devem usar cautela e discernimento razoáveis. Os colaboradores devem agir para o benefício de seus clientes e colocar os interesses deles acima de seus próprios interesses ou dos interesses do seu empregador.

c. Tratamento justo. Os colaboradores devem tratar de maneira justa e objetiva todos os clientes ao apresentarem análise de investimentos, fazerem recomendações de investimentos, tomarem uma decisão em relação a um investimento ou se envolverem em outras atividades profissionais.

d. Adequação dos Investimentos.

i. Quando os colaboradores estiverem em um relacionamento de consultoria de investimentos com um cliente, devem:

1. Conduzir uma investigação razoável em relação à experiência que o cliente (ou o provável cliente) tem a respeito de investimentos, objetivos de risco e retorno e restrições financeiras antes de fazer quaisquer recomendações de investimento ou tomar uma decisão de investimento e reavaliar e atualizar tais informações periodicamente.

2. Determinar se o investimento é adequado à situação financeira do cliente e coerente com os objetivos, resoluções e restrições escritas do cliente antes de fazer uma recomendação de investimento ou tomar uma decisão de investimento.

3. Avaliar a adequação dos investimentos no contexto do portfólio total do cliente.
- ii. Quando os colaboradores forem responsáveis pela gestão de um portfólio em relação a um mandato, estratégia ou estilo específico, eles devem apenas fazer recomendações de investimento ou tomar decisões de investimento uniformes com os objetivos e as restrições declaradas do portfólio.
- e. Apresentação do desempenho. Ao divulgar informações sobre o desempenho de um investimento, os colaboradores devem envidar esforços razoáveis para garantir que as informações sejam justas, precisas e completas.
- f. Preservação da confidencialidade. Os colaboradores devem manter a confidencialidade das informações de ex-clientes, clientes atuais e possíveis clientes, a não ser que:
  - i. As informações relacionem-se a atividades ilícitas por parte do cliente ou do provável cliente.
  - ii. A divulgação seja exigida por lei.
  - iii. O cliente ou o possível cliente permita a divulgação das informações.

#### IV. DEVERES PARA COM OS EMPREGADORES

- a. Lealdade. Em questões relacionadas ao emprego, os colaboradores devem agir para o benefício de seus empregadores e não privá-los das suas capacidades e habilidades; não devem divulgar informações confidenciais nem causar prejuízos de qualquer outra forma aos seus empregadores.
- b. Acordos de remuneração adicional. Os colaboradores não devem aceitar presentes, benefícios, remunerações nem pagamentos que concorram ou que talvez possam, razoavelmente, criar um conflito de interesse com os interesses de seu empregador, a menos que obtenham um consentimento por escrito por parte de todos envolvidos.
- c. Responsabilidades dos supervisores. Os colaboradores devem envidar esforços razoáveis para detectar e prevenir violações das leis, regras, regulamentos vigentes e do Manual e Padrões por qualquer indivíduo que esteja sujeito à sua supervisão ou autoridade.

#### V. CONFLITOS DE INTERESSE

- a. Divulgação de conflitos. Os colaboradores devem fazer divulgação plena e justa de todas as questões que possam razoavelmente vir a prejudicar a sua independência e objetividade ou interferir com os respectivos deveres para com os seus clientes, possíveis clientes e empregadores. Os colaboradores devem garantir que essas divulgações sejam relevantes, apresentadas em redação simples e comunicadas de maneira eficaz.
- b. Comissão por recomendação. Os colaboradores devem divulgar aos seus empregadores, clientes e prováveis clientes, como cabível, qualquer

remuneração, pagamento ou benefício recebido ou pago a terceiros pela recomendação de produtos ou serviços.

## DIRETORIA DE COMPLIANCE

- I. A diretoria de Compliance terá plena autonomia para o exercício de suas funções e será representado pelo Diretor de compliance.
  
- II. O diretor de compliance dentro de seus objetivos deve:
  - a. Assegurar, em conjunto com as outras disposições contidas no presente Manual de compliance, a adequação, fortalecimento e o funcionamento do sistema de controles internos da Moat, procurando mitigar eventuais riscos decorrentes da complexidade dos negócios da Moat, bem como disseminar a cultura de controles para assegurar o cumprimento às leis e regulamentação aplicáveis à Moat, relacionadas ao exercício de administração de carteira de valores mobiliários
  - b. Todos os Colaboradores da Moat que tiverem suas atividades profissionais relacionadas com a administração de ativos e carteiras de valores mobiliários devem atuar de forma condizente com as regras, normas e procedimentos estabelecidos, sendo importante que, em caso de dúvidas ou necessidade de aconselhamento, se busque auxílio imediato junto ao Diretor de Compliance.
  - c. Garantir o efetivo cumprimento das atividades relacionadas a administração de ativos e carteiras de valores mobiliários, nos termos do artigo 15, inciso I, da Instrução CVM nº 306, de 5 de maio de 1999 e também da Instrução CVM nº 301 de 16 de abril de 1999. As regras aqui contidas deverão ser observadas por todos os Colaboradores da Moat a fim de assegurar o estrito cumprimento das políticas estabelecidas no presente Manual de compliance
  
- III. As obrigações da Diretoria de Compliance São:
  - a. promover treinamentos visando manter seus Colaboradores constantemente atualizados em relação ao presente Manual de compliance da Moat e a outros de auto-regulação aos quais a Moat tenha aderido, inclusive o “Código de Auto-Regulação e Melhores Práticas da Anbima para Fundos de Investimentos”, o código de ética do CFA Institute e também o Código de ética para Gestores do CFA Institute e outros aos quais a Moat venha a aderir, bem como garantir o conhecimento dos Colaboradores acerca da legislação atual aplicável às atividades da Moat e às regras de compliance e controles internos constantes deste Capítulo .
  - b. Avaliar e revisar os procedimentos da Moat a fim de minimizar preventivamente eventuais riscos operacionais e de descumprimento do disposto neste Manual de compliance com periodicidade anual.
  - c. Assegurar pelo Diretor de Compliance, em conjunto com a Diretoria da Moat, que a estrutura organizacional determine, com clareza, a responsabilidade, autoridade e autonomia de cada área e a quem cada colaborador se reporta, afim de promover altos padrões éticos e de conduta, demonstrando a todos os

Colaboradores a importância do comprometimento com todos os controles internos implementados.

- d. Divulgar relatório para os diretores uma vez por semestre, sobre as atividades desenvolvidas pelo setor de compliance bem como todas ocorrências registradas durante o período em questão.
- e. Atender prontamente todos os Colaboradores da MOAT;
- f. Prestar suporte a todas as áreas da Moat no que concerne a esclarecimentos dos controles e do disposto nos capítulos do presente Manual
- g. Acompanhar sistematicamente a conformidade das atividades da Moat com as normas regulamentares (externas e internas, inclusive, mas não exclusivamente, conforme estabelecidas nos capítulos do presente Manual) em vigor
- h. Fiscalizar os controles internos da Moat, em particular no que diz respeito às seguintes atividades desempenhadas pela Moat: (a) execução dos controles de corretagens; (b) revisão dos cálculos de valor de cotas dos fundos geridos, para confrontação com o administrador do respectivo fundo; (c) elaboração de relatório gerencial de posição das carteiras administradas (fundos); e (d) controle das contas a pagar da Moat.
- i. Identificar possíveis condutas contrárias a este Manual;
- j. Definir os princípios éticos a serem observados por todos os Colaboradores da MOAT, constantes deste Manual ou de outros documentos que vierem a ser produzidos para este fim, elaborando sua revisão periódica;
- k. Promover a ampla divulgação e aplicação dos preceitos éticos no desenvolvimento das atividades de todos os Colaboradores da MOAT, inclusive por meio dos treinamentos previstos neste Manual;
- l. Apreciar todos os casos que cheguem ao seu conhecimento sobre o descumprimento dos preceitos éticos e de compliance previstos neste Manual ou nos demais documentos aqui mencionados, e também apreciar e analisar situações não previstas, tomando as medidas cabíveis, inclusive junto aos órgãos reguladores;
- m. Garantir o sigilo de eventuais denunciadores de delitos ou infrações, mesmo quando estes não solicitarem, exceto nos casos de necessidade de testemunho judicial;
- n. Solicitar sempre que necessário, para a análise de suas questões, o apoio da auditoria interna ou externa ou outros assessores profissionais;
- o. Tratar todos os assuntos que chegue ao seu conhecimento dentro do mais absoluto sigilo e preservando os interesses e a imagem institucional e corporativa da MOAT, como também dos Colaboradores envolvidos;
- p. Definir e aplicar eventuais sanções aos Colaboradores.

#### I. Competência

- a. Fiscalizar os atos dos administradores da Moat e de qualquer de seus Colaboradores, verificando o cumprimento de seus deveres legais, estatutários



- e nos termos do presente Manual de compliance e demais políticas aos quais estes ou a Moat venham a aderir
- b. Estabelecer controles internos em relação a práticas e procedimentos, bem como verificar a adequação e efetividade de referidos controles
  - c. Descrever, avaliar e revisar os procedimentos das áreas de atuação de cada um dos Colaboradores, visando minimizar preventivamente riscos operacionais, sempre que entenderem necessário e, obrigatoriamente, uma vez por ano
  - d. Avaliar os processos e procedimentos utilizados para assegurar o cumprimento do disposto nos capítulos do presente Manual de compliance e demais códigos, manuais e políticas aos quais a Moat venha a aderir;
  - e. Avaliar eventuais atos que possam caracterizar, direta ou indiretamente, um descumprimento pelos Colaboradores, do disposto no presente Manual de compliance e demais códigos, manuais e políticas aos quais a Moat venha a aderir;
  - f. Sempre que julgar conveniente e, para fins de apurar fatos cujo esclarecimento seja necessário ao desempenho de suas funções, formular questões a serem respondidas por Colaboradores ou, se for caso, por peritos indicados pela Diretoria da Moat;
  - g. Definir os procedimentos a serem adotados para a repressão de atos praticados em desacordo com o presente Manual de compliance e demais códigos, manuais e políticas aos quais a Moat venha a aderir, bem como estabelecer as penalidades ou mecanismos para a reparação de danos sofridos pela Moat ou terceiros em função do descumprimento, a serem aplicados pela diretoria da Moat; e
  - h. Rever anualmente o presente Manual de compliance e demais códigos, manuais e políticas aos quais a Moat venha a aderir, bem como, sempre que julgar necessário, propor alterações e ajustes a referidos documentos, de acordo com melhores práticas de mercado.

## II. Acompanhar as políticas descritas neste Manual

- a. Atender prontamente todos os Colaboradores da MOAT;
- b. Identificar possíveis condutas contrárias a este Manual;
- c. Definir os princípios éticos a serem observados por todos os Colaboradores da MOAT, constantes deste Manual ou de outros documentos que vierem a ser produzidos para este fim, elaborando sua revisão periódica;
- d. Promover a ampla divulgação e aplicação dos preceitos éticos no desenvolvimento das atividades de todos os Colaboradores da MOAT, inclusive por meio dos treinamentos previstos neste Manual;
- e. Apreciar todos os casos que cheguem ao seu conhecimento sobre o descumprimento dos preceitos éticos e de compliance previstos neste Manual ou nos demais documentos aqui mencionados, e também apreciar e analisar situações não previstas;

- f. Garantir o sigilo de eventuais denunciadores de delitos ou infrações, mesmo quando estes não solicitarem, exceto nos casos de necessidade de testemunho judicial;
  - g. Solicitar sempre que necessário, para a análise de suas questões, o apoio da auditoria interna ou externa ou outros assessores profissionais;
  - h. Tratar todos os assuntos que chegue ao seu conhecimento dentro do mais absoluto sigilo e preservando os interesses e a imagem institucional e corporativa da MOAT, como também dos Colaboradores envolvidos;
  - i. Mediante ocorrência de descumprimento, suspeita ou indício de descumprimento de quaisquer das regras estabelecidas neste Manual ou aplicáveis às atividades da MOAT que cheguem ao conhecimento do diretor de Compliance, de acordo com os procedimentos estabelecidos neste Manual, o diretor poderá se utilizar dos registros e sistemas de monitoramento eletrônico e telefônico referidos neste Manual para verificar a conduta dos Colaboradores envolvidos.
  - j. Todo conteúdo que está na rede poderá ser acessado pelo Diretor de Compliance, caso haja necessidade. Arquivos pessoais salvos em cada computador poderão ser acessados caso o Diretor de Compliance julgue necessário. A confidencialidade dessas informações deve ser respeitada e seu conteúdo será disponibilizado ou divulgado somente nos termos e para os devidos fins legais ou em atendimento a determinações judiciais
  - k. Diretor de Compliance poderá utilizar as informações obtidas em tais sistemas para decidir sobre eventuais sanções a serem aplicadas aos Colaboradores envolvidos, nos termos deste Manual.
  - l. A MOAT se reserva ainda o direito de realizar inspeções periódicas com base nos sistemas de monitoramento eletrônico e telefônico descritos neste Manual.
- IV. Para os fins do presente Manual, portanto, toda e qualquer solicitação que dependa de autorização, orientação ou esclarecimento expresso da diretoria de Compliance, bem como eventual ocorrência, suspeita ou indício de prática por qualquer Colaborador que não esteja de acordo com as disposições deste Manual e das demais normas aplicáveis às atividades da MOAT, deve ser dirigida ao diretor de Compliance, exclusivamente através do e-mail [compliance@moat.com.br](mailto:compliance@moat.com.br).
- V. Adicionalmente, o Diretor de Compliance será responsável por apresentar à Diretoria, para aprovação, um plano de ação anual para o setor de compliance da Moat, cabendo a este monitorar o cumprimento de prazos e o nível de excelência dos trabalhos desenvolvidos pelo diretor de Compliance

## PROCEDIMENTOS DISCIPLINARES (ENFORCEMENT)

- I. Todos os Colaboradores devem pautar suas atividades de acordo com as leis e regulamentos aplicáveis aos negócios da MOAT, as regras estabelecidas neste Manual de compliance e demais instruções de tempos em tempos emitidas pela MOAT. O descumprimento dessas disposições legais ou regulamentares acarretará em ação disciplinar que, dentre outras, poderá incluir a demissão por justa causa do Colaborador, nos termos do artigo 482 da Consolidação das Leis do Trabalho – CLT, ou a destituição do Diretor faltoso ou exclusão do quadro de colaboradores, sem prejuízo de indenização pelos eventuais prejuízos suportados, perdas e danos e/ou lucros cessantes, por meio das medidas cabíveis estabelecidas na legislação brasileira.
- II. O Colaborador deve observar também as normas de conduta para os responsáveis por administrar carteira de valores mobiliários descritas na Instrução da Comissão de Valores Mobiliários (“CVM”) nº 306 de 5 de maio de 1999 e alterações posteriores.
- III. Todo Colaborador, ao receber este Manual, firmará um Termo de Adesão e Responsabilidade, constante do Anexo I (“TERMO DE RESPONSABILIDADE E ADESÃO AO MANUAL DE COMPLIANCE”). Por esse documento, o Colaborador reconhece e confirma seu conhecimento e concordância com os termos deste Manual e das normas de compliance e princípios aqui contidos, devendo declarar no mesmo ato eventuais participações em ações ou operações nos mercados de derivativos que possua junto a quaisquer agentes de mercado.
- IV. Ao firmar o Termo de Responsabilidade, cada Colaborador compromete-se a zelar pela aplicação das normas de compliance e princípios contidos neste Manual.
- V. O descumprimento de quaisquer das regras estabelecidas neste Manual ou das demais normas aplicáveis às atividades da MOAT deverão ser levados para apreciação do Diretor de Compliance, de acordo com os procedimentos estabelecidos neste Manual.

## **POLÍTICA DE COMBATE E PREVENÇÃO A LAVAGEM DE DINHEIRO E FINANCIAMENTO AO TERRORISMO (PLDFT)**

Para prevenir a prática de lavagem de dinheiro na realização de seus negócios no País, em consonância com a legislação nacional, a MOAT mantém procedimentos e controles de verificação para que se possam identificar as operações suspeitas com base nos meios e nas informações que tem a sua disposição.

O Colaborador da MOAT deve conhecer e aplicar a íntegra da legislação referente à prevenção e combate ao crime de lavagem de dinheiro, especialmente, a Lei nº 9.613/98, a Circular BACEN nº 2.852/98, a Carta-Circular BACEN nº 2.826/98, a Instrução CVM nº 301/99 e demais normativos editados ou que venham a ser editados com relação à prevenção aos crimes de lavagem ou ocultação de bens, direitos e valores, bem como a política de prevenção e combate ao crime de lavagem de dinheiro. Desta forma a MOAT e seus colaboradores devem comunicar o Coaf se houver alguma situação atípica descrita abaixo.

A negociação de ativos e valores mobiliários financeiros e valores mobiliários para os Fundos de Investimento e carteiras administradas deve ser objeto de análise, avaliação e monitoramento.

### **1) Processo de Identificação de Contrapartes (Cadastro)**

Para ativos listados abaixo, devidos suas características já passaram por processo de PLDFT, portanto a Moat se exime de diligencia adicional em relação ao controle de contraparte:

Ofertas públicas iniciais e secundárias de valores mobiliários, registradas de acordo com as normas emitidas pela Comissão de Valores Mobiliários (CVM);  
Ofertas públicas de esforços restritos, dispensadas de registro de acordo com as normas emitidas pela CVM;

Ativos e valores mobiliários admitidos à negociação em bolsas de valores, de mercadorias e futuros, ou registrados em sistema de registro, custódia ou de liquidação financeira, devidamente autorizados em seus países de origem e supervisionados por autoridade local reconhecida;

Ativos e valores mobiliários cuja contraparte seja instituição financeira ou equiparada; e

Ativos e valores mobiliários de mesma natureza econômica daqueles acima listados, quando negociados no exterior, desde que (a) sejam admitidos à negociação em bolsas de valores, de mercadorias e futuros, ou registrados em sistema de registro, custódia ou de liquidação financeira, devidamente autorizados em seus países de origem e supervisionados por autoridade local reconhecida pela CVM, ou (b) cuja existência tenha sido assegurada por terceiros

devidamente autorizados para o exercício da atividade de custódia em países signatários do Tratado de Assunção ou em outras jurisdições, ou supervisionados por autoridade local reconhecida pela CVM.

Para os demais ativos e valores mobiliários, como títulos e valores mobiliários objeto de distribuição privada (renda fixa ou ações), direitos creditórios, empreendimentos imobiliários etc., a Moat deve verificar que a contraparte dispõe de mecanismos mínimos para análise de PLDFT

## **2) Monitoramento: Controle do Preço dos Ativos e Valores Mobiliários Negociados**

A Moat registra e guarda em sistema os preços dos ativos negociados e mantém registros de todas as transações feitas para os fundos de investimento ou carteiras administradas sob sua gestão. Deste modo eventuais operações efetuadas fora dos padrões praticados no mercado, de acordo com as características do negócio, sejam identificados e comunicados aos órgãos competentes.

As situações listadas abaixo podem configurar indícios da ocorrência dos crimes previstos na Lei nº 9.613, ou podem com eles relacionar-se, devendo ser analisadas com especial atenção e, se e quando consideradas suspeitas pela instituição, nos termos do art. 6º e 7º da ICVM 301/99, comunicadas ao Coaf:

Realização de operações ou conjunto de operações de compra ou de venda de ativos e valores mobiliários para o fundo, 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 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;

Solicitação de não observância ou atuação no sentido de induzir funcionários da instituição a não seguirem os procedimentos regulamentares ou formais para a realização de operações ou conjunto de operações de compra ou de venda de ativos e valores mobiliários para o fundo;

Quaisquer operações ou conjunto de operações de compra ou de venda de ativos e valores mobiliários para o fundo envolvendo pessoas relacionadas a atividades terroristas listadas pelo Conselho de Segurança das Nações Unidas;

Realização de operações ou conjunto de operações de compra ou de venda de títulos e valores mobiliários, qualquer que seja o valor da aplicação, por pessoas que reconhecidamente tenham cometido ou tentado cometer atos terroristas, ou deles participado ou facilitado o seu cometimento;

Quaisquer operações ou conjunto de operações de compra ou de venda de títulos e valores mobiliários com indícios de financiamento do terrorismo;

Operações ou conjunto de operações de compra ou de 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; investimentos significativos em produtos de baixa rentabilidade e liquidez, considerando a natureza do fundo ou o perfil do cliente/mandato da carteira administrada.

Operações nas quais haja deterioração do ativo sem fundamento econômico que a justifique.

### **3) As seguintes regras devem ser seguidas pelo Colaborador:**

Manter-se alerta e atento a transações não usuais envolvendo Clientes, Colaboradores, ou o nome da Moat; e

Comunicar por escrito qualquer transação suspeita ao diretor Compliance.

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

A Moat deverá dispensar especial atenção na contratação de serviços de administração de carteira por clientes (i) investidores não-residentes, especialmente quando constituídos sob a forma de trusts e sociedades com títulos ao portador; (ii) investidores com grandes fortunas geridas por áreas de instituições financeiras; e (iii) pessoas politicamente expostas

A Moat deverá tomar todas as medidas necessárias para prevenir a prática de atividades consideradas como suspeitas de lavagem de dinheiro e de qualquer outra atividade que facilite a lavagem de dinheiro ou o financiamento ao terrorismo ou atividades ilegais. O não cumprimento dessas regras sujeitará o infrator à demissão imediata e ainda o infrator poderá estar sujeito a responsabilidade criminal.

Todas as situações abaixo devem ser monitoradas continuamente:

Negócios realizados, repetidamente, entre as mesmas partes ou em benefício das mesmas partes, nas quais haja seguidos ganhos ou perdas no que se refere a algum dos envolvidos;

Negócios que evidenciem oscilação significativa em relação ao volume e/ou frequência de negócios de qualquer das partes envolvidas;

Negócios cujas características e/ou desdobramentos evidenciem atuação, de forma contumaz, em nome de terceiros;

Operações que evidenciem mudança repentina e objetivamente injustificada relativamente às modalidades operacionais usualmente utilizadas pelo(s) envolvido(s);

Operações realizadas com finalidade de gerar perda ou ganho para as quais falte, objetivamente, fundamento econômico;

Operações com a participação de pessoas naturais residentes ou entidades constituídas em países e territórios não cooperantes, nos termos das cartas circulares editadas pelo Conselho de Controle de Atividades Financeiras – COAF;

Situações e operações em que não seja possível identificar o beneficiário final

Situações em que não se pode confirmar informações dos clientes, nem as manter atualizadas e nem monitorar as operações por eles realizadas

O Diretor de Compliance deve se atentar para que sejam observados os seguintes parâmetros:

#### **4) Conheça seu cliente**

Em consonância com as boas práticas de mercado, e em atendimento aos regulamentos internos do mercado financeiro, como distribuidor a Moat realiza diversos procedimentos relacionados ao processo de KYC.

Antes de iniciar suas operações o Investidor deverá fornecer todas as informações cadastrais solicitadas, mediante o preenchimento de ficha cadastral, assinatura e a entrega de documentos conforme a regulamentação vigente.

Os procedimentos de KYC exigem a identificação adequada de cada Cliente prevendo a verificação da capacidade financeira do investidor.

#### **5) Pessoas Politicamente Expostas**

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

Ao iniciar o relacionamento com a Moat o investidor deve autodeclarar sua situação como pessoa politicamente exposta. Em paralelo, no *onboarding* do cliente, a Moat realizará pesquisa sobre a situação do cliente na rede mundial de computadores e novas pesquisas serão realizadas no mínimo a cada 24 meses no processo de atualização cadastral.

## 6) Conheça seu Colaborador

Serão considerados colaboradores todos aqueles que estão envolvidos na execução das atividades da MOAT. Dessa forma o termo colaborador abrange sócios, administradores, empregados e estagiários.

É responsabilidade da Instituição conhecer seus colaboradores, por meio de acompanhamento acerca dos aspectos comportamentais, padrões de vida e respectivos resultados operacionais, atentando para alterações inusitadas e significativas nestas variáveis, conforme previsto na Carta-circular 3.542/12, do Bacen.

A MOAT abstém-se de fornecer aos respectivos clientes, informações sobre eventuais comunicações efetuadas em decorrência de indícios de lavagem de dinheiro ou financiamento ao terrorismo.



## POLÍTICAS DE SEGREGAÇÃO DE ATIVIDADES

O capítulo em questão tem por objetivo garantir a completa segregação das atividades prestadas por esta Sociedade, em particular, as atividades de administração de carteiras e valores mobiliários, das demais atividades desenvolvidas.

A Sociedade atuará apenas na prestação de serviços de administração de carteiras de valores mobiliários, através de carteiras individuais e/ou fundos de investimento, portanto não há necessidade, tampouco a possibilidade, de formalizar uma política para o tema.

## POLÍTICA DE CONFIDENCIALIDADE

- I. São consideradas informações confidenciais (“Informações Confidenciais”):
- a. Todo tipo de informação escrita, verbal ou apresentada de modo tangível ou intangível geridas pela MOAT ou de qualquer natureza relativas às atividades da MOAT e a seus sócios ou clientes, independente destas informações estarem contidas em quaisquer tipos de mídia ou em documentos físicos ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.
  - b. O Colaborador compromete-se a utilizar as Informações Confidenciais a que venha a ter acesso estrita e exclusivamente para desempenho de suas atividades na MOAT, comprometendo-se, portanto, a não divulgar tais Informações Confidenciais para quaisquer fins, colaboradores não autorizados, mídia, ou pessoas estranhas à MOAT.
  - c. O Colaborador se obriga a, por prazo indeterminado após sua rescisão, manter absoluto sigilo pessoal e profissional das Informações Confidenciais a que teve acesso durante o seu período na MOAT, se comprometendo, ainda a não utilizar, praticar ou divulgar informações privilegiadas, *Insider Trading*, Divulgação Privilegiada e *“Front Running”*, seja atuando em benefício próprio, da MOAT ou de terceiros.
  - d. Definições:
    - i. Informação Privilegiada: qualquer informação relevante a respeito de qualquer companhia, que não tenha sido divulgada publicamente e que seja obtida de forma privilegiada;
    - ii. *Insider Trading*: compra e venda de títulos ou valores mobiliários com base na utilização de informação privilegiada, visando à obtenção de benefício próprio ou de terceiros;
    - iii. Divulgação Privilegiada: a divulgação, a qualquer terceiro, de informação privilegiada que possa ser utilizada com vantagem na compra e venda de títulos ou valores mobiliários;
    - iv. *Front Running*: a prática de aproveitar alguma informação privilegiada para concluir uma negociação antes de outros.
- II. O Colaborador entende que a revelação não autorizada de qualquer Informação Confidencial pode acarretar prejuízos irreparáveis e sem remédio jurídico para a

MOAT e terceiros, ficando deste já o Colaborador obrigado a indenizar a MOAT, seus sócios e terceiros prejudicados, nos termos estabelecidos a seguir.

- III. O descumprimento acima estabelecido será considerado ilícito civil e criminal, ensejando inclusive sua classificação como justa causa para efeitos de rescisão de contrato de trabalho, quando aplicável, nos termos do artigo 482 da Consolidação das Leis de Trabalho, ou desligamento ou exclusão por justa causa, conforme a função do Colaborador à época do fato, obrigando-lhe a indenizar a MOAT e/ou terceiros pelos eventuais prejuízos suportados, perdas e danos e/ou lucros cessantes, independente da adoção das medidas legais cabíveis.
- IV. O Colaborador reconhece e toma ciência que todos os documentos relacionados direta ou indiretamente com as Informações Confidenciais por este elaborados ou obtidos em decorrência do desempenho de suas atividades na MOAT são e permanecerão sendo propriedade exclusiva da MOAT, razão pela qual compromete-se a não utilizar tais documentos, no presente ou no futuro, para quaisquer fins que não o desempenho de suas atividades na MOAT.
- V. O Colaborador reconhece que nos termos da Lei 9.609/98, a base de dados, sistemas computadorizados desenvolvidos internamente, modelos computadorizados de análise, avaliação e gestão de qualquer natureza, bem como arquivos eletrônicos, são de propriedade exclusiva da MOAT, sendo terminantemente proibida sua reprodução total ou parcial, por qualquer meio ou processo; sua tradução, adaptação, reordenação ou qualquer outra modificação, ficando sujeito, em caso de infração, às penalidades dispostas na referida lei.
- VI. Esta política é parte integrante das regras que regem a relação de trabalho do Colaborador com a MOAT, que ao assinar o termo de responsabilidade está aceitando expressamente os termos e condições aqui estabelecidos.
- VII. Todo Colaborador, ao receber este Manual, firmará um Termo de Responsabilidade, constante do Anexo I (“TERMO DE RESPONSABILIDADE E ADESÃO AO MANUAL DE COMPLIANCE”). Por esse documento, o Colaborador reconhece e confirma seu conhecimento e concordância sobre que nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada fora da MOAT, bem como de que fica vedada qualquer divulgação, no âmbito pessoal ou profissional, que não esteja em acordo com as normas legais e de compliance da MOAT.

- VIII. A não observância da confidencialidade e do sigilo, mesmo após o término da vigência deste Termo, estará sujeita à responsabilização nas esferas cível e criminal e sujeitas às sanções da diretoria de compliance.

## POLÍTICA DE TREINAMENTO E CERTIFICAÇÕES

### I. Implementação

- a. Cada Colaborador no momento de sua contratação, antes do início efetivo de suas atividades, participará de um processo de treinamento onde irá adquirir conhecimento sobre as atividades da MOAT, suas normas internas, especialmente sobre este Manual, além de informações sobre as principais leis e normas que regem as atividades da MOAT, e terá oportunidade de esclarecer dúvidas relacionadas a tais princípios e normas.

### II. Continuidade

- a. Anualmente a MOAT promove através da diretoria de compliance uma palestra de reciclagem, sobre as atualizações sobre este Manual, além de informações sobre as principais leis e normas que regem as atividades da MOAT.
  - i. Os treinamentos abordarão as normas dispostas nos capítulos do presente Manual de compliance, apresentando aos Colaboradores seus principais aspectos e os mecanismos de execução dos mesmos. Assim, deverão proporcionar aos Colaboradores uma visão geral das políticas adotadas pela Sociedade, de forma que os mesmos se tornem aptos a exercer suas funções aplicando conjuntamente todas as normas nelas dispostas.
  - ii. A MOAT poderá, por deliberação dos seus diretores, financiar cursos de aprimoramento profissional, desde que julgue viável e interessante o conteúdo a ser lecionado. Caberá aos diretores responsáveis pela área administrativa e financeira da Sociedade a aprovação de participação em cursos, eventos ou palestras pelo Colaborador solicitante.

### III. Certificações

- a. Sempre que houver admissão, desligamento ou transferência interna de colaboradores, a Moat deverá consultar o status da certificação de cada um deles e proceder a devida atualização nos bancos de dados das entidades ou autarquias reguladoras; Tais atualizações devem ocorrer em até 5 dias úteis a contar da data da efetivação;
- b. As atividades que de acordo com a regulamentação em vigor exigirem algum tipo de certificação somente poderão ser exercidas por profissionais previamente certificados pela entidade reguladora. No caso da Moat CGA para os profissionais responsáveis pela gestão de recursos de terceiros e CPA-20 para os profissionais da área de distribuição de cotas de fundos de investimentos.
- c. A área de compliance será responsável por garantir que os profissionais certificados, que atuem em atividades elegíveis, atualizem os seus certificados (CPA-20) antes do prazo de vencimento, seja via: (i) participação em Programas de Treinamento, oferecidos ou validados pela Instituição Participantes, com este propósito específico ou (ii) realização de Exame presencial de Atualização.
- d. Profissionais que porventura não apresentem a devida certificação ou que tenham a sua certificação vencida serão notificados via “Carta de formalização de afastamento

das funções” e imediatamente afastados de suas atividades. O primeiro afastamento será por 15 dias (esse prazo poderá ser reduzido caso o colaborador seja aprovado em exame de certificação antes do prazo estipulado). Caso a situação não seja regularizada o prazo poderá ser estendido uma única vez por mais 15 dias, em caso de não regularização o profissional será afastado da função de forma definitiva.

- e. Fica a área de recursos humanos responsável pelo processo de atualização das informações referentes aos seus Profissionais nos Banco de Dados das entidades ou autarquias reguladoras. A atualização deverá acontecer em até 5 dias úteis a contar da data de admissão ou desligamento de colaboradores, aprovação ou atualização em exame de certificação ou vencimento da certificação.

## DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

Este documento têm o objetivo de estabelecer normas, critérios e responsabilidades sobre a segurança da informação da Rede Corporativa da MOAT CAPITAL, garantindo à mesma confidencialidade, integridade e disponibilidade.

Os itens considerados como fazendo parte do escopo em termos de Segurança da Informação são os seguintes:

- ◆ Controle e classificação dos ativos;
- ◆ Segurança pessoal;
- ◆ Segurança física;
- ◆ Controle de acesso às informações;
- ◆ Desenvolvimento e manutenção de sistemas;
- ◆ Gerenciamento da continuidade dos negócios;
- ◆ Conformidade.

Esta norma se aplica à todos os usuários da rede corporativa da MOAT CAPITAL.

### Normas

#### Disposições Gerais

Os sistemas de informação, a infra-estrutura tecnológica, os arquivos de dados e as informações internas ou externas, são considerados importantes ativos da empresa, em função da MOAT CAPITAL apresentar suas operações, dependentes em grande parte da tecnologia para conduzir seus negócios e atender às suas necessidades comerciais e estratégicas.

É necessário que as informações sejam armazenadas, conduzidas e processadas em ambiente seguro e também que todos os usuários da informação compartilhem da responsabilidade pelos processos de segurança definidos neste normativo, com a finalidade de se equiparar às boas práticas das organizações globais.

As normas de segurança da informação estabelecem objetivos, funções, ações, mecanismos de delegação e responsabilidades pelos processos, manipulação da informação e controles internos.

Os processos de segurança da informação devem assegurar a integridade, a disponibilidade e a confidencialidade dos ativos de informação da MOAT CAPITAL.

- ◆ As normas de segurança da informação devem:
  - Proteger os ativos da MOAT CAPITAL contra ameaças, internas ou externas, intencionais ou acidentais;
  - Limitar a um nível aceitável a exposição a perdas ou danos que possam resultar em falhas de segurança;
  - Minimizar as ameaças potenciais à segurança das informações, garantindo a manutenção da integridade, disponibilidade e confidencialidade;
  - Assegurar que os recursos adequados estarão disponíveis para implementar e manter um programa de segurança efetivo;
  - Conscientizar os associados e usuários da informação, sobre aspectos relacionados à segurança das informações.

#### Uso da Informação

Aplicam-se as seguintes atribuições aos usuários da informação:

- ◆ O proprietário é responsável pela geração, exatidão e classificação das informações;
- ◆ O gestor é responsável pela gerência das informações e pela definição dos direitos de acesso às mesmas;
- ◆ O custodiante é responsável pela guarda e disponibilidade das informações;
- ◆ O usuário é responsável pelo uso adequado das informações e seus ativos a que tenha acesso.

#### Responsabilidades

- ◆ Da Diretoria:



- Direcionar os esforços e recursos propostos para a segurança da informação, de acordo com a estratégia de negócios da empresa;
  - Aprovar as normas de segurança da informação e suas atualizações;
  - Aprovar os controles a serem utilizados para garantir a segurança das informações;
  - Acompanhar os indicadores de segurança e os incidentes reportados pela empresa prestadora de serviços de TI;
  - Comunicar o responsável por Compliance os casos de violações à Norma de Segurança da Informação para as providências necessárias;
  - Apoiar as iniciativas para melhoria contínua de medidas de proteção da informação da empresa, com vistas a reduzir os riscos identificados;
  - Aprovar o planejamento, alocação de verbas, os recursos humanos e de tecnologia, no que tange a segurança da informação;
  - Delegar as funções de segurança da informação aos profissionais responsáveis.
- ◆ Da Empresa Prestadora de Serviços de TI:
- Monitorar as violações de segurança e tomar ações corretivas visando saná-las e cuidando para que não haja recorrência;
  - Orientar os testes da infra-estrutura de tecnologia e de sistemas para avaliar os pontos fracos e detectar possíveis ameaças;
  - Assessorar as demais áreas da empresa no processo de classificação das informações;
  - Auxiliar as áreas de negócio na elaboração do Plano de Continuidade dos Negócios específico de cada uma;
  - Assegurar que exista um processo apropriado para a comunicação dos incidentes e violações de segurança detectados pelos usuários da informação, independentemente dos recursos tecnológicos utilizados;
  - Identificar recursos e fornecer orientação para a tomada de ações rápidas caso sejam detectados incidentes de segurança;
  - Manter a infraestrutura que suporta o ambiente controlado;
  - Manter a infraestrutura e sistemas atualizados;
  - Garantir a implementação e operação dos indicadores de segurança;
  - Notificar imediatamente os incidentes de segurança à diretoria;
  - Garantir a rápida tomada de ações em caso de incidentes de segurança.

- ◆ Do responsável por Compliance
  - Desenvolver, manter e implementar programas de treinamento e de conscientização aos colaboradores com vínculo empregatício com a empresa e colaboradores prestadores de serviço, sobre a Norma de Segurança da Informação, a forma como ela está estruturada e os principais conceitos de segurança da informação;
  - Gerenciar os problemas disciplinares resultantes de violações dos controles de segurança da informação, juntamente com os gestores dos envolvidos;
  - Emitir o Termo de Compromisso, conforme modelo do Manual de Ética e Compliance e garantir a ciência deste entre todos os colaboradores;
  - Gerenciar a assinatura do Acordo de Confidencialidade quando da contratação de terceiros ou prestadores de serviços, conforme modelo do Manual de Ética e Compliance;
  - Em conjunto com os demais membros do Comitê de Compliance, determinar as sanções cabíveis de acordo com a legislação em vigor.
  
- ◆ Dos Auditores Independentes:
  - Garantir, mediante verificações de conformidade, que a MOAT CAPITAL esteja operando de acordo com os princípios e controles estabelecidos na Norma de Segurança da Informação;
  - Emitir pareceres para a Diretoria da MOAT CAPITAL;
  - Revisar periodicamente a Norma de Segurança da Informação e sugerir as alterações necessárias.

#### Itens Abordados pela Segurança da Informação

##### Controle e Classificação dos Ativos

Este tópico visa assegurar que todos os ativos, físicos ou lógicos, estejam identificados, classificados e que sejam controlados.

- ◆ Todos os ativos da MOAT CAPITAL, sejam estes físicos ou lógicos, devem ser adequadamente controlados pela administração. Os ativos devem ser protegidos de acordo com o grau de criticidade que representam para o negócio da MOAT CAPITAL;
- ◆ É necessário que todos os ativos sejam classificados de acordo com os critérios definidos pela Diretoria da MOAT;

- Com base nessa classificação, devem ser adotados controles que garantam as três propriedades básicas desses ativos: integridade, disponibilidade e confidencialidade, em um nível proporcional à criticidade que representam para o negócio da MOAT CAPITAL.
- ◆ Em caso de dúvida, nenhuma informação deve ser divulgada.

### Segurança de Pessoal

Neste caso, a norma visa assegurar que todos os usuários da informação tenham conhecimento dos requisitos e das obrigações definidos pela Norma de Segurança da Informação, assim como minimizar a ocorrência de incidentes de segurança em função de problemas no uso, desvio de informações, fraudes e na interpretação das normas e procedimentos, e de falhas no processo de conscientização sobre segurança.

- ◆ Todos os usuários da informação e clientes devem conhecer e adotar as definições de segurança da informação instituídas pela MOAT CAPITAL e suas responsabilidades na manutenção da segurança corporativa;
- ◆ Os usuários da informação devem ser orientados sobre os procedimentos e o uso correto dos recursos de processamento das informações, por meio de treinamentos, de forma a minimizar possíveis riscos de segurança.

### Segurança Física

Em termos de segurança física, a norma deve definir os requisitos mínimos de segurança física que os ambientes considerados críticos, onde há informações sigilosas da MOAT CAPITAL, devem possuir para assegurar a proteção de seus ativos contra fatores que possam causar interrupção das atividades, alteração ou vazamento das informações e consequente prejuízo financeiro.

- ◆ Todas as áreas classificadas como críticas na MOAT CAPITAL devem estar protegidas por controles físicos apropriados;
  - Esses controles devem ser proporcionais à criticidade dos equipamentos, dos sistemas e das informações mantidas e manuseadas nestas áreas.
- ◆ As áreas classificadas como críticas devem estar devidamente protegidas por acesso não autorizado, dano ou interferência.

### Controle de Acesso à informações

O controle de acesso às informações deve definir os requisitos necessários para que o usuário da informação obtenha acesso ao ambiente de tecnologia da MOAT CAPITAL.

- ◆ O acesso a todos os sistemas e informações da MOAT CAPITAL deve ser concedido de acordo com as necessidades da função do usuário para a execução de suas atividades;
- ◆ O responsável pelos sistemas ou da informação é o responsável pela concessão de acesso a todos os recursos que estejam sob sua responsabilidade. Os acessos concedidos deverão ser periodicamente revisados;
- ◆ Os usuários devem se restringir às informações e ambientes aos quais estão autorizados, devendo acessá-los somente se houver a necessidade para desempenho de suas atividades profissionais.

#### Desenvolvimento e Manutenção de Sistemas

Este item enumera os requisitos de segurança para desenvolvimento, manutenção e parametrização de sistemas.

- ◆ Todos os sistemas desenvolvidos pela MOAT CAPITAL ou por empresas contratadas por esta, deverão atender aos requisitos de segurança definidos pela Norma de Segurança da Informação.

#### Gerenciamento da Continuidade dos Negócios

A Norma de Gerenciamento da Continuidade dos Negócios deve identificar atividades chaves que compõem um Plano de Continuidade de Negócios, a fim de assegurar que as operações da MOAT CAPITAL sejam rapidamente retomadas em caso de incidentes graves.

- ◆ É necessário que exista um Plano de Continuidade de Negócios que assegure a continuidade ou a rápida retomada das atividades em caso de falhas ou interrupções dos negócios;
  - O Plano de Continuidade de Negócios deve incluir os processos, procedimentos e alternativas para recuperação de qualquer interrupção do negócio, independentemente do agente causador, além da proteção dos processos críticos da MOAT CAPITAL contra efeitos de desastres significativos.

#### Conformidade

A Norma de Conformidade deve definir as ações necessárias para que a MOAT CAPITAL não viole nenhuma lei civil ou criminal, estatutos, regulamentações ou obrigações contratuais referentes a quaisquer requisitos de segurança.

- ◆ A empresa deve estar em conformidade com todas as regras e regulamentos instituídos por lei. Isto inclui qualquer lei civil ou criminal, estatutos ou obrigações contratuais feitas envolvendo a MOAT CAPITAL;
- ◆ É responsabilidade de todos os usuários de informações auxiliar na manutenção dos requisitos de segurança e nos regulamentos ditados por lei.

#### Controle do Documento

Esta seção do documento têm o objetivo de:

- ◆ Controlar as alterações realizadas no documento, através do estabelecimento de um controle de versões;
- ◆ Relacionar os responsáveis pelo controle, confecção e aprovação do documento;
- ◆ Estabelecer as diretrizes para atualização do documento;
- ◆ Definir como o documento deve ser distribuído.

#### Resumo das Atualizações

Versão	Data Publicação	Resumo	Nº da Revisão
1.3	10/2018	Versão Inicial	-

#### Responsáveis

Responsabilidade	Responsável	E-mail
Criador	Cleber Campos	cleber@tecnoqualify.com.br
Revisor	Clayton Campos	clayton@tecnoqualify.com.br
Aprovador	Rodrigo Carrera	Rodrigo.carrera@moat.com.br

#### Plano para Revisão do Documento

Este documento deverá ser revisto e atualizado, quando ocorrer qualquer uma das seguintes premissas:

- ◆ Quando necessário, para corrigir ou incluir informações;
- ◆ Quando ocorrerem mudanças organizacionais significativas e que afetem diretamente o processo definido;
- ◆ Após 6 meses da data de sua publicação, para efeito de melhoria contínua.

Sempre que ocorrer uma revisão do documento sua versão será alterada, conforme o seguinte critério:

- ◆ Alterações pouco significativas: Será mantido o número principal de versão e será alterada a numeração secundária de versão. (Exemplo: versão 1.1, 1.2, 1.3 ... 1.n)
- ◆ Alterações significativas ou revisões semestrais: Será alterado o número principal da versão para o número seguinte de numeração, começando sempre com o número secundário em 0. (Exemplo: versão, 2.0, 3.0, 4.0 ... n.0)

#### Distribuição do Documento

Este documento será distribuído eletronicamente para todos os usuários da MOAT CAPITAL, sempre que necessário.

Existirá uma versão impressa do documento, que estará organizada em uma pasta de documentação e que ficará disponível para consulta dos envolvidos, no processo da MOAT CAPITAL.

Quando ocorrerem revisões ou atualizações no documento, todos os envolvidos e os aprovadores receberão uma nova versão eletrônica. Uma nova versão impressa substituirá a versão anterior existente na MOAT CAPITAL e todas as versões anteriores deverão ser descartadas.

O Aprovador do documento é o responsável pela distribuição do mesmo na MOAT CAPITAL.

## PLANO DE CONTINGÊNCIA E CONTINUIDADE DOS NEGÓCIOS

### B.1.1 – Introdução ao BCP

O objetivo do Plano de Contingência e Continuidade dos Negócios (“BCP”) é possibilitar que a MOAT Capital de Recursos Ltda (“MOAT”) continue com as suas operações e serviços essenciais mesmo nos cenários de crise.

O presente documento define os procedimentos que deverão ser seguidos pela MOAT, no caso de contingência, de modo a impedir a descontinuidade operacional por problemas técnicos. Foram estipuladas estratégias e planos de ação com o intuito de garantir que os serviços essenciais da MOAT sejam devidamente identificados e preservados após a ocorrência de um imprevisto ou um desastre.

O Plano de Contingência prevê ações que durem até o retorno à situação normal de funcionamento da MOAT dentro do contexto de seu negócio.

#### B.1.1.1 – Cenários de Crise

A Alternative Investment Management Association (AIMA) lista em seu documento “Business Continuity Management for Hedge Fund Managers – version June 2012” 24 possíveis cenários de crise:

1. Explosão em uma grande área;	2. Fogo;	3. Falta localizada de energia;
---------------------------------	----------	---------------------------------

4. Explosão localizada;	5. Inundação;	6. Falha de circuito / terminal;
7. Explosão na vizinhança;	8. Pandemia;	9. Falha de hardware;
10. Bomba radiológica;	11. Clima extremo;	12. Virus / hackers;
13. Guerra ou insurreição civil;	14. Interrupção de transportes;	15. Roubo / sabotagem;
16. Alerta de segurança;	17. Acidentes (dentro ou fora do escritório);	18. Falha no sinal de telecom (internet e/ou voz);
19. Vazamento de gás;	20. Eletrocução;	21. Falha no hardware de telecom e
22. Terremoto;	23. Falta geral de energia (apagão);	24. Falha na rede de celular



Uma vez que ocorra algum incidente parecido com estes 24 cenários ou algo que chame a atenção do colaborador, o líder do BCP – que é o Compliance Officer ou na ausência deste o seu back-up – deverá ser imediatamente comunicado. (Ver B.1.4 – lista de contatos de emergência)

#### B.1.1.2 – Desdobramentos

A lista de cenários apresentadas em B.1.1.1 não tem a pretensão de ser definitiva. Além disto, cenários de crise são por definição imprevisíveis. No entanto os cenários acima geralmente levam a combinação de um ou mais dos desdobramentos abaixo:

1. Perda de Acesso ao Prédio: significa que todos os colaboradores e contratados da MOAT que estiverem no prédio no momento do incidente deverão evacuá-lo e quem estiver fora não poderá entrar.
2. Perda de Pessoal: afeta o staff e prestadores de serviços da MOAT. Inclui ferimentos, doenças, morte e incapacidade de chegar no escritório (ou potencialmente trabalhar de casa).
3. Perda de Infraestrutura de TI: inclui falha parcial ou completa da rede de TI, incluindo hardware e softwares essenciais. O fator-chave é envolver os prestadores de serviços assim que possível para instaurar os sistemas de back-up.



4. Perda de Infraestrutura de Telecom: inclui falha parcial ou completa da rede de telecomunicações, incluindo equipamentos, telefones fixos, celulares e a internet).
5. Perda de Energia Elétrica: Falta de energia devido a apagões ou interrupção da rede elétrica devido a chuvas e/ou quedas de árvores.

#### B.1.2 – Gestão da Crise, Recuperação e Retomada

Uma vez que o líder do BCP foi acionado devido a uma potencial crise, caso seja possível ele convocará (pessoalmente ou via call-tree) os colaboradores-chave da MOAT para formar o comitê de crise e avaliar conjuntamente a situação e próximos passos.



Na impossibilidade de decisão em conjunto – devido a situação onde a pressão é extrema – o líder do BCP poderá tomar decisões sozinho sobre os próximos passos para gerenciar a crise.

Existem geralmente três etapas a serem percorridas após a ocorrência de um evento:

1. Gestão da Crise;
2. Recuperação e
3. Retomada

##### B.1.2.1 – Gestão da Crise

1. Etapa Inicial: engloba vários aspectos e decisões fundamentais a serem tomados imediatamente após o incidente:
  - 1.1. Avaliação dos impactos: o foco da reunião do time de crise deve ser em
    - 1.1.1. Entender o que aconteceu;
    - 1.1.2. Quais são as consequências imediatas e gravidade da situação;
    - 1.1.3. Como manter o staff a salvo e
    - 1.1.4. O que nós devemos fazer AGORA e decidir pela formalização ou não da CRISE (Em caso afirmativo os próximos passos são seguidos)
  - 1.2. Comunicação ao restante dos colaboradores

- 1.3. Evacuação do prédio coordenada em conjunto com a administração predial;
- 1.4. Acionar assistência médica imediata se necessário;
- 1.5. Notificação dos serviços de emergência (bombeiros, polícia, SAMU) se necessário;
- 1.6. Condução de chamada para ver os membros do staff e visitantes presentes;
- 1.7. Retomada da reunião do comitê de crise;
- 1.8. Re-alocação do staff:
  - 1.8.1. Quem vai para casa e quem vai para o site de contingência;
  - 1.8.2. Combinar como serão as próximas comunicações (telefone, Whatsapp)
- 1.9. Notificação de parceiros-chave estratégicos: prestadores de serviços de TI e Telecom (Tecnoqualify); e administrador do fundo (INTRAG).



Tomar cuidado para manter a consistência da comunicação ao informar terceiros. Apenas os colaboradores autorizados a falar em nome da empresa deverão fazer isto (ver lista de autorizados no Manual de Compliance).

- 1.10. Iniciar a redundância de TI (caso seja aplicável) em conjunto com a Tecnoqualify e
- 1.11. Re-direcionamento das linhas de telefone para os celulares (caso seja aplicável)

## 2. Recuperação de Desastre – TI

Após determinar a necessidade ou não de redundância de TI, o comitê de crise deverá atuar em conjunto com a Tecnoqualify para garantir que qualquer aplicativo e hardware críticos continuem a operar via redundância/back-up. Isto inclui:

- acesso ao servidor de e-mails;
- acesso aos principais servidores (aplicativos e arquivos)
- acesso remoto aos sistemas.

## 3. Telecom

Caso a redundância de telecom seja necessária, o provedor deve ser instruído a desviar linhas de dados/e-mail.

## 4. Comunicação Externa

A gestão de relacionamentos externos durante uma interrupção das atividades normais é crítica para o curto e médio prazo da MOAT. No curto prazo os prestadores de serviços

críticos devem ser avisados para que eles adaptem os seus processos para a nova circunstância. No longo prazo, prover uma comunicação clara, pontual e consistente a clientes, distribuidores e contrapartes fortalece a confiança na organização

O comitê de Crise produzirá um script padrão para comunicar interna e externamente (demais prestadores de serviços, clientes, dentre outros). É muito importante que a comunicação externa seja consistente uma vez que confusão poderá resultar em perda de confiança.

Caso algum colaborador (que não esteja autorizado a falar em nome da empresa) seja questionado por terceiros, o colaborador deverá direcionar o terceiro para alguém que esteja autorizado.

#### B.1.2.2 – Recuperação

A fase de recuperação começa após a crise inicial ter sido contornada, ou seja, o staff já foi recolocado, a redundância de TI acionada e terceiros-chave notificados.

A fase de recuperação é composta das sub-fases a seguir:

1. Comunicação Interna: call diário de acompanhamento do comitê de Crise e outro call com os demais membros da MOAT. Ambos devem ser minutados pelo líder do BCP e conter os action points (atividade/dono/deadline);
2. Ações Iniciais de Recuperação:
  - 2.1. Comitê de Riscos e Compliance: deverá se reunir assim que possível para avaliar o impacto do incidente nos diversos riscos (mercado, crédito, operacional, dentre outros) e caso necessário tomar as devidas ações;
  - 2.2. Comitê de Investimentos: o CIO e o CRO devem juntamente convocar uma reunião para verificar se todas as informações necessárias ao portfólio estão seguras. Dados faltando ou corrompidos devem ser comunicados ao comitê de crise. O time de Gestão e o CRO devem decidir se decisões de investimento são requeridas embora o trading discricionário deva ser minimizado de acordo com as novas condições operacionais da empresa.
  - 2.3. Operações (Middle Office): este time deverá continuar a manter informados o administrador do fundo, prime brokers e outros contrapartes operacionais-chave.
3. Cobertura de funções críticas: todas as áreas funcionais deverão ter previamente identificado as suas atividades críticas e o seu pessoal-chave necessário. Estas

funções deverão ser conduzidas com qualquer problema sendo escalado ao comite de crise.

#### 4. Data Management:

4.1. Migração dos trabalhos conduzidos externamente durante a crise para os sistemas essenciais (ou back-up)

4.2. Back-up de dados em ambiente de Recuperação

#### 5. Comunicação Externa: stakeholders-chave externos devem ser atualizados regularmente.

#### 6. Cenários de Retificação/ Contingência

6.1. Acesso ao prédio: no caso do prédio ter sido evacuado, ou o acesso a ele estar negado. é provavel que documentos ou hardware importantes estejam dentro

6.2. Buscar acomodação alternativa: no caso do prédio ter sido gravemente danificado ou destruído e a re-ocupação não seja possível a médio prazo (ou nunca mais).

#### B.1.2.3 – Retomada

A terceira fase é a transição entre estar trabalhando em “modo recuperação” para voltar ao modo normal (business as usual). Deve ser tratada – e gerida – como um projeto incluindo atividades, check-lists e gráficos de Gantt com uma clara linha do tempo.

Os temas cobertos por esta fase são dependentes do evento ocorrido mas podem incluir:

- Como a organização volta a estar em compliance novamente ?
- Algum sistema necessita ser reconstruído ?
- A empresa irá mudar para um novo escritório ?

#### B.1.3 – Redundâncias e Contingências

Em caso de eventos de crise, a MOAT possui contingências e redundâncias de forma a permitir a continuação de suas atividades mesmo em condições adversas.

#### B.1.3.1 – Redundância de TI / Back-up de Arquivos

Backup Server: O servidor possui software de backup (backup Windows 2016 e Ibackup), responsável pela realização de backup predefinido pela política da MOAT.

A MOAT disponibiliza em seus servidores o serviço de backup e restore de arquivos, que tem o intuito de garantir a segurança das informações, a recuperação em caso de desastres e garantir a integridade, a confiabilidade e a disponibilidade dos dados armazenados.

Os Backups são feitos através da ferramenta de backup do Windows 2016 Server e Arcserv Cloud e são salvos em disco externo e cloud com agenda diária das pastas de dados de toda a empresa, devendo ser usado em casos em que não é mais possível a recuperação do arquivo danificado ou perdido.

O serviço de e-mail da MOAT é garantido por parceiro Microsoft que provém suporte 24/7, serviço de anti spam, anti vírus, recuperação de informação, site de recuperação de desastre e alertas relacionados ao vazamento de informações confidenciais e privilegiadas. A MOAT possibilita o acesso remoto de todas as mensagens pelos colaboradores.

O serviço de e-mail da MOAT é garantido por dispositivo de segurança que executa funções de firewall e antivírus no nível do roteador. Além disso, Antivirus (software) é ativado em cada computador individual na rede de escritório.

#### B.1.3.2 – Redundância de Infraestrutura (Telecom, Internet e Energia)

##### Telefonia

A MOAT conta com serviço VOIP de Telefone sendo 14 linhas VOIP e 2 linhas analógicas. Em caso de falhas nas linhas telefônicas VOIP, os colaboradores da MOAT ainda possuem celulares que podem substituir a telefonia fixa.

##### Internet

O acesso à internet é disponibilizado por 3 links de velocidade de 30 mbps no link dedicado (Algar) e 2 links ADSL de 100 mbps link VIVO e NET

##### Energia

Em caso de falha de fornecimento de energia, a MOAT possui nobreak para suportar o funcionamento de seus servidores, rede corporativa, telefonia e de 2 estações de

trabalho (desktops) para a efetiva continuidade dos negócios durante 6 horas. Após 3 horas caso não retorne a energia a equipe será deslocada para o site backup.

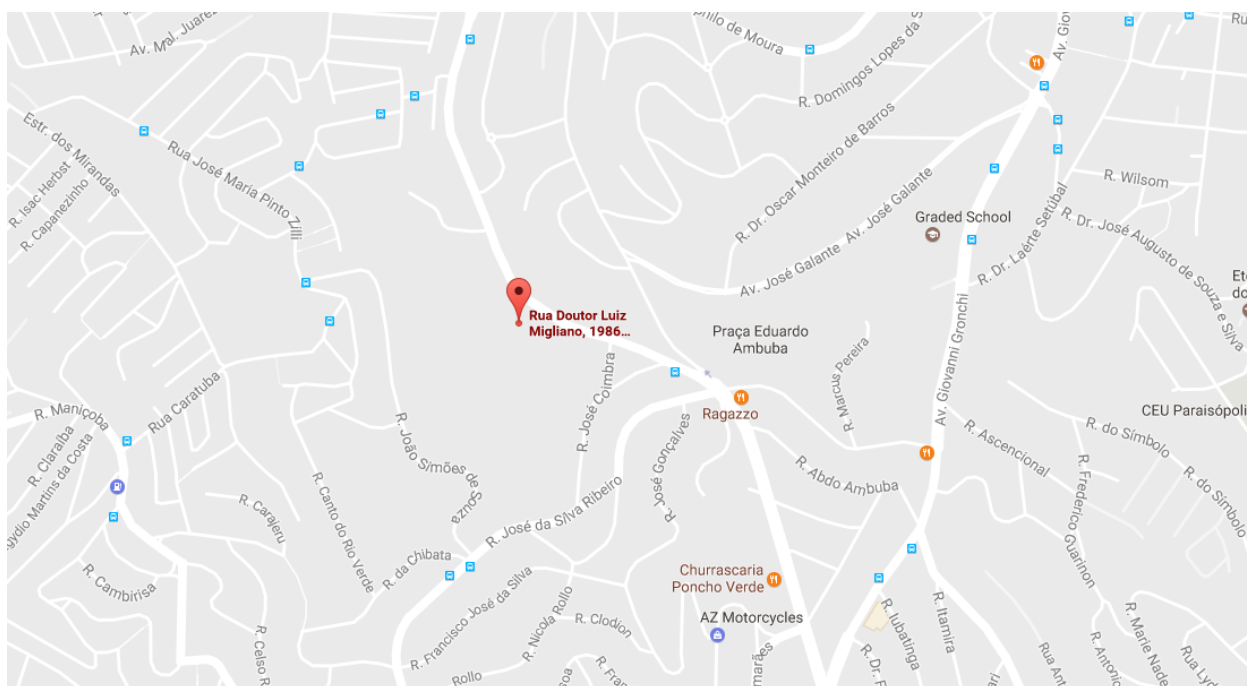
Teste de no-break realizado duas vezes por ano.

### B.1.3.3 – Site de Contingência e Home-Office

O escritório da MOAT encontra-se na Av. Brigadeiro Faria Lima, 3015, 11 andar, Itaim. Em caso da perda de acesso a este edifício, os colaboradores poderão: (a) acessar o site de contingência ou (b) trabalhar de casa com acesso VPN (home-office).

O site de contingência é o escritório do prestador de serviços (Tecoqualify) cujo endereço é:

**i** Rua Dr. Luiz Migliano, 1986 - 10 andar – São Paulo - SP  
 São Paulo/SP – CEP: 05711-001



O site de contingência fica a cerca de 8 km da sede da MOAT e pode ser acessado através de grandes vias como a Marginal Pinheiros. Em tráfego normal, pode-se chegar em 40 minutos.

No site de contingência, a MOAT possui posições de contingência. Estes postos possuem a “software-padrão” dos aplicativos essenciais da MOAT para operação e sistemas.

A MOAT também conta com acesso remoto via VPN à sua rede de dados e alguns aplicativos para os colaboradores que optarem pelo home-office. Tal acesso encontra-se disponível a todos os colaboradores autorizados pelo Compliance Officer.

Os aplicativos essenciais da MOAT estão listados abaixo bem como os a disponibilidade de acesso no site de contingência e no home-office via VPN:

Aplicativo	Site de Contingência	Home-Office (acesso VPN)
Email Outlook	✓	✓
Sophos Antivirus	✓	✓
Base de Dados	✓	✓
Feeders de cotações	✓ O software está instalado nos desktops de contingência.	✓



As informações dos portfólios além de estarem nos sistemas internos da MOAT são disponibilizadas diariamente pelo administrador, que também informará qualquer movimentação no passivo dos fundos para adequação do caixa dos fundos.

## B.1.4 – Lista de Contatos de Emergência


A MOAT desenvolveu uma lista de Contatos de Emergência que inclui os nomes, telefones, endereços de e-mail dentre outras informações críticas para o negócio. Esta lista inclui colaboradores-chave, distribuidores de fundos, clientes de carteiras administradas, contrapartes prestadores de serviços essenciais dentre outros contatos. Esta lista será revista e atualizada ao menos anualmente.

nome	empresa / função	telefone	celular	e-mail
------	------------------	----------	---------	--------

### Colaboradores

RODRIGO CARRERA	MOAT (líder BCP)	11 3181-8727	11 98301-7575	rodrigo.carrera@moat.com.br
DOUGLAS WANG	MOAT (back-up BCP)	11 3181-8726	11 97463-8477	Douglas.wang@moat.com.br

### Prestadores de Serviços / Contrapartes

 Antonio Rampazzo	Itau Corretora / Clearing	11 3073-3831		middlebovespa@itaubba.com
Clayton Campos	MOAT (Suporte TI)		11 98244 7988	clayton@tecnoqualify.com.br
Luis Sposito	Safra corretora	11 35759611		Luis.sposito@safra.com.br
Waldir	CS Corretora	11 3701-6285		
LUCIANO HADDAD	Itau Coroporate	11 3072-6182		Luciano.haddad@itau-unibanco.com.br
WALTER MORAIS	CAPITAL MARKETS	3842-9977		Walter.morais@cmcapital.com.br
PEDRO JUCA	XP CORRETORA			



## B.1.5 – Revisão Anual, Atualização, Treinamento e Testes

### B.1.5.1 – Revisão Anual e Atualização

O BCP deverá ser revisado anualmente e atualizado sempre que for necessário. Cada revisão deverá ser aprovada pelo Diretor de Compliance (Compliance Officer) e as cópias do plano revisado deverão ser distribuídas a todos os colaboradores-chave da MOAT. O BCP também será revisto caso aconteça alguma das situações abaixo:

- Mudanças materiais – organizacionais – no negócio da MOAT
- Mudanças de pessoal
- Mudança de endereço do escritório da MOAT ou abertura de um escritório adicional
- Introdução de novos processos ou alteração dos existentes
- Upgrade ou alterações na infraestrutura de IT e/ou sistemas
- Mudança de prestador de serviço relevante
- Alterações de informações de contatos (p.e., números de telefone)

### B.1.5.2 – Treinamento e Testes

O treinamento do staff em relação ao BCP ocorre fundamentalmente com os procedimentos de teste. O único treinamento adicional requerido é uma apresentação do BCP em uma única sessão a ser feita no momento de sua publicação. No caso de um novo colaborador a equipe de compliance fará para ele(a) a última apresentação feita.

O BCP deve ser testado para garantir que o mesmo funcione em caso de necessidade. Diferentes cenários de eventos devem ser testados ao menos anualmente. Os principais testes são elencados a seguir

#### Call Tree

O líder do BCP começará o teste fora do horário comercial - sem aviso prévio - transmitindo uma palavra código para os participantes do call tree. No dia seguinte, todos os participantes deverão reportar a palavra-código transmitida. Este teste avalia a viabilidade do call tree e se os números de telefone foram corretamente registrados.

#### Conectividade Remota e Site de Contingência

Todo o staff que possuir acesso remoto via VPN (Virtual Private Network) deverá se logar na rede da MOAT a partir de casa e checar se todos os sistemas essenciais e acessos funcionam perfeitamente. Um colaborador da equipe de Gestão e um de Middle-Office/Riscos deverão efetuar os testes através dos notebooks localizados no site de contingência.

#### Redundância de TI

Durante um final de semana, o provedor de serviços de TI (Technoqualify) irá acionar o sistema back-up e todo o staff tentará logar no sistema testando as aplicações essenciais. Posteriormente – no mesmo final de semana – o sistema principal/primário será acionado novamente, para testar o processo de retomada.

#### Redundância de Telecom

Durante um final de semana, todas as linhas fixas de telefone serão testadas e então estes serão testados através de um call tree para telefones fixos. Posteriormente – no mesmo final de semana – as linhas fixas serão reativadas e testadas como parte do processo de retomada.

#### Redundância de Energia (No-Breaks)

Durante um final de semana, a energia será desligada e o no-break interno entrará em funcionamento. Os acessos e os sistemas essenciais deverão ser checados. Posteriormente – no mesmo final de semana – a energia será reativada e os acessos novamente testados como parte do processo de retomada.

#### Teste Completo

Durante um dia útil a ser combinado, a estrutura primária de TI será desligada pela manhã e o sistema de back-up entrará em vigor; os telefones fixos serão desviados para os celulares e nenhum staff (incluindo prestadores de serviços de TI) serão permitidos no escritório. Todo o staff trabalhará de casa [OU SITE DE CONTINGENCIA] priorizando as atividades essenciais da análise de impacto no negócio. O time de Crise gerenciará ativamente o teste organizando conference calls conforme planejado. No final do dia, os sistemas primários de IT e a telefonia fixa serão restaurados. No dia seguinte, todo o staff deverá checar se os arquivos foram propriamente salvos nos servidores primários. Este teste também verificará se as atividades chaves foram corretamente identificadas dentre outros.

#### B.1.6 – Obrigações dos Colaboradores da MOAT em relação ao BCP

O BCP somente funcionará com o devido engajamento de todos os colaboradores-chave da MOAT. Os colaboradores da MOAT deverão obrigatoriamente:



- Manter uma versão impressa atualizada do BCP em casa e no escritório;
- Ter programado no seu celular os números dos telefones do líder do BCP, seus colegas imediatos e do seu supervisor;
- Ter o número do conference call do BCP programado no celular e a senha de acesso ao conference room facilmente acessível;
- Testar periodicamente o acesso aos sistemas primários e back-ups via VPN (aqueles que tiverem acesso e estrutura computador/internet para o home-office);
- Manter uma política de mesa limpa (clean desk policy): no caso de um roubo ou incêndio, os papéis guardados ficam muito mais seguros do que aqueles deixados soltos;
- Os colaboradores que gerenciem ou tenham relacionamentos com prestadores de serviços também devem manter programados os contatos destes no celular.

#### B.1.7 – Atividades e Responsabilidades relacionadas ao BCP

Os responsáveis pelas atividades relacionadas ao BCP da MOAT são listados a seguir:

Manutenção e Atualização do Plano	RODRIGO CARRERA	
Aprovação, Revisões e conduzir revisão anual	RODRIGO CARRERA	
Treinamento e Teste anual do plano	RODRIGO CARRERA	
Implementação do plano em caso de necessidade	Emergency Response Team	
Revisão Trimestral da lista de Contatos de Emergência	RODRIGO CARRERA	
Manutenção e distribuição da lista de Contatos de Emergência	RODRIGO CARRERA	

Prover informações do plano para investidores e CVM	RODRIGO CARRERA	
Revisar BCPs de prestadores de serviços essenciais <ul style="list-style-type: none"> <li>• Na contratação dos serviços</li> <li>• Na revisão anual do BCP da MOAT</li> </ul>	RODRIGO CARRERA	

#### B.1.8 – Controle do Documento

O presente documento deve ser aprovado e revisado no mínimo anualmente pelo Comitê de Riscos e Compliance (CRC) da MOAT:

Versão	Autor	Data	Comentário
1.3	RODRIGO CARRERA	Out/2018	Atualização

## POLÍTICA DE INVESTIMENTOS PESSOAIS

### OBJETIVO

O objetivo desta Política é estabelecer procedimentos e regras para os investimentos pessoais dos colaboradores da Moat Capital, bem como dos investimentos proprietários da gestora, evitando assim eventuais conflitos de interesse com as estratégias, operações e posições detidas nos fundos geridos.

### REGRAS

Os investimentos pessoais devem ser guiados de forma que não interfiram negativamente no desempenho das atividades profissionais. Os mesmos devem ser integralmente separados das operações de investimentos realizados em nome dos fundos geridos pela Moat Capital, de modo que sejam evitadas situações que configurem conflito de interesses. Sendo assim, A Moat Capital definiu as seguintes regras, que devem ser observadas por todos os seus colaboradores:

- I. São vedadas aplicações em quaisquer títulos e valores mobiliários que sejam objeto de cobertura pela equipe de gestão da MOAT Capital;
- II. Investimentos pessoais em cotas de fundos de investimentos de qualquer espécie são livres;
- III. Investimentos pessoais em cotas de fundos de investimentos de qualquer espécie, geridos por terceiros, são livres;
- IV. Instrumentos de renda fixa livremente negociados e de boa liquidez, exceto se tais instrumentos forem objeto de investimento dos fundos geridos pela Moat Capital;
- V. Não há obrigatoriedade na venda de posições já detidas quando do início do vínculo com a empresa, porém (i) as mesmas devem ser informadas tão logo efetivado o vínculo do Colaborador com a empresa e (ii) as vendas devem ser previamente informadas ao Diretor de Compliance;
- VI. Quaisquer exceções referentes a prazos e ativos não tratadas nesta política devem ser submetidas e autorizadas pelo Diretor de Compliance com

antecedência à efetivação da operação. O Colaborador deve atuar de forma a preservar sua própria reputação, bem como a imagem da Moat Capital e os interesses de seus clientes e do mercado em geral.

## **MONITORAMENTO**

É responsabilidade do Diretor de Compliance assegurar a implementação de mecanismos eficientes capazes de resguardar a observância das regras acerca de investimentos pessoais dos Colaboradores da Moat, bem como a identificação de quaisquer infrações às regras aprovadas no presente Capítulo.

Os Colaboradores deverão apresentar anualmente ao Diretor de Compliance, dentro de até 30 (trinta) dias contados do encerramento de cada ano civil, uma Declaração de Investimentos Pessoais (na forma do “Anexo II”), atestando que nada foi praticado durante o período em desacordo com a presente Política de Investimento Pessoal e apresentando uma descrição completa de sua carteira de investimentos pessoais no mercado financeiro no último dia do semestre imediatamente anterior, bem como em mais duas datas a serem selecionadas de forma aleatória pelo Diretor de Compliance para cada semestre, conforme comunicadas aos Colaboradores, no último dia após o encerramento do semestre.

O Diretor de Compliance poderá, a qualquer tempo e a seu exclusivo critério, solicitar a Colaboradores que apresentem uma descrição completa dos investimentos das demais pessoas diretamente vinculadas ao Colaborador na forma desta Política de Investimento Pessoal e cópias de extratos de suas contas pessoais mantidas junto a corretoras de valores mobiliários e outras instituições financeiras com quem o Colaborador tenha conta, dentro de até 15 (quinze) dias da data da solicitação.

## **VEDAÇÕES**

- I. É vedado ao Colaborador realizar operações com instrumentos derivativos (futuros, opções, termos etc.) sem autorização prévia e por escrito do Diretor de Compliance.

- II. É vedado ao Colaborador administrar recursos de terceiros diretamente, de forma não vinculada à MOAT, sejam eles com qualquer espécie de vínculo.
- III. O Colaborador não poderá conscientemente atuar como contraparte, direta ou indiretamente, em negócios com carteiras que administre.
- IV. É vedado ao colaborador possuir posições em que a MOAT tenha posições.

### **INVESTIMENTOS DA GESTORA – CARTEIRA PRÓPRIA**

A Moat Capital não possui carteira própria ativa, nem tampouco investe nos Fundos geridos pela própria Gestora. Os recursos são alocados de forma conservadora, em títulos públicos de emissão do tesouro nacional, ou fundos de investimentos de renda fixa com liquidez diária, mantidos em instituições de grande porte.

### **DISPOSIÇÕES GERAIS**

Quaisquer dúvidas em relação à interpretação desta Política de Investimentos Pessoais (ou de qualquer outra parte deste Manual) devem ser imediatamente informadas ao diretor de Compliance, para que sejam sanadas previamente à realização de quaisquer investimentos pessoais pelos Colaboradores.

O Colaborador fica obrigado a, sempre que detectar toda e qualquer situação de Conflito de Interesse, conforme acima definido, ainda que potencial, não realizar a operação ou se desfazer de sua posição de investimentos.

### **VIGÊNCIA E ATUALIZAÇÃO**

Esta política será revisada anualmente, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo. A presente política poderá ainda ser alterada a qualquer tempo em razão de circunstâncias que demandam tal providência.





## TERMO DE RESPONSABILIDADE E ADESÃO AO MANUAL DE OPERAÇÕES (ANEXO I)

Nome do Colaborador:

Função:

Eu, \_\_\_\_\_, inscrito no CPF \_\_\_\_\_ - \_\_\_\_,  
declaro para os devidos fins que:

Tenho total conhecimento da existência do Manual de operações da MOAT CAPITAL GESTÃO DE RECURSOS LTDA. (“MOAT”), o qual recebi e li, sendo que comprometo-me a observar integralmente seus termos e condições.

Estou ciente que a não observância dos termos do Manual de operações poderá implicar na caracterização de falta grave, fato que poderá ser passível da aplicação das penalidades cabíveis, inclusive demissão por justa causa.

Tenho ciência de que o descumprimento de qualquer regra estabelecida na Política de Confidencialidade, disposta neste Manual de Operações poderá me sujeitar a penalidades e responsabilização na esfera civil e criminal. Adicionalmente, sei que, caso haja o vazamento de informação confidencial advindo da utilização de minha senha pessoal, poderei ser responsabilizado tanto civil, quanto penalmente.

Reconheço e confirmo meu conhecimento e concordância sobre que nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada fora da MOAT, bem como de que fica vedada qualquer divulgação, no âmbito pessoal ou profissional, que não esteja em acordo com as normas legais e de compliance da MOAT.

Estou ciente que o disposto na política de confidencialidade do presente Manual de Operações, é aderido, por meio deste Termo de Adesão, em caráter irrevogável e irretratável, por prazo indeterminado, válido indefinidamente mesmo após o término de meu vínculo com a MOAT, não podendo ser rescindido sem expressa e inequívoca concordância da MOAT.

Estou ciente de que a política de investimentos pessoais constante do Manual de Operações da MOAT, como um todo e passa a fazer parte dos seus deveres como Colaborador da MOAT.

Li e entendi a legislação e regulamentação aplicável a negociação de valores mobiliários, em particular, conforme disposto na Instrução CVM nº 358/2002, conforme alterada, acerca de divulgação e o uso de informações sobre ato ou fato relevante na negociação de valores mobiliários de emissão de companhias abertas.

Comprometo-me a fornecer anualmente a Declaração de Investimentos Pessoais, constante do presente Código de Conduta da Sociedade, na forma do Anexo II.

Em [ ].[ ].[ ], participei do treinamento específico realizado em consonância com a política de treinamento do presente Manual de Operações, sendo que compreendi perfeitamente as regras estabelecidas pelo Manual de operações da MOAT e aderi ao mesmo, comprometendo-me a observar integralmente os termos e condições que me foram apresentados.

Para tanto, assino o presente Termo e declaro estar ciente das minhas responsabilidades no cumprimento das referidas regras e comprometo-me a zelar pelo desenvolvimento de minhas atividades de acordo com as determinações da MOAT especificadas no documento.

Local e Data

---

Assinatura

## DECLARAÇÃO ANUAL DE INVESTIMENTOS (ANEXO II)

Eu, \_\_\_\_\_, inscrito no CPF \_\_\_\_\_ - \_\_ declaro para os devidos fins que os meus investimentos pessoais, incluindo os investimentos pessoais de meu cônjuge ou companheiro(a), não possuem nenhum conflito com as posições da MOAT Capital Gestão de Recursos LTDA (“MOAT”), e que nada foi praticado durante o ano de [\_\_\_\_] em desacordo com o Manual de operações da MOAT

Declaro ainda que todos os investimentos por mim detidos estão plenamente de acordo com o Manual de operações da MOAT, não caracterizando quaisquer infrações ou conflitos de interesse, nos termos dos referidos documentos, exceção feita aos investimentos relacionados na tabela abaixo:

Ativo	Emissor	Quantidade	Valor	Data de Aquisição	Conflito

Local e data

\_\_\_\_\_

Assinatura