Manual de Regras, Procedimentos e Controles Internos

[Junho/2025]

ÍNDICE

1. INTRODUÇÃO 4

1.1. Aplicabilidade do Manual 5

1.2. Ambiente Regulatório 6

2 POLÍTICA DE COMPLIANCE 7

2.1. Responsabilidades e Obrigações 7

2.1.1. Diretora de Risco, Compliance e PLD/FTP 7

2.1.2. Comitê de Compliance e Risco 10

2.1.3. Área de Compliance e Risco 12

2.2. Garantia de Independência 14

2.3 Sanções ("*Enforcement*") 15

2.4. Dúvidas ou ações contrárias aos princípios e normas do Manual 15

2.5. Revisão de Compliance 16

2.6. Sistema de Gerenciamento de Compliance 18

3 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO 18

3.1. Objetivo e Definições de Segurança da Informação 18

3.1.1. Informações Confidenciais 19

3.1.2. Informações Privilegiadas 20

3.1.3. Insider Trading e "Dicas" 20

3.1.4. Front-running 21

3.2. Conduta dos Colaboradores visando Segurança da Informação 21

3.3. Divulgação de Fatos Relevantes 23

3.4. Identificação de Riscos à Segurança de Informação (risk assessment) 25

3.5. Barreiras e Controles de Acesso a Informações Confidenciais 25

3.5.1. Servidor (File Server) 26

3.5.2. Acesso Escalonado do Sistema 27

3.5.3. Acesso de Terceiros 27

3.5.4. Identificação dos Detentores da Informação, Manutenção de Registros e Logs 27

3.6. Proteção da Base de Dados 29

3.6.1. Comunicação de Incidente/Vazamento de Informações Confidenciais29
3.6.2. Procedimentos de Resposta a Incidente de Segurança de Informações 29
3.7. Testes e Treinamento de Segurança da Informação 30
4. POLÍTICA DE SEGURANÇA CIBERNÉTICA (CYBERSECURITY) 31
4.1. Objetivo e Definições de Cybersecurity 31
4.2. Responsabilidade da Equipe TI e Cybersecurity 33
4.3. Conduta dos Colaborares visando Cybersecurity 34
4.4. Identificação de Riscos de Cybersecurity....34
4.5. Prevenção e Proteção aos riscos de Cybersecurity 35
4.5.1. Internet, E-mail e Computadores....35
4.5.2. Senhas....37
4.5.3. Monitoramento e Testes 38
4.6. Resposta a Incidente de Cybersecurity 39
4.6.1. Recuperação....40
4.6.2. Retomada 40
4.7. Propriedade Intelectual 40
4.8. Atualização/Revisão e Conscientização de Cybersecurity 41
5. POLÍTICAS DE TREINAMENTO 42
5.1. Treinamento e Atualização 42
5.2. Implementação e Conteúdo 42
6. WEBSITE DA GESTORA 43
7. POLÍTICA DE ANTICORRUPÇÃO 44
7.1. Abrangência das Normas de Anticorrupção....44
7.2. Definições de Atos de Corrupção....45
7.3. Conduta dos Colaboradores às Normas de Anticorrupção....46
7.4. Proibição de Doações Eleitorais 46
7.5. Relacionamentos com Agentes Públicos 46
8. POLÍTICA DE CERTIFICAÇÃO 47
8.1. Atividades Elegíveis e Critérios de Identificação 47
8.2. Identificação de Profissionais Certificados e Atualização do Banco de Dados da Anbima....48
8.3. Rotinas de Verificação 49
8.4. Atualização das Certificações....50

8.5. Processo de Afastamento 50
9. VIGÊNCIA E ATUALIZAÇÃO 51
ANEXO I - TERMO DE RECEBIMENTO E COMPROMISSO 52
ANEXO II - TERMO DE CONFIDENCIALIDADE 54
ANEXO III - NORMATIVOS APLICÁVEIS 58
ANEXO IV - TERMO DE AFASTAMENTO 59
ANEXO V - TERMO DE PROPRIEDADE INTELECTUAL 60

1. INTRODUÇÃO

Este Manual de Regras, Procedimentos e Controles Internos ("Manual"), elaborado em conformidade com o disposto no item 2.7 do Ofício-Circular/CVM/SIN/Nº 05/2014, na Resolução CVM nº 21, de 25 de fevereiro de 2021, conforme alterada ("Resolução CVM nº 21"), na Resolução CVM nº 50, de 31 de agosto de 2021, conforme alterada ("Resolução CVM 50"), na Resolução CVM nº 175, de 23 de dezembro de 2022, conforme alterada ("Resolução CVM 175") e seus Anexos Normativos demais orientações da Comissão de Valores Mobiliários ("CVM"), no Código Anbima de Administração e Gestão de Recursos de Terceiros ("Código AGRT"), no Código Anbima de Ética ("Código Anbima de Ética") e nas Regras e Procedimentos do Código de Administração e Gestão de Recursos de Terceiros, especialmente seu Anexo Complementar III, Lei nº 12.846, de 1º de agosto de 2013 e Decreto nº 11.129, , de 11 de julho de 2022, conforme alterada ("Normas de Anticorrupção"), Lei 9.613, de 03 de março de 1998, conforme alterada e demais manifestações e ofícios orientadores dos órgãos reguladores e autorregulados aplicáveis às atividades da Gestora, conforme abaixo definida, tem por objetivo estabelecer normas, princípios, conceitos e valores que orientam a conduta de todos aqueles que possuam cargo, função, posição, relação societária, empregatícia, comercial, profissional, contratual ou de confiança ("Colaboradores") com a **TYTON CAPITAL INVESTIMENTOS LTDA** ("Gestora"), tanto na sua atuação interna quanto na comunicação com os diversos públicos.

Na busca incessante da satisfação dos clientes, a Gestora atua com total transparência, respeito às leis, normas e aos demais participantes do mercado financeiro e de capitais.

Dessa forma, o presente Manual reúne as diretrizes que devem ser observadas pelos Colaboradores no desempenho da atividade profissional, visando ao atendimento de padrões éticos cada vez mais elevados. Este documento reflete a identidade cultural e os compromissos que a Gestora assume nos mercados em que atua.

A Gestora e seus Colaboradores não admitem e repudiam qualquer manifestação de preconceitos relacionados à origem, etnia, religião, classe social, sexo, deficiência física ou qualquer outra forma de preconceito que possa existir.

A Gestora mantém em seu website versões atualizadas dos seguintes documentos: (i) Formulário de Referência, conforme Anexo E da Resolução CVM nº 21; (ii) Política de Gestão de Risco; (iii) Política de Rateio e Divisão de Ordens; (iv) este Manual de Regras, Procedimentos e Controles Internos; (v) Código de Ética; (vi) Política de Investimentos Pessoais; e (vii) Política de Voto.

Para fins de interpretação dos dispositivos previstos neste Manual, exceto se expressamente disposto de forma contrária: (a) os termos utilizados neste Manual terão o significado atribuído na Resolução CVM 175; (b) as referências a Fundos abrangem as Classes e Subclasses, se houver; (c) as referências a regulamento abrangem os anexos e apêndices, se houver, observado o disposto na Resolução CVM 175; e (d) as referências às Classes abrangem os Fundos ainda não adaptados à Resolução CVM 175.

As disposições do Manual são aplicáveis aos Fundos constituídos após o início da vigência da Resolução CVM 175 e aos Fundos constituídos previamente a esta data que já tenham sido adaptados às regras da referida Resolução. Com relação aos Fundos constituídos antes da entrada em vigor da Resolução CVM 175, a Gestora e os Fundos permanecerão observando as regras da Instrução CVM nº 555, de 17 de dezembro de 2014, conforme alterada ("Instrução CVM 555"), e de outras instruções aplicáveis às diferentes categorias de Fundos sob gestão, especialmente, no que diz respeito às responsabilidades e atribuições da Gestora, enquanto gestora da carteira dos Fundos, até a data em que tais Fundos estejam adaptados às disposições da Resolução CVM 175.

1.1. Aplicabilidade do Manual

O presente Manual aplica-se a todos os Colaboradores que, por meio de suas relações com ou funções na Gestora, possam ter ou vir a ter acesso a informações confidenciais ou informações privilegiadas de natureza financeira, técnica, comercial, estratégica, negocial ou econômica, dentre outras.

1.2. Ambiente Regulatório

Este Manual é parte integrante das regras que regem a relação societária ou de trabalho dos Colaboradores, os quais, deverão assinar o termo de recebimento e compromisso constante do **Anexo I** a este Manual ("Termo de Recebimento e Compromisso"), estão aceitando expressamente as normas, princípios, conceitos e valores aqui estabelecidos. Todos os Colaboradores devem se assegurar do perfeito entendimento das leis e normas aplicáveis à Gestora bem como do completo conteúdo deste Manual. Para melhor referência dos Colaboradores, as principais normas aplicáveis às atividades da Gestora foram apontadas no **Anexo III** do presente Manual.

O descumprimento, suspeita ou indício de descumprimento de quaisquer das normas, princípios, conceitos e valores estabelecidos neste Manual ou das demais normas aplicáveis às atividades da Gestora, deverá ser levado para apreciação da Diretora de Compliance, Risco e PLD/FTP abaixo definida, e/ou do Comitê de Compliance e Risco de acordo com os procedimentos estabelecidos neste Manual. Competirá ao Comitê de Compliance e Risco definir as sanções decorrentes de tais desvios, nos termos deste Manual, garantido ao Colaborador amplo direito de defesa.

É dever de todo Colaborador informar a Diretora de Compliance, Risco e PLD/FTP e/ou o Comitê de Compliance e Risco sobre violações ou possíveis violações dos princípios e normas aqui dispostos, de maneira a preservar os interesses dos clientes da Gestora, bem como zelar pela reputação da empresa. Caso a violação ou suspeita de violação recaia sobre a própria Diretora de Compliance, Risco e PLD/FTP e/ou membros do Comitê de Compliance e Risco da Gestora, o Colaborador deverá informar diretamente aos demais administradores da Gestora.

2 POLÍTICA DE COMPLIANCE

2.1. Responsabilidades e Obrigações

A Área de Compliance e Risco é responsável pela elaboração e manutenção do programa de compliance da Gestora ("Programa de Compliance"), sob responsabilidade final e coordenação direta da diretora estatutária da Gestora, indicada como diretora responsável pelo cumprimento de regras, políticas, procedimentos e controles internos da Gestora ("Diretora de Risco, Compliance e PLD/FTP"), nos termos da Resolução CVM nº 21, que inclui a revisão e atualização periódica desta Política e demais políticas e manuais da Gestora, bem como a implementação de controles internos e testes de aderência para monitorar a efetividade das políticas e, ainda, a realização de treinamentos aos Colaboradores.

O Programa de Compliance da Gestora foi desenvolvido com vistas a dar cumprimento às obrigações estabelecidas na Resolução CVM nº 21, nos códigos de autorregulação da Anbima pertinentes, bem como demais atos normativos aplicáveis, dentre outras melhores práticas nacionais e internacionais.

A Área de Compliance e Risco é a principal responsável pela disseminação e supervisão das regras, controles e procedimentos internos da Gestora, visando mitigar os riscos operacionais, regulatórios, reputacionais e legais de sua atividade.

2.1.1. Diretora de Risco, Compliance e PLD/FTP

Nos termos da Resolução CVM nº 21, a Sra. Camilla Tolusso de Sá Pereira é a Diretora de Risco, Compliance e PLD/FTP da Gestora, reportando-se diretamente apenas ao Comitê de Compliance e Risco e Risco, com plena autoridade sobre a implementação do Programa de Compliance da Gestora.

A Diretora de Risco, Compliance e PLD/FTP é uma das administradoras da Gestora, na forma do seu contrato social. Ademais, a parte mais substancial de sua remuneração é garantida, de forma totalmente independente da performance dos fundos, como mais uma maneira de garantir sua independência. O mesmo ocorre com os demais recursos humanos que integram a Área de Compliance e Risco da Gestora no que tange à forma de remuneração.

São obrigações da Diretora de Risco, Compliance e PLD/FTP, no âmbito desta Política:

(i) Atender prontamente todos os Colaboradores;

(ii) Identificar possíveis condutas contrárias a lei, regulação, autorregulação, políticas e manuais da Gestora;

(iii) Acompanhar as políticas descritas neste Manual;

(iv) Levar quaisquer pedidos de autorização, orientação ou esclarecimento ou casos de ocorrência, suspeita ou indício de prática que não esteja de acordo com as disposições deste Manual e das demais normas aplicáveis à atividade da Gestora para apreciação do Comitê de Compliance e Risco da Gestora;

(v) Centralizar informações e revisões periódicas dos processos de compliance, principalmente quando são realizadas alterações nas políticas vigentes ou se o volume de novos Colaboradores assim exigir;

(vi) Assessorar o gerenciamento dos negócios no que se refere ao entendimento, interpretação e impacto da legislação, monitorando as melhores práticas em sua execução, bem como analisar, periodicamente, as normas emitidas pelos órgãos competentes, como a CVM e outros organismos congêneres;

(vii) Elaborar relatório **anual** listando as operações identificadas como suspeitas que tenham sido comunicadas às autoridades competentes, no âmbito da Política de Combate e Prevenção à Lavagem de Dinheiro e de Cadastro da Gestora;

(viii) Encaminhar aos órgãos de administração da Gestora, até o **último dia útil do mês de abril** de cada ano, relatório referente ao ano civil imediatamente anterior à data de entrega, contendo: ***(a)*** as conclusões dos exames efetuados; ***(b)*** as recomendações a respeito de eventuais deficiências, com o estabelecimento de cronogramas de saneamento, quando for o caso; e ***(c)*** a manifestação do diretor responsável pela administração de carteiras de valores mobiliários ou, quando for o caso, pelo diretor responsável pela gestão de risco a respeito das deficiências encontradas em verificações anteriores e das medidas planejadas, de acordo com cronograma específico, ou efetivamente adotadas para saná-las; devendo referido relatório permanecer disponível à CVM na sede da Gestora;

(ix) Definir os princípios éticos a serem observados por todos os Colaboradores, constantes deste Manual ou de outros documentos que vierem a ser produzidos para este fim, elaborando sua revisão periódica;

(x) Promover a ampla divulgação e aplicação dos preceitos éticos no desenvolvimento

das atividades de todos os Colaboradores, inclusive por meio dos treinamentos periódicos previstos neste Manual;

(xi) Apreciar todos os casos que cheguem ao seu conhecimento sobre o potencial descumprimento dos preceitos éticos e de compliance previstos neste Manual ou nos demais documentos aqui mencionados, e apreciar e analisar situações não previstas;

(xii) Garantir o sigilo de eventuais denunciantes de delitos ou infrações, mesmo quando estes não solicitarem, exceto nos casos de necessidade de testemunho judicial;

(xiii) Solicitar sempre que necessário, para a análise de suas questões, o apoio da auditoria interna ou externa ou outros assessores profissionais;

(xiv) Aplicar eventuais sanções aos Colaboradores, que devem ser previamente definidas pelo Comitê de Compliance e Risco; e

(xv) Analisar e, conforme o caso, encaminhar ao Comitê de Compliance e Risco da Gestora, as situações que cheguem ao seu conhecimento e que possam ser caracterizadas como "conflitos de interesse" pessoais e profissionais. Esses conflitos podem acontecer, inclusive, mas não limitadamente, em situações que envolvam:

- Investimentos pessoais;
- Transações financeiras com clientes fora do âmbito da Gestora;
- Recebimento de favores/presentes de administradores e/ou sócios de companhias investidas, fornecedores ou clientes;
- Análise financeira ou operação com empresas cujos sócios, administradores ou funcionários, o Colaborador possua alguma relação pessoal;
- Análise financeira ou operação com empresas em que o Colaborador possua investimento próprio; ou
- Participações em alguma atividade política.

Todo e qualquer Colaborador da Gestora que souber de informações ou situações em andamento que possam afetar os interesses da Gestora, gerar conflitos ou, ainda, se revelarem contrárias aos termos previstos nesta Política, deverá informar à Diretora de Risco, Compliance e PLD/FTP e/ou ao Comite de Compliance e Risco da Gestora, para que sejam tomadas as providências cabíveis.

Ainda, cabe à Diretora de Risco, Compliance e PLD/FTP analisar situações que possam ser caracterizadas como "conflitos de interesse" pessoais e profissionais e eventuais

condutas descritas no Código de Ética, respeitada a competência do Comitê de Compliance e Risco da Gestora, acompanhar o resultado dos testes de aderência e supervisionar as atividades de controles internos da Gestora.

2.1.2. Comitê de Compliance e Risco

A Gestora conta com um Comitê de Compliance e Risco para assessorar sobre as questões de compliance da Gestora, com autonomia para o exercício das suas funções.

O Comitê de Compliance e Risco é um órgão consultivo e deliberativo, conforme o caso, cuja finalidade é o controle e monitoramento das atividades da Gestora relacionadas à adoção de estratégias, políticas e medidas voltadas para a definição e monitoramento dos controles internos e de sua adequação às disposições da regulamentação e autorregulamentação aplicáveis, bem como para a gestão e mitigação de riscos inerentes às carteiras dos veículos de investimento sob gestão, segundo as normas e a legislação aplicáveis.
O Comitê de Compliance e Risco será composto pelos seguintes membros permanentes:

I. Diretora de Risco, Compliance e PLD/FTP;
II. Analistas da Área de Compliance e Risco;
III. Alta Administração da Gestora;

O Comitê de Compliance e Risco poderá ser composto ainda pelo Diretor de Gestão e/ou por outros membros da Equipe de Gestão, desde que convidados pela Diretora de Risco, Compliance e PLD/FTP de acordo com a pauta prevista da reunião.

O coordenador do Comitê de Compliance e Risco será a Diretora de Risco, Compliance e PLD/FTP ("Coordenador do Comitê de Compliance e Risco).

Compete ao Comitê de Compliance e Risco:

I. Avaliar a efetividade, conformidade e implementação das políticas internas da Gestora, especialmente, mas não limitadamente, dos listados a seguir e recomendar melhorias caso julgue necessário: (i) este Manual; (ii) Política de Investimentos Pessoais; (iii) Política de Rateio e Divisão de Ordens; (iv)

Política de PLD/FTP e Manual de Cadastro; (v) Código de Ética; (vi) Plano de Contingência, dentre outros;

II. Analisar eventuais ações erroneamente praticadas pela Diretora de Risco, Compliance e PLD/FTP sobre as atividades e rotinas de compliance, se o caso;
III. Revisar e aprovar as políticas, metodologias e parâmetros de controle existentes;
IV. Certificar a conformidade dos procedimentos internos da Gestora com as normas, regulamentos e legislação aplicáveis, recomendando e propondo a adoção de orientações e políticas novas;
V. Avaliar as situações relativas a potenciais ou efetivos conflitos de interesse;
VI. Analisar eventuais casos de infringência das regras descritas neste Manual, no Código de Ética da Gestora e nas demais políticas e manuais internos da Gestora, das regras contidas na regulamentação em vigor, ou de outros eventos relevantes e definir sobre as sanções a serem aplicadas;
VII. Garantir a independência da Área de Compliance e Risco;
VIII. Analisar eventuais mudanças no perfil dos fundos de investimentos que impactam em sua governança de controle.

Compete ao Coordenador do Comitê de Compliance e Risco:

I. Propor ao Comitê de Compliance e Risco, o calendário anual de reuniões para o seu exercício;
II. Convocar e presidir as reuniões; e
III. Cumprir e fazer cumprir as normas deste Manual.

As deliberações serão tomadas por manifestação da maioria dos seus membros permanentes, ressalvado que o Diretor de Gestão ou qualquer pessoa da Equipe de Gestão que vier a participar não terá poder de voto nas matérias que forem de natureza estritamente de compliance, sendo a sua presença apenas para fins de reporte.

Sem prejuízo do disposto na presente cláusula, a Diretora de Risco, Compliance e PLD/FTP possui voto de qualidade, na hipótese de empate, bem como detém a prerrogativa de veto das decisões tomadas pelo Comitê de Compliance e Risco.

O Comitê de Compliance e Risco é instituído em caráter permanente de funcionamento.

A função de membro do Comitê de Compliance e Risco é indelegável e deverá ser exercida direta e pessoalmente por ele.

O Comitê de Compliance e Risco se reunirá, no mínimo, **mensalmente** para discussão da pauta de controles internos da Gestora e, extraordinariamente, sob demanda.

As reuniões do Comitê de Compliance e Risco ocorrerão validamente com a presença de no mínimo 2 (dois) de seus membros permanentes, sendo necessariamente um deles o Coordenador do Comitê de Compliance e Risco.

Em caso de ausências de membros permanentes o Coordenador do Comitê de Compliance e Risco poderá nomear um substituto.

O conteúdo das deliberações, as decisões tomadas e os debates serão registrados por e-mail e/ou ata de reunião.

Após as reuniões, as deliberações serão registradas no software Compliasset e arquivadas em pasta eletrônica da Gestora, ficando à disposição para fins de transparência e melhores práticas de governança.

2.1.3. Área de Compliance e Risco

As seguintes atividades são de responsabilidade primária da Área de Compliance e Risco:

(i) Aconselhamento e suporte consultivo às áreas de negócios, comitês internos e à Diretoria a respeito de regras e normas emanadas de órgãos reguladores e autorreguladores;

(ii) Gestão do Código de Ética, zelando pela manutenção do dever fiduciário perante os clientes e investidores, prevendo e implementando procedimentos para mitigação de eventuais conflitos de interesse, bem como zelando pela observância das vedações normativas previstas no artigo 18 da Resolução CVM nº 21.

(iii) Implementar programas de treinamento dos Colaboradores, nos termos da

Política de Treinamento;

(iv) Identificar, documentar e avaliar os riscos associados à conformidade das atividades da Gestora aos preceitos normativos, analisando o impacto do oferecimento de novos produtos e serviços ou de relacionamento com determinados investidores que envolvam grau de risco;

(v) Manutenção dos formulários regulatórios, em especial o Formulário de Referência, responsabilizando-se pela atualização e revisão periódica daqueles documentos, inclusive mantendo as informações atualizadas no *website* da Gestora e junto à CVM e à Anbima, zelando ainda pela sua completude, veracidade e adequação de sua linguagem;

(vi) Acompanhamento das principais normas, diretrizes e alertas emanados de órgãos reguladores e autorreguladores;

(vii) Manutenção e atualização de agenda regulatória contendo todos os prazos emanados de normas regulatórias e autorregulatórias, devendo usar sistemas eletrônicos ou planilhas para tanto;

(viii) Realização de testes periódicos a fim de monitorar e avaliar a efetividade das políticas estabelecidas na Política e dos sistemas e controles da Gestora, sugerindo e acompanhando as ações de melhorias decorrentes de tais testes, podendo utilizar-se de sistema eletrônico próprio para tanto;

(ix) Realização de testes de controles de acesso em recursos computacionais (diretórios internos e sistemas), bem como outros testes para verificação das funcionalidades dos sistemas eletrônicos utilizados pela Gestora e disponibilização efetiva de backups dos documentos e sistemas;

(x) Desenvolver e disponibilizar à Diretoria da Gestora ou alta adminsitração um relatório de controles internos conforme estabelecido no artigo 25 da Resolução CVM nº 21, o qual deverá ser elaborado anualmente e disponibilizado **até o último dia útil do mês de abril**, relativo ao ano civil imediatamente anterior à data de entrega (com base nos testes de aderência referidos no item acima);

(xi) Manter atualizadas e disponíveis no website da Gestora as políticas previstas no artigo 16 da Resolução CVM nº 21, bem como aquelas cuja publicidade seja exigida pela Anbima e/ou outro órgão regulador;

(xii) Interação com os órgãos reguladores e autorreguladores em nome da Gestora, bem como o atendimento a fiscalizações e supervisões de órgãos reguladores e autorreguladores, auditorias terceirizadas e *due dilligence*, fazendo a interface entre as solicitações destes e as áreas internas da Gestora, respeitadas as regras

dispostas no Manual de Ética da Gestora;

(xiii) Gestão das Atividades de Prevenção à Lavagem de Dinheiro e Não Financiamento do Terrorismo, implementando a política e seus procedimentos de forma a prevenir a ocorrência de situações atípicas e permitindo sua imediata identificação na ocorrência e eventual comunicação ao COAF;

(xiv) *Cross border issues*: avaliar questões regulatórias aplicáveis nas jurisdições estrangeiras com as quais a Gestora realize operações ou, por ventura, venha a obter registro;

(xv) Gestão das Políticas de Investimentos Pessoais de Colaboradores, incluindo a concessão de aprovações quando for o caso, e monitoramentos periódicos;

(xvi) Informar à CVM sempre que verifique, no exercício das suas atribuições, a ocorrência ou indícios de violação da legislação que incumbe à CVM fiscalizar, no prazo máximo de 10 (dez) dias úteis da ocorrência ou identificação;

(xvii) Verificar se os devidos profissionais da área de Gestão estão com sua certificação ou isenção vigentes, bem como verificar se os demais procedimentos exigidos pela regulação e autorregulamentação aplicáveis estão sendo cumpridos;

(xviii) Realizar monitoramento de e-mails corporativos de Colaboradores, sempre que julgar necessário;

(xix) Verificar **anualmente** se os Colaboradores, em especial controladores e demais sócios ou diretores da Gestora, estão envolvidos em processos administrativos da CVM ou Anbima, ou processos criminais de qualquer natureza; e

(xx) Confirmar, por meio do CVMWeb, até o dia 31 de março de cada ano, que as informações contidas no formulário cadastral da Gestora previsto na Resolução CVM nº 51/21 continuam válidas, bem como atualizar o referido formulário cadastral sempre que qualquer dos dados neles contido for alterado, em até 7 (sete) dias úteis contados do fato que deu causa à alteração.

Sempre que entender necessário ou conveniente, a Diretora de Risco, Compliance e PLD/FTP poderá levar qualquer assunto de sua competência para apreciação ou deliberação pelo Comitê de Compliance e Risco.

2.2. Garantia de Independência

Os Colaboradores que desempenharem as atividades de compliance formarão a Área de

Compliance e Risco, sob a coordenação da Diretora de Risco, Compliance e PLD/FTP, sendo certo que a Área de Compliance e Risco exerce suas atividades de forma completamente independente das outras áreas da Gestora e poderá exercer seus poderes e autoridade com relação a qualquer Colaborador.

2.3 Sanções ("*Enforcement*")

A Gestora não assume a responsabilidade de Colaboradores que transgridam a lei ou cometam infrações no exercício de suas funções.

Neste sentido, conforme mencionado acima, a Diretora de Risco, Compliance e PLD/FTP, desde que decidido em Comitê de Compliance e Risco, poderá aplicar sanções aos Colaboradores em decorrência de descumprimentos das normas relativas a todas Políticas da Gestora, garantido ao Colaborador, contudo, amplo direito de defesa.

Os Colaboradores, desta forma, estarão sujeitos, entre outras, às penas de advertência, suspensão, desligamento, exclusão ou demissão por justa causa, ou, ainda, rescisão contratual, conforme o regime aplicável, sem prejuízo de eventuais outras medidas adicionais no âmbito cível (incluindo o direito de regresso) e criminal que se fizerem cabíveis.

2.4. Dúvidas ou ações contrárias aos princípios e normas do Manual

Este Manual possibilita avaliar muitas situações de problemas éticos que podem eventualmente ocorrer no cotidiano da Gestora, mas seria impossível detalhar todas as hipóteses. É natural, portanto, que surjam dúvidas ao enfrentar uma situação concreta que contrarie as normas de compliance e princípios que orientam as ações da Gestora.

Em caso de dúvida em relação a quaisquer das matérias constantes deste Manual, também é imprescindível que se busque auxílio imediato junto à Diretora de Risco, Compliance e PLD/FTP e/ou ao Comitê de Compliance e Risco para obtenção de orientação mais adequada.

Mesmo que haja apenas a suspeita de potencial situação de conflito ou ocorrência de

uma ação que vá afetar os interesses da Gestora, o Colaborador deverá seguir essa mesma orientação. Esta é a maneira mais transparente e objetiva para consolidar os valores da cultura empresarial da Gestora e reforçar os seus princípios éticos.

Para os fins do presente Manual, portanto, toda e qualquer solicitação que dependa de autorização, orientação ou esclarecimento expresso da Diretora de Risco, Compliance e PLD/FTP e/ou do Comitê de Compliance e Risco, bem como eventual ocorrência, suspeita ou indício de prática por qualquer Colaborador que não esteja de acordo com as disposições deste Manual e das demais normas aplicáveis às atividades da Gestora, deve ser dirigida pela pessoa que necessite da autorização, orientação ou esclarecimento ou que tome conhecimento da ocorrência ou suspeite ou possua indícios de práticas em desacordo com as regras aplicáveis, à Diretora de Risco, Compliance e PLD/FTP e/ou ao Comitê de Compliance e Risco, exclusivamente por meio de e-mail.

2.5. Revisão de Compliance

Mediante ocorrência de descumprimento, suspeita ou indício de descumprimento de quaisquer das regras estabelecidas neste Manual ou aplicáveis às atividades da Gestora, que cheguem ao conhecimento da Diretora de Risco, Compliance e PLD/FTP e/ou do Comitê de Compliance e Risco, de acordo com os procedimentos estabelecidos neste Manual, a Diretora de Risco, Compliance e PLD/FTP e/ou o Comitê de Compliance e Risco utilizarão os registros e sistemas de monitoramento eletrônico referidos neste Manual para verificar a conduta dos Colaboradores envolvidos.

Todo conteúdo que está na rede será acessado pela Diretora de Risco, Compliance e PLD/FTP e/ou pelo Comitê de Compliance e Risco, caso haja necessidade, inclusive arquivos pessoais salvos em cada computador serão acessados caso a Diretora de Risco, Compliance e PLD/FTP e/ou o Comitê de Compliance e Risco julguem necessário. Da mesma forma, mensagens de correio eletrônico de Colaboradores poderão ser gravadas e, quando necessário, interceptadas e analisadas, sem que isto represente invasão da privacidade dos Colaboradores, já que se trata de ferramentas de trabalho disponibilizadas pela Gestora.

Adicionalmente, será realizado um monitoramento **semestral**, a cargo da Diretora de Risco, Compliance e PLD/FTP, sobre uma amostragem significativa dos Colaboradores, escolhida aleatoriamente pela Diretora de Risco, Compliance e PLD/FTP, para que sejam verificados os arquivos eletrônicos, inclusive e-mails, com o objetivo de verificar possíveis situações de descumprimento às regras contidas no presente Manual.

A Diretora de Risco, Compliance e PLD/FTP poderá utilizar as informações obtidas em tais sistemas para sugerir ao Comitê de Compliance e Risco acerca de eventuais sanções a serem aplicadas aos Colaboradores envolvidos, nos termos deste Manual. No entanto, a confidencialidade dessas informações é respeitada e seu conteúdo será disponibilizado ou divulgado somente nos termos deste Manual e para os devidos fins legais ou em atendimento a determinações judiciais.

Adicionalmente, a Diretora de Risco, Compliance e PLD/FTP deverá ainda verificar rotineiramente os níveis de controles internos e compliance junto a todas as áreas da Gestora, com o objetivo de promover ações para esclarecer e regularizar eventuais desconformidades. Analisará também os controles previstos neste Manual, bem como em outras políticas da Gestora, propondo a criação de novos controles e melhorias naqueles considerados deficientes, monitorando as respectivas correções.

Além dos procedimentos de supervisão periódica, a Diretora de Risco, Compliance e PLD/FTP poderá, quando julgar oportuno e necessário, realizar inspeções, nas ferramentas de trabalho, a qualquer momento sobre quaisquer Colaboradores.

Por fim, ao menos uma vez por ano, a Área de Compliance e Risco deverá conduzir uma revisão completa de todo Programa de Compliance, que inclui esta Política, a agenda regulatória, o programa de treinamento, inclusive da própria Área de Compliance e Risco, as revisões de formulários e testes de aderência, detalhados em sistema interno.

Como resultado da revisão anual, a Área de Compliance e Risco deverá elaborar relatório de conclusões de controles internos de que trata o artigo 25 da Resolução CVM nº 21, sob condução e responsabilidade final da Diretora de Risco, Compliance e PLD/FTP.

2.6. Sistema de Gerenciamento de Compliance

A Gestora utiliza sistema para gestão de compliance denominado CompliAsset. O sistema possui, ainda, uma biblioteca digital para armazenamento de documentos e registro de eventos. Portanto, os registros e arquivamentos a cargo da Área de Compliance e Risco poderão ser realizados no referido sistema, a seu critério.

Além disso, todas as atividades, eventos e demais registros imputados no referido sistema possuem logs de registro para fins de auditoria e *backups* automáticos.

3 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

3.1. Objetivo e Definições de Segurança da Informação

A Política de Segurança da Informação da Gestora ("Política de Segurança da Informação") tem por objetivo, o adequado gerenciamento das informações de posse temporária ou de propriedade da Gestora. Assim, deverá ser seguida por todos os seus Colaboradores (conforme definidos no Código de Ética), independentemente do nível hierárquico ou função na instituição, bem como de vínculo empregatício ou prestação de serviços.

A responsabilidade em relação à segurança da informação deve ser comunicada no início do vínculo com a Gestora, devendo cada Colaborador assinar o Termo de Responsabilidade e Confidencialidade, de acordo com o **Anexo II** desta Política.

A Área de Compliance e Risco realizará a revisão e atualização desta Política **anualmente** ou sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão da Diretora de Risco, Compliance e PLD/FTP.

As medidas de segurança da informação têm por finalidade minimizar as ameaças aos negócios da Gestora e às disposições deste Manual, buscando, principal, mas não exclusivamente, a proteção de Informações Confidenciais.

Conforme disposto no Termo de Responsabilidade e Confidencialidade, nenhuma Informação Confidencial, conforme abaixo definido, deve, em qualquer hipótese, ser

divulgada fora da Gestora. Fica vedada qualquer divulgação, no âmbito pessoal ou profissional, que não esteja em acordo com as normas legais (especialmente, mas não de forma limitada, aquelas indicadas no **Anexo III** deste Manual) e de compliance da Gestora.

3.1.1. Informações Confidenciais

São consideradas informações confidenciais, reservadas ou privilegiadas ("Informações Confidenciais"), para os fins deste Manual, independente destas informações estarem contidas em discos, pen-drives, fitas, e-mails, outros tipos de mídia ou em documentos físicos, ou serem escritas, verbais ou apresentadas de modo tangível ou intangível, qualquer informação sobre a Gestora, sobre as empresas pertencentes ao seu conglomerado, seus sócios e clientes, aqui também contemplados os próprios fundos sob gestão da Gestora, incluindo:

(i) *Know-how*, técnicas, cópias, diagramas, modelos, amostras, programas de computador;
(ii) Informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e dos fundos geridos pela Gestora;
(iii) Operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento sob gestão Gestora;
(iv) Estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços;
(v) Informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da Gestora e a seus sócios e clientes, incluindo alterações societárias (fusões, cisões e incorporações), informações sobre compra e venda de empresas, títulos ou valores mobiliários, inclusive ofertas iniciais de ações (*IPO*), projetos e qualquer outro fato que seja de conhecimento em decorrência do âmbito de atuação da Gestora e que ainda não foi devidamente levado à público;
(vi) Informações a respeito de resultados financeiros antes da publicação dos balanços, balancetes e/ou demonstrações financeiras dos fundos de investimento;
(vii) Transações realizadas e que ainda não tenham sido divulgadas publicamente; e
(viii) Assim como, outras informações sensíveis eventualmente obtidas junto a sócios, diretores, funcionários, *trainees*, estagiários ou jovens aprendizes da Gestora ou,

ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.

3.1.2. Informações Privilegiadas

Considera-se informação privilegiada e portanto, confidencial, qualquer informação, não pública, material, e relevante a respeito de qualquer companhia, e que seja obtida de forma privilegiada (ou seja, decorrente de relação profissional ou pessoal mantida com a Tyton Capital, um cliente ou pessoas relacionadas aos ativos dos fundos geridos. Nos termos da regulamentação aplicável, é vedada a utilização de informação relevante ainda não divulgada, por qualquer pessoa que a ela tenha tido acesso, com a finalidade de auferir vantagem, para si ou para outrem, mediante negociação de valores mobiliários. Neste sentido, todas as informações privilegiadas devem ser mantidas em sigilo por aqueles que tiverem acesso, seja em decorrência do exercício da atividade profissional ou de relacionamento pessoal.

Sem prejuízo da colaboração da Gestora com as autoridades fiscalizadoras de suas atividades, a revelação de Informações Confidenciais a autoridades governamentais ou em virtude de decisões judiciais, arbitrais ou administrativas, deverá ser prévia e tempestivamente informada à Diretora de Risco, Compliance e PLD/FTP para que esta decida sobre a forma mais adequada para tal revelação, após exaurirem todas as medidas jurídicas apropriadas para evitar a supramencionada revelação.

Em nenhuma hipótese as Informações Confidenciais poderão ser utilizadas para a prática de atos que configurem *Insider Trading*, Dicas ou *Front-running*.

3.1.3. Insider Trading e "Dicas"

Insider Trading significa a compra e venda de títulos ou valores mobiliários com base no uso de Informação Confidencial e Privilegiada, com o objetivo de conseguir benefício próprio ou de terceiros (compreendendo os Colaboradores).

"Dica" é a transmissão, a qualquer terceiro, estranho às atividades da Gestora, de Informação Confidencial que possa ser usada com benefício na compra e venda de títulos ou valores mobiliários.

3.1.4. Front-running

Front-running significa a prática que envolve o aproveitamento de alguma Informação Confidencial para realizar ou concluir uma operação antes de outra pessoa, considerando, para tanto, o conhecimento de que a pessoa lesada também executaria a mesma espécie de ação. Esta operação demanda: (i) conhecimento, por parte do praticante, de que a pessoa lesada efetuará determinada prática; e (ii) vontade de valer-se desse conhecimento para auferir vantagem própria por executar sua própria ação em momento anterior.

3.2. Conduta dos Colaboradores visando Segurança da Informação

Os Colaboradores deverão observar as regras de confidencialidade previstas neste Manual, inclusive no que refere ao conceito de "Informações Confidenciais" e "Informações Privilegiadas" abordados nesta Política de Segurança de Informação, por qualquer meio, seja eletrônica, escrita ou oral.

O disposto nos itens acima deve ser observado, pelo Colaborador, não só durante a vigência de seu relacionamento profissional com a Gestora, mas também após o seu término.

Os Colaboradores deverão guardar sigilo sobre qualquer Informação Confidencial à qual tenham acesso, até sua divulgação ao mercado, bem como zelar para que subordinados e terceiros de sua confiança também o façam, respondendo pelos danos causados na hipótese de descumprimento.

Caso os Colaboradores tenham acesso, por qualquer meio, a Informação Confidencial, deverão levar tal circunstância ao imediato conhecimento da Diretora de Risco, Compliance e PLD/FTP indicando, além disso, a fonte da Informação Confidencial assim obtida. Tal dever de comunicação também será aplicável nos casos em que a Informação Confidencial seja conhecida de forma acidental, em virtude de comentários casuais ou por negligência ou indiscrição das pessoas obrigadas a guardar segredo. Os Colaboradores que, desta forma, acessarem a Informação Confidencial, deverão abster-

se de fazer qualquer uso dela ou comunicá-la a terceiros, exceto quanto à comunicação à Diretora de Risco, Compliance e PLD/FTP anteriormente mencionada.

É expressamente proibido valer-se das práticas descritas acima para obter, para si ou para outrem, vantagem indevida mediante negociação, em nome próprio ou de terceiros, de títulos e valores mobiliários, sujeitando-se o Colaborador às penalidades descritas neste Manual e na legislação aplicável, incluindo eventual demissão por justa causa.

De forma não exaustiva, as seguintes condutas devem ser observadas:

(i) Os Colaboradores devem evitar circular em ambientes externos à Gestora com cópias (físicas ou digitais) de arquivos contendo Informações Confidenciais, devendo essas cópias serem mantidas através de senha de acesso;

(ii) O descarte de Informações Confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação, sempre com a orientação do superior hierárquico;

(iii) As informações que possibilitem a identificação de um cliente da Gestora devem se limitar a arquivos de acesso restrito e apenas poderão ser copiadas ou impressas se forem para o atendimento dos interesses da Gestora ou do próprio cliente;

(iv) Os Colaboradores devem estar atentos a eventos externos que possam comprometer o sigilo das informações da Gestora, como, por exemplo, vírus de computador, fraudes, entre outros;

(v) Assuntos confidenciais não devem ser discutidos em ambientes públicos ou locais considerados expostos;

(vi) A troca de informações entre os Colaboradores da Gestora deve sempre se pautar no conceito de que o receptor deve ser alguém que necessita receber tais informações para o desempenho de suas atividades e que não está sujeito a nenhuma barreira que impeça o recebimento daquela informação. Em caso de dúvida, a Área de Compliance e Risco deve ser acionada previamente à revelação;

(vii) Os Colaboradores não deverão, em qualquer hipótese, deixar em suas respectivas estações de trabalho ou em outro espaço físico da Gestora qualquer documento que contenha Informação Confidencial durante a ausência do respectivo usuário, principalmente após o encerramento do expediente;

(viii) Qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora, pois pode conter informações restritas e confidenciais mesmo no ambiente interno da Gestora. A Gestora não mantém arquivo físico centralizado, sendo cada Colaborador responsável direto pela boa conservação, integridade e segurança de quaisquer informações em meio físico que tenha armazenadas consigo;

(ix) Os Colaboradores devem se abster de utilizar pen-drivers, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na Gestora. É proibida a conexão de equipamentos na rede da Gestora que não estejam previamente autorizados pela área de informática e pelos administradores da Gestora;

(x) Cada Colaborador é responsável ainda por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade. Todo Colaborador deve ser cuidadoso na utilização do seu próprio equipamento e sistemas e zelar pela boa utilização dos demais. Caso algum Colaborador identifique a má conservação, uso indevido ou inadequado de qualquer ativo ou sistemas deve comunicar a Diretora de Risco, Compliance e PLD/FTP.

A Gestora permite o acesso remoto pelos Colaboradores. Ademais, os Colaboradores serão instruídos a (i) manter a utilização apenas em dispositivos que requeiram a inclusão de login e senha previamente ao acesso, (ii) manter softwares de proteção contra malware/antivírus nos dispositivos remotos, e (iii) relatar à Diretora de Risco, Compliance e PLD/FTP qualquer violação ou ameaça de segurança cibernética ou outro incidente que possa afetar informações da Gestora e que ocorram durante o trabalho remoto.

3.3. Divulgação de Fatos Relevantes

Em que pese seja responsabilidade do administrador fiduciário do fundo a operacionalização da divulgação de qualquer fato relevante ocorrido ou relacionado ao funcionamento do fundo, da classe ou aos ativos integrantes da carteira, assim que dele tiver conhecimento, é responsabilidade dos demais prestadores de serviços, incluindo a Gestora, informar imediatamente ao administrador fiduciário sobre os fatos relevantes de que venham a ter conhecimento, para a devida divulgação.

Nesse sentido, são considerados relevantes, nos termos do artigo 64, §1º da Parte Geral da Resolução CVM 175, quaisquer fatos que possam influir de modo ponderável no valor das cotas ou na decisão dos investidores de adquirir, resgatar, alienar ou manter cotas.

A seguinte lista não é exaustiva e apresenta exemplos de fatos potencialmente relevantes:

- alteração no tratamento tributário conferido ao fundo, à classe ou aos cotistas;
- contratação de formador de mercado e o término da prestação desse serviço;
- contratação de agência de classificação de risco, caso não estabelecida no regulamento do fundo ou no anexo da classe;
- mudança na classificação de risco atribuída ao fundo, à classe ou à subclasse de cotas;
- alteração de prestador de serviço essencial;
- fusão, incorporação, cisão ou transformação do fundo ou da classe de cotas;
- alteração do mercado organizado em que seja admitida a negociação de cotas do fundo;
- cancelamento da admissão das cotas do fundo ou da classe à negociação em mercado organizado; e
- emissão de cotas de fundo fechado.

Os fatos relevantes podem, de formar excepcional, deixar de ser divulgados, caso seja entendido pela Gestora e pelo administrador fiduciário do fundo que sua revelação põe em risco interesse legítimo dos fundos ou de seus cotistas. Neste caso, tais informações serão tratadas como confidenciais até a Gestora julgar como oportuno o momento para sua divulgação.

Por outro lado, o administrador fiduciário fica obrigado a divulgar imediatamente fato relevante na hipótese de a informação escapar ao controle ou se ocorrer oscilação atípica na cotação, preço ou quantidade negociada de cotas, em havendo negociação em mercado regulado. A Gestora deverá notificar o administrador fiduciário caso tenha conhecimento de qualquer situação neste sentido.

A Gestora deverá disponibilizar os fatos relevantes relativos aos fundos sob sua gestão em seu website.

3.4. Identificação de Riscos à Segurança de Informação (risk assessment)

No âmbito de suas atividades, a Gestora identificou os seguintes principais riscos internos e externos que precisam de proteção:

(i) Dados e Informações: as Informações Confidenciais, incluindo informações a respeito de investidores, clientes, Colaboradores e da própria Gestora, operações e ativos investidos pelas carteiras de valores miliários sob sua gestão, e as comunicações internas e externas (por exemplo: correspondências eletrônicas e físicas);

(ii) Sistemas: informações sobre os sistemas utilizados pela Gestora e as tecnologias desenvolvidas internamente e por terceiros, suas ameaças possíveis e sua vulnerabilidade;

(iii) Processos e Controles: processos e controles internos que sejam parte da rotina das áreas de negócio da Gestora; e

(iv) Governança da Gestão de Risco: a eficácia da gestão de risco pela Gestora quanto às ameaças e planos de ação, de contingência e de continuidade de negócios.

Com base no exposto acima, a Gestora avalia e define planos de prevenção e acompanhamento para a mitigação ou eliminação do risco, assim como as eventuais modificações necessárias e o plano de retomada das atividades normais e reestabelecimento da segurança devida.

3.5. Barreiras e Controles de Acesso a Informações Confidenciais

Todo acesso a diretórios e sistemas de informações da Gestora deve ser controlado. Somente poderão acessar tais diretórios e sistemas de informação os Colaboradores previamente autorizados pela Diretora de Risco, Compliance e PLD/FTP, observado o disposto na Política de Segurança Cibernética.

As instalações da Gestora são protegidas por controles de entrada apropriados para assegurar a segurança dos Colaboradores e proteger o sigilo, a integridade e a disponibilidade da informação. Dessa forma, o controle do acesso a sistemas de informações da Gestora levará em conta as seguintes premissas:

(i) Garantia de que o nível de acesso concedido ao Colaborador é adequado ao seu perfil; e

(ii) Cancelamento imediato do acesso concedido a Colaboradores desligados, afastados ou que tenham sua função alterada na Gestora.

Todos os equipamentos da rede deverão estar acomodados em uma sala fechada, de acesso restrito. As estações de trabalho serão fixas, com computadores seguros e as sessões abertas deverão ser trancadas quando deixadas sem supervisão do Colaborador responsável por seu computador.

A Política leva em consideração diversos riscos e possibilidades considerando o porte, perfil de risco, modelo de negócio e complexidade das atividades desenvolvidas pela Gestora.

A coordenação direta das atividades relacionadas à política de segurança da informação e segurança cibernética ficará a cargo da Diretora de Risco, Compliance e PLD/FTP, que será o responsável inclusive por sua revisão, realização de testes e treinamento dos Colaboradores, conforme aqui descrito.

3.5.1. Servidor (File Server)

Todos os e-mails e arquivos da Gestora são armazenados em um *file server* com altos padrões de segurança e ética, possibilitando controle de acesso e rastreamento de uso dos arquivos por usuário, o que garante a preservação de informações confidenciais e a restrição de acesso aos arquivos sensíveis. Toda a base de dados conta com a realização de *backups* simultâneos que ficam armazenados nas nuvens e que permitem, em caso de falhas operacionais, recuperação de dados e arquivos.

O *file server* da Gestora é acessado pelos Colaboradores mediante *login* com usuário e senha próprios, tendo os usuários permissões diferenciadas de acordo com as funções

e atividades desempenhadas por cada profissional. Dessa forma, os diferentes níveis de permissão viabilizam melhor controle de acesso e de reprodução dos dados e arquivos pelos profissionais da Gestora.

3.5.2. Acesso Escalonado do Sistema

O acesso como "administrador" de área de *desktop* para computadores da Gestora fornecidos aos seus colaboradores (i.e., esta regra acesso não se aplica ao uso de computadores pessoais utilizados em acesso remoto) é limitado aos usuários aprovados pela Diretora de Risco, Compliance e PLD/FTP e, com isso, serão determinados privilégios/credenciais e níveis de acesso de usuários apropriados para os Colaboradores. As combinações de *login* e senha são utilizadas para autenticar as pessoas autorizadas e conferir acesso à rede da Gestora necessária ao exercício de suas atividades. A implantação destes controles é projetada para limitar a vulnerabilidade dos sistemas da Gestora em caso de violação;

3.5.3. Acesso de Terceiros

A Gestora possui uma rede de acesso à internet exclusiva para eventuais terceiros que visitem a Gestora, fortalecendo, assim, a estrutura geral das redes da Gestora contra-ataques cibernéticos.

O acesso de pessoas estranhas à Gestora a áreas restritas somente é permitido com a autorização expressa de Colaboradores autorizados pelos administradores da Gestora. Tendo em vista que a utilização de computadores, telefones, internet, e-mail e demais aparelhos se destina exclusivamente para fins profissionais, como ferramenta para o desempenho das atividades dos Colaboradores, a Gestora monitora a utilização de tais meios.

3.5.4. Identificação dos Detentores da Informação, Manutenção de Registros e Logs

Conforme acima exposto, será atribuído a cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo os usuários (*login*) individuais de

Colaboradores internos de responsabilidade do próprio. Assim, é possível realizar a identificação dos detentores da informação para eventual responsabilização, se for o caso.

Com relação ao monitoramento e auditoria do ambiente, a Gestora possui sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede. A informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado.

A Gestora informa, ainda, que poderá tomar as seguintes medidas:

(i) tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial ou por determinação da Diretora de Risco, Compliance e PLD/FTP;
(ii) realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;
(iii) instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso;
(iv) Monitoramento, por amostragem, do acesso dos Colaboradores a sites, blogs, fotologs, webmails, entre outros, bem como os e-mails enviados e recebidos;
(v) Verificação, por amostragem, das informações de acesso ao espaço do escritório, a desktops, pastas e sistemas, de forma a avaliar sua aderência às regras de restrição de acesso e escalonamento.

A Diretora de Risco, Compliance e PLD/FTP poderá adotar medidas adicionais para monitorar os sistemas de computação e os procedimentos aqui previstos para avaliar o seu cumprimento e sua eficácia.

O não cumprimento dos requisitos previstos nesta Política acarretará violação às regras internas da Gestora e sujeitará o usuário às sanções administrativas e legais cabíveis, observado o disposto no Código de Ética da Gestora.

Para fins de ilustração, segue uma lista não exaustiva de eventuais exemplos que podem ocasionar sanções:

(i) uso ilegal de software;
(ii) introdução (intencional ou não) de vírus de informática;
(iii) tentativas de acesso não autorizado a dados e sistemas; ou
(iv) divulgação de informações sensíveis da Gestora.

3.6. Proteção da Base de Dados

Os recursos computacionais da Gestora devem ser: **(i)** protegidos contra adulterações; e **(ii)** permitir a realização de auditorias e inspeções.

Todos os registros eletrônicos realizados pela Gestora deverão ser mantidos e estar disponíveis para atender os prazos legais e regulatórios praticados pelos órgãos reguladores locais e de jurisdições que a Gestora atue em mercado regulado.

As informações mantidas em meios eletrônicos devem ser salvas em bases replicadas (*backups*). O acesso a essas bases devem ser limitadas somente a pessoas autorizadas pela Área de Compliance e Risco.

3.6.1. Comunicação de Incidente/Vazamento de Informações Confidenciais

Os Colaboradores deverão comunicar à Área de Compliance e Risco quaisquer casos de violações às normas de segurança da informação que tenham conhecimento. Toda violação ou desvio é investigado para a determinação das medidas necessárias, visando a correção da falha ou reestruturação de processos. Em caso de vazamento de informação confidencial, a Diretora de Risco, Compliance e PLD/FTP discutirá com o Comitê de Compliance e Risco qual o melhor plano efetivo de recuperação e medidas para minimizar e prevenir danos.

Ademais, o Comitê de Compliance e Risco determinará quais clientes ou investidores, se houver, deverão ser contatados com relação eventual à violação.

3.6.2. Procedimentos de Resposta a Incidente de Segurança de Informações

Conforme acima destacado, a Diretora de Risco, Compliance e PLD/FTP discutirá com o Comitê de Compliance e Risco acerca de eventual resposta a qualquer informação de suspeita de infecção, acesso não autorizado ou outro comprometimento da rede ou dos dispositivos da Gestora de acordo com os critérios abaixo:

(i) Avaliação do tipo de incidente ocorrido (por exemplo, infecção de *malware*, intrusão da rede, furto de identidade), as informações acessadas e a medida da respectiva perda;
(ii) Identificação de quais sistemas, se houver, devem ser desconectados ou de outra forma desabilitados;
(iii) Determinação dos papéis e responsabilidades do pessoal apropriado;
(iv) Avaliação da necessidade de recuperação e/ou restauração de eventuais serviços que tenham sido prejudicados;
(v) Avaliação da necessidade de notificação de todas as partes internas e externas apropriadas (por exemplo, clientes ou investidores afetados, segurança pública);
(vi) Avaliação da necessidade de publicação do fato ao mercado, nos termos da regulamentação vigente, (por exemplo: em sendo Informações Confidenciais de fundo de investimento sob gestão da Gestora, a fim de garantir a ampla disseminação e tratamento equânime da Informação Confidencial);
(vii) Determinação do responsável (ou seja, a Gestora ou o cliente ou investidor afetado) que arcará com as perdas decorrentes do incidente. A definição ficará a cargo do Comitê de Compliance e Risco, após a condução de investigação e uma avaliação completa das circunstâncias do incidente.

3.7. Testes e Treinamento de Segurança da Informação

A Gestora realizará testes periódicos de segurança para os sistemas de informações (sem se limitar a, mas em especial, para os meios eletrônicos) **anualmente**, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

O treinamento sobre segurança de informação fará parte do treinamento inicial e periódico da Gestora, conforme previsto na Política de Treinamento da Gestora, o qual deverá, dentre outros, assegurar que todos os Colaboradores tenham conhecimento dos procedimentos e das obrigações aqui previstos, assim como minimizar a ocorrência de

incidentes de segurança em função de problemas no uso, desvio de informações, fraudes e na interpretação das normas e procedimentos.

4. POLÍTICA DE SEGURANÇA CIBERNÉTICA (CYBERSECURITY)

4.1. Objetivo e Definições de Cybersecurity

A Política de Segurança Cibernética ("Política de Cybersecurity") tem por objetivo estabelecer as regras, procedimentos e controles de segurança cibernética da Gestora. Assim, deverá ser seguida por todos os seus Colaboradores, independentemente do nível hierárquico ou função na instituição, bem como de vínculo empregatício ou prestação de serviços.

A Política segue práticas de mercado, bem como está de acordo com as leis, regulamentação e autorregulação aplicáveis, incluindo o Código AGRT e o Guia de Cibersegurança de junho de 2021. A presente Política deve ser divulgada a todos os Colaboradores, de forma que seu conteúdo possa ser consultado a qualquer momento.

No que se refere à segurança cibernética, a Gestora identificou as seguintes principais ameaças em relação as suas atividades, nos termos inclusive do Guia de Cibersegurança da Anbima:

- **Malwares**
  softwares desenvolvidos para corromper computadores e redes (tais como: Vírus, Cavalo de Troia, *Spyware* e *Ransomware*);

- **Engenharia social (Pharming, Phishing, Vishing, Smishing, e Acesso Pessoal)**
  métodos de manipulação para obter informações confidenciais;

- **Ataques de DDoS (Distributed Denial of Services) e botnets**
  ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição;

- **Invasões (advanced persistent threats)**
  ataques realizados por invasores sofisticados utilizando conhecimentos e

ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Com base no exposto acima, a Gestora avalia e define o plano estratégico de prevenção e acompanhamento para a mitigação ou eliminação do risco, assim como as eventuais modificações necessárias e o plano de retomada das atividades normais e reestabelecimento da segurança devida.

O objetivo das regras sobre segurança cibernética da Gestora é primordialmente assegurar a proteção de seus ativos de informação contra ameaças, internas ou externas, reduzir a exposição a perdas ou danos decorrentes de falhas de cibersegurança e garantir que os recursos adequados estarão disponíveis, mantendo um programa de segurança efetivo e conscientizando seus Colaboradores a respeito.

Os processos de segurança de dados e da informação da Gestora devem assegurar:

(i) a integridade (garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais);
(ii) a disponibilidade (garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário); e
(iii) a confidencialidade dos ativos de informação (garantia de que o acesso à informação seja obtido somente por pessoas autorizadas) da Gestora, observadas as regras de sigilo e confidencialidade constantes do Manual.

Além disso, esta Política dá ciência a cada Colaborador de que os ambientes, sistemas, computadores e redes da Gestora poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

A Gestora exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus Colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

4.2. Responsabilidade da Equipe TI e Cybersecurity

A equipe de Tecnologia da Informação ("T.I"), em conjunto com a Diretora de Risco, Compliance e PLD/FTP, sendo a principal responsável dentro da Gestora para tratar e responder questões de segurança cibernética ("Responsável pela Cybersecurity"), bem como por implementar as regras e normas aqui estabelecidas e a sua revisão.

Seguem abaixo uma lista não exaustiva dos deveres e responsabilidades do Responsável pela Cybersecurity:

(i) Testar a eficácia dos controles utilizados e informar à Diretoria/alta administração os riscos residuais;

(ii) Acordar com a Diretoria o nível de serviço que será prestado por terceiros contratados e os procedimentos de resposta aos incidentes;

(iii) Configurar os equipamentos e sistemas concedidos aos Colaboradores com todos os controles necessários para cumprir os requerimentos de segurança aqui estabelecidos, bem como definir e assegurar a segregação das funções administrativas a fim de restringir poderes de cada indivíduo e reduzir o número de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações;

(iv) Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio;

(v) Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da Gestora em processos de mudança, sendo ideal a proteção contratual para controle e responsabilização no caso de uso de terceiros;

(vi) Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da Gestora, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da Gestora;

(vii) Promover a conscientização dos Colaboradores em relação à relevância da segurança da informação para o negócio da Gestora, mediante treinamentos.

Na ocorrência de qualquer incidente envolvendo risco cibernético, todo e qualquer Colaborador que perceba ou desconfie de tal incidente deverá imediatamente informar

o Responsável pela Cybersecurity, que poderá convocar reunião do Comitê de Compliance e Risco.

4.3. Conduta dos Colaborares visando Cybersecurity

Caberá a todos os Colaboradores conhecer e adotar as disposições da Política de Segurança da Informação e da presente Política, e seus deveres e responsabilidades na manutenção da segurança corporativa. Deverão, ainda, proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados, assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades adequadas e buscar orientação do gestor imediato em caso de dúvidas, o qual recorrerá ao Responsável pela Cybersecurity, se for o caso.

Em caso de incidente que afete a segurança cibernética da Gestora, o Colaborador deverá comunicar imediatamente ao Responsável pela Cybersecurity, diretamente ou por meio do canal apropriado. Em caso de descumprimento, ainda que involuntário, estará sujeito às sanções internas aplicáveis e a eventual responsabilização na forma da lei.

4.4. Identificação de Riscos de Cybersecurity

A Gestora, a cada **24 (vinte e quatro) meses**, deverá identificar os riscos internos e externos, bem como os ativos de hardware e software e processos que precisam de proteção. Esse processo será conduzido pelo Responsável pela Cybersecurity e documentado pela Área de Compliance e Risco, com o fim de dar visibilidade à metodologia utilizada para avaliar e gerir as vulnerabilidades da Gestora. A Gestora poderá contratar uma empresa terceirizada para tanto, caso o Responsável pela Cybersecurity julgue necessário e mediante aprovação da Diretoria.

Após a condução do referido processo, a Diretoria deverá discutir as opções de tratamento a serem adotadas, considerando a seleção de controles para manter os riscos dentro de limites aceitáveis pela Gestora, considerados os possíveis impactos financeiros, operacionais e reputacionais, em caso de um evento de segurança, assim como a probabilidade de o evento acontecer.

Segue abaixo uma lista não exaustiva de alguns riscos de segurança cibernética identificados:

(i) Invasão sistêmica que prejudique dados internos, incluindo vírus ou ataque de hackers;
(ii) Comunicações falsas utilizando os dados coletados para ter credibilidade e enganar vítimas e comprometimento de estações de trabalho decorrente de cliques em link malicioso ("Phishing");
(iii) Exposição do ambiente devido a uma brecha de segurança, por diversos motivos como a instalação de software em contrariedade com as aprovações e condições estabelecidas nesta Política; ou
(iv) Vazamento de informações durante tráfego de dados não criptografados.

Periodicamente, a cada **12 (doze) meses**, a Gestora deverá revisar o processo de cibersegurança com o fim de estabelecer, manter e monitorar a estrutura de governança de cibersegurança, assegurando que as atividades de gerenciamento de segurança requeridas sejam executadas corretamente e de forma consistente pelos profissionais designados.

4.5. Prevenção e Proteção aos riscos de Cybersecurity

A Gestora estabeleceu um conjunto de medidas buscando mitigar os riscos identificados, ou seja, buscar impedir previamente a ocorrência de um ataque cibernético, incluindo a programação e implementação de controles, na forma abaixo. Cada Colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos sob sua responsabilidade.

4.5.1. Internet, E-mail e Computadores

A Gestora oferece a seus Colaboradores uma completa estrutura material e tecnológica para o exercício das atividades. É de responsabilidade do Colaborador manter e zelar pela integridade dessas ferramentas de trabalho.

A Gestora utiliza os serviços do SonicWall para se proteger de ameaças cibernéticas. A ferramenta de *firewall* realiza o bloqueio de sites com conteúdo inadequado, conserva

a largura de banda da rede e protege contra sites mal-intencionados, vírus, spam, tentativas de *phishing*, *malwares*, *ransomwares* e violação de dados. O firewall gerencia todas as redes da Gestora, evitando a perda de dados e detectando se informações sensíveis estão tentando deixar sua rede, por qualquer meio.

Além disso, o Colaborador é responsável pela proteção de seu banco de dados, seja ele composto por planilhas, e-mails e/ou conversas telefônicas contendo dados confidenciais de clientes e/ou da Gestora, dentre outros.

Não obstante as medidas descritas na Política de Segurança da Informação da Gestora, as seguintes medidas devem ser tomadas para fins de prevenção e proteção de dados:

(i) Os equipamentos e computadores disponibilizados aos Colaboradores devem ser utilizados com a finalidade de atender aos interesses comerciais legítimos da Gestora e sob nenhuma hipótese servirão de instrumento à discriminação em virtude de raça, religião, cor, origem, idade, sexo, incapacidade física e mental ou de qualquer outra forma não autorizada expressamente em lei.

(ii) A utilização de equipamentos é permitida para fins particulares relevantes, sendo expressamente proibida a divulgação de mensagens com conteúdo religioso, racial, pornográfico ou político no âmbito da Gestora.

(iii) A instalação de cópias de arquivos de qualquer extensão, obtido de forma gratuita ou remunerada, em computadores da Gestora, deverá observar os direitos de propriedade intelectual pertinentes, tais como *copyright*, licenças e patentes.

(iv) As mensagens enviadas ou recebidas através do correio eletrônico corporativo (*e-mails* corporativos), seus respectivos anexos, e a navegação através da rede mundial de computadores (*internet*) através de equipamentos da Gestora poderão ser monitoradas.

(v) Os *e-mails* corporativos recebidos pelos Colaboradores, quando abertos, deverão ter sua adequação às regras desta Política imediatamente verificada. Não será admitida, sob qualquer hipótese, a manutenção ou arquivamento de mensagens de conteúdo ofensivo, discriminatório, pornográfico ou vexatório, sendo a responsabilidade apurada de forma específica em relação ao destinatário da mensagem.

(vi) Nos equipamentos e computadores disponibilizados pela Gestora não é recomendado o uso de e-mails públicos (*webmails*) ou qualquer outro tipo de correio eletrônico que não seja o correio corporativo da Gestora.

4.5.2. Senhas

Senhas de caráter sigiloso, pessoal e intransferível serão fornecidas aos Colaboradores para acesso aos computadores, à rede corporativa e ao correio eletrônico corporativo. Em nenhuma hipótese as senhas deverão ser transmitidas a pessoas que não sejam Colaboradores, sendo os Colaboradores responsáveis pela manutenção de cada senha com suas características.

Observado o disposto na Política de Segurança da Informação, a senha e *login* para acesso aos dados contidos em todos os computadores, bem como nos e-mails, que também devem ser acessados via webmail, devem ser conhecidas pelo respectivo usuário de computador e são pessoais e intransferíveis, não devendo ser divulgados para quaisquer terceiros. O Colaborador poderá ser responsabilizado caso disponibilize a terceiros as senhas acima referidas para quaisquer fins.

É proibido o compartilhamento de *login* para funções de administração de sistemas.

Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel etc.) compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

Caso o Colaborador esqueça sua senha, ele deverá requisitar formalmente a troca, para que a equipe de T.I realize o cadastro de uma nova senha. Deverá ser estabelecido um processo para a renovação de senha. Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

A periodicidade máxima para troca das senhas é de **6 (seis) meses**, não podendo ser repetidas as últimas senhas. Os sistemas devem forçar a troca das senhas dentro desse prazo máximo. Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for demitido ou solicitar demissão, a área de recursos humanos deverá imediatamente comunicar tal fato à equipe de T.I, a fim de que essa providência seja tomada. Referida conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

Todo computador deverá exigir a inserção de senhas de acesso, sendo seu uso exclusivo de seu operador e controlado pela área de informática da Gestora. O controle de acesso à rede será atribuído conforme perfil do usuário. Isso permitirá que todas as movimentações por eles efetuadas sejam armazenadas no servidor da rede.

O supervisor da rede será o único autorizado a atribuir senhas de acesso para a rede. O acesso dos Colaboradores aos e-mails é interrompido automaticamente **a cada 6 (seis) meses** para novo login.

4.5.3. Monitoramento e Testes

Os mecanismos de supervisão se encontram descritos abaixo, de forma a verificar sua efetividade e identificar eventuais incidentes, detectar as ameaças em tempo hábil, reforçando os controles, caso necessário, e identificar possíveis anomalias no ambiente tecnológico, incluindo a presença de usuários, componentes ou dispositivos não autorizados.

O ambiente de TI da Gestora será monitorado, por meio de indicadores e geração de históricos: **(i)** do uso da capacidade instalada da rede e dos equipamentos; **(ii)** tempo de resposta no acesso à internet e aos sistemas críticos da Gestora; **(iii)** de períodos

de indisponibilidade no acesso à internet e aos sistemas críticos da Gestora; **(iv)** de incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante); e **(v)** das atividade de todos os Colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros).

Para garantir as regras mencionadas nesta Política, a Gestora deverá:

(i) Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede. A informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

(ii) Realizar, a qualquer tempo, inspeção física nas máquinas de hardware, se mantido servidor físico;

(iii) Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso; e

(iv) Testar a vulnerabilidade e penetração do website da Gestora, bem como de todo e qualquer sistema eletrônico desenvolvido internamente pela Gestora, a cada **24 (vinte e quatro) meses**.

Na realização dos testes e monitoramentos aqui referidos, arquivos pessoais salvos em cada computador ou equipamento da Gestora poderão ser acessados, caso o Comitê de Compliance e Risco julgue necessário. A confidencialidade dessas informações deve ser respeitada e seu conteúdo será divulgado somente se determinado por decisão judicial.

4.6. Resposta a Incidente de Cybersecurity

A Gestora deverá levar em consideração o plano de resposta a incidentes previstos no seu Plano de Continuidade de Negócios, considerando os cenários de ameaças lá previstos (que inclui falha de segurança cibernética grave) e os descritos abaixo para os demais casos.

Os Colaboradores poderão reportar incidentes diretamente ao Responsável pela Segurança Cibernética.

Uma vez que o Responsável pela Segurança Cibernética tenha sido acionado devido a um potencial incidente, este deverá observar os procedimentos descritos na Política de Segurança da Informação contida neste Manual, respeitadas as peculiaridades no processo de recuperação e retomada abaixo descrito:

4.6.1. Recuperação

Essa fase começa após o incidente inicial ter sido contornado, já tendo sido a redundância de TI acionada e terceiros-chave notificados. Será realizado um *call* ou uma reunião presencial, conforme o caso, em periodicidade a ser definida, para acompanhamento pela Diretora de Risco, Compliance e PLD/FTP, para estabelecer as medidas a serem tomadas, responsabilidades e prazos.

Também deverá ser avaliado o impacto do incidente nos diversos riscos (mercado, crédito, operacional, dentre outros) e, caso necessário, tomar as devidas ações, tais como manifestação pública na mídia, enquanto a Diretora de Risco, Compliance e PLD/FTP verificará se todas as informações necessárias ao portfólio gerido estão seguras. Quaisquer dados faltando ou corrompidos, ou problemas identificados por Colaboradores da Gestora, devem ser comunicados à Diretora de Risco, Compliance e PLD/FTP. Colaboradores externos relevantes deverão ser mantidos atualizados.

4.6.2. Retomada

Tal fase refere-se ao período de transição do retorno ao modo normal de operação e pode incluir a análise de projetos, reconstrução de eventuais sistemas e eventuais mudanças e medidas de prevenção. A Área de Compliance e Risco deverá registrar o histórico em local adequado.

4.7. Propriedade Intelectual

Todos os documentos e arquivos, incluindo, sem limitação, aqueles produzidos, modificados, adaptados ou obtidos pelos Colaboradores, relacionados, direta ou indiretamente, com suas atividades profissionais junto à Gestora, tais como minutas de contrato, memorandos, cartas, apresentações a clientes, e-mails, correspondências

eletrônicas, arquivos e sistemas computadorizados, planilhas, fórmulas, planos de ação, bem como modelos de avaliação, análise e gestão, em qualquer formato, são e permanecerão sendo propriedade exclusiva da Gestora, razão pela qual o Colaborador compromete-se a não utilizar tais documentos, no presente ou no futuro, para quaisquer fins que não o desempenho de suas atividades na Gestora, devendo todos os documentos permanecer em poder e sob a custódia da Gestora, sendo vedado ao Colaborador, inclusive, apropriar-se de quaisquer desses documentos e arquivos após seu desligamento da Gestora, salvo se autorizado expressamente pela Gestora e ressalvado o disposto abaixo.

Caso um Colaborador, ao ser admitido, disponibilize à Gestora documentos, planilhas, arquivos, fórmulas, modelos de avaliação, análise e gestão ou ferramentas similares para fins de desempenho de sua atividade profissional junto à Gestora, o Colaborador deverá assinar declaração nos termos do **Anexo V** da presente Política, confirmando que: (i) a utilização ou disponibilização de tais documentos e arquivos não infringe quaisquer contratos, acordos ou compromissos de confidencialidade, bem como não viola quaisquer direitos de propriedade intelectual de terceiros; e (ii) quaisquer alterações, adaptações, atualizações ou modificações, de qualquer forma ou espécie, em tais documentos e arquivos, serão de propriedade exclusiva da Gestora, sendo que o Colaborador não poderá apropriar-se ou fazer uso de tais documentos e arquivos alterados, adaptados, atualizados ou modificados após seu desligamento da Gestora, exceto se aprovado expressamente pela Gestora.

4.8. Atualização/Revisão e Conscientização de Cybersecurity

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

Também realizará campanha de conscientização em cibersegurança com o fim de garantir que todos os Colaboradores tenham as habilidades necessárias para proteger as informações como parte de suas responsabilidades, por meio do Programa de Treinamento previsto na Política de Treinamento da Gestora.

O Responsável pela Cybersecurity, em conjunto com a Área de Compliance e Risco, realizará a revisão e atualização desta Política a cada **12 (doze) meses**, ou em prazo inferior sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão da Diretora de Risco, Compliance e PLD/FTP.

5. POLÍTICAS DE TREINAMENTO

5.1. Treinamento e Atualização

A Gestora possui um processo de treinamento **inicial** de todos os seus Colaboradores, especialmente aqueles que tenham acesso à Informações Confidenciais ou participem de processos de decisão de investimento, em razão de ser fundamental que todos tenham sempre conhecimento atualizado dos seus princípios éticos, das leis e normas.

Assim que cada Colaborador for contratado, ele participará de um processo de treinamento em que irá adquirir conhecimento sobre as atividades da Gestora e terá oportunidade de esclarecer dúvidas relacionadas a tais princípios e normas.

Neste sentido, a Gestora adota um programa de atualização **anual** dos seus Colaboradores, à medida que as normas, princípios, conceitos e valores contidos neste Manual sejam atualizados, com o objetivo de fazer com que eles estejam sempre atualizados, estando todos obrigados a participar de tais programas de atualização.

5.2. Implementação e Conteúdo

A implementação do processo de treinamento inicial e do programa de atualização fica sob a responsabilidade da Área de Compliance e Risco e exige o comprometimento total dos Colaboradores quanto a sua assiduidade e dedicação.

Tanto o processo de treinamento inicial quanto o programa de atualização deverão abordar as atividades da Gestora, seus princípios éticos e de conduta, as normas de compliance, as políticas de segregação, quando for o caso, e as demais políticas descritas nesta Manual (especialmente aquelas relativas à confidencialidade, segurança das informações, segurança cibernética e conflitos de interesse), bem como aquelas descritas no Código de Ética e na Política de Investimentos Pessoais da Gestora e, ainda,

as penalidades aplicáveis aos Colaboradores decorrentes do descumprimento de tais regras, além das principais leis e normas aplicáveis às referidas atividades, constantes do **Anexo III** deste Manual.

A Diretora de Risco, Compliance e PLD/FTP poderá contratar profissionais especializados para conduzirem o treinamento inicial e programas de atualização, conforme as matérias a serem abordadas.

6. WEBSITE DA GESTORA

A Gestora deverá disponibilizar em seu website as Políticas exigidas pela Resolução CVM 21, bem como os seguintes documentos e informações relativos aos fundos sob gestão, conforme exigido pela regulamentação em vigor:

Documento ou Informação1	Base Legal
Regulamento anexos e apêndices atualizados	Art. 47, Parte Geral, Resolução CVM 175
Descrição da tributação aplicável ao Fundo e/ou Classe	Art. 47, Parte Geral, Resolução CVM 175
Política de Voto	Art. 47, Parte Geral, Resolução CVM 175
As informações periódicas e eventuais de cada Fundo e/ou Classe	Art. 61, Parte Geral, Resolução CVM 175
Fatos Relevantes	Art. 64, §2º, Parte Geral, Resolução CVM 175
Convocação da assembleia de cotistas geral do fundo de investimento e especial das classes e subclasses	Art. 72, Parte Geral da Resolução CVM 175
Identificação dos Prestadores de Serviço contratados	Art. 48, inciso I, Resolução CVM 175
Sumário Anbima (na hipótese de utilização de taxas globais no regulamento dos fundos)	Ofício-Circular nº 3/2024/CVM/SIN
Demonstração de desempenho dos Fundos de	Art. 13 do Anexo I (FIFs),

[1] Os seguintes documentos poderão ser, alternativamente, disponibilizados exclusivamente no site do administrador fiduciário, conforme alinhamento entre os Prestadores de Serviços Essenciais: demonstração de desempenho, lâmina, regulamentos, anexos e apêndices, descrição da tributação aplicável ao Fundo ou à Classe.

Investimento Financeiros	Resolução CVM 175
Lâmina dos Fundos de Investimento Financeiros]	Art. 13 do Anexo I (FIFs), Resolução CVM 175

7. POLÍTICA DE ANTICORRUPÇÃO

A Gestora está sujeita às leis e normas de anticorrupção, incluindo, mas não se limitando, à Lei nº 12.846/13 e Decreto nº 8.420/15 ("Normas de Anticorrupção").

Qualquer violação desta Política de Anticorrupção e das Normas de Anticorrupção pode resultar em penalidades civis e administrativas severas para a Gestora e/ou seus Colaboradores, bem como impactos de ordem reputacional, sem prejuízo de eventual responsabilidade criminal dos indivíduos envolvidos.

7.1. Abrangência das Normas de Anticorrupção

As Normas de Anticorrupção estabelecem que as pessoas jurídicas serão responsabilizadas objetivamente, nos âmbitos administrativo e civil, pelos atos lesivos praticados por seus sócios e colaboradores contra a administração pública, nacional ou estrangeira, sem prejuízo da responsabilidade individual do autor, coautor ou partícipe do ato ilícito, na medida de sua culpabilidade.

Considera-se agente público e, portanto, sujeito às Normas de Anticorrupção, sem limitação: (i) qualquer indivíduo que, mesmo que temporariamente e sem compensação, esteja a serviço, empregado ou mantendo uma função pública em entidade governamental, entidade controlada pelo governo, ou entidade de propriedade do governo; (ii) qualquer indivíduo que seja candidato ou esteja ocupando um cargo público; e (iii) qualquer partido político ou representante de partido político.

Considera-se administração pública estrangeira os órgãos e entidades estatais ou representações diplomáticas de país estrangeiro, de qualquer nível ou esfera de governo, bem como as pessoas jurídicas controladas, direta ou indiretamente, pelo poder público de país estrangeiro e as organizações públicas internacionais.

As mesmas exigências e restrições também se aplicam aos familiares de funcionários públicos até o segundo grau (cônjuges, filhos e enteados, pais, avós, irmãos, tios e

sobrinhos).

Representantes de fundos de pensão públicos, cartorários e assessores de funcionários públicos também devem ser considerados "agentes públicos" para os propósitos desta Política de Anticorrupção e das Normas de Anticorrupção.

7.2. Definições de Atos de Corrupção

Nos termos das Normas de Anticorrupção, constituem atos lesivos contra a administração pública, nacional ou estrangeira, todos aqueles que atentem contra o patrimônio público nacional ou estrangeiro, contra princípios da administração pública ou contra os compromissos internacionais assumidos pelo Brasil, assim definidos:

(i) prometer, oferecer ou dar, direta ou indiretamente, vantagem indevida a agente público, ou a terceira pessoa a ele relacionada;

(ii) comprovadamente, financiar, custear, patrocinar ou de qualquer modo subvencionar a prática dos atos ilícitos previstos nas Normas de Anticorrupção;

(iii) comprovadamente utilizar-se de interposta pessoa física ou jurídica para ocultar ou dissimular seus reais interesses ou a identidade dos beneficiários dos atos praticados;

(iv) no tocante a licitações e contratos:

(a) frustrar ou fraudar, mediante ajuste, combinação ou qualquer outro expediente, o caráter competitivo de procedimento licitatório público;

(b) impedir, perturbar ou fraudar a realização de qualquer ato de procedimento licitatório público;

(c) afastar ou procurar afastar licitante, por meio de fraude ou oferecimento de vantagem de qualquer tipo;

(d) fraudar licitação pública ou contrato dela decorrente;

(e) criar, de modo fraudulento ou irregular, pessoa jurídica para participar de licitação pública ou celebrar contrato administrativo;

(f) obter vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações de contratos celebrados com a administração pública, sem autorização em lei, no ato convocatório da licitação pública ou nos respectivos instrumentos contratuais; ou

(g) manipular ou fraudar o equilíbrio econômico-financeiro dos contratos celebrados

com a administração pública.

(h) dificultar atividade de investigação ou fiscalização de órgãos, entidades ou agentes públicos, ou intervir em sua atuação, inclusive no âmbito das agências reguladoras e dos órgãos de fiscalização do sistema financeiro nacional.

7.3. Conduta dos Colaboradores às Normas de Anticorrupção

É terminantemente proibido dar ou oferecer qualquer valor ou presente a agente público sem autorização prévia do Comitê de Compliance e Risco.

Os Colaboradores deverão se atentar, ainda, que (i) qualquer valor oferecido a agentes públicos, por menor que seja, poderá caracterizar violação às Normas de Anticorrupção e ensejar a aplicação das penalidades previstas; e (ii) a violação às Normas de Anticorrupção estará configurada mesmo que a oferta de suborno seja recusada pelo agente público.

Os Colaboradores deverão questionar a legitimidade de quaisquer pagamentos solicitados pelas autoridades ou funcionários públicos que não encontram previsão legal ou regulamentar.

Nenhum sócio ou colaborador poderá ser penalizado devido a atraso ou perda de negócios resultantes de sua recusa em pagar ou oferecer suborno a agentes públicos.

7.4. Proibição de Doações Eleitorais

A Gestora não fará, em hipótese alguma, doação a candidatos e/ou partidos políticos via pessoa jurídica. Em relação às doações individuais dos Colaboradores, a Gestora e seus Colaboradores têm a obrigação de seguir estritamente a legislação vigente.

7.5. Relacionamentos com Agentes Públicos

Quando se fizer necessária a realização de reuniões e audiências ("Audiências") com agentes públicos, sejam elas internas ou externas, a Gestora será representada por, ao menos, 2 (dois) Colaboradores, que deverão se certificar de empregar a cautela exigida para a ocasião, com o objetivo de resguardar a Gestora contra condutas ilícitas no

relacionamento com agentes públicos. Dentre os procedimentos adotados, os Colaboradores que estiverem representando a Gestora deverão elaborar relatórios de tais Audiências, e os apresentar à Diretora de Risco, Compliance e PLD/FTP imediatamente após sua ocorrência.

8. POLÍTICA DE CERTIFICAÇÃO

A Gestora observa as disposições das Regras e Procedimentos de Certificação Anbima, devendo garantir que todos os profissionais elegíveis estejam devidamente certificados.

8.1. Atividades Elegíveis e Critérios de Identificação

Tendo em vista a atuação da Gestora como gestora de recursos de terceiros para fundos líquidos e fundos de investimento em participação, foi identificado que a CGA e a CGE são as certificações pertinentes às suas atividades, aplicáveis aos profissionais com alçada/poder discricionário de investimento.

Nesse sentido e nos termos da legislação vigente, a Gestora definiu que apenas o Colaborador com poder final para ordenar a compra ou venda de posições, sem a necessidade de aprovação prévia do Diretor de Gestão, ou seja, o Colaborador que tenha, de fato, alçada/poder discricionário de investimentos, é elegível à CGA e CGE, a depender do Fundo gerido, uma vez que a CGA é a certificação aplicável aos profissionais que atuam em carteiras administradas, fundo de investimento financeiros, e/ou fundos de índice e a CGE é aplicável aos profissionais que atuam em fundo de investimento em participações, fundo de investimento em direitos creditórios e/ou fundo de investimento imobiliário.

Em complemento, a Gestora destaca que as certificações são de cunho pessoal e intransferíveis, observado que, a partir de 02 de janeiro de 2026, a Gestora deverá manter, no mínimo 2 (dois) profissionais certificados, conforme detalhado adiante.

As Regras e Procedimentos de Certificação Anbima determinam que as gestoras de recurso deverão manter em sua estrutura um Profissional Titular e, no mínimo, um Profissional Suplente com poder discricionário de investimento na atividade de Gestão de Recursos de Terceiros em caso de indisponibilidade transitória do Profissional Titular.

Portanto, a partir de 02 de janeiro de 2026, os Profissionais Titulares e Suplentes deverão integrar o quadro permanente de colaboradores da Gestora e atuar direta e regularmente na atividade de gestão de recursos de terceiros, sendo vedada a indicação de prestadores de serviços externos, excetuados os casos em que a prestação de serviços.

Desse modo, a Gestora assegurará que os Colaboradores que atuem nas atividades elegíveis participem do procedimento de atualização de suas respectivas certificações, de modo que a certificação obtida esteja devidamente atualizada dentro dos prazos estabelecidos neste Manual e nos termos previstos nas Regras e Procedimentos de Certificação.

8.2. Identificação de Profissionais Certificados e Atualização do Banco de Dados da Anbima

Antes da contratação, admissão ou transferência de área de qualquer Colaborador, a Diretora de Risco, Compliance e PLD/FTP deverá solicitar esclarecimentos ou confirmar junto ao supervisor direto do potencial Colaborador o cargo e as funções a serem desempenhadas, avaliando a necessidade de certificação, bem como verificar no Banco de Dados se o Colaborador possui alguma certificação Anbima, uma vez que, em caso positivo, a Gestora deverá inserir o Colaborador no Banco de Dados da Gestora.

O Diretor de Gestão deverá esclarecer à Diretora de Risco, Compliance e PLD/FTP se Colaboradores que integrarão o departamento técnico terão ou não alçada/poder discricionário de decisão de investimento.

Caso seja identificada a necessidade de certificação, a Diretora de Risco, Compliance e PLD/FTP deverá solicitar a comprovação da certificação pertinente ou sua isenção, se aplicável, anteriormente ao ingresso do novo Colaborador.

A Diretora de Risco, Compliance e PLD/FTP também deverá checar se os Colaboradores que estejam se desligando da Gestora estão indicados no Banco de Dados da Anbima como profissionais elegíveis/certificados vinculados à Gestora.

Todas as atualizações no Banco de Dados da ANBIMA devem ocorrer **até o último dia útil do mês subsequente à data do evento** que deu causa a atualização, nos termos do Art. 10, §1º, I das Regras e Procedimentos de Certificação Anbima, sendo que a manutenção das informações contidas no Banco de Dados deverá ser objeto de análise e confirmação pela Diretora de Risco, Compliance e PLD/FTP, conforme disposto abaixo.

8.3. Rotinas de Verificação

Mensalmente, a Diretora de Risco, Compliance e PLD/FTP deverá verificar as informações contidas no Banco de Dados da Anbima, a fim de garantir que todos os profissionais certificados/em processo de certificação, conforme aplicável, estejam devidamente identificados, bem como se as certificações estão dentro dos prazos de validade estabelecidos nas Regras e Procedimentos de Certificação Anbima.

Ainda, a Diretora de Risco, Compliance e PLD/FTP deverá, **trimestralmente**, contatar o Diretor de Gestão que deverá informá-lo se houve algum tipo de alteração nos cargos e funções dos Colaboradores que integram o departamento técnico envolvido na gestão de recursos, confirmando, ainda, todos aqueles Colaboradores que atuem com alçada/poder discricionário de investimento, se for o caso.

Colaboradores que não tenham CGA ou CGE, conforme aplicável (e que não tenham a isenção concedida pelo Conselho de Certificação), estão impedidos de ordenar a compra e venda de ativos sem a aprovação prévia do Diretor de Gestão, tendo em vista que não possuem alçada/poder final de decisão para tanto.

Ademais, no curso das atividades de compliance e fiscalização desempenhadas pela Diretora de Risco, Compliance e PLD/FTP, caso seja verificada qualquer irregularidade com as funções exercidas por Colaborador, incluindo, sem limitação, a tomada de decisões de investimento sem autorização prévia do Diretor de Gestão por profissionais não certificados ou, de maneira geral, que o Colaborador está atuando em atividade elegível sem a certificação pertinente ou com a certificação vencida, a Diretora de Risco, Compliance e PLD/FTP deverá declarar, de imediato, o afastamento do Colaborador, devendo tal diretor, ainda, apurar potenciais irregularidades e eventual responsabilização dos envolvidos, inclusive dos superiores do Colaborador, conforme aplicável, bem como para traçar um plano de adequação.

Sem prejuízo do disposto acima, **anualmente** deverão ser discutidos os procedimentos e rotinas de verificação para cumprimento do Código de Certificação, sendo que as análises e eventuais recomendações, se for o caso, deverão ser objeto do relatório anual de compliance.

Por fim, serão objeto do treinamento **anual** de compliance assuntos de certificação, incluindo, sem limitação: (i) treinamento direcionado a todos os Colaboradores, descrevendo as certificações aplicáveis à atividade da Gestora, suas principais características e os profissionais elegíveis; (ii) treinamento direcionado aos membros do departamento técnico envolvidos na atividade de gestão de recursos, reforçando que somente os Colaboradores com CGA e CGE podem ter alçada/poder discricionário de decisão de investimento em relação aos ativos integrantes das carteiras sob gestão da Gestora, devendo os demais buscar aprovação junto ao Diretor de Gestão; (iii) treinamento direcionado aos Colaboradores da Área de Compliance e de Risco, para que os mesmos tenham o conhecimento necessário para operar no Banco de Dados da Anbima e realizar as rotinas de verificação necessárias.

8.4. Atualização das Certificações

As certificações CGA e CGE, inclusive as obtidas antes de 02 de janeiro de 2026, possuem prazo de validade de 5 (cinco) anos.

Portanto, previamente ao vencimento das certificações, os Profissionais Elegíveis deverão participar do procedimento de atualização estabelecido pela Anbima, a fim de que a certificação obtida esteja devidamente atualizada dentro dos prazos estabelecidos.

Adicionalmente, [semestralmente / OU / anualmente], a Equipe de Compliance, Risco e PLD/FTP realizará a verificação da vigência das certificações dos Profissionais Elegíveis para cumprimento das Regras e Procedimentos de Certificação.

8.5. Processo de Afastamento

Todos os profissionais não certificados ou em processo de certificação, e para os quais

a certificação seja exigível, nos termos previstos neste Manual, serão, nos termos do art. 8º, §1ª, inciso V do Código ANBIMA de Certificação, imediatamente afastados das atividades elegíveis aplicáveis, até que se certifiquem.

Os profissionais já certificados, caso deixem de ser Colaboradores da Gestora, deverão assinar a documentação prevista no **Anexo IV** a este Manual denominado "Termo de Afastamento", comprovando o seu afastamento da Gestora. O mesmo procedimento de assinatura do **Anexo IV** aqui em referência, será aplicável, de forma imediata, aos profissionais não certificados ou em processo de certificação que forem afastados por qualquer dos motivos acima mencionados.

9. VIGÊNCIA E ATUALIZAÇÃO

Este Manual será revisado **anualmente**, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterado a qualquer tempo em razão de circunstâncias que demandem tal providência.

Histórico das atualizações		
Data	Versão	Responsável
10-2022	1ª	Diretor de Risco, Compliance e PLD/FTP
06-2023	2ª	Diretora de Risco, Compliance e PLD/FTP
05-2024	3ª	Diretora de Risco, Compliance e PLD/FTP
06-2025	4ª	Diretora de Risco, Compliance e PLD/FTP

ANEXO I - TERMO DE RECEBIMENTO E COMPROMISSO

Pelo presente Termo de Recebimento e Compromisso, [*nome do novo Colaborador, nacionalidade, estado civil, profissão, identidade, CPF, residência*] ("Aderente"), na qualidade de [cargo] da **TYTON CAPITAL INVESTIMENTOS.**, sociedade limitada com sede na Cidade e Estado de São Paulo , inscrita no CNPJ/MF sob o nº 46.503.558/0001-90, declara, se compromete e adere conforme abaixo:

(i) O Aderente declara, neste ato, ter recebido, lido e compreendido na sua integralidade o Manual de Regras, Procedimentos e Controles Internos, e as obrigações nele contidas aplicáveis a si próprio, conforme documento anexo a este Termo de Recebimento e Compromisso, que, rubricado pelo Aderente, é parte integrante do mesmo ("Manual").

(ii) O Aderente declara, neste ato, estar ciente de que o Manual como um todo passa a fazer parte dos seus deveres como Colaborador da Gestora, incorporando-se às demais regras internas adotadas pela Gestora.

(iii) O Aderente também declara, neste ato, que recebeu, leu e compreendeu todas as demais políticas da Gestora, bem como recebeu o treinamento de integração inicial, momento no qual lhe foi explicado todas as principais normas e regras da Gestora.

(iv) O Aderente está ciente de que poderá vir a responder perante a Gestora e seus Colaboradores por eventuais perdas e danos que causar em razão do descumprimento das regras constantes do Manual, e das demais políticas, mesmo após o seu desligamento da Gestora.

(v) Os termos utilizados neste Termo de Adesão, quando aqui não definidos, terão o significado constante do Manual.

(vi) O Aderente se declara ciente de que os termos do Manual, e das demais políticas, podem ser alterados ou excluídos a qualquer momento, independentemente da concordância de qualquer Colaborador, sendo certo que se ocorrer alteração ou exclusão, as mudanças serão divulgadas às partes afetadas por tais mudanças e não terão qualquer efeito retroativo.

(vii) O Aderente se declara ciente do seu compromisso de comunicar a Diretora de Risco, Compliance e PLD/FTP e/ou o Comitê de Compliance e Risco da Gestora acerca de qualquer situação que chegue ao seu conhecimento que esteja em desacordo com as regras definidas neste Manual.

(viii) O Aderente firma o presente Termo de Adesão de forma irrevogável e irretratável, em 2 (duas) vias, de igual teor e forma.

Declaro, por fim, estar ciente de que a apresentação de falsa declaração me sujeitará não somente às penalidades estabelecidas neste Manual, mas também às penalidades da Lei.

São Paulo, [*data*]

_____

[*Nome do Aderente*]

ANEXO II - TERMO DE CONFIDENCIALIDADE

Pelo presente Termo, eu, _____, inscrito no CPF/MF sob o nº _____ ("Colaborador"), na qualidade de [cargo] na **TYTON CAPITAL INVESTIMENTOS**, sociedade limitada com sede na Cidade e Estado de São Paulo , inscrita no CNPJ/MF sob o nº 46.503.558/0001-90 ("Gestora"), para fim de preservação de informações pessoais e profissionais dos clientes e da Gestora, firmo o presente termo de confidencialidade ("Termo"), que deve ser regido de acordo com as cláusulas que seguem:

1. São consideradas informações confidenciais, reservadas ou privilegiadas ("Informações Confidenciais"), para os fins deste Termo, independente destas informações estarem contidas em discos, disquetes, pen-drives, fitas, outros tipos de mídia ou em documentos físicos, ou serem escritas, verbais ou apresentadas de modo tangível ou intangível, qualquer informação sobre a Gestora, seus sócios e clientes, aqui também contemplados os próprios FUNDOS, incluindo:

(i) *Know-how,* técnicas, cópias, diagramas, modelos, amostras, programas de computador;

(ii) Informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes, dos clubes, fundos de investimento sob gestão da Gestora;

(iii) Operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os clubes, fundos de investimento sob gestão da Gestora;

(iv) Informações estratégicas ou mercadológicas e outras, de qualquer natureza, obtidas junto a sócios, sócios-diretores, funcionários, *trainees* ou estagiários da Gestora ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral, incluindo alterações societárias (fusões, cisões e incorporações), informações sobre compra e venda de empresas, títulos ou valores mobiliários, inclusive ofertas iniciais de ações (*IPO*), projetos e qualquer outro fato que seja de conhecimento em decorrência do âmbito de atuação da Gestora e que ainda não foi devidamente levado à público;

(v) Informações a respeito de resultados financeiros antes da publicação dos

balanços e balancetes dos fundos;

(vi) Transações realizadas e que ainda não tenham sido divulgadas publicamente; e

(vii) Outras informações obtidas junto a sócios, diretores, funcionários, *trainees* ou estagiários da Gestora ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.

2. O Colaborador compromete-se a utilizar as Informações Confidenciais a que venha a ter acesso estrita e exclusivamente para desempenho de suas atividades na Gestora, comprometendo-se, portanto, a não divulgar tais Informações Confidenciais para quaisquer fins, Colaboradores não autorizados, mídia, ou pessoas estranhas à Gestora, inclusive, nesse último caso, cônjuge, companheiro(a), ascendente, descendente, qualquer pessoa de relacionamento próximo ou dependente financeiro do Colaborador.

2.1. O Colaborador se obriga a, durante a vigência deste Termo e por prazo indeterminado após sua rescisão, manter absoluto sigilo pessoal e profissional das Informações Confidenciais a que teve acesso durante o seu período na Gestora, se comprometendo, ainda a não utilizar, praticar ou divulgar Informações Confidenciais, "*Insider Trading*", "Dicas" e "*Front Running*", seja atuando em benefício próprio, da Gestora ou de terceiros.

2.2. A não observância da confidencialidade e do sigilo, mesmo após o término da vigência deste Termo, estará sujeita à responsabilização nas esferas cível e criminal.

3. O Colaborador entende que a revelação não autorizada de qualquer Informação Confidencial pode acarretar prejuízos irreparáveis, ficando deste já o Colaborador obrigado a indenizar a Gestora, seus sócios e terceiros prejudicados, nos termos estabelecidos a seguir.

3.1. O descumprimento acima estabelecido será considerado ilícito civil e criminal, ensejando inclusive sua classificação como justa causa para efeitos de rescisão de contrato de trabalho, quando aplicável, nos termos do artigo 482 da Consolidação das Leis de Trabalho.

3.2. O Colaborador tem ciência de que terá a responsabilidade de provar que a informação divulgada indevidamente não se trata de Informação Confidencial.

4. O Colaborador reconhece e toma ciência que:

(i) Todos os documentos relacionados direta ou indiretamente com as Informações Confidenciais, inclusive contratos, minutas de contrato, cartas, fac-símiles, apresentações a clientes, e-mails e todo tipo de correspondências eletrônicas, arquivos e sistemas computadorizados, planilhas, planos de ação, modelos de avaliação, análise, gestão e memorandos por este elaborados ou obtidos em decorrência do desempenho de suas atividades na Gestora são e permanecerão sendo propriedade exclusiva da Gestora e de seus sócios, razão pela qual compromete-se a não utilizar tais documentos, no presente ou no futuro, para quaisquer fins que não o desempenho de suas atividades na Gestora, devendo todos os documentos permanecer em poder e sob a custódia da Gestora, salvo se em virtude de interesses da Gestora for necessário que o Colaborador mantenha guarda de tais documentos ou de suas cópias fora das instalações da Gestora;

(ii) Em caso de rescisão do contrato individual de trabalho, desligamento ou exclusão do Colaborador, o Colaborador deverá restituir imediatamente à Gestora todos os documentos e cópias que contenham Informações Confidenciais que estejam em seu poder;

(iii) Nos termos da Lei 9.609/98, a base de dados, sistemas computadorizados desenvolvidos internamente, modelos computadorizados de análise, avaliação e gestão de qualquer natureza, bem como arquivos eletrônicos, são de propriedade exclusiva da Gestora, sendo terminantemente proibida sua reprodução total ou parcial, por qualquer meio ou processo; sua tradução, adaptação, reordenação ou qualquer outra modificação; a distribuição do original ou cópias da base de dados ou a sua comunicação ao público; a reprodução, a distribuição ou comunicação ao público de informações parciais, dos resultados das operações relacionadas à base de dados ou, ainda, a disseminação de boatos, ficando sujeito, em caso de infração, às penalidades dispostas na referida lei.

5. Ocorrendo a hipótese do Colaborador ser requisitado por autoridades brasileiras ou estrangeiras (em perguntas orais, interrogatórios, pedidos de informação ou documentos, notificações, citações ou intimações, e investigações de qualquer

natureza) a divulgar qualquer Informação Confidencial a que teve acesso, o Colaborador deverá notificar imediatamente a Gestora, permitindo que a Gestora procure a medida judicial cabível para atender ou evitar a revelação.

5.1. Caso a Gestora não consiga a ordem judicial para impedir a revelação das informações em tempo hábil, o Colaborador poderá fornecer a Informação Confidencial solicitada pela autoridade. Nesse caso, o fornecimento da Informação Confidencial solicitada deverá restringir-se exclusivamente àquela que o Colaborador esteja obrigado a divulgar.

5.2. A obrigação de notificar a Gestora subsiste mesmo depois de rescindido o contrato individual de trabalho, ao desligamento ou exclusão do Colaborador, por prazo indeterminado.

6. Este Termo é parte integrante das regras que regem a relação contratual e/ou societária do Colaborador com a Gestora, que ao assiná-lo está aceitando expressamente os termos e condições aqui estabelecidos.

7. A transgressão a qualquer das regras descritas neste Termo, sem prejuízo do disposto no item 3 e seguintes acima, será considerada infração contratual, sujeitando o Colaborador às sanções que lhe forem atribuídas pelos sócios da Gestora.

Assim, estando de acordo com as condições acima mencionadas, assina o presente.

[local], [data].

_____

[COLABORADOR]

ANEXO III - NORMATIVOS APLICÁVEIS

1. Resolução CVM Nº 50/21
2. Resolução CVM nº 175
3. Resolução CVM Nº 21/21
4.
5. Ofício-Circular/CVM/SIN/Nº 05/2014
6. Código ANBIMA de Administração e Gestão de Recursos de Terceiros
7. Regras e Procedimentos de Certificação Anbima
8. Código ANBIMA de Ética
9. Lei 9.613 de 03 de março de 1998, conforme alterada
10. Lei nº 12.846, de 1º de agosto de 2013 e Decreto nº 11.129, de 11 de julho de 2022, conforme alterada ("Normas de Anticorrupção").

ANEXO IV - TERMO DE AFASTAMENTO

Por meio deste instrumento, eu, _____, inscrito(a) no CPF/MF sob o nº _____, declaro para os devidos fins que, a partir desta data, estou afastado das atividades de gestão de recursos de terceiros da **TYTON CAPITAL INVESTIMENTOS**, inscrita no CNPJ/MF sob o nº. 46.503.558/0001-90 ("Gestora") por prazo indeterminado:

[ ] até que me certifique pela CGA e/ou CGE; ou

[ ] até que o Conselho de Certificação me conceda a isenção de obtenção da CGA e/ou CGE.

[ ] tendo em vista que não sou mais Colaborador da Gestora;

São Paulo, [•] de [•] de [•].

_____

[COLABORADOR]

_____

TYTON CAPITAL INVESTIMENTOS

Testemunhas:

1._____ 2._____

Nome: Nome:

CPF/MF: CPF/MF:

ANEXO V - TERMO DE PROPRIEDADE INTELECTUAL

Por meio deste instrumento eu, _____, inscrito no CPF/MF sob o nº _____ ("Colaborador"), DECLARO para os devidos fins:

(i) que a disponibilização pelo Colaborador à **TYTON CAPITAL INVESTIMENTOS** ("GESTORA"), nesta data, dos documentos contidos no *pen drive* da marca [•], número de série [•] ("Documentos"), bem como sua futura utilização pela Gestora, não infringe quaisquer contratos, acordos ou compromissos de confidencialidade que o Colaborador tenha firmado ou que seja de seu conhecimento, bem como não viola quaisquer direitos de propriedade intelectual de terceiros;

(ii) ciência e concordância de que quaisquer alterações, adaptações, atualizações ou modificações, de qualquer forma ou espécie, nos Documentos, serão de propriedade exclusiva da Gestora, sendo que o Colaborador não poderá apropriar-se ou fazer uso de tais documentos e arquivos alterados, adaptados, atualizados ou modificados após seu desligamento da Gestora, exceto se aprovado expressamente pela Gestora.

Para os devidos fins, o Colaborador atesta que os Documentos foram duplicados no pen drive da marca [•], número de série [•], que ficará com a Gestora e cujo conteúdo é idêntico ao *pen drive* disponibilizado pelo Colaborador.

Os *pen drives* fazem parte integrante do presente termo, para todos os fins e efeitos de direito. A lista de arquivos constantes dos *pen drives* se encontra no Apêndice ao presente termo.

[•], [•] de [•] de [•].

_____

[COLABORADOR]