PROA CAPITAL

Gestão de Recursos em Ativos Judiciais

PROA GESTORA DE RECURSOS LTDA - CNPJ: 62.200.538/0001-05

MANUAL DE COMPLIANCE

SUMÁRIO DO DOCUMENTO	Dispõe sobre as regras, procedimentos e controles internos da empresa, estabelece os seus padrões de ética e conduta, inclusive quanto à negociação de valores mobiliários por colaboradores e questões de rateio e
Referência	Dezembro/2025
Confidencialidade	Público
Versão	1
Estado	Aprovado
Emissor	Risco e Compliance
Autor	Andressa Vianna Santos Viceconti
Cargo do Autor	Diretora de Risco e Compliance
Data de Criação	03/12/2025
Última Atualização	03/12/2025
Data de Publicação	03/12/2025

MANUAL DE COMPLIANCE

1 INTRODUÇÃO

A **PROA GESTORA DE RECURSOS LTDA** ("PROA") possui estrito compromisso para com o cumprimento de toda e qualquer legislação e regulação aplicável ao escopo das suas atividades, e em especial para com a manutenção de padrões de ética e conduta que zelem:

- pela integridade dos mercados, do ambiente regulatório, e do sistema econômico-social como um todo;
- pela defesa dos melhores interesses dos seus cotistas/investidores;
- pelo desenvolvimento de seus colaboradores.

A **PROA**, como gestora de recursos é regulada, principalmente, pela Comissão de Valores Mobiliários ("CVM"), observando também as disposições contidas nos códigos de autorregulação da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais ("ANBIMA"), a qual deseja ser associada.

Este documento determina e descreve as diversas práticas adotadas pela **PROA** para garantir que as suas atividades se desenvolvam zelando pela integridade dos mercados, interesses dos cotistas/investidores, ao mesmo tempo que atende à exigência da regulação vigente quanto à existência de documentação e descrição de tais práticas.

1.1 ABRANGÊNCIA

Este documento ("Manual de Compliance") abrange e aplica-se a todos os sócios, diretores, funcionários, colaboradores e administradores ("colaboradores") da **PROA**. Os colaboradores devem de forma prévia ao início da sua efetiva participação nos negócios da empresa tomar conhecimento do Manual de Compliance, assinando inclusive termo de ciência e compromisso de cumprimento para com o aqui disposto.

1.2 TREINAMENTO

O treinamento e desenvolvimento das competências dos colaboradores será parte integrante da operação da **PROA** para o contínuo aprimoramento da qualidade do serviço de gestão de recursos prestado. Nesse contexto, e em específico no que diz respeito ao disposto por este documento, todos os colaboradores após tomarem ciência do Manual de Compliance, participam de treinamento presencial específico. Serão ainda realizados treinamentos de assuntos que permeiam a área de Risco e Compliance, como Prevenção a Lavagem de Dinheiro, Financiamento ao Terrorismo e Proliferação de Armas de Fogo ("PLD/FTP"), Segurança da Informação, *Insider Trading*, Ética e demais temas, que a diretoria entender necessário para manter a integridade e aderência de seus colaboradores as boas práticas de mercado, sendo os treinamentos no mínimo, anuais, aplicável a todos os colaboradores.

A área de Risco e Compliance manterá comunicação contínua com os colaboradores, informando-os conforme existam alterações às disposições legais aplicáveis, ou a este documento, circulando-as por meio de correio eletrônico ("e-mail").

1.2.1 CERTIFICAÇÃO PROFISSIONAL

Para o exercício de atividades relacionadas diretamente ao processo de gestão de recursos, os colaboradores devem possuir certificações profissionais compatíveis com as funções desempenhadas, conforme regras da ANBIMA e demais normas aplicáveis. A área de Risco e Compliance é responsável por manter o controle das certificações vigentes dos colaboradores, seus prazos de renovação e, quando aplicável, a atualização das informações junto à ANBIMA.

Colaboradores recém-contratados para funções que exijam certificação específica poderão ingressar na PROA sem a certificação, desde que assumam o compromisso de obtê-la no prazo de até 6 (seis) meses contados do início de suas atividades. O não cumprimento desse prazo poderá ensejar medidas disciplinares, incluindo eventual afastamento.

A área de Risco e Compliance comunicará aos colaboradores, com antecedência mínima de 3 (três) meses, a proximidade do vencimento das certificações, bem como a necessidade de renovação. Caso a certificação expire

durante o exercício das atividades, o colaborador deverá apresentar justificativa formal e plano de regularização, sujeito à avaliação da Diretora de Risco e Compliance.

O Diretor de Gestão, responsável perante a CVM pelo exercício da atividade de administração de carteiras, bem como eventuais colaboradores que participem do processo decisório de investimentos, deverão manter certificação ANBIMA CGA e/ou CGE ativa(s), em conformidade com o Código ANBIMA de Certificação. O cumprimento desses requisitos será monitorado pela área de Risco e Compliance.

1.3 SEGREGAÇÃO DE FUNÇÕES

A área de Risco e Compliance é única e atua de forma independente das demais áreas da PROA. Cabe à Diretora de Risco e Compliance a coordenação das atividades, bem como a delegação de tarefas aos colaboradores que integram a área. A estrutura funciona com segregação funcional e lógica, assegurando autonomia para reportar inconformidades, solicitar informações e acessar os dados necessários ao desempenho de suas atribuições.

As atividades desempenhadas pela área abrangem duas frentes principais:

Compliance: refere-se ao cumprimento das políticas internas, normas aplicáveis, padrões de conduta, regras de relacionamento com contrapartes e observância dos deveres fiduciários, além do monitoramento de potenciais riscos decorrentes dessas práticas.

Risco: inclui o monitoramento dos limites regulamentares e normativos aplicáveis aos veículos sob gestão, acompanhamento das exposições de risco, análise da precificação de ativos e verificação da consistência da infraestrutura de sistemas e controles operacionais relacionados ao processo de investimento.

A área de Risco e Compliance é independente da área de Gestão, tanto em suas funções quanto em sua linha de reporte. Os integrantes da área respondem diretamente à Diretora de Risco e Compliance, com plena autonomia para levantar dúvidas, solicitar informações e apontar eventuais irregularidades. A relação entre a Diretora de Risco e Compliance e o Diretor de Gestão é horizontal e funcional, garantindo a necessária segregação e independência entre as atividades de investimento e as atividades de controle.

2 CÓDIGO DE ÉTICA E CONDUTA

A PROA e os seus colaboradores comprometem-se a exercer as suas atividades com boa fé, transparência, diligência e lealdade para com os objetivos de investimento e melhores interesses dos seus cotistas/investidores, bem como pela integridade dos mercados. Os princípios norteadores devem ser os de liberdade de iniciativa, livre concorrência, e de clareza de comunicação, inclusive no que diz respeito à remuneração dos seus serviços.

Para fins do disposto acima, a PROA e os seus colaboradores devem empregar na condução das suas atividades de gestão de recursos os mesmos cuidados que qualquer pessoa prudente deve ter na administração dos seus próprios negócios, podendo responder por quaisquer infrações ou irregularidades que venham a ser cometidas decorrentes de falta de diligência.

Devem evitar qualquer prática que infrinja a legislação e regulação vigente, os regulamentos e políticas de investimento dos veículos sob gestão, ou venha a ferir o relacionamento fiduciário assumido para com os cotistas/investidores em sentido amplo.

Qualquer benefício que a PROA ou os seus colaboradores venham a ter em função da sua condição de gestor de recursos deverá ser transferido ao veículo de investimento em questão, salvo à existência de disposição específica para essas circunstâncias nas normas do veículo, ou enquadramento do benefício nos casos permitidos pelas regras de *soft dollar* indicadas no item 2.2 deste documento.

Independentemente da existência de treinamentos com periodicidade pré-definida e da contínua comunicação da área de Risco e Compliance com os colaboradores em questões de observância legal, é de responsabilidade individual dos colaboradores o conhecimento de qualquer disposição legal aplicável às suas atividades.

Os colaboradores devem respeitar e tratar com respeito e cordialidade todos os agentes, internos ou externos, com quem venham a estabelecer contato no exercício das suas atividades. A PROA repudia qualquer tipo ou forma de assédio ou discriminação, seja ela étnica, de gênero, de orientação sexual, ou de qualquer outra natureza.

Os colaboradores têm a obrigação e autonomia necessária para reportar diretamente ao Diretor de Risco e Compliance qualquer tipo de observação em relação à condução dos negócios da empresa que entendam ir contra as disposições legais aplicáveis ao disposto neste documento, e os princípios de idoneidade moral e profissional.

2.1 CONFLITO DE INTERESSES

A existência de conflitos de interesses surge, principalmente, quando existe relação, seja ela direta ou indireta, entre a PROA ou qualquer um dos seus colaboradores com empresas, cotistas e demais contrapartes que venham a estar envolvidas nos negócios.

É de responsabilidade dos colaboradores atentarem-se para o potencial surgimento de qualquer tipo de conflito de interesses e, caso identificado, reportá-lo imediatamente ao Diretor de Risco e Compliance. Após recebimento de tal comunicação, o Diretor de Risco e Compliance deverá deliberar quanto à necessidade de afastamento do colaborador da operação em questão.

2.1.1 PARTICIPAÇÃO DOS SÓCIOS EM OUTRAS EMPRESAS

Os sócios e diretores da PROA possuem participação em outras empresas e, assim sendo, encontram-se em situação de potencial surgimento de conflitos de interesses. Para mitigação de situações em que tais conflitos se venham a efetivamente materializar, é vedada a aprovação estrutural de qualquer parte relacionada enquanto contraparte para realização de operações em regime normal de negócios.

2.1.2 OPERAÇÕES COM PARTES LIGADAS

Operações em que partes ligadas figurem como contraparte podem ser realizadas, desde que observadas medidas específicas de controle e mitigação de conflitos de interesses. Para sua aprovação, a operação deverá:

- ser apresentada para análise da área de Risco e Compliance, que avaliará a pertinência, a regularidade e a compatibilidade da operação com os melhores interesses dos cotistas;
- ser comunicada aos cotistas dos veículos envolvidos, quando aplicável, conforme exigências regulatórias;
- contar, quando necessário, com declaração formal dos sócios e diretores envolvidos, atestando que a operação atende aos melhores interesses dos cotistas e não configura benefício próprio, direto ou indireto.

Para identificar operações que possam caracterizar conflito de interesses, bem como prevenir e mitigar riscos relacionados, a PROA adotará as seguintes práticas:

- monitoramento das operações e rotinas diárias da empresa;
- revisão periódica de correspondências eletrônicas e demais comunicações relacionadas ao processo de investimento, quando aplicável;
- promoção contínua da cultura ética, incentivando colaboradores a reportarem situações que possam configurar conflito de interesses.

Nos casos em que algum dos veículos envolvidos seja fundo de investimento regido pelo Anexo Normativo IV da Resolução CVM nº 175, conforme alterada, a operação deverá ser submetida à aprovação dos cotistas em assembleia geral, quando exigido pela regulamentação aplicável.

2.2 *SOFT DOLLAR*

Entendem-se como práticas de *soft dollar* o recebimento por parte da PROA, dos seus sócios, diretores, funcionários, colaboradores ou administradores, de regalias oferecidas por corretoras, ou demais intermediários, em função da existência de relacionamento de execução de ordens remunerado por taxas de corretagem, ou qualquer outro tipo de vínculo remuneratório associado às suas atividades de gestão de recursos.

A PROA permite relacionamentos que envolvam práticas de *soft dollar*, desde que:

- O valor dos serviços recebidos pela prática de *soft dollar* tenham razoabilidade e sejam compatíveis com o relacionamento existente entre a PROA e a corretora ou demais intermediários; e

- O recebimento de tais serviços tenha como objetivo trazer benefícios para a qualidade do serviço de gestão de recursos prestado aos seus cotistas e investidores.

Tendo o acima exposto, é, portanto, vedado o recebimento de regalias de qualquer natureza que visem o benefício próprio, ou de terceiros, por parte da PROA, dos seus sócios, diretores, funcionários, colaboradores ou administradores.

As principais formas de *soft dollar* aceitas são: serviços de pesquisa ("*research*"), cursos e convites para eventos.

A aceitação de práticas de *soft dollar* devem ser reportadas previamente à área de Risco e Compliance, caso a caso, a qual analisará a regularidade e compatibilidade das regalias recebidas para com aqui disposto.

2.3 SIGILO DA INFORMAÇÃO

No exercício de suas atividades, os colaboradores da PROA terão acesso a informações não públicas relacionadas à empresa, aos veículos sob gestão, a estratégias de investimento, a contrapartes e a demais dados sensíveis. Tais informações devem ser tratadas com sigilo e utilizadas exclusivamente para fins profissionais, sendo vedada qualquer divulgação ou compartilhamento indevido, inclusive após o término do vínculo do colaborador com a empresa.

É proibido o envio ou armazenamento de informações da PROA em dispositivos pessoais, contas de e-mail particulares, unidades externas (como pen-drives) ou quaisquer meios não autorizados. O compartilhamento de documentos deve ocorrer somente pelos canais corporativos autorizados, como a plataforma Microsoft 365, que possui controles de acesso e rastreabilidade.

A impressão de documentos físicos somente deve ocorrer quando estritamente necessária, cabendo ao colaborador garantir sua guarda adequada e posterior descarte seguro.

Classificação da Informação

Para fins de organização e proteção, os documentos e arquivos da PROA são classificados em duas categorias principais:

- Confidencial: informações não públicas, acessíveis apenas a colaboradores autorizados. Seu compartilhamento externo exige autorização prévia da Diretora de Risco e Compliance.
- Uso Interno: informações destinadas exclusivamente ao ambiente interno da PROA, cujo compartilhamento externo é vedado.

Em situações que envolvam terceiros prestadores de serviços que necessitem acessar informações sigilosas, será exigida a assinatura de termo de confidencialidade específico.

2.3.1 ASSINATURA DE TERMO DE CONFIDENCIALIDADE

Todos os colaboradores da PROA assinam de forma prévia ao início efetivo da sua participação nos negócios da empresa um termo de estrito compromisso e confidencialidade em relação às informações que venham a obter como consequência do exercício das suas atividades, nos termos do Anexo II do Código de Ética, o qual se entende, inclusive, após eventual encerramento da sua relação com a empresa.

2.3.2 TRATAMENTO DE VAZAMENTO DE INFORMAÇÕES

Para lidar com possíveis situações que gerem o vazamento de informações sigilosas, ainda que involuntariamente, toda a circulação de informação é acompanhada de um aviso legal relacionado ao eventual mau direcionamento. No aviso legal é informado que a mensagem é confidencial, e solicita-se, caso o receptor identifique não ser o destinatário pretendido, que ele imediatamente elimine quaisquer registros da mensagem, comunique o remetente do ocorrido, e abstenha-se de divulgar ou de qualquer forma utilizar a informação obtida.

Havendo a ciência de mau direcionamento / vazamento de informação confidencial, o Diretor de Risco e Compliance deverá ser imediatamente informado, de tal forma que este possa analisar e mensurar a gravidade da situação, e possíveis cursos de ação em resposta ao incidente. Tais cursos de ação poderão levar:

- Ao desligamento do quadro da empresa, caso a infração tenha sido cometida por funcionário;

- À rescisão do respetivo contrato, caso a infração tenha sido cometida por um prestador de serviços;
- À comunicação aos agentes envolvidos no contexto da informação vazada, e cujos interesses possam vir a ser prejudicados; e/ou
- À comunicação aos órgãos reguladores de mercado aplicáveis, para que, em determinada materialidade da informação, caso entendam necessário, estabeleçam plano de supervisão específico e/ou apliquem sanções.

3 NEGOCIAÇÃO DE ATIVOS E VALORES MOBILIÁRIOS POR COLABORADORES

A detenção de informações sigilosas abre espaço para que um colaborador investido de má-fé tenha atitudes contra a integridade do mercado, em especial no que diz respeito à concorrência desleal. As principais práticas nesse contexto dizem respeito ao conceito de *insider trading* em sentido amplo, entendido aqui como a negociação, de forma direta ou indireta, de ativos e valores mobiliários para benefício próprio, ou de terceiros, através do uso de informações sigilosas que tenha vindo a obter no exercício das suas atividades.

Em linha com o exposto nos itens anteriores no que se refere à obtenção de informação sigilosa, é completamente vedado aos colaboradores qualquer tipo de prática que se configure como *insider trading*.

Ainda que não estabeleça vedações estritas à negociação de ativos e valores mobiliários por parte dos seus colaboradores, para fins de prevenção de tal prática, os mesmos deverão prestar declarações semestrais ao Diretor de Risco atestando que não realizaram qualquer tipo de operação, de forma direta ou indireta, com uso de informação sigilosa, nem qualquer outro tipo de prática que prejudique a integridade do mercado, sendo os únicos responsáveis por qualquer ato ou omissão relacionada a tal afirmação.

4 SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA

Além dos padrões de ética, conduta, confidencialidade e prevenção a conflitos de interesses, a PROA adota controles e práticas de segurança da informação compatíveis com o seu porte e com a natureza das atividades desempenhadas pela gestora. Esses controles têm como objetivo mitigar riscos operacionais, proteger dados sensíveis e monitorar eventuais descumprimentos das políticas internas.

Cada colaborador é responsável pela proteção das informações às quais tem acesso, devendo seguir as diretrizes deste Manual, o Código de Ética e as instruções operacionais aplicáveis às suas funções. O uso correto dos sistemas corporativos, o respeito às permissões de acesso e a adoção de boas práticas de segurança são essenciais para garantir a integridade das informações.

A PROA mantém controles capazes de identificar os acessos realizados por cada colaborador, garantindo rastreabilidade e permitindo a apuração de eventuais incidentes, mau uso ou práticas indevidas relacionadas às informações ou sistemas da empresa.

4.1 CONTROLE DE ACESSO

Para prevenir acessos indevidos e garantir a proteção das informações da PROA, são adotados controles de acesso compatíveis com o porte e a estrutura operacional da gestora. A segregação ocorre de forma funcional e lógica, assegurando que cada colaborador tenha acesso apenas aos sistemas, pastas e documentos necessários ao desempenho de suas atividades.

O acesso aos computadores, diretórios e arquivos é protegido por senhas individuais, que devem ser mantidas sob sigilo. Sempre que disponível, é utilizada autenticação em dois fatores, além de permissões diferenciadas conforme função e área de atuação. É expressamente proibido o compartilhamento de senhas ou credenciais entre colaboradores.

As informações corporativas devem ser acessadas exclusivamente pelos canais autorizados (como Microsoft 365), que permitem rastreamento e controle de permissões. O ambiente físico de trabalho segue boas práticas de segurança, incluindo cuidados básicos quanto à visualização de telas e guarda adequada de documentos impressos quando estritamente necessários.

Esses controles têm como objetivo mitigar riscos de vazamento de informações, prevenir conflitos de interesses e garantir que decisões e atividades sejam conduzidas com independência e segurança.

4.2 REGISTRO E RASTREABILIDADE DE COMUNICAÇÕES

A PROA utiliza sistema de telefonia VoIP em nuvem, que permite comunicação estável entre colaboradores, prestadores de serviço e contrapartes. Embora não haja gravação automática de chamadas, a gestora adota mecanismos formais para assegurar rastreabilidade e registro adequado das informações relevantes.

Qualquer orientação operacional, instrução de investimento, comunicação sensível, decisão relevante ou manifestação que possa gerar obrigação para a empresa deve ser formalizada em meio rastreável, preferencialmente por e-mail corporativo ou mensagem registrada em sistemas autorizados. Tais registros são armazenados nos ambientes corporativos de nuvem da PROA (Microsoft 365), com controle de acesso e histórico de versões.

A área de Risco e Compliance poderá solicitar, sempre que necessário, a formalização posterior de informações discutidas verbalmente, garantindo que decisões sejam documentadas de forma íntegra, auditável e aderente à regulamentação aplicável.

4.3 ARMAZENAGEM DE DADOS

A PROA realiza o armazenamento de documentos, registros e informações operacionais exclusivamente em ambiente corporativo em nuvem, por meio da plataforma Microsoft 365, que oferece infraestrutura segura, com controle de acesso, autenticação multifator e histórico de versões.

Todos os arquivos são mantidos em diretórios estruturados no SharePoint e no OneDrive corporativo, com permissões de acesso definidas conforme função, garantindo segregação, rastreabilidade e integridade das informações.

A solução em nuvem utilizada executa rotinas automáticas de backup e retenção, permitindo recuperação de arquivos alterados ou excluídos dentro das janelas de retenção previstas pelo provedor. Documentos classificados como confidenciais ou restritos são acessíveis apenas a usuários autorizados.

O ambiente em nuvem oferece criptografia em repouso e em trânsito, além de monitoramento contínuo de segurança e prevenção a acessos indevidos, alinhado às práticas recomendadas de cibersegurança para o setor financeiro.

4.4 AMBIENTES DE ARMAZENAGEM E *BACKUP*

A PROA utiliza exclusivamente ambientes em nuvem corporativos para armazenamento, organização e controle de documentos, por meio da plataforma Microsoft 365 (SharePoint e OneDrive), que garante segurança, redundância e disponibilidade contínua.

Os ambientes de armazenamento são estruturados da seguinte forma:

- Ambiente de Produção: diretórios oficiais da empresa no SharePoint, onde são mantidos todos os arquivos operacionais, administrativos e regulatórios.
- Backup e retenção automática: o Microsoft 365 mantém histórico de versões, backup automático contínuo e políticas de retenção que permitem restaurar arquivos excluídos ou modificados indevidamente dentro dos prazos definidos pelo provedor.
- Recuperação de arquivos: tanto o SharePoint quanto o OneDrive oferecem recursos nativos de restauração de arquivos e pastas, possibilitando retorno a estados anteriores em caso de erro, falha ou necessidade de auditoria.
- Ambiente de contingência: como toda a infraestrutura é hospedada em nuvem, o acesso aos documentos e sistemas pode ser restabelecido de qualquer local seguro, garantindo continuidade operacional por meio de autenticação multifator.

A solução em nuvem oferece criptografia em repouso e em trânsito, além de redundância geográfica dos dados provida pelo próprio provedor, dispensando a necessidade de equipamentos físicos, VPN dedicada ou estruturas paralelas de backup.

4.4.1 CONTROLE DE ACESSO AO NAS

O acesso aos arquivos da PROA é realizado exclusivamente por meio do ambiente corporativo do Microsoft 365, utilizando contas individuais com autenticação multifator (MFA).

As permissões são configuradas de acordo com a função de cada colaborador, garantindo que apenas áreas autorizadas possam acessar determinadas pastas e documentos.

A plataforma registra eventuais tentativas de acesso indevido e permite bloqueio imediato de usuários pela área de Risco e Compliance, sempre que necessário para preservar a segurança das informações.

4.4.2 CRIPTOGRAFIA

Os arquivos da PROA são armazenados na plataforma Microsoft 365, que utiliza criptografia em repouso e em trânsito como padrão, protegendo os dados tanto durante o armazenamento quanto no envio e recebimento de informações.

Documentos sensíveis podem receber camadas adicionais de proteção, como restrições de acesso, bloqueio de download ou criptografia individual aplicada pela área de Risco e Compliance.

5 INVESTMENT COMPLIANCE

Entende-se como *Investment Compliance* a execução de ordens de compra e venda de ativos de acordo com certos critérios que, caso não observados, poderão ir contra a integridade do mercado e os melhores interesses dos cotistas/investidores.

As principais práticas identificadas e controladas encontram-se descritas nas seções abaixo, tendo cada um relatório específico para fins de monitoramento e prevenção.

5.1 NEGÓCIOS ENTRE-FUNDOS (“*CROSS-TRADES*”)

Em determinadas circunstâncias é aplicável a realização de operações em que um ou mais veículos sob gestão sejam contraparte de outro ou outros (“*cross-trades*”). Essa prática é, no entanto, permitida apenas em situação que:

- exista efetiva demanda alocativa de todas as contrapartes envolvidas para a realização dessa operação, em linha com as disposições legais, estratégias de investimento e fatores de risco pré-estabelecidos;
- os preços praticados sejam justos, ou seja, compatíveis com os preços que seriam obtidos junto a terceiros para a mesma operação.

O relatório específico para fins de monitoramento e prevenção a práticas de *cross-trading* que firam a integridade do mercado, ou o melhor interesse dos cotistas/investidores, atenta-se, principalmente, a esses dois critérios.

5.2 ALOCAÇÃO JUSTA (“*FAIR-ALLOCATION*”)

O conceito de *fair allocation*, ou “alocação justa”, diz respeito à distribuição e rateio de ordens executadas para os diferentes veículos de investimento sob gestão, a qual deve respeitar critérios específicos definidos no comitê, ou subcomitês, de investimentos, conforme definido na Política de Investimentos da gestora.

O princípio norteador é o de equidade no tratamento de cotistas, tanto em termos de exposição ao risco, quanto de distribuição de ordens de um mesmo ativo executadas em diferentes preços. É vedada a alocação de operações de tal forma que exista o benefício de determinados cotistas/investidores em detrimento de outros.

Para fins de controle e prevenção a tal prática, após decidir implementar determinada estratégia de investimento ou desinvestimento, o comitê, ou subcomitê, de investimentos (nos termos da Política de Investimentos da gestora), analisa as diferentes restrições legais dos veículos sob gestão, os seus objetivos de retorno e tolerância ao risco específicos.

Através dessa análise determina-se o qual é o tamanho base de exposição para essa estratégia a ser implementada, e fatores alocativos (“fator de risco”) específicos a cada veículo que se entenda aplicável participar. A

alocação das ordens deve seguir os fatores pré-estabelecidos, além de respeitar a alocação das ordens para cada veículo de tal forma que os preços médios executados por cada sejam o mais próximo possível entre eles.

5.3 MELHOR EXECUÇÃO ("*BEST EXECUTION*")

A PROA e os seus colaboradores devem na condução das suas atividades de negociação de ativos buscar realizá-las da melhor forma possível ("*best execution*") em atendimento dos interesses dos cotistas/investidores. Essa prática de *best execution* é observada, essencialmente, pelo preço das ordens de compra ou venda executadas.

Para fins de monitoramento de que os preços praticados e os custos de transação envolvidos foram "os melhores possíveis" dadas as condições de liquidez e volatilidade, existe o acompanhamento de estatísticas de negociação, tais quais: preços médios, mínimos e máximos praticados por ativo; *bid-ask spreads*; e volumes de negociação. Observando essas estatísticas de mercado e as condições de negociação efetivamente praticadas pela Área de Gestão, é possível validar se as ordens estão a ser executadas da melhor forma possível dada a liquidez e a volatilidade no preço dos ativos.

Adicionalmente, as negociações por corretora e demais intermediários serão monitoradas, de tal forma a avaliar qualquer concentração de negociação não justificável/indevida. A existência de concentração de volume de negociação em uma ou poucas corretoras, caso venha a ocorrer, deve ser justificada pela comprovação da superioridade do serviço prestado, inclusive em questões de preço, liquidez e compatibilidade do valor de taxa de corretagem praticada.

5.4 MANIPULAÇÃO DE PREÇOS

A manipulação de preços ocorre quando são colocadas ordens de venda ou compra de ativos em que tais ordens têm como objetivo conduzir/pressionar o preço dos ativos em determinado sentido, e não o cumprimento de determinada tese investimento ou desinvestimento. O monitoramento e prevenção de tal prática dá-se através dos dados contidos no relatório de *best execution*.

6 CONHEÇA A SUA CONTRAPARTE ("*KNOW YOUR COUNTERPARTY*")

A PROA não realiza nesta data atividades de distribuição de cotas de fundos. Independente disso, e ainda que assim sendo não exista a necessidade de apresentar uma política de "*Know Your Client*", a PROA GESTORA DE RECURSOS LTDA adota uma postura para estabelecimento de qualquer relacionamento conhecido como "*Know Your Counterparty*".

O assunto é tratado pela Política de PLD, que tem como objetivo principal a prevenção à lavagem de dinheiro, do financiamento ao terrorismo, da proliferação de armas de fogo, corrupção, ou qualquer outro tipo envio/recebimento de recursos cuja origem ou destino sejam ilícitos de acordo com as legislações e regulações vigentes. Esse procedimento aplica-se a qualquer contraparte com a qual a PROA venha a estabelecer relacionamento, sendo as principais:

- administradores fiduciários e distribuidores de cotas de fundos de investimento,
- emissores de títulos de dívida privada, seja qual for a estrutura de títulos emitidos ou natureza jurídica do emissor;
- corretoras e demais intermediários de negociação de ativos;
- gestores de recursos externos.

O processo é, essencialmente, um processo de verificação de antecedentes (*background check*), buscando observar qualquer tipo de relação que possa sugerir ou aparentar a ocorrência das mencionadas práticas. Havendo tal suspeita, caberá ao Diretor de Risco e Compliance aprofundar-se na análise de viabilidade de tal relacionamento, podendo, inclusive utilizar-se de assistência jurídica externa, ou determinar o veto em tal prospecto de relacionamento.

Para fins de levantamento de dados e análise, conta-se com o suporte de sistemas de informação pública. São as principais fontes públicas de consulta: CVM; Receita Federal; Supremo Tribunal Federal (STF); Supremo Tribunal de Justiça (STJ); BM&F Supervisão de Mercados (BSM); ANBIMA; Associação Nacional das Corretoras e Distribuidoras de

Títulos e Valores Mobiliários, Câmbio e Mercadorias (ANCORD); Juntas Comerciais das diferentes Unidades Federativas da União; Google.

A PROA poderá contratar ferramenta ou serviços externos de verificação de antecedentes a terceiros qualificados.

6.1 RISCO DE IMAGEM

Ainda que o objetivo principal do processo de "*Know Your Counterparty*" seja o de prevenção à lavagem de dinheiro, do financiamento ao terrorismo, da proliferação de armas de fogo, corrupção, ou qualquer outro tipo envio/recebimento de recursos cuja origem ou destino sejam ilícitos, existe o objetivo secundário de mitigação de risco de imagem da PROA que pode decorrer dos seus relacionamentos estabelecidos.

A PROA busca evitar qualquer relacionamento que venha a prejudicar a sua imagem e reputação perante os diferentes agentes econômicos e de mercado, podendo, inclusive, encerrar tempestivamente qualquer relacionamento e estabelecer sanções à contraparte em questão.

7 ASSISTÊNCIA JURÍDICA EXTERNA

A PROA conta com assessoria jurídica externa sempre que necessário.

8 PLANO DE CONTINUIDADE DE NEGÓCIOS

A PROA possui plano e recursos tecnológicos preparados para permitir a continuidade dos negócios, e a consequente preservação do patrimônio dos seus cotistas/investidores, na ocorrência de circunstâncias de força maior e que fujam à sua capacidade de intervenção.

8.1 PRINCIPAIS RISCOS IDENTIFICADOS

Nas subseções abaixo encontram-se elencados os principais riscos identificados, bem como as medidas adotadas para contorná-los e permitir a continuidade dos negócios.

8.1.1 RECURSOS COMPUTACIONAIS

Para se defender de eventuais falhas dos recursos computacionais, entendidos aqui como os computadores e sistemas de armazenagem de dados, a PROA possui para fins de contingência e continuidade dos negócios computadores portáteis (notebooks), telefones celulares e soluções de backup e armazenamento seguro em nuvem, conforme descrito na seção de Segurança da Informação.

8.1.2 LINHAS TELEFÔNICAS E DE DADOS

A PROA mantém dois provedores distintos de internet para garantir redundância em caso de falhas. Se um dos links apresentar indisponibilidade, o outro assegura a continuidade das operações.

A comunicação telefônica é realizada por meio de serviço de telefonia VoIP contratado, que permite funcionamento tanto no escritório quanto de forma remota, garantindo disponibilidade mesmo em situações de contingência.

8.1.3 SEDE DA EMPRESA

Caso o escritório se torne inacessível por qualquer motivo, as atividades da PROA podem ser imediatamente transferidas para trabalho remoto. Isso é possível porque todos os sistemas, arquivos e ferramentas operacionais estão em ambiente seguro na nuvem (Microsoft 365), acessíveis por notebooks corporativos e com autenticação multifator. Dessa forma, a continuidade das operações é garantida a partir de qualquer local seguro, sem prejuízo às atividades essenciais da gestora.

8.1.4 ENERGIA ELÉTRICA

Em caso de queda de energia no escritório, as operações podem ser rapidamente transferidas para o regime remoto, uma vez que todos os sistemas e arquivos da PROA estão hospedados em ambiente seguro em nuvem. Os colaboradores podem continuar suas atividades utilizando notebooks e conexões externas, garantindo a continuidade das operações até o restabelecimento normal do fornecimento de energia no local.

8.1.5 PLANO "ANYWHERE SAFE"

O plano de contingência "*Anywhere Safe*" tem como base essencial o deslocamento de dois colaboradores designados para qualquer local considerado seguro, de forma a dar continuidade do exercício das atividades em casos de impossibilidade de acessar ou permanecer na sede da empresa. Tal como comentado, esse plano é possibilitado pela manutenção de uma estrutura de recursos tecnológicos específica de VPN e serviços "na nuvem".

8.1.6 REALIZAÇÃO DE TESTES PERIÓDICOS

Todos os sistemas, processos e controles descritos neste documento passarão por testes periódicos quanto à sua estabilidade e normal funcionamento, devendo tais testes serem realizados semestralmente. A área de Risco e Compliance elaborará relatório contendo os resultados observados para apresentação em comitê específico.

9 ARQUIVAMENTO DE DADOS E DOCUMENTOS

Os dados referentes às atividades desenvolvidas, e em especial ao cumprimento do disposto neste documento, tais como atas, apresentações, relatórios e gravações telefônicas, serão arquivados por um prazo de 5 (cinco) anos, estando à disposição para consulta das autoridades aplicáveis sob solicitação.

10 VALIDADE DESTE DOCUMENTO

Este documento, "Manual de Compliance", entra em vigor na data de publicação que consta na sua capa, e com prazo de validade indeterminado. Deverá, no entanto, ser revisto em períodos não maiores que 12 (doze) meses.

ANEXO I

TERMO DE CIÊNCIA E COMPROMISSO

Por meio deste instrumento eu, _____, inscrito no CPF sob o nº_____, DECLARO para os devidos fins:

(i) Ter recebido, na presente data, o Manual de Compliance atualizado ("Manual") da **PROA GESTORA DE RECURSOS LTDA**, CNPJ – 62.200.538/0001-05

(ii) Ter lido, sanado todas as minhas dúvidas e entendido integralmente as disposições constantes no Manual;

(iii) Estar ciente de que o Manual como um todo passa a fazer parte dos meus deveres como Colaborador da Gestora, incorporando-se às demais regras internas adotadas pela Gestora; e

(iv) Estar ciente do meu compromisso de comunicar ao Diretor de Risco e Compliance da Gestora qualquer situação que chegue ao meu conhecimento que esteja em desacordo com as regras definidas no Manual.

São Paulo, de 20

_____

[COLABORADOR]