BAOBÁ GESTÃO DE RECURSOS LTDA.

(“Gestor”)

MANUAL DE REGRAS, PROCEDIMENTOS E DESCRIÇÃO DE CONTROLES INTERNOS

Junho de 2022

REGRAS, PROCEDIMENTOS E DESCRIÇÃO DE CONTROLES INTERNOS

1. Objetivo e Abrangência

Este manual de Regras, Procedimentos e Descrição de Controles Internos ("Manual") está de acordo com os termos da Resolução CVM 21, de 25 de fevereiro de 2021 ("Resolução 21"), e é aplicável a todos os sócios, Diretores e funcionários que participem, de forma direta, das atividades diárias e negócios, representando o Gestor ("Colaboradores"), devendo ser aplicado em conjunto com o Manual de Segregação de Atividades e Segurança da Informação, bem como com o Código de Ética e as demais normas e políticas do Gestor.

Os Colaboradores devem atender às diretrizes e procedimentos estabelecidos neste Manual, informando qualquer ocorrência à área de *Compliance* e Risco, responsável também pela Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo ("PLDFT"), de modo que sejam alcançados os objetivos abaixo e viabilizado o funcionamento do Gestor conforme estrutura proposta no item 2 deste Manual:

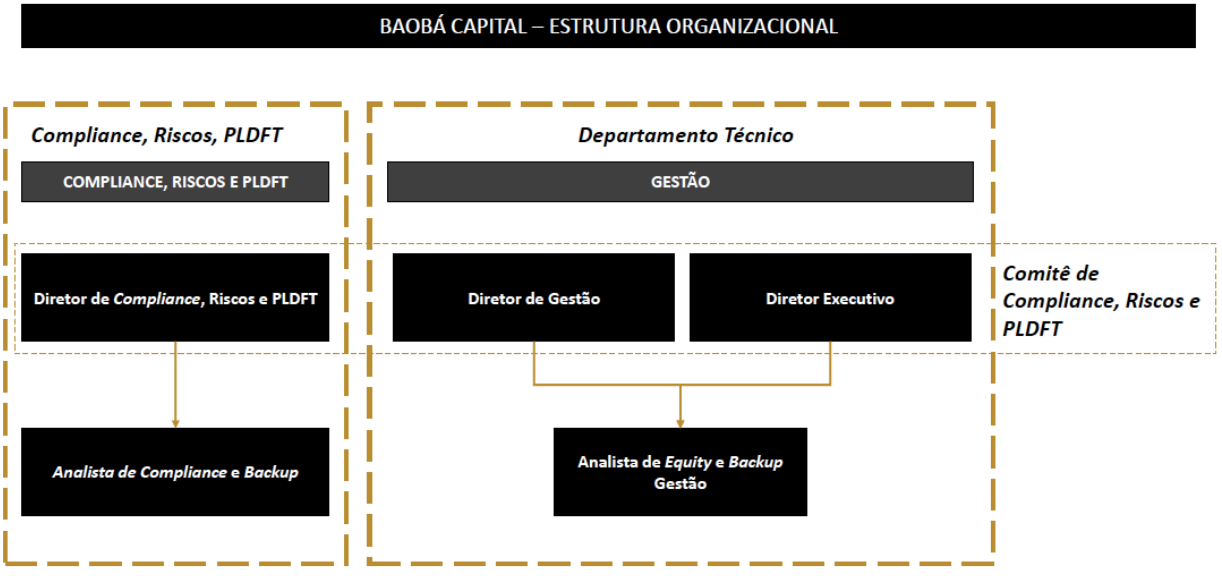
(i) estabelecer uma estrutura para possibilitar que os Colaboradores atuem com imparcialidade, tenham conhecimento do Código de Ética, da legislação e regulamentação aplicáveis, bem como das demais políticas internas do Gestor;

(ii) monitorar a adequação do Gestor e de seus Colaboradores a esta estrutura, para identificar, administrar e eliminar eventuais conflitos de interesses que possam afetar a imparcialidade dos Colaboradores ligados à área de gestão; e

(iii) prevenir, controlar e mitigar os riscos envolvidos nas atividades desenvolvidas pelo Gestor.

2. Estrutura Organizacional

O Gestor irá organizar-se da seguinte forma e conforme as atribuições descritas na sequência:



2.1. Diretorias:

O Gestor será administrado por uma Diretoria, composta por **(i)** 02 (dois) Diretores(as), a serem designados(as) no Contrato Social, para atuar por prazo indeterminado, sendo um responsável pela administração de carteiras de valores mobiliários ("Diretor de Gestão") e um responsável pelas atividades de *Compliance*, Riscos e PLDFT ("Diretor de *Compliance* e Riscos") responsáveis pelo dia a dia de cada uma das suas respectivas áreas,conforme abaixo:

(i) A Diretoria de Gestão será responsável, nos termos da Resolução 21, pelo Departamento Técnico,que: (a) contará com 3 (três) Colaboradores, incluindo o Diretor de Gestão e mais 2 (dois) profissionais ("Analista de Equity"); e (b) será responsável pela gestão dos ativos das carteiras dos fundos de investimento sob gestão.

O Diretor de Gestão será diretamente responsável pelas decisões de investimento e desinvestimento dos fundos sob gestão, bem como pela análise de desempenho dos investimentos para reporte aos investidores, sendo assessorado pelo Analista de Equity em todas as atribuições.

Adicionalmente, o Diretor de Gestão será responsável por garantir o arquivamento de relatórios, análises e quaisquer documentos que deem suporte às suas decisões de investimento e/ou desinvestimento, em meio eletrônico e passível de verificação, no diretório do Gestor.

Considerando que o Gestor não atuará na atividade de distribuição de cotas de emissão dos fundos de investimento sob sua gestão, o Gestor optou por não ter uma área destinada à referida atividade.

O Departamento Técnico, ficará responsável pelas atividades de natureza financeira e administrativa, bem como pela supervisão dos prestadores de serviços responsáveis pela área de tecnologia da informação, contabilidade e outros contratados em base *ad hoc.*

Os prestadores de serviço de tecnologia da informação serão responsáveis pela implantação e racionalização de processos, manutenção dos sistemas de informática, segurança da informação com controle de acesso dos usuários e *backup* de dados.

(ii) A *Diretoria de Compliance e Risco* ficará responsável **(a)** pelo cumprimento de regras, políticas, procedimentos e controles internos e da Resolução 21; **(b)** pela gestão de risco; **(c)** pelocumprimento das obrigações estabelecidas na Instrução CVM 617, de 05 de dezembro de 2019 ("Instrução CVM 617"), relativas à PLDFT; e **(d)** pelo cumprimento e verificação dos dispositivoslegais e regulatórios.

O *Diretor de Compliance* e Riscos contará com um Analista de *Compliance* para auxiliá-lo em suas atribuições (i. *Compliance*; ii. Gestão de Riscos; e iii. PLDFT) e/ou suprir eventuais ausências por agenda, férias, licenças médicas etc. A área deverá manter a atuação do Gestor, dos Colaboradores e, no que couber, dos prestadores de serviço, em conformidade com as regras, procedimentos e controles internos, bem como com a regulamentação vigente.

O *Analista de Compliance* atuará junto ao Diretor de Compliance e Riscos.

❾ *Backups dos Diretores:*

Considerando a possibilidade de que os Diretores de Gestão e de *Compliance* e Risco, responsável também por PLDFT, podem tanto não estar disponíveis, quanto precisar de suporte

para o exercício diligente de suas funções, o *Analista de Equity* e o *Analista de Compliance* (juntos, os "*Backups*") deverão suprir suas respectivas ausências temporárias e auxiliá-los no bom cumprimento de suas funções junto ao Gestor, aos Colaboradores, aos investidores dos fundos, aos prestadores de serviço e, quando aplicável, à CVM e à ANBIMA.

2.2. Comitês

Além da Diretoria e das áreas descritas acima, o Gestor contará também com um *Comitê de Compliance e Risco, que será composto por 02 (dois) membros – os Diretores de Gestão e de Compliance e Riscos.*

O Comitê de Compliance e Risco será um fórum de discussão voltado para a manutenção da atuação do Gestor e de seus Colaboradores em conformidade com a legislação e regulação vigentes e aplicáveis, referentes aos investimentos dos fundos geridos, à atividade de gestão de recursos e aos padrões ético e profissional esperados dos Colaboradores. Este Comitê também será responsável por acompanhar questões de PLDFT e terá poder de decisão apenas no que se refere à aplicação de penalidades decorrentes da violação aos termos deste e dos demais normativos internos do Gestor.

O *Comitê de Compliance e Riscos* deverá reunir-se sempre que houver necessidade, mas, ao menos, trimestralmente. As reuniões terão como foco o acompanhamento das atividades inerentes ao Gestor com a identificação de pontos de atenção e adoção de medidas para seu monitoramento ou solução.

Apesar do Gestor não ter um Comitê de Investimentos, a necessidade e conveniência de constituir, eventualmente, um órgão deliberativo para suportar o processo de investimento poderá ser reavaliada a qualquer momento. Em sendo o caso, os regulamentos dos fundos geridos serão oportunamente alterados, com base em proposta do Gestor ao administrador fiduciário dos fundos, visando refletir os novos processos.

Sem prejuízo, o Diretor de Gestão poderá, a qualquer tempo e se assim entender necessário, realizar reuniões com o(s) Analista(s) de Equity para discussões referentes aos investimentos, bem como às formas de ampliar a criação de valor para os cotistas dos fundosgeridos.

As discussões e deliberações das reuniões do Comitê de *Compliance* e Risco e, eventualmente, do Diretor de Gestão com o(s) Analista(s) de Equity, serão documentadas e passíveis de verificação por meio de atas - assinadas pelos participantes, sendo permitida a participação por videoconferência e a assinatura digital – e/ou de relatórios, elaborados posteriormente às reuniões, que ficarão arquivados em meio eletrônico no diretório do Gestor.

Caberá aos diretores, e/ou às pessoas por eles expressa e formalmente indicadas, a responsabilidade pelo arquivamento dos registros das referidas reuniões em meio eletrônico, no Diretório do Gestor.

3. Descrição dos Controles Internos

Visando garantir a mensuração e o alcance dos objetivos deste Manual, o Gestor implementará controles internos, conforme ou similares ao rol exemplificativo abaixo:

Segurança da Informação – o Gestor atuará por meio de rotinas elaboradas por prestadores de serviço especializados para assegurar um ambiente resguardado de qualquer tipo de risco para as informações e para a rede interna de computadores, evitando que a qualidade da gestão seja afetada por contingências;

Monitoramento de E-mails - o Gestor terá equipamentos atualizados e seu servidor de e-mails será hospedado junto a Google, o que garantirá alta disponibilidade e segurança e viabilizará o trabalho remoto e via computadores reserva, se e quando necessário, sem prejuízo da manutenção de registros que irão viabilizar a realização de auditorias e inspeções;

Identidade dos Colaboradores – a administração ocorrerá de forma centralizada através de servidor, onde (i) usuários e suas atividades podem ser monitorados; (ii) o particionamento das pastas é viabilizado; e (iii) os perfis de acesso são configurados conforme as prerrogativas e necessidades inerentes aos cargos dos colaboradores;

Software de suporte ao Compliance– Os Colaboradores e a área de *Compliance*, Riscos e PLDFT contarão com as funcionalidades de *Compliance* do software *Lote 45 Asset Portfolio Management*, que viabiliza centralizar, automatizar e dar mais segurança às referidas atividades por meio (i) de agenda regulatória; (ii) dos controles relacionados ao atendimento dos requisitos normativos inerentes à atividade do Gestor; e (iii) guarda de evidências e emissão de relatórios;

Aspectos Contratuais – a efetiva celebração de quaisquer contratos e acordos pelo Gestor será precedida de (i) validação pelo Diretor de Compliance e Riscos e/ou pelos assessores jurídicos contratados; (ii) verificação de poderes de representação; (ii) alinhamento de trâmites de assinatura – eletrônica sempre que possível -; e (iii) arquivamento das versões assinadas, com controle de prazos de obrigações contratuais centralizado; e

Contratação de Prestadores de Serviço - a efetiva contratação de novos Colaboradores ou prestadores de serviço para o Gestor (ou para os fundos, quando aplicável), será precedida de *background checks* e/ou *due diligence* específica, visando identificar o grau de risco apresentado pelo potencial contratado e o estabelecimento de critérios para acompanhamento de suas atribuições (contratuais ou não).

Os referidos procedimentos terão como finalidades verificar o envolvimento (incluídos indícios de envolvimento) de indivíduos e entidades com potencial de contratação pelo Gestor em atividades ilícitas, incluindo as ligadas à lavagem de dinheiro e financiamento a terrorismo. Neste sentido, os Colaboradores e terceiros afetados serão informados de forma ostensiva acerca do escopo e abrangência de *background checks* e do monitoramento e registro constante de perfis, acessos, utilização de sistemas, contatos e comunicações realizados pelos equipamentos e sistemas corporativos na forma desta política.

Todas as informações coletadas serão de acesso restrito ao Comitê de *Compliance* e Riscos, colaboradores e prestadores de serviços necessários à extração e análise dessas informações, autoridades públicas na forma da legislação aplicável e aos próprios Colaboradores, neste último caso ressalvada a necessidade de sigilo para resguardar uma investigação ou procedimento em curso.

Fazemos referência à Política de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo ("Política de PLDFT") do Gestor para informações adicionais sobre os Controles Internos relacionados ao tema.

4. Responsabilidades e Reporte às Autoridades Competentes

Uma vez aprovado em sede de Reunião de Sócios, o acompanhamento e a responsabilidade pelo cumprimento das disposições do presente Manual serão do Diretor de *Compliance* e Riscos, que deverá:

(i) desenvolver e manter procedimentos para garantir que as atividades do Gestor respeitem as exigências legais e regulatórias, avaliando a adequação, abrangência e efetividade dos sistemas de *Compliance* e controles internos;

(ii) fiscalizar os serviços prestados por terceiros contratados por meio de controle de obrigações contratuais e avaliação de qualidade;

(iii) contratar consultores (e/ou software) específicos para realização de *background checks* de parceiros, mantendo os relatórios recebidos arquivados no Diretório do Gestor; e

(iv) consolidar as comunicações entre o Gestor e os órgãos reguladores e autorreguladores.

Adicionalmente, nos termos do artigo 25 da Resolução 21, será dever da Diretoria de *Compliance* e Riscos encaminhar aos órgãos de administração do Gestor, até o último dia útil do mês de abril de cada ano, relatório relativo ao ano civil imediatamente anterior à data de entrega, contendo: (a) as conclusões dos exames efetuados conforme acima; (b) as recomendações de eventuais

deficiências, com o estabelecimento de cronogramas de saneamento, quando for o caso; e (c) a manifestação da Diretoria a respeito das deficiências encontradas em verificações anteriores e das medidas planejadas, de acordo com cronograma específico, ou efetivamente adotadas para saná-las.

Por fim, o relatório acima deverá atender também ao disposto no artigo 6º da Instrução CVM 617, relativo à PLDFT, devendo ainda ser elaborado com base nas informações e evidências disponíveis.

5. Segregação da Atividade de Gestão

Fazemos referência ao Manual de Segregação de Atividades e Segurança da Informação para maiores informações com relação a este tema, cuja manutenção será de responsabilidade da área de *Compliance* e Risco.

6. Confidencialidade e Sigilo

6.1. Informações Confidenciais:

No exercício de suas atividades, os Colaboradores poderão ter acesso a informações de clientes do Gestor, bem como de terceiros, que não sejam de conhecimento do público em geral e que, portanto, possam ser consideradas confidenciais ("Informações Confidenciais" ou, no singular, "Informação Confidencial"). É terminantemente proibida a divulgação de qualquer Informação Confidencial para terceiros, para benefício próprio ou de terceiro (*tipping*), ou mesmo que não haja intenção de beneficiar alguém. A obrigação de confidencialidade se aplica mesmo após o desligamento do Colaborador de suas atividades no Gestor.

O Gestor e os Colaboradores possuem o dever legal e profissional de manter o sigilo quanto às Informações Confidenciais de seus clientes, de modo que pedidos, tentativas ou ações visando a quebra do sigilo deverão ser imediatamente comunicados ao Diretor de *Compliance*, para que decida quanto à sua regularidade e necessidade.

6.2. Informações Sigilosas:

Informações Sigilosas incluem tanto as Informações Confidenciais quanto aquelas que, caso venham à tona, podem resultar em perda do nível de segurança do Gestor.

Perda, mau uso, modificação ou acesso não autorizado às Informações Sigilosas podem afetar adversamente a privacidade de um indivíduo, desfazer negócios, macular a imagem do Gestor e a continuidade de seus negócios.

O Gestor tem a responsabilidade legal de prezar pelo sigilo de seus clientes e, portanto, informações relativas aos clientes e entidades investidas por fundos de investimento geridos pelo Gestor jamais poderão ser enviadas a terceiros, com exceção das solicitações dos órgãos públicos, dos órgãos reguladores e do Poder Judiciário e, mesmo nessas hipóteses, nos estritos limites das ordens recebidas.

A divulgação e acesso às Informações Confidenciais e às Informações Sigilosas devem ser feitos apenas aos Colaboradores que venham a auxiliar e participar do desenvolvimento das atividades

do Gestor e somente na exata medida em que seja necessário conhecimento de tais Informações Confidenciais.

Fazemos referência ao Manual de Segregação de Atividades e Segurança da Informação do Gestor para mais informações sobre as regras de sigilo e conduta.

7. Segurança da Informação

As medidas de segurança da informação têm por finalidade a proteção contra ameaças, de modo a garantir a continuidade dos negócios, minimizar riscos e maximizar os retornos aos investidores. Tais medidas, assim como a realização de testes de intrusão anuais e as varreduras de vulnerabilidades, serão implementadas pelos prestadores de serviços de tecnologia da informação – terceirizada para garantia de qualidade – com base nas orientações do Diretor de Compliance e Riscos, devendo ser observadas por todos os Colaboradores. Além dos testes de intrusão (Pentest ou Penetratio *test*), serão também realizados treinamentos e testes de *phishing* com todos os Colaboradores.

Causam situações de risco à Segurança da Informação:

(i) Acesso a sites não relacionados às atividades do Gestor;

(ii) Utilização de mídias ("pen-drives", CDs, entre outras) para armazenamento de arquivos digitais, com exceção das disponibilizadas pelo Gestor;

(iii) Acesso ou arquivamento de informações sensíveis e Informações Confidenciais em pastas virtuais de acesso público;

(iv) Arquivamentos pessoais na rede de computadores institucional; (v) Utilização de mídias para transporte de informações não criptografadas; (vi) Compartilhamento de senhas.

As restrições de acesso às Informações Sigilosas – bem como aos documentos contidos na rede de computadores e sistemas do Gestor - respeitam a divisão de cargos e as linhas pontilhadas do organograma funcional que integra o item 2 deste Manual (Gestão + *Compliance*, Riscos e PLDFT), sendo separados por meio de *Chinese Wall*[1] e de sistemas que permitem a identificação dos detentores de informações, para responsabilização em caso de eventual vazamento.

Exceções às regras supra poderão ser avaliadas pelo Diretor de *Compliance* e Riscos, conforme solicitação formal fundamentada e avaliação de conveniência e oportunidade. As evidências da análise das referidas solicitações deverão ser arquivadas em meio eletrônico, sendo de

[1] *Chinese Wall* é o termo utilizado para a referência à barreira de comunicação entre diferentes indivíduos ou setores de uma mesma entidade, visando assegurar (i) o cumprimento das normas que exigem a segregação entre a atividade de administração de carteiras de valores mobiliários e outras atividades relacionadas ou não ao mercado de capitais, (ii) a identificação dos detentores de informações – privilegiadas ou não, conforme abaixo definido -, para eventual responsabilização em caso de vazamento, bem como (iii) a segregação entre ativos financeiros próprios do Gestor e os ativos financeiros de titularidade de terceiros.

responsabilidade do Diretor de *Compliance* e Riscos garantir tal procedimento, ainda que por meio da delegação desta atribuição a outro Colaborador.

Mais informações poderão ser encontradas no Anexo II do presente Manual, que contém algumas regras referentes ao Gerenciamento e Segurança de Informações Confidenciais.

8. Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo

De acordo com a Lei nº 9.613, de 03 de março de 1998, bem como a Instrução CVM 617, a prevenção da utilização dos ativos e sistemas do Gestor para fins ilícitos, tais como crimes de lavagem de dinheiro e financiamento ao terrorismo, ocultação de bens, direitos e valores, é dever de todos os Colaboradores.

O Gestor cumpre todas as leis e regulamentos aplicáveis na condução de seus negócios e atividades nas quais está envolvido. Qualquer Colaborador que violar uma lei ou regulamento aplicável à prevenção e combate à lavagem de dinheiro ficará sujeito às sanções disciplinares cabíveis. Caso algum Colaborador viole intencionalmente uma destas leis ou regulamentos, o Diretor de *Compliance* e Riscos notificará o fato às autoridades competentes nos termos da legislação e da Política de PLDFT do Gestor.

Caso o Colaborador suspeite de operações financeiras que possam envolver atividade de corrupção ou lavagem de dinheiro, deverá imediatamente comunicar ao Diretor de *Compliance* e Riscos para que atitudes cabíveis sejam tomadas.

É obrigatório que todos os Colaboradores mantenham arquivada toda e qualquer informação, tais como documentos e extratos que possam vir a ser necessários para o monitoramento ou investigação de clientes suspeitos de corrupção ou lavagem de dinheiro, desde que, no caso de conterem dados pessoais, não ultrapassem o prazo necessário para o cumprimento de obrigações legais e regulatórias, bem como o tempo razoável para a expiração dos prazos prescricionais aplicáveis, conforme limites estabelecidos pela Lei 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - "LGPD").

Para maiores informações, fazemos referência à Política de PLDFT, que também contém disposições referentes às Normas de Combate à Corrupção e às políticas de *Know Your Client*, *Know Your Partner*, e *Know Your Employee* ("KYC", "KYP", "KYE", respectivamente).

9. Treinamentos

Todos os Colaboradores do Gestor receberão cópias do Código de Ética, deste Manual e dos demais normativos internos, devendo analisar as disposições neles contidas e, em caso de dúvidas, contatar o Diretor de *Compliance* e Riscos para esclarecimentos e orientações. Ainda, conforme avaliação de necessidade e conveniência do referido Diretor, o Gestor poderá contratar profissionais especializados para conduzir treinamentos periódicos e programas de reciclagem.

Adicionalmente, os Colaboradores que venham a ser contratados para atuação no Departamento Técnico serão treinados e supervisionados diretamente pelo Analista de Equity e/ou pelo Diretor de Gestão, ficando sob sua responsabilidade direta durante o período de treinamento, que não será inferior a 90 (noventa) dias.

Haverá, ainda, incentivo por parte do Gestor para que o colaborador busque a permanente capacitação técnica e profissional e, para tanto, poderão ser disponibilizados subsídios educacionais com base em análise *ad hoc*.

10. Plano de Contingência

O Gestor atuará sempre por meio de rotinas elaboradas para assegurar um ambiente resguardado de qualquer tipo de risco para as informações e para a rede interna de computadores. Fazemos referência ao Manual de Segregação de Atividades e Segurança da Informação para os procedimentos adotados com tal finalidade. Dentre eles, cumpre ao Gestor destacar: *backups* periódicos, servidores, acesso remoto, uso de aplicativos e equipamentos pessoais.

Os procedimentos contínuos relacionados à segurança em tecnologia da informação ("TI") estão também relacionados a *software* de antivírus e ao acesso a atendimento relacionado a TI por diferentes canais (telefone central, celular dos Colaboradores e ainda por meio de visitas periódicas e/ou emergenciais).

Os procedimentos acima assegurarão um ambiente de sistema de informação eficiente, confiável e seguro, prevenindo que a qualidade da gestão seja afetada adversamente por perda de informações até mesmo em possíveis situações contingenciais.

11. Reporte e Penalidades

A violação deste Manual sujeitará o Colaborador às medidas previstas no Código de Ética do Gestor, sendo dever de todos os Colaboradores informar ao Diretor de *Compliance* e Riscos acerca de violações - ou possíveis violações - das disposições aqui estabelecidas, de maneira a (i) garantir o tratamento justo e equitativo aos colaboradores e investidores do Gestor, zelando, assim, pela sua reputação.

O descumprimento de qualquer regra estabelecida neste Manual deverá ser levado ao Comitê de *Compliance* e Risco, que decidirá quanto à aplicabilidade das seguintes penalidades, a depender da gravidade do descumprimento e da eventual reincidência: (i) advertência por escrito; (ii) suspensão temporária e não remunerada das atividades; ou (iii) desligamento.

Qualquer Colaborador que acredite ter violado este Manual ou tenha conhecimento de violação deverá notificar o fato direta e imediatamente área de *Compliance* e Risco, sendo que eventual ação disciplinar levará o reporte em consideração. Ainda, poderão ser tomadas ações disciplinares contra Colaborador que (i) autorize, coordene ou participe de violações a este Manual; (ii) possuindo informação ou suspeita de violações, deixe de reportá-las; (iii) deixe de

reportar violações ocorridas que, pelo seu dever de ofício, deveria ter conhecimento ou suspeita; e/ou (iv) promova retaliações, direta ou indiretamente, ou encoraje outros a fazê-lo.

12. Diretor(a) Responsável

Abaixo apresentamos informações cadastrais do Diretor de *Compliance* e Riscos do Gestor:

Nome	**Fernando Fontenele Silva**
E-mail	fernando@baobacapital.com.br
Telefone	(85) 3111 - 5681

Por fim, o Gestor atesta que o Diretor de *Compliance* e Riscos não está subordinado(a) às demais áreas de atuação, incluindo o Departamento Técnico.

13. Atualização

Esta política será submetida à revisão anual ou em períodos inferiores a este, sempre que o Diretor de *Compliance* e Riscos considerar necessário, com o intuito de preservar as condições de segurança para o Gestor.

Versão	Data	Responsabilidade
1	30 de julho de 2021	Bruno Barreto Souza
2	14 de junho de 2022	Fernando Fontenele Silva

ANEXO I – ESCOPO DE ATUAÇÃO DA ÁREA DE COMPLIANCE, GESTÃO DE RISCO E PLDFT

Temas Normativos

- Controlar a aderência às novas leis, regulamentações, práticas e diretrizes de autorregulação aplicáveis ao Gestor, e apresentar o resultado de suas verificações periodicamente ao Comitê de *Compliance* e Riscos;
- Controlar e monitorar as licenças legais, registros e certificações necessárias (registros na CVM, ANBIMA e demais aplicáveis), bem como sua renovação/manutenção junto às autoridades;
- Auxiliar a alta administração do Gestor no relacionamento com órgãos reguladores e assegurar que as informações requeridas sejam fornecidas no prazo e qualidade requeridos;
- Realizar revisões e relatórios obrigatórios nas frequências definidas na legislação em vigor.

Boas Práticas

- Designar pessoa responsável pela promoção e acessibilidade das informações necessárias para o cumprimento das normas internas legais, infralegais e de autorregulação, bem como pela coleta dos termos de ciência e aderência assinados por todos os Colaboradores;
- Estabelecer controles para que todos os Colaboradores do Gestor atuem com independência e atentem ao devido dever fiduciário para com seus clientes, evitando conflitos de interesse;
- Garantir que os controles internos sejam compatíveis com os riscos do Gestor em suas atividades, bem como efetivos e consistentes com a natureza, complexidade e risco das operações realizadas para o exercício profissional de administração de carteiras de valores mobiliários;
- Analisar informações, indícios ou identificar, administrar e, se necessário, levar o tema para análise e deliberação no Comitê de *Compliance* e Risco, no caso de eventuais conflitos de interesses ou descumprimentos regulatórios e de políticas e normas; e
- Comunicar aos órgãos competentes, nos prazos regulatórios, a respeito de eventuais descumprimentos normativos.

Governança

- Aprovar novos procedimentos e submeter novas políticas e manuais à aprovação dos sócios do Gestor, mediante parecer do Comitê de *Compliance* e Risco;
- Apresentar o resultado de seus controles e verificações ao Comitê de *Compliance* e Risco;

- Monitorar e buscar a efetiva aplicação dos documentos de *Compliance* e Controles Internos;

- Servir como canal para comunicações de desconformidades regulatórias e/ou de temas relacionados ao Código de Ética do Gestor; e

- Elaborar as atas do Comitê de *Compliance* e Risco, garantindo, seu devido arquivamento em meio eletrônico.

ANEXO II – SISTEMA DE GERENCIAMENTO E SEGURANÇA DE INFORMAÇÕES

O Gestor considera o gerenciamento das informações um assunto de âmbito estratégico, uma vez que as decisões que permeiam a gestão de seus ativos dependem da confiabilidade, segurança e acessibilidade ao sistema de gerenciamento de informações.

Para atingir estes objetivos, o Gestor estabeleceu regras de *Compliance* e de gestão de segurança em TI.

Gerenciamento de Informações Confidenciais

Quanto aos parâmetros de C*ompliance*, o Gestor define os perfis de acesso de cada usuário da rede interna de computadores de forma que as Informações Confidenciais e Sigilosas fiquem acessíveis somente por determinadas pessoas do Gestor. Ficam preservadas as informações de clientes e ao mesmo tempo evitam-se problemas relacionados a conflitos de interesses ou uso indevido de dados.

Além disso, o controle de tráfego de dados entre Colaboradores é realizado por meio de sistemas de "*firewall*" e controle de acessos à rede de computadores, que são responsáveis pela proteção de Informações Confidenciais e Sigilosas, bem como pela segregação das informações entre os grupos de Colaboradores que a elas devem ter acesso. Tais controles são estabelecidos nas autorizações de perfis de acesso e restrição de usuários da rede. Dessa forma, controla-se quem efetivamente acessou determinados dados e/ou sistemas e ficam impedidos acessos não autorizados.

Assim, foram definidos níveis de acesso para os membros do Comitê de *Compliance* e Riscos, o Departamento Técnico.

No que se refere ao gerenciamento de riscos referentes à segurança da informação, o Gestor atuará por meio de rotinas elaboradas por prestadores de serviço especializados para assegurar um ambiente resguardado de qualquer tipo de risco para as informações e para a rede interna de computadores, evitando que a qualidade da gestão seja afetada por contingências.

Estrutura de Tecnologia de Informação e *Hardware*:

Em complemento às informações contidas no item acima, o Gestor terá uma rede integrada de computadores, revisados quanto à capacidade, segurança e nível de atualização de seus componentes, com o suporte técnico de empresa terceirizada contratada. Ainda, serão realizados *backups* em servidores, inclusive de e-mails e serão adotados procedimentos contínuos relacionados aos antivírus, responsáveis por proteger, sem interrupção, a rede interna de computadores do Gestor e o computador de cada Colaborador.

Ainda, com relação aos e-mails, o Gestor utilizará equipamentos atualizados e seu servidor de e-mails será hospedado junto a Microsoft, o que garantirá alta disponibilidade e segurança e viabilizará o trabalho remoto e via computadores reserva, se e quando necessário, sem prejuízo

da manutenção de registros que irá viabilizar a realização de auditorias e inspeções nos termos dos manuais e políticas do Gestor.

Adicionalmente, com relação à estrutura de telefonia, o Gestor terá PABX com canais na sala de gestão, linha exclusiva para uso de fax e linhas móveis corporativas (para uso dos Colaboradores sempre que necessário) como meios de comunicação.

Por fim, todos os Colaboradores do Gestor terão acesso a atendimento relacionado aos sistemas de tecnologia da informação por diferentes canais, podendo optar pelo atendimento via telefone central, via celular dos colaboradores e, ainda, por meio de visitas periódicas e/ou emergenciais.

Sistema de Segurança da Informação:

O Gestor possuirá mecanismo de controle de tráfego de dados entre computadores da rede interna com rede externa ("*firewall*"), evitando tentativas de intrusões ou invasões praticadas por pessoas que pretendem acessar, roubar ou sequestrar dados confidenciais e/ou informações privilegiadas, capturar dados para realização de fraudes, causar danos a sistemas ou aplicativos.

O acesso a todos os sistemas, incluindo armazenamento em nuvem, tem controle feito por meio de perfis de acesso ou segregação de acesso por pastas, tendo o Departamento de *Compliance* e Risco acesso a todos os arquivos. Todos os sistemas utilizados possuem rastreabilidade acesso, sendo possível auditar quais usuários acessaram quais informações, bem como a data de tais acessos.

Por fim, o Gestor realizará, por meio da contratação de prestadores de serviços especializados, testes periódicos com intuito de garantir a segurança das informações e reduzir vulnerabilidades. Tais testes deverão ter periodicidade anual e consistirão em: (i) Teste de Intrusão (*Pentest* ou *Penetratio test*); e (ii) treinamentos e testes de *phishing* com todos os colaboradores.