**PIEMONTE CAPITAL GESTORA DE RECURSOS LTDA.**
**(“PIEMONTE CAPITAL”)**

# MANUAL DE REGRAS, PROCEDIMENTOS E CONTROLES INTERNOS

**agosto/2024**

R. Lauro Muller, 116 - sala 4103
Botafogo, Rio de Janeiro RJ
CEP 22290 160 – Brasil

**PIEMONTECAPITAL.COM.BR**

**ÍNDICE**

**I. POLÍTICA DE COMPLIANCE** ..... 4
1.1. Introdução ..... 4
1.2. Aplicabilidade do Manual ..... 4
1.3. Ambiente Regulatório ..... 4
1.4. Responsabilidades e Obrigações ..... 5
1.5. Garantia de Independência ..... 8
1.6. Dúvidas ou ações contrárias aos princípios e normas do Manual ..... 8
1.7. Acompanhamento das Políticas descritas neste Manual ..... 9
1.8. Sanções ("*Enforcement*") ..... 10
1.9. Dever de Reportar ..... 10
1.10. Novos Negócios / Produtos ..... 10
1.11. PLD/FTP ..... 11
1.12. Planos de Contingência ..... 11
**II. POLÍTICAS DE CONFIDENCIALIDADE** ..... 11
2.1. Sigilo e Conduta ..... 11
2.2. Dever de Reportar ..... 14
2.3. *Insider Trading, "Dicas" e Front-running* ..... 14
**III. POLÍTICAS DE TREINAMENTO** ..... 16
3.1. Treinamento e Processo de Reciclagem ..... 16
3.2. Implementação e Conteúdo ..... 17
**IV. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA** ..... 17
4.1. Introdução ..... 17
4.2. Identificação de Riscos (*risk assessment*) ..... 18
4.3. Ações de Prevenção e Proteção ..... 19
4.4. Monitoramento e Testes ..... 23
4.5. Plano de Identificação e Resposta ..... 23
4.6. Arquivamento de Informações ..... 25
4.7. Propriedade Intelectual ..... 25
4.8. Treinamento ..... 25
4.9. Revisão da Política ..... 26
**V. POLÍTICA DE SUSTENTABILIDADE** ..... 26
**VI. POLÍTICA DE CERTIFICAÇÃO** ..... 26
6.1. Introdução ..... 26
6.2. Atividades Elegíveis e Critérios de Identificação ..... 26
6.3. Identificação de Profissionais Certificados e Atualização do Banco de Dados da ANBIMA ..... 27

6.4. Rotinas de Verificação ..... 28
6.5. Processo de Afastamento ..... 29
**VII. VIGÊNCIA E ATUALIZAÇÃO** ..... 29
**ANEXO I** ..... 30
**ANEXO II** ..... 31
**ANEXO III** ..... 36
**ANEXO IV** ..... 38

# I. POLÍTICA DE COMPLIANCE

## 1.1. Introdução

Este Manual de Regras, Procedimentos e Controles Internos ("Manual") da **PIEMONTE CAPITAL GESTORA DE RECURSOS LTDA.** ("Gestora"), foi elaborado em conformidade com o disposto na Resolução da Comissão de Valores Mobiliários ("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 ("Resolução CVM 50"), demais orientações da CVM, Código da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais ("ANBIMA") de Ética ("Código ANBIMA de Ética"), no Código ANBIMA de Administração e Gestão de Recursos de Terceiros ("Código ANBIMA de AGRT"), no Código ANBIMA de Regulação e Melhores Práticas para o Programa de Certificação Continuada ("Código ANBIMA de Certificação"), bem como a Lei nº 12.846, de 1º de agosto de 2013, a Lei nº 12.683, de 9 de julho de 2012, a Lei nº 9.613, de 3 de março de 1998, e demais leis e diretrizes internacionais de anticorrupção e prevenção à lavagem de dinheiro, tais como: *Foreign Corrupt Practices Act (FCPA)*, Organização para a Cooperação e Desenvolvimento Econômico (OCDE), *Global Pact* (ONU), *UK Bribery Act*, entre outras, e tem por objetivo estabelecer as 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") na Gestora.

O presente Manual, em conjunto com o Código de Ética e demais políticas, constitui o instrumento formal para definição de princípios, diretrizes e regras a serem observadas na concepção, implantação e manutenção de estratégias, processos e normativos sobre regras, procedimentos e controles internos da Gestora (*compliance*).

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

A Gestora mantém versões atualizadas de suas Políticas no website (http://www.piemontecapital.com.br).

## 1.2. Aplicabilidade do Manual

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

## 1.3. Ambiente Regulatório

Este Manual é parte integrante das regras que regem a relação societária ou de trabalho dos Colaboradores, que, ao receberem o presente Manual, concordam expressamente com as normas, princípios, conceitos e valores aqui estabelecidos. Os colaboradores deverão assinar o termo de recebimento e compromisso constante do **Anexo I** a este Manual ("Termo de Adesão ao Manual de Regras, Procedimentos e Controles Internos"), aceitando expressamente as normas, princípios, conceitos e valores aqui estabelecidos.

Diante de atualizações neste Manual que alterem substancialmente o seu conteúdo, os Colaboradores deverão confirmar, por meio da assinatura de um novo Termo de Adesão ao Manual de Regras, Procedimentos e Controles Internos, a concordância com os novos termos deste Manual.

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.

É compromisso de todo Colaborador informar o Diretor de Compliance, Risco e PLD/FTP sobre violações ou possíveis violações dos princípios e normas aqui elencados, de maneira a preservar os interesses dos clientes da Gestora, bem como zelar pela reputação da Gestora. Caso a violação ou suspeita de violação recaia sobre o próprio Diretor de Compliance, Risco e PLD/FTP, o Colaborador deverá informar diretamente aos demais administradores da Gestora.

### 1.4. Responsabilidades e Obrigações

A coordenação direta das atividades relacionadas a este Manual é uma atribuição do diretor estatutário da Gestora indicado como diretor responsável pelo cumprimento de regras, políticas, procedimentos e controles internos da Gestora ("Diretor de Compliance, Risco e PLD/FTP"), nos termos da Resolução CVM nº 21.

São obrigações do Diretor de Compliance, Risco e PLD/FTP:

**(i)** Cumprir e garantir que os demais Colaboradores da Gestora cumpram o disposto nas políticas descritas neste Manual;

**(ii)** Identificar e monitorar condutas que possam violar o disposto neste Manual;

**(iii)** Garantir o permanente atendimento às normas, políticas e regulamentações vigentes, referentes às diversas modalidades de investimento, à própria atividade de administração de carteira de valores mobiliários e aos padrões ético e profissional;

**(iv)** Manter todos os Colaboradores atualizados acerca da regulamentação aplicável vigente e zelar pelo seu cumprimento;

**(v)** 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 dos administradores da Gestora;

**(vi)** 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;

**(vii)** 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;

**(viii)** 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 da Gestora;

**(ix)** 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;

**(x)** 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;

**(xi)** 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;

**(xii)** 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;

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

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

**(xv)** Aplicar as eventuais sanções aos Colaboradores, conforme definido pelo Diretor de Compliance, Risco e PLD/FTP; e

**(xvi)** Analisar 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:

**a)** Investimentos pessoais;

**b)** Transações financeiras com clientes fora do âmbito da Gestora;

**c)** Recebimento de favores/presentes de administradores e/ou sócios de companhias investidas, fornecedores ou clientes;

**d)** Análise financeira ou operação com empresas cujos sócios, administradores ou funcionários, o Colaborador possua alguma relação pessoal;

**e)** Análise financeira ou operação com empresas em que o Colaborador possua investimento próprio; ou

**f)** Participações em alguma atividade política.

**(xvii)** Assuntos de Certificação, tratados na Política de Certificação, incluindo, sem limitação: (i) as certificações aplicáveis à atividade da Gestora, suas principais características e os profissionais elegíveis; (ii) explicação de que os Colaboradores que tenham alçada/poder discricionário de decisão de investimento em fundo de investimento em participações, fundos imobiliários, fundos de investimento em direitos creditórios e/ou fundos de índice sob gestão da Gestora, devem, obrigatoriamente, ser isentos ou aprovados na Certificação de Gestores ANBIMA para Fundos Estruturados ("CGE"), devendo os demais buscar a aprovação da decisão de investimento junto ao Diretor de Gestão; e (iii) indicação sobre a necessidade de monitoramento e atualização do Banco de Dados da ANBIMA pela Área de Compliance e Risco.

Todo e qualquer Colaborador 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 neste Manual, deverá informar o Diretor de Compliance, Risco e PLD/FTP, para que sejam tomadas as providências cabíveis.

O Diretor de Compliance, Risco e PLD/FTP poderá contar, ainda, com outros Colaboradores para as atividades e rotinas de compliance e de risco, com as atribuições a serem definidas caso a caso, a depender da necessidade da Gestora em razão de seu crescimento e de acordo com a senioridade do Colaborador.

**1.5. Garantia de Independência**

Os Colaboradores que desempenharem as atividades de risco, *compliance* e de prevenção à lavagem de dinheiro, financiamento ao terrorismo e financiamento de proliferação de armas de destruição em massa, formarão a Área de Compliance e Risco, sob a coordenação do Diretor de Compliance, Risco e PLD/FTP, observado que a Área de Compliance e Risco exerce suas atividades de forma completamente independente e segregada das outras áreas da Gestora e poderá exercer seus poderes e autoridade com relação a qualquer Colaborador.

**1.6. 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 ao Diretor de Compliance, Risco e PLD/FTP, 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 do Diretor de Compliance, Risco e PLD/FTP, 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, ao Diretor de Compliance, Risco e PLD/FTP, exclusivamente por meio de e-mail.

## 1.7. Acompanhamento das Políticas descritas neste Manual

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 do Diretor de Compliance, Risco e PLD/FTP, de acordo com os procedimentos estabelecidos neste Manual, o Diretor de Compliance, Risco e PLD/FTP utilizará os registros e sistemas de monitoramento eletrônico referidos neste Manual para verificar a conduta dos Colaboradores envolvidos.

Todo conteúdo que está na rede da Gestora poderá ser acessado pelo Diretor de Compliance, Risco e PLD/FTP, caso seja necessário para a apuração das possíveis violações ao disposto neste Manual, inclusive arquivos pessoais salvos em cada computador serão acessados caso o Diretor de Compliance, Risco e PLD/FTP julgue necessário. Da mesma forma, mensagens de correio eletrônico de Colaboradores serão gravadas e, quando necessário, interceptadas e escutadas, observando-se os direitos garantidos pela regulamentação em vigor, sem que isto represente invasão da privacidade dos Colaboradores já que se trata de ferramentas de trabalho disponibilizadas pela Gestora.

O Diretor de Compliance, Risco e PLD/FTP realizará um monitoramento **anual**, sobre uma amostragem significativa dos Colaboradores, escolhida aleatoriamente pelo Diretor de Compliance, Risco 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 Gestora realizará inspeções com periodicidade **anual**, a cargo do Diretor de Compliance, Risco e PLD/FTP, com base em sistemas de monitoramento eletrônico, independentemente da ocorrência de descumprimento ou suspeita ou indício de descumprimento de quaisquer das regras estabelecidas neste Manual ou aplicáveis às atividades da Gestora, sendo tal inspeção realizada de forma aleatória.

Adicionalmente, o Diretor de Compliance, Risco e PLD/FTP deverá ainda verificar **anualmente** 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, o Diretor de Compliance, Risco e PLD/FTP poderá, quando julgar oportuno e necessário, realizar inspeções, nas ferramentas de trabalho, a qualquer momento sobre quaisquer Colaboradores.

O Diretor de Compliance, Risco e PLD/FTP poderá utilizar as informações obtidas e nos monitoramentos descritos acima para decidir sobre 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 e para os devidos fins legais ou em atendimento a determinações judiciais.

**1.8. Sanções ("*Enforcement*")**

A eventual aplicação de sanções decorrentes do descumprimento dos princípios estabelecidos neste Manual é de responsabilidade do Diretor de Compliance, Risco e PLD/FTP, garantido ao Colaborador, contudo, amplo direito de defesa. Podem ser aplicadas, entre outras, penas de advertência, suspensão, desligamento ou exclusão por justa causa, no caso de Colaboradores que sejam sócios da Gestora, ou demissão por justa causa, no caso de Colaboradores que sejam empregados da Gestora, nesse último caso, nos termos do artigo 482 da Consolidação das Leis do Trabalho – CLT, sem prejuízos do direito da Gestora de pleitear indenização pelos eventuais prejuízos suportados, perdas e danos e/ou lucros cessantes, por meio das medidas legais cabíveis.

A Gestora não assume a responsabilidade de Colaboradores que transgridam a lei ou cometam infrações no exercício de suas funções. Caso a Gestora venha a ser responsabilizada ou sofra prejuízo de qualquer natureza por atos de seus Colaboradores, pode exercer o direito de regresso em face dos responsáveis.

**1.9. Dever de Reportar**

O Colaborador que tiver conhecimento ou suspeita de ato não compatível com os dispositivos deste Manual deverá reportar, imediatamente, tal acontecimento ao Diretor de Compliance, Risco e PLD/FTP. Nenhum Colaborador sofrerá retaliação por comunicar, de boa-fé, violações ou potenciais violações a este Manual. Além disso, todos os comunicados e investigações serão tratados de maneira confidencial, na medida do possível nestas circunstâncias. Contudo, o Colaborador que se omitir de tal obrigação poderá sofrer além de ação disciplinar, demissão por justa causa, conforme regime jurídico.

Caso a violação ou suspeita de violação recaia sobre o próprio Diretor de Compliance, Risco e PLD/FTP, o Colaborador deverá informar diretamente aos demais administradores da Gestora.

**1.10. Novos Negócios / Produtos**

Quando estiver envolvido no desenvolvimento de um novo negócio e/ou produto para a Gestora, os Colaboradores devem procurar *a* Área de Compliance e Risco para ter

certeza de que todos os riscos, inclusive os legais, regulamentares e reputacionais, foram devidamente avaliados.

### 1.11. PLD/FTP

As regras e procedimentos relacionadas à prevenção ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa e combate à corrupção estão previstas na Política de PLD/FTP da Gestora.

### 1.12. Planos de Contingência

A Gestora possui um Plano de Contingência e Continuidade de Negócios em documento específico, onde define um guia de como montar e manter um planejamento que permita à Gestora a manutenção de seus serviços críticos durante uma interrupção de negócios não planejada.

O Plano de Contingência e Continuidade de Negócios é elaborado e revisado pelo Diretor de Compliance, Risco e PLD/FTP da Gestora em conjunto com os profissionais responsáveis pela Segurança da Informação e conta com a participação de todos os envolvidos nas atividades operacionais da Gestora.

O Plano de Contingência e Continuidade de Negócios será revisado **anualmente** ou sempre que novos acontecimentos motivem sua alteração.

## II. POLÍTICAS DE CONFIDENCIALIDADE

### 2.1. Sigilo e Conduta

A Gestora valoriza o compromisso com seus clientes e contrapartes de manter a confidencialidade das informações recebidas. Para tanto, Gestora elaborou esta política de confidencialidade para estabelecer os princípios e regras aos quais os Colaboradores devem observar no exercício de suas atividades, além de identificar os detentores de informações privilegiadas em função de seu cargo ou atribuição, de forma a estabelecer uma barreira de informações com os demais Colaboradores.

As disposições do presente Capítulo se aplicam aos Colaboradores que, por meio de suas funções na Gestora, possam ter ou vir a ter acesso a informações confidenciais, reservadas ou privilegiadas de natureza financeira, técnica, comercial, estratégica, negocial ou econômica, dentre outras.

Todos os Colaboradores deverão ler atentamente e entender o disposto neste Manual, bem como deverão firmar o acordo de confidencialidade, conforme modelo constante no **Anexo II** ("Acordo de Confidencialidade").

Conforme disposto no Acordo de 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.

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)** Informações relacionadas aos clientes, Colaboradores, terceiros e contrapartes da Gestora;

**(iv)** Operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento e carteiras geridas pela Gestora;

**(v)** Estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços;

**(vi)** 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;

**(vii)** Informações a respeito de resultados financeiros antes da publicação dos balanços, balancetes e/ou demonstrações financeiras dos fundos de investimento;

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

**(ix)** Outras informações 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.

Apesar das atividades da Gestora e seu modelo de negócio exigirem o fluxo de informações entre determinadas áreas, dentro dos limites regulatórios, estas devem ser tratadas com cautela e não devem ser divulgadas a quem não tenha o dever profissional de conhecê-las, sendo vedada a transmissão de informações confidenciais a Colaboradores não autorizados ou terceiros, não só durante a vigência de seu relacionamento profissional com a Gestora, mas também após o seu término.

Todos e quaisquer arquivos referentes às áreas da Gestora deverão ser salvos nos diretórios da respectiva área, os quais somente poderão ser acessados pelos Colaboradores que possuírem a devida autorização para tal acesso. A habilitação dos Colaboradores aos diretórios de rede ocorrerá mediante determinação e aprovação da Área de Compliance e Risco.

Quaisquer dados dos clientes (e.g., nome, CPF, documento, foto, finanças, comportamento de gastos, investimentos) são estritamente confidenciais, portanto, os Colaboradores não devem acessá-los para qualquer outro motivo/finalidade que não o exercício normal/rotineiro das atividades de gestão da Gestora.

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.

Adicionalmente, os Colaboradores devem ser extremamente cautelosos ao discutirem assuntos que envolvam informações confidenciais por e-mail, telefone, outros meios de comunicação ou em locais públicos, de modo a mitigarem o risco de propagação de Informações Confidenciais.

Se algum Colaborador ou equipe possuir informações que não possam ser compartilhadas nem com outras equipes em razão da existência de conflitos de interesses ou determinação regulatória, poderão ser levantadas barreiras à informação, inclusive físicas (*ethical wall*).

Os Colaboradores não deverão, em qualquer hipótese, deixar em suas respectivas estações de trabalho ou em outro espaço físico de livre circulação da Gestora qualquer documento que contenha Informações Confidenciais durante a ausência do respectivo usuário, principalmente após o encerramento do expediente. Ademais, após a utilização

do respectivo documento que contenha Informação Confidencial, o Colaborador deverá destruí-lo, ou arquivá-lo.

Além disso, o contrato de trabalho assinado por cada Colaborador possui uma cláusula que proíbe a divulgação de informações que receber em virtude do exercício de suas funções.

### 2.2. Dever de Reportar

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 ao Diretor de Compliance, Risco e PLD/FTP, para que este decida sobre a forma mais adequada para tal revelação, após exaurirem todas as medidas jurídicas apropriadas para evitar a supramencionada revelação.

Caso os Colaboradores tenham acesso, por qualquer meio, a Informação Confidencial, deverão levar tal circunstância ao imediato conhecimento do Diretor de Compliance, Risco 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 ao Diretor de Compliance, Risco e PLD/FTP.

### 2.3. *Insider Trading, "Dicas" e Front-running*

A legislação brasileira proíbe tanto a Gestora quanto os Colaboradores de negociarem títulos e valores mobiliários, incluindo ações, títulos de dívida e instrumentos derivados, com base em Informações Privilegiadas ou "informações materiais que não sejam públicas", tais como:

**(i)** certas operações, tais como controle societário comum e/ou compartilhado, refinanciamentos, ofertas públicas de aquisição, recapitalizações, *leveraged buy-outs*, aquisições, fusões, reestruturações e/ou compras ou vendas de ativos;

**(ii)** aumentos ou diminuições de dividendos;

**(iii)** lucros ou ganhos estimados, variações nos lucros lançadas anteriormente ou estimativas de ganhos;

**(iv)** as ofertas públicas de valores mobiliários por entidades privadas ou públicas, incluindo planos de oferecer valores mobiliários, cancelamentos de ofertas planejadas e as mudanças no tempo ou termos de ofertas públicas;

**(v)** operações por um emitente relativas aos seus próprios títulos, incluindo os programas de recompra de ações e derivativos;

**(vi)** as baixas contábeis de ativos;

**(vii)** ampliação ou redução de operações;

**(viii)** novos produtos, descobertas e invenções;

**(ix)** captações e encargos para as reservas destinada a devedores duvidosos;

**(x)** contencioso e provisões;

**(xi)** problemas de liquidez;

**(xii)** financiamentos e alterações de avaliações de títulos de dívida;

**(xiii)** fiscalizações governamentais; e

**(xiv)** outros eventos que afetam os mercados de valores mobiliários ou um determinado setor de forma significativa.

Esta lista não é exaustiva e pode haver outros tipos de informação, eventos ou circunstâncias que constituam informações confidenciais e materiais não-públicas.

Sendo assim, em nenhuma hipótese as Informações Confidenciais poderão ser utilizadas para a prática de atos que configurem:

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

**(ii)** "Dica", ou seja, 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; e/ou

**(iii)** *Front-running*, ou seja, a prática que envolve aproveitar alguma Informação Confidencial para realizar ou concluir uma operação antes de outros.

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

**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.**

## III. POLÍTICAS DE TREINAMENTO

### 3.1. Treinamento e Processo de Reciclagem

A Gestora possui um processo de treinamento **inicial** de todos os seus Colaboradores, 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.

Após o treinamento inicial e cada treinamento de reciclagem o Colaborador deverá assinar o Termo de Participação em Programa de Treinamento, conforme modelo previsto no **Anexo V** do presente Manual.

Nesse sentido, a Gestora adota um programa de reciclagem **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 reciclagem. Os treinamentos devem abordar:

**(i)** As atividades da Gestora;

**(ii)** Os princípios éticos e de conduta da Gestora;

**(iii)** As normas de compliance da Gestora;

**(iv)** As Políticas de Segregação, quando for o caso;

**(v)** As demais Políticas descritas neste Manual, especialmente, aquelas relativas à Confidencialidade, Segurança das Informações e Segurança Cibernética, bem como aquelas descritas no Código de Ética, na Política de Investimentos Pessoais e na Política de PLD/FTP; e

**(vi)** As penalidades aplicáveis aos Colaboradores decorrentes do descumprimento das regras da Gestora.

### 3.2. Implementação e Conteúdo

A implementação do processo de treinamento inicial e do programa de reciclagem continuada fica sob a responsabilidade do Diretor de Compliance, Risco e PLD/FTP e exige o comprometimento total dos Colaboradores quanto a sua assiduidade e dedicação.

Tanto o processo de treinamento inicial quanto o programa de reciclagem 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 neste Manual (especialmente aquelas relativas à confidencialidade, segurança das informações e segurança cibernética),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.

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

## IV. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

### 4.1. Introdução

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.

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.

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 de segurança da informação e segurança cibernética 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 Área de Compliance e Risco, que será o responsável inclusive por sua revisão, realização de testes e treinamento dos Colaboradores, conforme aqui descrito.

### 4.2. Identificação de Riscos (*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.

Ademais, no que se refere especificamente à segurança cibernética, a Gestora identificou as seguintes principais ameaças, nos termos inclusive do Guia de Cibersegurança da ANBIMA:

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

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

**(iii)** Ataques de DDoS (*distributed denial of services*) e *botnets*: ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição;

**(iv)** 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 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.

### 4.3. Ações de Prevenção e Proteção

Após a identificação dos riscos, a Gestora adota as medidas a seguir descritas para proteger suas informações e sistemas.

**(i)** Regra Geral de Conduta:

A Gestora realiza efetivo controle do acesso a arquivos que contemplem Informações Confidenciais em meio físico, disponibilizando-os somente aos Colaboradores que efetivamente estejam evolvidos no projeto que demanda o seu conhecimento e análise.

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

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

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.

Neste sentido, 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.

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 também mantém arquivo físico centralizado, em especial para guarda e armazenamento de documentos societários da Gestora. Adicionalmente, cada Colaborador é o responsável pela boa conservação, integridade e segurança de quaisquer Informações Confidenciais que estejam em meio físico sob a sua guarda.

O descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. Os documentos físicos que contenham informações confidenciais ou de suas cópias deverão ser triturados e descartados imediatamente após seu uso de maneira a evitar sua recuperação ou leitura.

Em consonância com as normas internas acima, 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.

O envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é também terminantemente proibido, bem como o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam difamar a imagem e afetar a reputação da Gestora.

O recebimento de e-mails muitas vezes não depende do próprio Colaborador, mas espera-se bom senso de todos para, se possível, evitar receber mensagens com as características descritas previamente. Na eventualidade do recebimento de mensagens com as características acima descritas, o Colaborador deve apagá-las imediatamente, de modo que estas permaneçam o menor tempo possível nos computadores da Gestora.

A visualização de *sites*, *blogs*, *fotologs*, *webmails*, entre outros, que contenham conteúdo discriminatório, preconceituoso (sobre origem, etnia, religião, classe social, opinião política, idade, sexo, orientação sexual ou deficiência física), obsceno, pornográfico ou ofensivo é terminantemente proibida.

**(ii)** Acesso Escalonado do Sistema

O acesso como "administrador" de área de *desktop* é limitado aos usuários aprovados pelo Diretor de Compliance, Risco e PLD/FTP e, com isso, serão determinados privilégios/credenciais e níveis de acesso de usuários apropriados para os Colaboradores.

A Gestora mantém diferentes níveis de acesso a pastas e arquivos eletrônicos de acordo com as funções e senioridade dos Colaboradores. As combinações de *login* e senha são utilizadas para autenticar as pessoas autorizadas e conferir acesso à parte da 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

**(iii)** Senha e Login

Todo ativo ou informação classificado como confidencial ou restrito deve ser protegido por mecanismos de controle de acesso para prevenir que seja indevidamente divulgado, modificado, deletado ou danificado. Os mecanismos de controle de acesso em uso devem manter trilhas de auditoria (registros) detalhando quando e quem acessou cada informação.

Os Colaboradores têm acesso apenas àquelas informações que necessitam para desenvolver suas atividades de trabalho. Sistemas devem ser configurados para negar acesso a qualquer informação classificada que está além da necessidade do funcionário para a realização de suas tarefas específicas.

A senha e *login* para acesso aos dados contidos em todos os computadores, bem como nos e-mails que também possam ser acessados via webmail, devem ser conhecidas somente pelo respectivo usuário do computador e são pessoais e intransferíveis, não devendo ser divulgadas para quaisquer terceiros.

Para segurança dos perfis de acesso, as senhas de acesso dos Colaboradores são parametrizadas conforme as regras estabelecidas pela área de informática da Gestora, conforme definido em conjunto com a Área de Compliance e Risco, para implementação nos perfis de acesso dos Colaboradores, sendo certo que tais senhas são alteradas **anualmente**, conforme aviso fornecido pelo responsável pela área de informática.

Dessa forma, o Colaborador pode ser responsabilizado inclusive caso disponibilize a terceiros a senha e *login* acima referidos, para quaisquer fins.

**(iv)** Uso de Equipamentos e Sistemas

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

A utilização dos ativos e sistemas da Gestora, incluindo computadores, telefones, internet, e-mail e demais aparelhos se destina prioritariamente a fins profissionais. O uso indiscriminado destes para fins pessoais deve ser evitado e nunca deve ser prioridade em relação a qualquer utilização profissional.

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 o Diretor de Compliance, Risco e PLD/FTP.

**(v)** Acesso Remoto

A Gestora permite o acesso remoto pelos Colaboradores, de acordo com a seguinte regra: a todos os Colaboradores, conforme requisição por estes e autorização pelo Diretor de Compliance, Risco e PLD/FTP, no que se refere ao acesso ao e-mail sendo que a rede e diretório apenas os Diretores da Gestora terão permissão.

Ademais, os Colaboradores autorizados 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, (iii) relatar ao Diretor de Compliance, Risco 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, e (iv) não armazenar Informações Confidenciais ou sensíveis em dispositivos pessoais.

**(vi)** Controle de Acesso

O acesso dos Colaboradores à seção do prédio onde a Gestora está alocada é realizado por meio de crachá de acesso, pessoal e intransferível, o qual é disponibilizado a cada Colaborador no momento de sua contratação pela Gestora e recolhido no momento de seu desligamento.

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 mediante a identificação de indícios de uso indevido.

Nesse sentido, o acesso como "administrador" de área de desktop será limitado aos usuários da equipe de Tecnologia e Inovação da Gestora, que forem devidamente aprovados pelo Diretor de Compliance, Risco e PLD/FTP e, com isso, serão determinados privilégios/credenciais e níveis de acesso de usuários apropriados para os Colaboradores.

Adicionalmente, o ambiente de armazenamento em nuvem é segregado por pastas com diferentes níveis de acesso e os Colaboradores da Gestora possuem acesso apenas aos arquivos necessários para a execução de suas respectivas tarefas no dia a dia. Para acessar ou modificar as permissões de acesso é necessária a aprovação pelo criador da respectiva pasta ou arquivo.

**(vii)** *Firewall, Software*, Varreduras e *Backup*

A Gestora utiliza um *hardware* de *firewall* projetado para evitar e detectar conexões não autorizadas e incursões maliciosas. O Diretor de Compliance, Risco e PLD/FTP é responsável por determinar o uso apropriado de *firewalls* (por exemplo, perímetro da rede).

A Gestora contratou Serviço de Antivírus Gerenciado (Global Data Solutions) para detectar, evitar e, quando possível, limpar programas conhecidos que afetem de forma maliciosa os sistemas da empresa (por exemplo, *vírus*, *worms*, *spyware*). Serão conduzidas varreduras **semanais** para detectar e limpar qualquer programa que venha a obter acesso a um dispositivo na rede da Gestora.

A Gestora utiliza um plano de manutenção projetado para guardar os seus dispositivos e *softwares* contra vulnerabilidades com o uso de varreduras e patches. O Diretor de Compliance, Risco e PLD/FTP é responsável por patches regulares nos sistemas da Gestora.

A Gestora mantém e testa regularmente medidas de backup consideradas apropriadas pelo Diretor de Compliance, Risco e PLD/FTP. As informações da Gestora são atualmente objeto de backup **diário** com o uso de computação na nuvem.

### 4.4. Monitoramento e Testes

O Diretor de Compliance, Risco e PLD/FTP (ou pessoa por ele incumbida) adota as seguintes medidas para monitorar determinados usos de dados e sistemas em um esforço para detectar acessos não autorizados ou outras violações potenciais, sempre que houver indícios de alguma irregularidade ou descumprimentos:

**(i)** Monitoramento, por amostragem, do acesso dos Colaboradores a sites, blogs, fotologs, webmails, entre outros, bem como os e-mails enviados e recebidos; e

**(ii)** 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.

O Diretor de Compliance, Risco 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.

### 4.5. Plano de Identificação e Resposta

**(i)** Identificação de Suspeitas

Qualquer suspeita de infecção, acesso não autorizado, outro comprometimento da rede ou dos dispositivos da Gestora (incluindo qualquer violação efetiva ou potencial), ou ainda no caso de vazamento de quaisquer Informações Confidenciais, mesmo que de forma involuntária, deverá ser informada ao Diretor de Compliance, Risco e PLD/FTP prontamente. O Diretor de Compliance, Risco e PLD/FTP determinará quais membros da administração da Gestora e, se aplicável, de agências reguladoras e de segurança pública, deverão ser notificados.

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

**(ii)** Procedimentos de Resposta

A medida adotada pelo Diretor de Compliance, Risco e PLD/FTP diante de quaisquer suspeitas de infecção, acesso não autorizado ou outro comprometimento da rede ou dos dispositivos da Gestora listadas acima será determinada de acordo com os seguintes critérios:

**(a)** 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;

**(b)** Identificação de quais sistemas, se houver, devem ser desconectados ou de outra forma desabilitados;

**(c)** Determinação dos papéis e responsabilidades do pessoal apropriado;

**(d)** Avaliação da necessidade de recuperação e/ou restauração de eventuais serviços que tenham sido prejudicados;

**(e)** Avaliação da necessidade de notificação de todas as partes internas e externas apropriadas (por exemplo, clientes ou investidores afetados, segurança pública);

**(f)** 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); e

**(g)** 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 Diretor de Compliance, Risco e PLD/FTP, após a condução de investigação e uma avaliação completa das circunstâncias do incidente.

## 4.6. Arquivamento de Informações

Devem ser mantidos arquivados pelo prazo de, no mínimo, 5 (cinco) anos, ou por prazo superior por determinação expressa da CVM, conforme disposto na Política de PLD/FTP da Gestora, toda e qualquer informação, bem como documentos que venham a ser necessários para a efetivação satisfatória de possível auditoria ou investigação em torno de possíveis investimentos e/ou clientes suspeitos de corrupção, lavagem de dinheiro ou financiamento ao terrorismo e a proliferação de armas de destruição em massa.

## 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, fac-símiles, 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 IV** ao presente Manual, 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. Treinamento

O Diretor de Compliance, Risco e PLD/FTP organizará treinamento **anual** dos Colaboradores com relação às regras e procedimentos acima, sendo que tal treinamento poderá ser realizado em conjunto com o treinamento anual de compliance (conforme descrito no item 4 acima).

### 4.9. Revisão da Política

O Diretor de Compliance, Risco e PLD/FTP realizará uma revisão desta Política de Segurança da Informação e Segurança Cibernética a cada **24 (vinte e quatro) meses**, para avaliar a eficácia da sua implantação, identificar novos riscos, ativos e processos e reavaliando os riscos residuais.

A finalidade de tal revisão será assegurar que os dispositivos aqui previstos permaneçam consistentes com as operações comerciais da Gestora e acontecimentos regulatórios relevantes.

## V. POLÍTICA DE SUSTENTABILIDADE

A Gestora deve sempre buscar adotar práticas e ações sustentáveis para minimizar eventuais impactos ambientais, incluindo, mas não se limitando a: (a) utilização de papel reciclável para impressão de documentos; (b) utilização de refil de cartuchos e toners para impressão; (c) separação do material reciclável para fins de coleta seletiva de lixo; (d) utilização de lâmpadas de baixo consumo energético; e (e) incentivo à utilização de meios de transporte alternativos ou de menor impacto ambiental por seus Colaboradores, como transportes coletivos, caronas ou bicicletas.

Além disso, a Gestora incentiva seus Colaboradores a adotar postura semelhante no dia a dia de suas atividades, por exemplo: (a) evitar imprimir e-mails e arquivos eletrônicos, exceto se necessário; (b) optar por utilizar canecas ou copos reutilizáveis; (c) desligar os computadores todos os dias ao final do expediente; (d) apagar as luzes das salas ao sair; e (e) desligar as torneiras de pias de cozinha e banheiros quando não estiver fazendo uso.

## VI. POLÍTICA DE CERTIFICAÇÃO

### 6.1. Introdução

A Gestora aderiu e está sujeita às disposições do Código ANBIMA de Regulação e Melhores Práticas para o Programa de Certificação Continuada ("Código ANBIMA de Certificação"), devendo garantir que todos os profissionais elegíveis estejam devidamente certificados.

### 6.2. Atividades Elegíveis e Critérios de Identificação

Tendo em vista a atuação da Gestora como gestora de recursos de terceiros, foi identificado, segundo o Código ANBIMA de Certificação, que a Certificação de Gestores ANBIMA para Fundos Estruturados ("CGE") é a única certificação pertinente às suas

atividades, sendo a CGE aplicável aos profissionais da Gestora com alçada/poder discricionário de investimento, conforme aplicável.

Nesse sentido, 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 CGE, uma vez que esta certificação é aplicável aos profissionais que atuam em fundo de investimento em participações, fundo de investimento em direitos creditórios não padronizados, fundo de índice, fundo de investimento em direitos creditórios, fundo de investimento em cotas de fundos de investimento em direitos creditórios e/ou fundo de investimento imobiliário.

Em complemento, a Gestora destaca que a CGE é certificação pessoal e intransferível. Caso o Colaborador esteja exercendo a atividade elegível de CGE na Gestora, conforme acima indicada, e a certificação não esteja vencida a partir do vínculo do Colaborador com a Gestora, o prazo de validade da certificação CGE será indeterminado, enquanto perdurar o seu vínculo com a Gestora. Por outro lado, caso o Colaborador não esteja exercendo a atividade elegível de CGE na Gestora, a validade da certificação será de 3 (três) anos, contados da data de aprovação no exame, ou da data em que deixou de exercer a atividade elegível de CGE.

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 no Código ANBIMA de Certificação.

### 6.3. Identificação de Profissionais Certificados e Atualização do Banco de Dados da ANBIMA

Antes da contratação, admissão ou transferência de área de qualquer Colaborador, o Diretor de Compliance, Risco 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 ao Diretor de Compliance, Risco 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 Área de Compliance e Risco deverá solicitar a comprovação da certificação pertinente ou sua isenção, se aplicável, anteriormente ao ingresso do novo Colaborador.

A Área de Compliance e Risco também deverá checar se 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. 12, §1º, I do Código ANBIMA de Certificação, sendo que a manutenção das informações contidas no Banco de Dados deverá ser objeto de análise e confirmação pelo Diretor de Compliance, Risco e PLD/FTP, conforme disposto abaixo.

### 6.4. Rotinas de Verificação

**Trimestralmente**, o Diretor de Compliance, Risco 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 no Código ANBIMA de Certificação.

Ainda, o Diretor de Gestão deverá contatar a Área de Compliance e Risco prontamente, sempre que houver 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 CGE (e que não tenham a dispensa concedida pelo Conselho de Certificação, nos termos do Art. 16 do Código ANBIMA de Certificação) estão impedidos de ordenar a compra e venda de ativos para os fundos de investimento sob gestão da Gestora 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 pelo Diretor de Compliance, Risco 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, o Diretor de Compliance, Risco 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 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 Risco, para que os mesmos tenham o conhecimento necessário para operar no Banco de Dados da ANBIMA e realizar as rotinas de verificação necessárias.

### 6.5. 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. 9º, §1º, 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.

## VII. VIGÊNCIA E ATUALIZAÇÃO

Este Manual será revisado **anualmente**, ou sempre que necessário, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo.

| **Histórico das atualizações** | | |
|---|---|---|
| **Data** | **Versão** | **Responsável** |
| agosto/2024 | V.1 | Diretor de Compliance, Risco e PLD/FTP |

**ANEXO I**
**TERMO DE ADESÃO AO MANUAL DE REGRAS, PROCEDIMENTOS E CONTROLES INTERNOS**

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

**(i)** Ter recebido, na presente data, o Manual de Regras, Procedimentos e Controles Internos atualizado ("Manual") da **PIEMONTE CAPITAL GESTORA DE RECURSOS LTDA.** ("Gestora");

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

**(iii)** Aceitar e expressar total concordância e irrestrita adesão aos termos e regras do Código;

**(iv)** Ter recebido treinamento com relação ao seu conteúdo;

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

**(vi)** Estar ciente do meu compromisso de comunicar ao Diretor de Compliance, Risco e PLD/FTP da Gestora qualquer situação que chegue ao meu conhecimento que esteja em desacordo com as regras definidas neste Manual.

[local], [data].

_____
[COLABORADOR]

**ANEXO II**
**ACORDO DE CONFIDENCIALIDADE**

Por este instrumento particular, de um lado:

**PIEMONTE CAPITAL GESTORA DE RECURSOS LTDA.**, sociedade empresária limitada com sede na Cidade do Rio de Janeiro, Estado do Rio de Janeiro, na Rua Lauro Muller, nº 116, sala 4103, Botafogo, CEP 22.290-160, inscrita no CNPJ/MF sob o nº 52.958.962/0001-51, neste ato representada na forma de seu Contrato Social ("Piemonte Capital");

_____, inscrito no CPF/MF sob o nº _____, colaborador da Piemonte Capital ("Colaborador").

Piemonte Capital e Colaborador, abaixo denominadas, em conjunto, "Partes", e, isoladamente, "Parte".

Cada uma das Partes ("Parte Divulgadora") poderá disponibilizar à outra Parte ("Parte Receptora") materiais compostos de documentos e informações de natureza financeira, contábil, técnica, operacional, comercial e jurídica, fornecidos oralmente ou por escrito, incluindo, sem limitações, informações relativas aos negócios, projeções, operações, contratos, estrutura organizacional, aspectos regulatórios, situação fiscal, processos, documentos de natureza trabalhista, licenças e autorizações, aspectos ambientais e estrutura financeira relacionados à gestão de recursos ("Projeto" e "Material de Avaliação", respectivamente).

Para fins deste Acordo, "Informações Confidenciais" significa: (a) o Material de Avaliação; (b) quaisquer outras informações de natureza diversa relacionada total ou parcialmente ao Projeto ou a este Acordo (incluindo sua respectiva existência de conteúdo, discussões ou negociações com relação a cada um desses, bem como a identidade das partes envolvidas), fornecidas à Parte Receptora, bem como a seus Representantes (conforme definido abaixo); e (c) qualquer relatório, análise, compilações, estudos ou qualquer outro documento preparado por, em nome da ou para a Parte Receptora, que contenham, derivem ou reflitam de qualquer outra forma qualquer informação descrita nas alíneas (a), (b) e (c) acima.

Como condição de, e em consideração ao fornecimento de tais Informações Confidenciais, a Parte Receptora concorda em tratar toda a Informação Confidencial de

acordo com os termos e condições previstos nesse Acordo de Confidencialidade ("Acordo"):

1. As Partes concordam que as Informações Confidenciais serão usadas com o propósito único e exclusivo de determinar o interesse da Parte Receptora em apresentar uma proposta de serviços profissionais.

2. A Parte Receptora concorda em manter a confidencialidade das Informações Confidenciais, obrigando-se a não revelar, copiar, reproduzir ou distribuir as Informações Confidenciais, exceto se expressamente autorizada pela Parte Divulgadora.

3. As Partes poderão franquear o acesso às Informações Confidenciais para seus executivos, diretores, empregados, advogados, consultores financeiros e legais, se qualquer deles (coletivamente, os "Representantes") estiverem envolvidos na gestão de recursos, desde que estes Representantes se obriguem a manter a confidencialidade sobre as Informações Confidenciais e a cumprir as obrigações contidas nesse Acordo, como se fossem parte integrante deste. A Parte Receptora será responsável por quaisquer violações dos termos deste Acordo por qualquer de seus Representantes como se estes fossem a parte que violou os termos deste Acordo.

4. Este Acordo será independente de qualquer outro acordo celebrado entre as Partes.

5. O termo "Informação Confidencial" não inclui qualquer informação: (a) que seja ou se torne pública por outro motivo que não o inadimplemento deste Acordo; (b) que seja ou se torne disponível para a Parte Receptora por outra fonte que não a Parte Reveladora, desde que a fonte reveladora não esteja vinculada a qualquer acordo de confidencialidade em relação a tal informação; ou (c) seja comprovadamente conhecida pela Parte Receptora antes de sua revelação pela Parte Reveladora.

6. Esse Acordo não deve ser interpretado de modo a proibir a divulgação das Informações Confidenciais ou qualquer parte dele (i) por força de lei ou regulamento aplicável, ou (ii) em cumprimento a ordem judicial; em qualquer dessas hipóteses, a Parte Receptora divulgadora da informação deverá notificar a Parte Reveladora, por escrito, acerca da informação que será revelada, em tempo hábil para que a Parte Reveladora cuja informação foi divulgada ou seus clientes possam adotar as medidas legais disponíveis com o intuito de evitar tal divulgação ou minimizar a extensão de suas consequências, devendo a Parte Receptora divulgadora, ainda, pleitear tratamento confidencial para a informação divulgada aos destinatários desta divulgação.

7. A revelação de informações gerais, comerciais ou confidenciais não implicará em obrigação de reciprocidade.

8. Se qualquer das Partes decidir não prosseguir com o Projeto, deverá informar a outra Parte e devolver todas as Informações Confidenciais, bem como qualquer material contendo parte delas, sem manter qualquer cópia.

9. A divulgação a terceiros de qualquer informação contida em qualquer Informação Confidencial disponibilizada, em violação ao presente Acordo, sujeitará a Parte Receptora reveladora da informação a terceiros, ao pagamento de indenização à Parte proprietária da informação e a seus clientes, por quaisquer prejuízos, perdas, danos, custos e/ou despesas (incluindo todas as custas legais) por ela incorridos ou sofridos em decorrência desta violação.

10. Este Acordo contém o acordo integral entre as Partes a respeito de Informações Confidenciais e revoga qualquer acordo anterior relativo a este.

11. Este Acordo apenas poderá ser modificado por escrito, mediante assinatura dos representantes legais de ambas as Partes.

12. O Acordo somente vinculará e surtirá efeitos com relação às suas Partes e aos Representantes que, para ter acesso às Informações Confidenciais, deverão aderir ao presente instrumento e passarão a ser tratados como Partes.

13. Qualquer responsabilidade oriunda ou decorrente deste Acordo, como consequência de qualquer infração contratual, somente poderá ser assumida e suportada por suas Partes.

14. Nenhuma disposição, expressa ou implícita, neste Acordo, deverá ser interpretada de modo a conferir a terceiros, qualquer direito, benefício ou reparação de qualquer natureza resultantes do presente Acordo.

15. Prazo. Este Acordo entra em vigor na data de sua assinatura e permanecerá em vigor pelo prazo de 02 (dois) anos.

16. Compliance. As Partes, bem como seus representantes legais, declaram neste ato, para todos os fins e na melhor forma de direito, que cumprem e cumprirão com todas as leis anti-corrupção, anti-suborno e de prevenção à lavagem de dinheiro, em especial,

mas não limitadas às (i) Lei Anticorrupção - Lei n° 12.846, de 1° de agosto de 2013; (ii) Lei de Prevenção à Lavagem de Dinheiro - Lei n° 9.613, de 3 de março de 1998, incluindo suas alterações posteriores, integrantes do ordenamento jurídico brasileiro; (iii) Lei sobre Práticas de Corrupção no Exterior (*Foreign Corruption Practice Act – FCPA* e o *UK Bribery Act*).

16.1. Ainda no que concerne ao assunto, declaram que não autorizaram, ofereceram, prometeram, ou pagaram, transferiram, seja direta ou indiretamente, qualquer suborno, desconto, pagamento, rebate, vantagem ou qualquer outro pagamento ilícito a qualquer agente público e/ou membros ou representantes de qualquer Autoridade Governamental.

16.2. Entende-se por Autoridade Governamental o governo federal, estadual e municipal; qualquer entidade, autoridade ou órgão exercendo funções executivas, legislativas, judiciais, regulatórias ou administrativas atribuídas ao governo, inclusive qualquer autoridade governamental, agência, departamento, conselho, comissão ou autarquia no Brasil ou, caso aplicável, em qualquer outro país com jurisdição onde as Partes desenvolvem suas atividades; qualquer corte, tribunal ou árbitros.

16.3. A violação de qualquer das práticas declaradas acima ensejará na obrigação da Parte culpada de indenizar a Parte inocente por todas as perdas e danos incorridos.

17. Lei aplicável. Este Acordo deverá ser regido e interpretado de acordo com as leis da República Federativa do Brasil.

18. Foro. As Partes elegem o foro da comarca da capital do Estado do Rio de Janeiro, com renúncia expressa a qualquer outro, por mais privilegiado que seja, para discutir toda e qualquer controvérsia oriunda ou relacionada a este instrumento, dentre outras, aquelas que envolvam sua validade, eficácia, violação, interpretação, término, rescisão e suas consequências, etc., que não sejam resolvidas amigavelmente entre as Partes.

19. Privacidade e Proteção de Dados. As Partes reconhecem que poderá ser necessária a realização de algum tipo de Tratamento de Dados Pessoais nos termos da Legislação Aplicável de Proteção de Dados. "Legislação Aplicável de Proteção de Dados" significa, enquanto permanecer em vigor, Lei Geral de Proteção de Dados (Lei nº 13.709/2018 ou "LGPD") e quaisquer outras leis e regulamentos em relação ao Tratamento de Dados Pessoais e privacidade que são aplicáveis a quaisquer das Partes e, se aplicáveis, todas as orientações e códigos de prática emitidos pela Autoridade Nacional de Proteção de Dados ("ANPD") ou outra autoridade de supervisão ou proteção de dados pertinente. Com efeito, as Partes se comprometem a realizar o Tratamento dos

Dados Pessoais em conformidade com a Legislação Aplicável de Proteção de Dados. A menos que definido de outra forma no Acordo, os termos nesta Cláusula terão o significado que lhes é atribuído na Legislação Aplicável de Proteção de Dados.

19.1. Cada Parte permanecerá total e integralmente responsável pelos Dados Pessoais dos quais realizar o Tratamento, obrigando-se a manter a outra Parte indene de qualquer obrigação e responsabilidade por eventuais atos, omissões, erros ou danos cometidos ou provocados exclusivamente por ela ou eventuais Suboperadores no Tratamento dos Dados Pessoais, se tiverem sido Tratados em desconformidade com a Legislação Aplicável de Proteção de Dados.

20. Cada uma das Partes arcará com seus próprios custos com advogados e contabilidade decorrentes de e em conexão com o presente Acordo.

As Partes assinam o presente instrumento em 2 (duas) vias de igual teor e forma, juntamente com as testemunhas infra-assinadas.

Rio de Janeiro, [dia] de [mês] de [ano].

[*página de assinatura na sequência*]

**ANEXO III**
**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 **PIEMONTE CAPITAL GESTORA DE RECURSOS LTDA.** ("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.

[local], [data].

_____
[COLABORADOR]

## Apêndice
## Lista dos Arquivos Gravados nos *Pen Drives*

**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 **PIEMONTE CAPITAL GESTORA DE RECURSOS LTDA.** ("Gestora") por prazo indeterminado:

[ ] até que me certifique pela CGE, no caso da atividade de gestão de recursos de terceiros com alçada/poder discricionário de investimento;

[ ] ou até que o Conselho de Certificação, nos termos do Art. 17 do Código de Certificação, me conceda a isenção de obtenção da CGE;

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

[local], [data].

_____
[COLABORADOR]

_____
**PIEMONTE CAPITAL GESTORA DE RECURSOS LTDA.**

Testemunhas:

1._____
Nome:
CPF/MF:

2._____
Nome:
CPF/MF:

**ANEXO V**

**MODELO DE TERMO DE PARTICIPAÇÃO EM PROGRAMA DE TREINAMENTO**

Por meio deste instrumento, eu, _____, inscrito(a) no CPF/MF sob o nº _____, doravante denominado Colaborador da **PIEMONTE CAPITAL GESTORA DE RECURSOS LTDA.** ("Gestora"), declaro para os devidos fins que participei do programa de treinamento de [·] em [data] oferecido pela Gestora.

[local], [data].

_____
[COLABORADOR]

_____
**PIEMONTE CAPITAL GESTORA DE RECURSOS LTDA.**

Testemunhas:

1._____
Nome:
CPF/MF:

2._____
Nome:
CPF/MF: