BRIO INVESTIMENTOS

MANUAL DE CONTROLES INTERNOS (*COMPLIANCE*)

Edição	Datas			Aprovação
4ª	1ª versão	Última versão	Próxima revisão	Diretoria de *Compliance*
	Jun/2016	Jul/2024	Dez/2025	

ÍNDICE

1. INTRODUÇÃO E OBJETIVO

O termo *compliance* é originário do verbo, em inglês, *to comply*, e significa "estar em conformidade com regras, normas e procedimentos".

A **BRIO INVESTIMENTOS LTDA.** ("Gestora") adotou em sua estrutura as atividades de "Controles Internos" ou "*Compliance*". A Diretora responsável pelo *compliance* ("Diretora de *Compliance*") tem como objetivo garantir o cumprimento das leis e regulamentos emanados de autoridades competentes aplicáveis às atividades de Gestora, bem como as políticas e manuais da Gestora e obrigações de fidúcia e lealdade devidas aos investidores ("Investidores"), prevenindo a ocorrência de violações, detectando as violações que ocorram e punindo ou corrigindo quaisquer descumprimentos.

Este Manual de Controles Internos ("Manual de *Compliance*") foi elaborado para atender especificamente às atividades desempenhadas nesta data pela Gestora, de acordo com natureza, complexidade e riscos a elas inerentes, observada a obrigação de revisão e atualização periódica nos termos do item 2 abaixo.

Este Manual de *Compliance* é aplicável a todos os sócios, diretores, funcionários e estagiários da Gestora (em conjunto os "Colaboradores" e, individualmente e indistintamente, o "Colaborador").

Este Manual de *Compliance* deve ser lido em conjunto com o Código de Ética da Gestora, que também contém regras que visam a atender aos objetivos aqui descritos.

2. PROCEDIMENTOS

2.1. Designação de um Diretor Responsável

A área de *compliance* da Gestora é formada apenas pela Diretora de *Compliance*, Sra. **Juliana Marcondes de Oliveira Domingos**, devidamente nomeada no contrato social da Gestora.

A Diretora de *Compliance* exerce suas funções com plena independência e a área de *compliance* não está sujeita a qualquer ingerência por parte da equipe de gestão.

A Diretora de *Compliance* é a responsável pela implementação geral dos procedimentos previstos neste Manual de *Compliance* e, caso tenha que se ausentar por um longo período, deverá ser substituída ou deverá designar um responsável temporário para cumprir suas funções durante este período de ausência. Caso esta designação não seja realizada pela Diretora de *Compliance*, caberá aos sócios da Gestora a fazer.

A Diretora de *Compliance* tem como principais atribuições e responsabilidades o suporte a todas as áreas da Gestora no que concerne a esclarecimentos de todos os controles e regulamentos internos (*compliance*), bem como no acompanhamento de conformidade das operações e atividades da Gestora com as normas regulamentares (internas e externas) em vigor, definindo os planos de ação, monitorando o cumprimento de prazos e do nível excelência dos trabalhos efetuados e assegurando que quaisquer desvios identificados possam ser prontamente corrigidos (*enforcement*).

São também atribuições da Diretora de *Compliance*, sem prejuízo de outras descritas neste Manual de *Compliance*:

(i) Implantar o conceito de controles internos através de uma cultura de *compliance*, visando melhoria nos controles;

(ii) Propiciar o amplo conhecimento e execução dos valores éticos na aplicação das ações de todos os Colaboradores;

(iii) Analisar todas as situações acerca do não-cumprimento dos procedimentos ou valores éticos estabelecidos neste Manual de *Compliance*, ou no "Código de Ética", assim como avaliar as demais situações que não foram previstas nas políticas internas da Gestora;

(iv) Definir estratégias e políticas pelo desenvolvimento de processos que identifiquem, mensurem, monitorem e controlem contingências;

(v) Assegurar o sigilo de possíveis delatores de crimes ou infrações, mesmo quando estes não pedirem, salvo nas situações de testemunho judicial;

(vi) Solicitar a tomada das devidas providências nos casos de caracterização de conflitos de interesse;

(vii) Reconhecer situações novas no cotidiano da administração interna ou nos negócios da Gestora que não foram planejadas, fazendo a análise de tais situações;

(viii) Propor estudos para eventuais mudanças estruturais que permitam a implementação ou garantia de cumprimento do conceito de segregação das atividades desempenhadas pela Gestora;

(ix) Examinar de forma sigilosa todos os assuntos que surgirem, preservando a imagem da Gestora, assim como das pessoas envolvidas no caso.

2.2. Revisão Periódica e Preparação de Relatório

A Diretora de *Compliance* deverá revisar pelo menos anualmente este Manual de *Compliance* para verificar a adequação das políticas e procedimentos aqui previstos e sua efetividade. Tais revisões periódicas deverão levar em consideração, entre outros fatores, as violações ocorridas no período anterior e quaisquer outras atualizações decorrentes da mudança nas atividades realizadas pela Gestora.

A Diretora de *Compliance* deve encaminhar aos diretores da Gestora, até o último dia do mês de janeiro de cada ano, relatório relativo ao ano civil imediatamente anterior à data de entrega, contendo: (i) a conclusão dos exames efetuados; (ii) as recomendações a respeito de eventuais deficiências, com o estabelecimento de cronogramas de saneamento, quando for o caso; e (iii) a manifestação a respeito das verificações anteriores e das medidas planejadas, de acordo com o cronograma específico, ou efetivamente adotadas para saná-las, que deverá seguir o formato previsto no Anexo I ("Relatório Anual de *Compliance*").

O relatório referido no parágrafo acima deverá ficar disponível para a Comissão de Valores Mobiliários ("CVM") na sede da Gestora.

2.3. Treinamento

A Gestora possui um processo de treinamento inicial e um programa de reciclagem contínua dos conhecimentos sobre este Manual de *Compliance* e todas as políticas internas da Gestora, inclusive o Código de Ética, Política de Investimento Pessoal e Política de Gestão de Risco ("Políticas Internas"), aplicável a todos os Colaboradores, especialmente àqueles que tenham acesso a informações confidenciais e/ou participem do processo de decisão de investimento.

A Diretora de *Compliance* deverá conduzir sessões de treinamento aos Colaboradores periodicamente, conforme entender ser recomendável, de forma que os Colaboradores entendam e cumpram as disposições previstas neste manual, e deve estar frequentemente disponível para responder questões que possam surgir em relação aos termos deste Manual de *Compliance* e quaisquer regras relacionadas a *compliance*.

A periodicidade mínima do processo de reciclagem continuada será anual.

Os materiais, carga horária e grade horária serão definidos pela Diretora de *Compliance*.

2.4. Apresentação do Manual de Compliance e suas Modificações

A Diretora de *Compliance* deverá entregar uma cópia deste Manual de *Compliance* e de todas as Políticas Internas da Gestora para todos os Colaboradores por ocasião do início de suas atividades na Gestora e sempre que esses documentos forem modificados. Mediante o recebimento deste Manual de *Compliance*, o Colaborador deverá confirmar que leu, entendeu e cumpre com os termos deste Manual de *Compliance* e das Políticas Internas, mediante assinatura do termo de adesão que deverá seguir o formato previsto no Anexo II ("Termo de Adesão").

2.5. Atividades Externas

Os Colaboradores devem obter a aprovação escrita da Diretora de *Compliance* antes de envolverem-se em negócios externos à Gestora. "Atividades Externas" incluem ser um diretor, conselheiro ou sócio de sociedade ou funcionário ou consultor de qualquer entidade ou organização (seja em nome da Gestora ou não). Os Colaboradores que desejem ingressar ou engajar-se em tais Atividades Externas devem obter a aprovação prévia por escrito da Diretora de *Compliance* por meio da "Solicitação para Desempenho de Atividade Externa" na forma do Anexo III.

Não será necessária a prévia autorização da Diretora de *Compliance* para Atividades Externas relacionadas a caridade, organizações sem fins lucrativos, clubes ou associações civis.

2.6. Supervisão e Responsabilidades

Todas as matérias de violações a obrigações de *compliance*, ou dúvidas a elas relativas, que venham a ser de conhecimento de qualquer Colaborador devem ser prontamente informadas à Diretora de *Compliance*, que deverá investigar quaisquer possíveis violações de regras ou procedimentos de *compliance* e determinar quais as sanções aplicáveis. A Diretora de *Compliance* poderá, consideradas as circunstâncias do caso e a seu critério razoável, concordar com o não cumprimento de determinadas regras.

2.7. Sanções

As sanções decorrentes do descumprimento das regras estabelecidas neste Manual de *Compliance* e/ou das Políticas Internas serão definidas e aplicadas pela Diretora de *Compliance*, a seu critério razoável, garantido ao Colaborador, contudo, amplo direito de defesa. Poderão ser aplicadas, entre outras, penas de advertência, suspensão, desligamento ou demissão por justa causa, se aplicável, nos termos da legislação vigente, sem prejuízo da aplicação de penalidades pela CVM e do direito da Gestora de pleitear indenização pelos eventuais prejuízos suportados, perdas e danos e/ou lucros cessantes, por meio dos procedimentos legais cabíveis.

3. POLÍTICA DE CONFIDENCIALIDADE E TRATAMENTO DA INFORMAÇÃO

Nos termos da Instrução CVM nº 558, de 26 de março de 2015, especialmente o Artigo 24, III e Artigo 25, II, a Gestora adota procedimentos e regras de condutas para preservar informações confidenciais e permitir a identificação das pessoas que tenham acesso a elas.

A informação alcançada em função da atividade profissional desempenhada por cada Colaborador na Gestora é considerada confidencial e não pode ser transmitida de forma alguma a terceiros não Colaboradores ou a Colaboradores não autorizados.

3.1. Segurança da Informação Confidencial

Nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada a pessoas, dentro ou fora da Gestora, que não necessitem de ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais.

Qualquer informação sobre a Gestora, ou de qualquer natureza relativa às atividades da Gestora, aos seus sócios e clientes, obtida em decorrência do desempenho das atividades normais do Colaborador na Gestora, só poderá ser fornecida ao público, mídia ou demais órgãos caso autorizado por escrito pela Diretora de *Compliance*.

É terminantemente proibido que os Colaboradores façam cópias ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da Gestora e circulem em ambientes externos à Gestora com esses arquivos, uma vez que tais arquivos contêm informações consideradas confidenciais.

A proibição acima referida não se aplica quando as cópias ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da Gestora e de seus clientes. Nestes casos, o Colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

Qualquer Colaborar responsável pela impressão de documentos nas máquinas impressoras deverá retirar imediatamente das máquinas impressoras os respectivos documentos, pois pode conter informações restritas e confidenciais, mesmo no ambiente interno da Gestora.

De forma análoga, o Colaborar responsável pelo descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação e a desobediência a esta regra será considerada infração similar ao esquecimento de materiais nas máquinas de impressão. A Diretora de *Compliance* poderá apagar a qualquer tempo todos os arquivos digitalizados em pastas temporárias, garantindo que nenhum arquivo ali permaneça.

O descarte de documentos físicos que contenham informações confidenciais ou de suas cópias deverá ser realizado pelo Colaborador imediatamente após seu uso, de maneira a evitar sua recuperação.

Os Colaboradores devem se abster de utilizar *hard drives*, *pen-drives*, disquetes, fitas, discos ou quaisquer outros meios que não que não sirvam exclusivamente para o desempenho de suas atividades na Gestora.

É proibida a conexão de equipamentos na rede da Gestora que não estejam previamente autorizados pela área de informática e pela área de *compliance*.

Cada Colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade.

O envio ou repasse por *e-mail* de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é terminantemente proibido, assim como são o envio ou o repasse de *e-mails* com opiniões, comentários ou mensagens – inclusive de cunho político – que possam impactar a imagem e/ou afetar a reputação da Gestora.

Em nenhuma hipótese um Colaborador pode emitir opinião por *e-mail* em nome da Gestora, ou utilizar material, marca e logotipos da Gestora para assuntos não corporativos ou após o rompimento do seu vínculo com a Gestora, salvo se expressamente autorizado para tanto.

A Diretora de *Compliance* monitorará o acesso aos diretórios, incluindo os *logins* virtuais, dos servidores protegidos por senha e, no caso de tentativa de acesso por algum Colaborador não autorizado, este será avisado por *e-mail* e a Diretora de *Compliance* elucidará as circunstâncias da ocorrência, eventualmente aplicando as devidas punições.

Programas instalados nos computadores, principalmente via *internet* (*downloads*), sejam de utilização profissional ou pessoal, devem obter autorização prévia do responsável pela área de informática na Gestora. Não é

permitida a instalação de nenhum *software* ilegal ou que possua direitos autorais protegidos. A instalação de novos *softwares*, com a respectiva licença, deve também ser precedida de autorização do responsável pela informática. Este deverá aprovar ou vetar a instalação e utilização dos *softwares* dos Colaboradores para aspectos profissionais e pessoais.

A Gestora se reserva o direito de gravar qualquer ligação telefônica e/ou qualquer comunicação dos seus Colaboradores realizada ou recebida por meio das linhas telefônicas ou qualquer outro meio disponibilizado pela Gestora para a atividade profissional de cada Colaborador. A Diretora de *Compliance* é encarregado de, periodicamente, monitorar, por amostragem, as ligações e demais comunicações realizadas pelos Colaboradores. Qualquer informação suspeita encontrada será esclarecida imediatamente pela Diretora de *Compliance*.

Todas as informações do servidor da Gestora, do banco de dados dos clientes e os modelos dos analistas são enviados para o servidor interno. Nesse servidor, as informações são segregadas por área e transformadas em pacotes criptografados, sendo armazenadas com *backup*.

Em caso de divulgação indevida de qualquer informação confidencial, a Diretora de *Compliance* irá apurar o responsável por tal divulgação, o qual será identificado através da verificação no servidor de quem teve acesso ao referido documento por meio do acesso individualizado de cada Colaborador.

O Colaborador, caso assim queira, poderá utilizar seu telefone celular particular para assuntos profissionais, incluindo os aplicativos de comunicação como WhatsApp, Telegram, Skype, Zoom, entre outros, sempre observando as políticas contidas no Manual de Compliance, incluindo, mas não se limitando a, a políticas de segurança de informação confidencial e/ou Informação Relevante, propriedade intelectual, *Insider trading*/Dicas, entre outros. Entretanto, a partir de seu desligamento da Gestora, o Colaborador deverá imediatamente apagar quaisquer informações existentes em seu telefone celular referentes à Gestora e às atividades por ele até então desenvolvidas em nome da Gestora, procedendo, inclusive, sua exclusão de grupos de discussão em tais aplicativos de assuntos relacionados à Gestora.

3.2. Propriedade intelectual

Todos os documentos desenvolvidos na realização das atividades da Gestora ou a elas diretamente relacionados, tais quais, sistemas, arquivos, modelos, metodologias, fórmulas, projeções, relatórios de análise etc., são propriedade intelectual da Gestora.

A utilização e/ou divulgação de qualquer ativo de propriedade intelectual da Gestora dependerá de prévia e expressa autorização por escrito da Diretora de *Compliance*.

3.3. Prazo de Aderência do Colaborador à Política de Tratamento da Informação

Uma vez rompido com a Gestora o vínculo do Colaborador, este permanecerá obrigado a observar todas as regras e restrições tratadas neste Capítulo 3 deste Manual de *Compliance*, sob pena de responsabilização nas esferas civil e criminal.

4. INFORMAÇÃO PRIVILEGIADA E *INSIDER TRADING*

É considerada como informação privilegiada qualquer Informação Relevante (conforme definido abaixo) a respeito de um valor mobiliário negociado em mercado regulamentado, que não tenha sido publicada e que seja conseguida de maneira privilegiada, em consequência da ligação profissional ou pessoal mantida com um cliente, com colaboradores de empresas estudadas ou investidas ou com terceiros, ou em razão da condição de Colaborador.

Considera-se "Informação Relevante", para os efeitos deste Manual de *Compliance*, qualquer informação, decisão, deliberação, ou qualquer outro ato ou fato de caráter político-administrativo, técnico, negocial ou econômico-financeiro ocorrido ou relacionado aos negócios da Gestora que possa influir de modo ponderável: *(a)* na rentabilidade dos valores mobiliários administrados pela Gestora; *(b)* na decisão de investidores de comprar, vender ou manter cotas de fundos de investimento administrados pela Gestora; e *(c)* na decisão dos investidores de exercer quaisquer direitos inerentes à condição de titular de cotas de fundos de investimento administrados pela Gestora.

As informações privilegiadas precisam ser mantidas em sigilo por todos que as acessarem em função da prática da atividade profissional ou do relacionamento pessoal.

Caso o Colaborador tenha acesso a uma informação privilegiada que não deveria ter, deverá informar imediatamente à Diretora de *Compliance*, não podendo comunicá-la a ninguém mais, nem mesmo a outros membros da Gestora, profissionais de mercado, amigos e parentes, e nem a usar, em seu próprio benefício ou de terceiros. Se não houver certeza quanto ao caráter privilegiado da informação, deve-se, igualmente, consultar a Diretora de *Compliance* para que esta avalie o caráter privilegiado ou não da informação.

4.1. Insider Trading e "Dicas"

Insider trading baseia-se na compra e venda de títulos ou valores mobiliários com base no uso de informação privilegiada, com o objetivo de conseguir benefício próprio ou de terceiros (compreendendo a própria Gestora e seus Colaboradores).

"Dica" é a transmissão, a qualquer terceiro, de informação privilegiada que possa ser usada com benefício na compra e venda de títulos ou valores mobiliários.

É terminantemente proibida a prática de *insider trading* e/ou "Dicas" por qualquer membro da empresa, seja agindo em benefício próprio, da Gestora ou de terceiros.

A prática de qualquer ato em violação a este Manual de *Compliance* pode sujeitar o infrator à responsabilidade civil e criminal, por força de lei. O artigo 27-D da Lei nº 6.385, de 07 de dezembro de 1976, tipifica como crime a utilização de informação relevante ainda não divulgada ao mercado, da qual o agente tenha conhecimento e da qual deva manter sigilo, capaz de propiciar, para si ou para outrem, vantagem indevida, mediante negociação, em nome próprio ou de terceiro, com valores mobiliários. As penalidades previstas para esse crime são tanto a pena de reclusão, de 1 (um) a 5 (cinco) anos, bem como multa de 3 (três) vezes o montante da vantagem ilícita obtida em decorrência do crime. Além de sanções de natureza criminal, qualquer violação da legislação vigente e, portanto, deste Manual de *Compliance*, poderá, ainda, sujeitar o infrator a processos de cunho civil e administrativo, bem como à imposição de penalidades nesse âmbito, em conformidade com a Lei nº 6.404, de 15 de dezembro de 1976, e a Instrução CVM nº 358, de 03 de janeiro de 2002 ("Instrução CVM 358").

É de responsabilidade da Diretora de *Compliance* verificar e processar, periodicamente, as notificações recebidas a respeito do uso pelos Colaboradores de informações privilegiadas, *insider trading* e "dicas". Casos envolvendo o uso de informação privilegiada, *insider trading* e "dicas" serão analisados pela área de *compliance* não só durante a vigência do relacionamento profissional do Colaborador com a Gestora, mas mesmo após o término do vínculo, com a comunicação do ocorrido às autoridades competentes, conforme o caso.

5. POLÍTICA DE SEGREGAÇÃO DAS ATIVIDADES

5.1. Segregação física

A área de gestão da Gestora é segregada das demais, sendo o acesso restrito aos Colaboradores integrantes da área, por meio de controle de acesso nas portas.

Não será permitida a circulação de Colaboradores em seções que não destinada ao respectivo Colaborador.

Reuniões com terceiros não Colaboradores serão agendadas e ocorrerão em local específico. Será feito o controle e triagem prévia do terceiro não Colaborador, inclusive clientes, sendo este encaminhado diretamente à devida sala.

É de competência da Diretora de *Compliance*, ao longo do dia, fiscalizar a presença dos Colaboradores em suas devidas seções, sendo, ainda, informado imediatamente por *e-mail* se o acesso às áreas restritas for negado aos Colaboradores por mais de 5 (cinco) vezes. A Diretora de *Compliance* elucidará as circunstâncias da ocorrência deste fato e aplicará as devidas sanções. Eventual infração à regra estabelecida será devidamente esclarecida e todos os responsáveis serão advertidos e passíveis de punições a serem definidas pela Diretora de *Compliance*.

As tarefas contábeis da empresa serão terceirizadas, de modo que sejam exercidas no local de atuação das empresas contratadas.

5.2. Segregação Eletrônica

A Gestora segregará operacionalmente suas áreas a partir da adoção dos seguintes procedimentos: cada Colaborador possuirá microcomputador e telefone de uso exclusivo, de modo a evitar o compartilhamento do mesmo equipamento e/ou a visualização de informações de outro Colaborador. Ademais, não haverá compartilhamento de equipamentos entre os Colaboradores da área de administração de recursos e os demais Colaboradores, sendo que haverá impressora destinados exclusivamente à utilização da área de administração de recursos.

Especificamente no que diz respeito à área de informática e de guarda, conservação, restrição de uso e acesso a informações técnicas/arquivos, dentre outros, o acesso aos arquivos/informações técnicas é restrito e

controlado, sendo tal restrição/segregação feita em relação a: (i) cargo/nível hierárquico; e (ii) equipe.

Ademais, cada Colaborador possuirá um código de usuário e senha para acesso à rede, o qual é definido pelo responsável de cada área, sendo que somente os Colaboradores autorizados poderão ter acesso às informações da área de administração de recursos. Ainda, a rede de computadores da Gestora permitirá a criação de usuários com níveis de permissão diferentes, por meio de uma segregação lógica nos servidores que garantem que cada departamento conte com uma área de armazenamento de dados distinta no servidor com controle de acesso por usuário. Além disso, a rede de computadores manterá um registro de acesso e visualização dos documentos, o que permitirá identificar as pessoas que têm e tiveram acesso a determinado documento.

Cada Colaborador terá à disposição uma pasta de acesso exclusivo para digitalizar os respectivos arquivos, garantindo acesso exclusivo do usuário aos documentos de sua responsabilidade. Em caso de desligamento do Colaborador, todos os arquivos salvos na respectiva pasta serão transmitidos à pasta do seu superior direto, a fim de evitar a perda de informações.

5.3. Especificidades dos mecanismos de controles internos

A Gestora, por meio da Diretora de *Compliance*, mantém disponível, para todos os Colaboradores, todas as diretrizes internas, que devem ser sempre respeitadas, podendo atender, entre outros, os seguintes pontos:

(i) Definição de responsabilidades dentro da Gestora;

(ii) Meios de identificação e avaliação de fatores internos e externos que possam afetar adversamente a realização dos objetivos da empresa;

(iii) Existência de canais de comunicação que assegurem aos Colaboradores, segundo o correspondente nível de atuação, o acesso a confiáveis, tempestivas e compreensíveis informações consideradas relevantes para suas tarefas e responsabilidades;

(iv) Contínua avaliação dos diversos riscos associados às atividades da empresa; e

(v) Acompanhamento sistemático das atividades desenvolvidas, de forma que se possa avaliar se os objetivos da Gestora estão sendo alcançados, se os limites estabelecidos e as leis e regulamentos aplicáveis estão

sendo cumpridos, bem como assegurar que quaisquer desvios identificados possam ser prontamente corrigidos.

Caso qualquer Colaborador identifique situações que possam configurar como passíveis de conflito de interesse, deverá submeter imediatamente sua ocorrência para análise da Diretora de *Compliance*.

Adicionalmente, serão disponibilizados a todos os Colaboradores equipamentos e *softwares* sobre os quais a Gestora possua licença de uso, acesso à *internet*, bem como correio eletrônico interno e externo com o exclusivo objetivo de possibilitar a execução de todas as atividades inerentes aos negócios da Gestora. A esse respeito, a Diretora de *Compliance* poderá disponibilizar a diretriz para utilização de recursos de tecnologia, detalhando todas as regras que devem ser seguidas por todo e qualquer Colaborador, independentemente do grau hierárquico dentro da Gestora.

São realizados testes periódicos de segurança para os sistemas de informações utilizados pela Gestora para garantir a efetividade dos controles internos mencionados neste Manual de *Compliance*, especialmente as informações mantidas em meio eletrônico.

6. DIVULGAÇÃO DE MATERIAL DE *MARKETING*

Todos os Colaboradores devem ter ciência de que a divulgação de materiais de *marketing* deve ser realizada estritamente de acordo com as regras emitidas pela CVM e pela Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais – ANBIMA e que não devem conter qualquer informação falsa ou que possa levar o público a erro.

Materiais de *marketing* devem ser entendidos como qualquer nota, circular, carta ou outro tipo de comunicação escrita, destinada a pessoas externas à Gestora, ou qualquer nota ou anúncio em qualquer publicação, rádio ou televisão que ofereça qualquer serviço de consultoria ou gestão prestado pela Gestora, ou um produto de investimento da Gestora no mercado de valores mobiliários (incluindo fundos geridos).

Quaisquer materiais de *marketing* devem ser previamente submetidos à Diretora de *Compliance*, que deverá verificar se está ou não de acordo com as várias regras aplicáveis, incluindo sem limitação a Instrução CVM nº 400, de 29 de dezembro de 2003, a Instrução CVM nº 476, de 16 de janeiro de 2009, a Instrução CVM nº 555, de 17 de dezembro de 2014 ("Instrução CVM 555"), o Código ANBIMA de Regulação e Melhores Práticas de Fundos de Investimento, e diretrizes escritas emanadas da ANBIMA. A Diretora de *Compliance* deverá, quando necessário, valer-se de assessores externos para verificar o cumprimento das referidas normas. Somente após a aprovação por escrito da Diretora de *Compliance* é que qualquer material de *marketing* pode ser utilizado.

Abaixo encontra-se uma lista não exaustiva de regras aplicáveis a materiais de *marketing* de fundos de investimento.

Nos termos da Instrução CVM 555, qualquer material de divulgação do fundo deve, observadas as exceções previstas nas regras aplicáveis:

(i) ser consistente com o regulamento e com a lâmina, se houver;

(ii) ser elaborado em linguagem serena e moderada, advertindo seus leitores para os riscos do investimento;

(iii) ser identificado como material de divulgação;

(iv) mencionar a existência da lâmina, se houver, e do regulamento, bem como os endereços na rede mundial de computadores nos quais tais documentos podem ser obtidos;

(v) ser apresentado em conjunto com a lâmina, se houver;

(vi) conter as informações do item 12 do Anexo 42 da Instrução CVM 555, se a divulgação da lâmina não for obrigatória;

(vii) conter informações: (a) verdadeiras, completas, consistentes e não induzir o investidor a erro; (b) escritas em linguagem simples, clara, objetiva e concisa; e (c) úteis à avaliação do investimento; e (d) que **não** assegurem ou sugiram (d.1) a existência de garantia de resultados futuros ou (d.2) a inexistência de risco para o investidor.

Informações factuais devem vir acompanhadas da indicação de suas fontes e ser diferenciadas de interpretações, opiniões, projeções e estimativas.

Qualquer divulgação de informação sobre os resultados de fundo só pode ser feita, por qualquer meio, após um período de carência de 6 (seis) meses, a partir da data da primeira emissão de cotas.

Toda informação divulgada por qualquer meio, na qual seja incluída referência à rentabilidade do fundo, deve obrigatoriamente:

(i) mencionar a data do início de seu funcionamento;

(ii) contemplar, adicionalmente à informação divulgada, a rentabilidade mensal e a rentabilidade acumulada nos últimos 12 (doze) meses, não sendo obrigatória, neste caso, a discriminação mês a mês, ou no período decorrido desde a sua constituição, se inferior, observado que a divulgação de rentabilidade deve ser acompanhada de comparação, no mesmo período, com índice de mercado compatível com a política de investimento do fundo, se houver;

(iii) ser acompanhada do valor do patrimônio líquido médio mensal dos últimos 12 (doze) meses ou desde a sua constituição, se mais recente;

(iv) divulgar a taxa de administração e a taxa de *performance*, se houver, expressa no regulamento vigente nos últimos 12 (doze) meses ou desde sua constituição, se mais recente; e

(v) destacar o público alvo do fundo e as restrições quanto à captação, de forma a ressaltar eventual impossibilidade, permanente ou temporária, de acesso ao fundo por parte de Investidores em geral.

Ficam incorporadas por referência, ainda, as disposições das “Diretrizes para Publicidade e Divulgação de Material Técnico de Fundos de Investimento” da ANBIMA, disponível publicamente no *website* desta instituição.

7. *SOFT DOLLARS*

O termo "*soft dollars*" pode ser definido como sendo o benefício econômico, de natureza não-pecuniária, eventualmente concedido a uma determinada gestora ou a seus colaboradores por corretoras de títulos e valores mobiliários ou outros fornecedores, em contraprestação ao direcionamento de transações das carteiras e dos fundos de investimento geridos pela referida gestora.

São vedados quaisquer acordos envolvendo *soft dollars* entre os Colaboradores da Gestora e quaisquer fornecedores.

8. POLÍTICA DE *KNOW YOUR CLIENT* (KYC) E PREVENÇÃO À LAVAGEM DE DINHEIRO

O termo "lavagem de dinheiro" abrange diversas atividades e processos com o propósito de ocultar o proprietário e a origem precedente de atividade ilegal, para simular uma origem legítima. A Gestora e seus Colaboradores devem obedecer a todas as regras que previnem a lavagem de dinheiro, aplicáveis às atividades de gestão de fundos de investimento, em especial a Lei nº 9.613/1998 conforme alterada ("Lei de Lavagem de Dinheiro") e a Instrução CVM nº 301, de 16 de abril de 1999 ("Instrução CVM 301"), ambas refletidas neste Manual de *Compliance*.

A Diretora de *Compliance* será responsável perante a CVM pelo cumprimento de todas as normas e regulamentação vigentes relacionados ao combate e à prevenção à lavagem de dinheiro.

A Diretora de *Compliance* estabelecerá o devido treinamento dos Colaboradores da Gestora – na forma deste Manual de *Compliance* – para que estes estejam aptos a reconhecer e a combater a lavagem de dinheiro, bem como providenciará novos treinamentos, se necessários, no caso de mudanças na legislação aplicável.

A Diretora de *Compliance* deve estabelecer mecanismos de controle interno para o combate à lavagem de dinheiro e reportar certas operações à CVM e/ou ao Conselho de Controle de Atividades Financeiras ("COAF"). Geralmente, as obrigações contra a lavagem de dinheiro são:

(i) identificação dos clientes e dos beneficiários finais (incluindo os sócios de sociedades empresariais e seus procuradores) e manutenção dos registros atualizados dos clientes;

(ii) constituição e manutenção dos registros de envolvimento em transações;

(iii) reporte à CVM das transações que envolvam certas características específicas, ou que sejam geralmente suspeitas de lavagem de dinheiro;

(iv) identificação de pessoas politicamente expostas;

(v) verificação das relações comerciais com pessoas politicamente expostas, especialmente, propostas para o início de relações comerciais

e demais operações das quais pessoas politicamente expostas sejam parte; e

(vi) estabelecimento e manutenção de regras e procedimentos de controle internos destinados à identificação da origem dos recursos utilizados nas operações cujos clientes ou beneficiários finais sejam identificados como pessoas politicamente expostas.

A Gestora adota procedimentos que permitem o monitoramento das faixas de preços dos ativos e valores mobiliários negociados para os fundos de investimento por ela geridos, de modo que eventuais operações efetuadas fora dos padrões praticados no mercado, de acordo com as características do negócio, sejam identificadas e, se for o caso, comunicadas aos órgãos competentes.

Nos termos da regulamentação e dos ofícios circulares da CVM, bem como do *Guia de Prevenção à "Lavagem de Dinheiro" e ao Terrorismo no Mercado de Capitais Brasileiro da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais*, a responsabilidade primária pelo processo de identificação de clientes (cadastro) e dos procedimentos de *Know Your Client* ("KYC") em fundos de investimento, no que diz respeito aos investidores de um determinado Fundo (passivo), cabe ao respectivo administrador fiduciário, instituição intermediária ou distribuidor, conforme o caso. Sendo assim, as regras de identificação de clientes (cadastro) e dos procedimentos de KYC referidos nesta política não se aplicam à Gestora na qualidade de gestora de fundo de investimento, sem prejuízo da responsabilidade da Gestora pela análise, avaliação e monitoramento dos investimentos realizados pelo fundo de investimento (ativo) e suas contrapartes, nos termos aqui descritos, exceto nas seguintes hipóteses, para as quais a Gestora não está obrigada a realizar o controle de contraparte:

(i) Ofertas públicas iniciais e secundárias de valores mobiliários, registradas de acordo com as normas emitidas pela CVM;

(ii) Ofertas públicas de esforços restritos, dispensadas de registro de acordo com as normas emitidas pela CVM;

(iii) 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;

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

(v) Ativos e valores mobiliários de mesma natureza econômica daqueles acima listados, quando negociados no exterior, desde que (i) 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 (ii) 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.

Nas operações ativas (investimentos) realizadas pelo fundo de investimento, que não se enquadrem nas situações listadas acima, o "cliente" deve ser entendido como a contraparte da operação, sendo a Gestora responsável por tomar todas as medidas necessárias, segundo as leis aplicáveis e as regras de KYC presentes neste Manual de *Compliance* e na legislação vigente, para estabelecer e documentar a verdadeira e completa identidade, situação financeira e o histórico de cada contraparte. Estas informações devem ser obtidas de uma potencial contraparte antes que a Gestora aceite-a como tal.

(i) Pessoa Física: Se a contraparte for pessoa física, a Gestora deve obter, no mínimo, as seguintes informações: *(a)* nome completo, sexo, profissão, data de nascimento, naturalidade, nacionalidade, estado civil, filiação, nome do cônjuge ou companheiro; *(b)* natureza e número do documento de identificação, nome do órgão expedidor e data de expedição; *(c)* número de inscrição no Cadastro de Pessoas Físicas ("CPF/MF"); *(d)* endereço completo (logradouro, complemento, bairro, cidade, unidade da federação e CEP) e número de telefone; *(e)* endereço eletrônico para correspondência; *(f)* ocupação profissional e entidade para a qual trabalha; *(g)* informações sobre os rendimentos e a situação patrimonial; *(h)* datas das atualizações do cadastro; *(i)* assinatura do cliente; *(j)* cópia dos seguintes documentos: documento de identidade e comprovante de residência ou domicílio; e *(k)* cópias dos seguintes documentos, se for o caso: procuração e documento de identidade do procurador.

(ii) Pessoa Jurídica: Se o cliente for pessoa jurídica, a Gestora deve obter, no mínimo, as seguintes informações: *(a)* a denominação ou razão social; *(b)* nomes e CPF/MF dos controladores diretos ou razão social e inscrição no Cadastro Nacional de Pessoa Jurídica ("CNPJ") dos

controladores diretos; *(c)* nomes e CPF/MF dos administradores; *(d)* nomes dos procuradores; *(e)* número de CNPJ e NIRE; *(f)* endereço completo (logradouro, complemento, bairro, cidade, unidade da federação e CEP); *(g)* número de telefone; *(h)* endereço eletrônico para correspondência; *(i)* atividade principal desenvolvida; *(j)* faturamento médio mensal dos últimos doze meses e a situação patrimonial; *(k)* denominação ou razão social de pessoas jurídicas controladoras, controladas ou coligadas; *(l)* qualificação dos representantes ou procuradores e descrição de seus poderes; *(m)* datas das atualizações do cadastro; *(o)* assinatura do cliente; *(n)* cópia dos seguintes documentos: CNPJ, documento de constituição da pessoa jurídica devidamente atualizado e registrado no órgão competente, e atos societários que indiquem os administradores da pessoa jurídica, se for o caso; e (xvi) cópias dos seguintes documentos, se for o caso: procuração e documento de identidade do procurador.

(iii) Contrapartes no Exterior: Para operações com ativos e fundos de investimentos no exterior, deverão ser observadas as norma e preceitos da Instrução CVM 555, especialmente o Artigo 98 e seguintes.

As contrapartes devem informar a Gestora a respeito de quaisquer alterações que vierem a ocorrer nos seus dados cadastrais, conforme acima. Não obstante, os Colaboradores da Gestora deverão atualizar o cadastro de todas suas contrapartes em intervalos não superiores a 24 (vinte e quatro) meses.

A Gestora deve: (i) adotar continuamente medidas de controle que procurem confirmar as informações cadastrais de suas contrapartes, de forma a identificar os beneficiários finais das operações; (ii) identificar as pessoas consideradas politicamente expostas[1]; (iii) supervisionar de maneira mais

[1] Nos termos da Instrução CVM 301, *pessoa politicamente exposta* é aquela que desempenha ou tenha 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. O prazo de 5 (cinco) anos deve ser contado, retroativamente, a partir da data de início da relação de negócio ou da data em que o cliente passou a se enquadrar como pessoa politicamente exposta. No Brasil, são consideradas *pessoas politicamente expostas*: (i) os detentores de mandatos eletivos dos Poderes Executivo e Legislativo da União; (ii) os ocupantes de cargo, no Poder Executivo da União: (a) de Ministro de Estado ou equiparado; (b) de natureza especial ou equivalente; (c) de Presidente, Vice-Presidente e diretor, ou equivalentes, de autarquias, fundações públicas, empresas públicas ou sociedades de economia mista; ou (d) do grupo direção e assessoramento superiores - DAS, nível 6, e equivalentes; (iii) os membros do Conselho Nacional de Justiça, do Supremo Tribunal Federal e dos tribunais superiores; (iv) os membros do Conselho Nacional do Ministério Público, o Procurador-Geral da República, o Vice-Procurador-Geral da República, o Procurador-Geral do Trabalho, o Procurador-Geral da Justiça Militar, os Subprocuradores-Gerais da República e os Procuradores-Gerais de Justiça dos Estados e do Distrito Federal; (v) os membros do Tribunal de Contas da União e o Procurador-Geral do

rigorosa a relação de negócio mantida com pessoa politicamente exposta; e (iv) dedicar especial atenção a propostas de início de relacionamento e a operações executadas com pessoas politicamente expostas oriundas de países com os quais o Brasil possua elevado número de transações financeiras e comerciais, fronteiras comuns ou proximidade étnica, linguística ou política.

Se algum Colaborador perceber ou suspeitar da prática de atos relacionados à lavagem de dinheiro ou outras atividades ilegais por parte de qualquer cliente, este deverá imediatamente reportar suas suspeitas à Diretora de *Compliance*. A Diretora de *Compliance* deverá, então, instituir investigações adicionais para determinar se as autoridades relevantes devem ser informadas sobre as atividades em questão. Entre outras possibilidades, uma atividade pode ser considerada suspeita se constituir:

(i) operações cujos valores se afigurem objetivamente incompatíveis com a ocupação profissional, os rendimentos e/ou a situação patrimonial ou financeira de qualquer das partes envolvidas, tomando-se por base as informações cadastrais respectivas;

(ii) operações realizadas 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;

(iii) operações que evidenciem oscilação significativa em relação ao volume e/ou frequência de negócios de qualquer das partes envolvidas;

(iv) operações cujos desdobramentos contemplem características que possam constituir artifício para burla da identificação dos efetivos envolvidos e/ou beneficiários respectivos;

(v) operações cujas características e/ou desdobramentos evidenciem atuação, de forma contumaz, em nome de terceiros;

Ministério Público junto ao Tribunal de Contas da União; (vi) os Governadores de Estado e do Distrito Federal, os Presidentes de Tribunal de Justiça, de Assembleia Legislativa e de Câmara Distrital e os Presidentes de Tribunal e de Conselho de Contas de Estados, de Municípios e do Distrito Federal; e (vii) os Prefeitos e Presidentes de Câmara Municipal de capitais de Estados. Considera-se (i) *cargo*: emprego ou função pública relevante exercido por chefes de estado e de governo, políticos de alto nível, altos servidores dos poderes públicos, magistrados ou militares de alto nível, dirigentes de empresas públicas ou dirigentes de partidos políticos; e (ii) *familiares da pessoa politicamente exposta*: seus parentes, na linha direta, até o primeiro grau, assim como o cônjuge, companheiro e enteado.

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

(vii) operações realizadas com finalidade de gerar perda ou ganho para as quais falte, objetivamente, fundamento econômico;

(viii) operações com a participação de pessoas naturais residentes ou entidades constituídas em países que não aplicam ou aplicam insuficientemente as recomendações do Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo - GAFI;

(ix) operações liquidadas em espécie, se e quando permitido;

(x) transferências privadas, sem motivação aparente, de recursos e de valores mobiliários;

(xi) operações cujo grau de complexidade e risco se afigurem incompatíveis com a qualificação técnica do cliente ou de seu representante;

(xii) depósitos ou transferências realizadas por terceiros, para a liquidação de operações de cliente, ou para prestação de garantia em operações nos mercados de liquidação futura;

(xiii) pagamentos a terceiros, sob qualquer forma, por conta de liquidação de operações ou resgates de valores depositados em garantia, registrados em nome do cliente;

(xiv) situações em que não seja possível manter atualizadas as informações cadastrais de seus clientes;

(xv) situações e operações em que não seja possível identificar o beneficiário final; e

(xvi) situações em que as diligências para identificação de pessoas politicamente expostas não possam ser concluídas.

A Gestora deverá dispensar especial atenção às operações em que participem as seguintes categorias de clientes:

(i) clientes não-residentes, especialmente quando constituídos sob a forma de *trusts* e sociedades com títulos ao portador;

(ii) clientes com grandes fortunas geridas por áreas de instituições financeiras voltadas para clientes com este perfil (*private banking*); e

(iii) pessoas politicamente expostas.

A Gestora deverá analisar as operações em conjunto com outras operações conexas e que possam fazer parte de um mesmo grupo de operações ou guardar qualquer tipo de relação entre si.

Os Colaboradores não devem divulgar suas suspeitas ou descobertas em relação a qualquer atividade para pessoas que não sejam a Diretora de *Compliance*. Qualquer contato entre a Gestora e a autoridade relevante sobre atividades suspeitas deve ser feita somente pela Diretora de *Compliance*. Os Colaboradores devem cooperar com a Diretora de *Compliance* durante a investigação de quaisquer atividades suspeitas.

A Gestora deve manter atualizados os livros e registros, incluindo documentos relacionados a todas as transações ocorridas nos últimos 5 (cinco) anos, podendo este prazo ser estendido indefinidamente pela CVM, na hipótese de existência de processo administrativo.

A Diretora de *Compliance* deve assegurar que a Gestora previna qualquer danificação, falsificação, destruição ou alteração indevida dos livros e registros por meio de adoção de métodos necessários e prudentes.

Consideram-se operações relacionadas com terrorismo ou seu financiamento aquelas executadas por pessoas que praticam ou planejam praticar atos terroristas, que neles participam ou facilitam sua prática, bem como por entidades pertencentes ou controladas, direta ou indiretamente, por tais pessoas e as pessoas ou entidades que atuem sob seu comando.

Os colaboradores passarão por treinamento anual para reciclagem das boa praticas aqui mencionadas.

9. PLANO DE CONTINUIDADE DO NEGÓCIO

9.1. Contingência Interna

Em casos de contingências na sede da Gestora, como, por exemplo, queda de energia, a Gestora dispõe de:

(i) No-breaks;
(ii) Link de dados com redundância; e
(iii) Backup diário da rede.

Em casos da impossibilidade de atuação por parte da Diretora responsável pela administração de recursos, seu substituto direto irá assumir a referida responsabilidade, nos termos do Art. 5º da Instrução nº 558, de 26 de março de 2015 da Comissão de Valores Mobiliários ("Instrução CVM 558").

9.2. Contingência Externa

A Gestora trabalha com o *backup* de seus computadores, suportado por servidor mantido na nuvem, possibilitando o acesso às últimas 30 (trinta) versões de cada arquivo para restauração (em caso de problemas ou solicitação do responsável pela área).

Todas as informações do servidor da Gestora, do banco de dados dos clientes e os modelos dos analistas são armazenados em *backup* em *data center* remoto.

Os principais executivos da Gestora possuem acesso remoto aos seus *e-mails* e ao servidor de arquivos da empresa, de modo que possam acessá-los de fora do escritório, se necessário.

A Gestora dispõe de infraestrutura (servidores em nuvem e *backups*) preparada para se restabelecer em curto espaço de tempo a partir de qualquer ponto onde o Colaborador tenha acesso à internet.

Os registros contábeis da Gestora ficarão com o contador responsável (terceirizado) e as informações sobre os fundos de investimento cujas carteiras pela Gestora ficarão com a respectiva instituição administradora fiduciária.

Back-up

Os contatos relevantes, informações e relação dos principais prestadores de serviço estarão disponíveis por meio de backup.

Testes

São realizados periodicamente testes efetivos de utilização do sistema de *backup*.

10. SEGURANÇA CIBERNÉTICA

A Gestora adota mecanismos de segurança cibernética com a finalidade de assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados.

O responsável pelo cumprimento das regras e procedimentos de segurança cibernética é a Diretora de *Compliance*.

10.1. Avaliação dos riscos

No exercício das suas atividades, a Gestora poderá estar sujeita a riscos cibernéticos que ameacem a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados. Entre os riscos mais comuns, estão:

i) *Malwares*: *softwares* desenvolvidos para corromper computadores e redes:
   a. Vírus: *software* que causa danos à máquina, rede, outros *softwares* e bancos de dados;
   b. Cavalo de Tróia: aparece dentro de outro *software* e cria uma porta para a invasão do computador;
   c. *Spyware*: *software* malicioso para coletar e monitorar o uso de informações; e
   d. *Ransomware*: *software* malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.

ii) Engenharia social: métodos de manipulação para obter informações confidenciais, como senhas, dados pessoas e número de cartão de crédito:
   a. *Pharming*: direciona o usuário para um *website* fraudulento, sem o seu conhecimento;
   b. *Phishing*: *links* transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;
   c. *Vishing*: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;
   d. *Smishing*: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais; e

e. Acesso pessoal: pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

iii) Ataques de DDoS (*distributed denial of services*) e *botnets*: ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos *botnets*, o ataque vem de um grande número de computadores infectados utilizados para criar e mandar *spam* ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços; e

iv) Invasões (*advanced persistent threats*): ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

10.2. Ações de prevenção e proteção

Com a finalidade de mitigar os riscos cibernéticos e proteger seus sistemas, informações, base de dados, equipamentos e o andamento dos seus negócios, a Gestora adota as seguintes medidas de prevenção e proteção:

i) Controle de acesso adequado aos ativos da Gestora, por meio de procedimentos de identificação, autenticação e autorização dos usuários, ou sistemas, aos ativos da Gestora;

ii) Estabelecimento de regras mínimas (complexidade, periodicidade e autenticação de múltiplos fatores) na definição de senhas de acesso a dispositivos corporativos, sistemas e rede em função da relevância do ativo acessado. Além disso, os eventos de *login* e alteração de senha são auditáveis e rastreáveis;

iii) Limitação do acesso de cada Colaborador a apenas recursos relevantes para o desempenho das suas atividades e restrição do acesso físico às áreas com informações críticas/sensíveis;

iv) Rotinas de *backup*;

v) Criação de *logs* e trilhas de auditoria sempre que permitido pelos sistemas;

vi) Realização de diligência na contratação de serviços de terceiros, prezando, sempre que necessário, pela celebração de acordo de

confidencialidade e exigência de controles de segurança na própria estrutura dos terceiros;

vii) Implementação de recursos *anti-malware* em estações e servidores de rede, como antivírus e *firewalls* pessoais; e

viii) Restrição à instalação e execução de *softwares* e aplicações não autorizadas por meio de controles de execução de processos (por exemplo, aplicação de *whitelisting*).

10.3. Monitoramento

A Gestora possui mecanismos de monitoramento das ações de proteção implementadas, para garantir seu bom funcionamento e efetividade.

Nesse sentido, a Gestora mantém inventários atualizados de *hardware* e *software*, bem como realiza verificações periódicas, no intuito de identificar elementos estranhos à Gestora, como computadores não autorizados ou *softwares* não licenciados.

Além disso, a Gestora mantém os sistemas operacionais e *softwares* de aplicação sempre atualizados, instalando as atualizações sempre que forem disponibilizadas. As rotinas de *backup* são monitoradas diariamente, com a execução de testes regulares de restauração dos dados.

São realizados, periodicamente, testes de invasão externa e *phishing*, bem como análises de vulnerabilidades na estrutura tecnológica, sempre que houver mudança significativa em tal estrutura.

Ainda, a Gestora analisa regularmente os *logs* e as trilhas de auditoria criados, de forma a permitir a rápida identificação de ataques, sejam internos ou externos.

10.4. Plano de resposta

Caso seja identificado um potencial incidente relacionado à segurança cibernética, a Diretora de *Compliance* deverá ser imediatamente comunicada.

Num primeiro momento, a Diretora de *Compliance* se reunirá com os demais diretores da Gestora para compreender o evento ocorrido, os motivos e consequências imediatas, bem como a gravidade da situação.

Caso os diretores avaliem que o incidente ocorrido pode gerar danos iminentes à Gestora, serão tomadas, em conjunto com os assessores de

tecnologia da informação da Gestora, as medidas imediatas de cibersegurança cabíveis, que podem incluir a redundância de TI, redirecionamento das linhas de telefone para os celulares, instrução do provedor de telefonia para que desvie linhas de dados e e-mails, entre outros.

Na hipótese de o incidente comprometer, dificultar ou mesmo impedir a continuidade das operações da Gestora, serão observados os procedimentos previstos no plano de continuidade do negócio, descrito no item 9 acima.

Além disso, os diretores avaliarão a pertinência da adoção de medidas como (i) registro de boletim de ocorrência ou queixa crime; (ii) comunicação do incidente aos órgãos regulatórios e autorregulatórios; (ii) consulta com advogado para avaliação dos riscos jurídicos e medidas judiciais cabíveis para assegurar os direitos da Gestora.

10.5. Reciclagem e revisão

A Gestora manterá o programa de segurança cibernética continuamente atualizado, identificando novos riscos, ativos e processos e reavaliando os riscos residuais.

A Diretora de *Compliance*, responsável pela implementação dos procedimentos de segurança cibernética, realizará a revisão e atualização deste plano de segurança cibernética a cada 24 (vinte e quatro) meses, ou em prazo inferior sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão da Diretora de *Compliance*.

ANEXO I - Modelo de Relatório Anual de Compliance

São Paulo, ___ de _____ de 20___.

Aos Diretores,

Ref.: Relatório Anual de *Compliance*

Prezados,

Em vista do processo de reciclagem anual das regras, políticas, procedimentos e controles internos da **BRIO INVESTIMENTOS LTDA.** ("Gestora"), nos termos do Manual de Controles Internos *(compliance)* da Gestora ("Manual de *Compliance*"), e do Artigo 22 da Instrução nº 558, de 26 de março de 2015 da Comissão de Valores Mobiliários ("Instrução CVM 558"), e na qualidade de diretor responsável pela implementação, acompanhamento e fiscalização das regras, políticas, procedimentos e controles internos constantes do Manual de *Compliance* e da Instrução CVM 558 ("Diretora de *Compliance*"), informo o quanto segue a respeito do período compreendido entre 1º de janeiro e 31 de dezembro de 20[--].

Por favor, encontrem abaixo: (i) a conclusão dos exames efetuados; (ii) as recomendações a respeito de deficiências e cronogramas de saneamento; e (iii) manifestação da Diretora responsável por ajustar a exposição a risco das carteiras, assim como pelo efetivo cumprimento da "Política de Gestão de Riscos" da Gestora ("Diretor de Risco"), a respeito das verificações anteriores e das medidas planejadas, de acordo com o cronograma específico, ou efetivamente adotadas para saná-las.

I. Conclusão dos Exames Efetuados:

[●]

II. Recomendações e Cronogramas de Saneamento

[●]

III. Manifestação sobre Verificações Anteriores

[●]

Fico à disposição para eventuais esclarecimentos que se fizerem necessários.

_____

Juliana Marcondes de Oliveira Domingos

Diretora de *Compliance* e de Risco

ANEXO II - Termo de Adesão

Eu, ..., portador da Cédula de Identidade nº ..... e/ou Carteira de Trabalho e Previdência Social nº ..... série ....., declaro para os devidos fins que:

1. Estou ciente da existência do "Manual de Controles Internos *(compliance)*" da **BRIO INVESTIMENTOS LTDA.**" ("Manual de *Compliance*" e "Gestora", respectivamente) e de todas as políticas internas da Gestora, inclusive o "Código de Ética", a "Política de Investimento Pessoal" e a "Política de Gestão de Risco" ("Políticas Internas"), que recebi, li e tenho em meu poder.
2. Tenho ciência do inteiro teor do Manual de *Compliance* e das Políticas Internas, do qual declaro estar de acordo, passando este a fazer parte de minhas obrigações como Colaborador (conforme definido no Manual de *Compliance*), acrescentando às normas previstas no Contrato Individual de Trabalho, se aplicável, e as demais normas de comportamento estabelecidas pela Gestora, e comprometo-me a comunicar, imediatamente, aos sócios-administradores da Gestora qualquer quebra de conduta ética das regras e procedimentos, que venha a ser de meu conhecimento, seja diretamente ou por terceiros.
3. Tenho ciência e comprometo-me a observar integralmente os termos da política de confidencialidade estabelecida no Manual de *Compliance* da Gestora, sob pena da aplicação das sanções cabíveis, nos termos do item 4 abaixo.
4. O não-cumprimento do Código de Ética e/ou das Políticas Internas, a partir desta data, implica na caracterização de falta grave, podendo ser passível da aplicação das sanções cabíveis, inclusive demissão por justa causa, se aplicável. Não obstante, obrigo-me a ressarcir qualquer dano e/ou prejuízo sofridos pela Gestora e/ou os respectivos sócios e administradores, oriundos do não-cumprimento do Manual de *Compliance* e/ou das Políticas Internas, sujeitando-me à responsabilização nas esferas civil e criminal.
5. Participei do processo de integração e treinamento inicial da Gestora, onde tive conhecimento dos princípios e das normas aplicáveis às minhas atividades e da Gestora, notadamente aquelas relativas à segregação de atividades, e tive oportunidade de esclarecer dúvidas relacionadas a tais princípios e normas, de modo que as compreendi e me comprometo a observá-las no desempenho das minhas atividades, bem como a participar assiduamente do programa de treinamento continuado.
6. As normas estipuladas no Manual de *Compliance* e nas Políticas Internas não invalidam nenhuma disposição do Contrato Individual de Trabalho, se aplicável, e nem de qualquer outra norma mencionada pela Gestora, mas servem de complemento e esclarecem como lidar em determinadas situações relacionadas à minha atividade profissional.

7. Autorizo a divulgação de meus contatos telefônicos aos demais Colaboradores, sendo que comunicarei a Gestora a respeito de qualquer alteração destas informações, bem como de outros dados cadastrais a meu respeito, tão logo tal modificação ocorra.

8. Declaro ter pleno conhecimento que o descumprimento deste Termo de Adesão pode implicar no meu afastamento imediato da empresa, sem prejuízo da apuração dos danos que tal descumprimento possa ter causado.

A seguir, informo as situações hoje existentes que, ocasionalmente, poderiam ser enquadradas como infrações ou conflitos de interesse, de acordo com os termos do Manual de *Compliance*, salvo conflitos decorrentes de participações em outras empresas, descritos na "Política de Investimento Pessoal", os quais tenho ciência que deverão ser especificados nos termos previstos no Manual de *Compliance*:

_____

_____

_____

_____

_____

_____

_____

_____

_____

São Paulo, ... de ..... de 20..... .

_____

[DECLARANTE]

ANEXO III - Solicitação para Desempenho de Atividade Externa

1. Nome da instituição na qual será realizada a Atividade Externa / descrição da Atividade Externa:_____
_____
_____

2. Você terá uma posição de diretor ou administrador? [ ] sim [ ] não

3. Descreva suas responsabilidades decorrentes da Atividade Externa:_____
_____
_____.

4. Tempo estimado que será requerido de você para desempenho da Atividade Externa (em bases anuais):
_____.

5. Você ou qualquer parte relacionada irá receber qualquer remuneração ou contraprestação pela Atividade Externa: [ ] sim [ ] não
Se sim, descreva:_____.

O Colaborador declara que a Atividade Externa que pretende desempenhar, conforme acima descrita, não viola nenhuma lei ou regulamentação aplicável, ou os manuais e códigos da **BRIO INVESTIMENTOS LTDA.** ("Gestora"), e que não interfere com suas atividades na Gestora, não compete ou conflita com quaisquer interesses da Gestora. O Colaborador declara e garante, ainda, que irá comunicar aa Diretora de *compliance* da Gestora quaisquer conflitos de interesses que possam surgir com relação à Atividade Externa acima descrita.

São Paulo, _____ de _____ de 20_____

_____
Assinatura do Colaborador

Resposta da Diretora de *Compliance:*

[ ] Solicitação Aceita [ ] Solicitação Negada

_____
Juliana Marcondes de Oliveira Domingos
Diretora de *Compliance*