BERKANA INVESTIMENTOS E GESTÃO DE RECURSOS LTDA.

MANUAL DE REGRAS, PROCEDIMENTOS E CONTROLES INTERNOS

02 de abril de 2026

ÍNDICE

I. Regras, Procedimentos e Controles Internos

1. Objetivo e Aplicabilidade

Este Manual de Regras, Procedimentos e Controles Internos ("Manual") tem por objetivo estabelecer as normas, os princípios, os conceitos e os 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 **BERKANA INVESTIMENTOS E GESTÃO DE RECURSOS LTDA.** ("Gestora"), tanto na sua atuação interna quanto na comunicação com os diversos públicos, visando ao atendimento de padrões éticos cada vez mais elevados.

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.

2. Termo de Compromisso

Este Manual é parte integrante das regras que regem a relação societária e/ou de trabalho dos Colaboradores, que, ao receberem o presente Manual, deverão assinar termo de recebimento e compromisso a este Manual, a fim de demonstrar que aceitam expressamente as normas, princípios, conceitos e valores estabelecidos neste documento e nas demais políticas internas da Gestora. Periodicamente, em caso de atualização deste Manual e/ou de outras políticas internas da Gestora será requisitado aos Colaboradores que assinem novos Termos de Recebimento e Compromisso, reforçando o conhecimento e concordância com os novos termos deste Manual e das demais políticas internas da Gestora.

3. Responsabilidades e Obrigações

A coordenação da aplicação deste Manual é uma atribuição do diretor estatutário da Gestora responsável pelo cumprimento de regras, políticas, procedimentos e controles internos da Gestora ("Diretor de Compliance, Risco e PLD"), que contará com o auxílio de analistas na condução das atividades de gestão de compliance, risco e PLD, os quais, em conjunto, comporão o Comitê de Compliance, Risco e PLD.

São obrigações do Comitê de Compliance, Risco e PLD, sob a responsabilidade do Diretor de Compliance, Risco e PLD:

(i) Acompanhar a efetiva implementação do disposto neste Manual;

(ii) 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;

(iii) Atender prontamente todos os Colaboradores;

(iv) Identificar possíveis condutas contrárias a este Manual;

(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) Encaminhar aos órgãos de administração da Gestora, até o **último dia útil do mês de abril** de cada ano, relatório **anual** de compliance 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; **(c)** as operações identificadas como suspeitas que tenham sido comunicadas às autoridades competentes, no âmbito da Política de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e ao Financiamento da Proliferação de Armas de Destruição em Massa – PLDFTP e de Cadastro da Gestora ("Política de PLDFTP"); e **(d)** a manifestação do diretor responsável pela administração de carteiras de valores mobiliários ("Diretor de Gestão") 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

(viii) Manter o relatório a que se refere o inciso "(vii)" acima arquivado na sede da Gestora e disponível à CVM;

(ix) Definir os princípios éticos a serem observados por todos os Colaboradores, constantes deste Manual e das outras Políticas internas da Gestora;

(x) 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;

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

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

(xiii) Aplicar as eventuais sanções aos Colaboradores;

(xiv) Analisar situações que cheguem ao seu conhecimento e que possam ser caracterizadas como "conflitos de interesse"

(xv) Promover a ampla divulgação e aplicação dos princípios, regras, manuais e políticas internas da Gestora a todos os Colaboradores, inclusive por meio da realização de **treinamento inicial**, quando da contratação do Colaborador, e **treinamento periódico de reciclagem**, anualmente ou quando da revisão de políticas e manuais internos da Gestora, podendo profissionais especializados serem contratados para conduzirem os treinamentos.

4. Garantia de Independência

Os Colaboradores do Comitê de Compliance, Risco e PLD atuam sob a coordenação e responsabilidade do Diretor de Compliance, Risco e PLD, sendo lhes assegurado o exercício de suas atividades de forma completamente independente das outras áreas da Gestora.

5. 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.

Toda e qualquer solicitação que dependa de autorização, orientação ou esclarecimento expresso do Diretor de Compliance, Risco e PLD, 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 aplicável ao Diretor de Compliance, Risco e PLD.

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. Nenhum Colaborador sofrerá retaliação por comunicar, de boa-fé, violações ou potenciais violações a este Manual. O Colaborador que se omitir de tal obrigação poderá sofrer as sanções definidas neste Manual.

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

6. 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, de acordo com os procedimentos estabelecidos neste Manual, este utilizará os registros e sistemas de monitoramento eletrônico referidos neste Manual para verificar a conduta dos Colaboradores envolvidos.

O Comitê de Compliance, Risco e PLD:

(i) Poderá acessar, quando julgar oportuno e necessário, todo conteúdo que está na rede, inclusive arquivos pessoais salvos em cada computador. Da mesma forma, mensagens de correio eletrônico de Colaboradores serão gravadas e, quando necessário, interceptadas e escutadas, sem que isto represente invasão da privacidade dos Colaboradores já que se tratam de ferramentas de trabalho disponibilizadas pela Gestora;

(ii) Escolherá aleatoriamente uma amostragem significativa dos Colaboradores e realizará um monitoramento, **anual**, 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;

(iii) Verificará, **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; e

(iv) Analisará os controles previstos neste Manual, bem como em outras políticas da Gestora, propondo a criação de novos controles e melhorias naqueles que eventualmente sejam considerados deficientes, monitorando as respectivas correções, sendo que as análises e eventuais correções, se for o caso, deverão ser objeto do relatório anual de compliance.

O Diretor de Compliance, Risco e PLD poderá utilizar as informações obtidas 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.

7. Sanções ("*Enforcement*")

Responsável pela Definição: Comitê de Compliance, Risco e PLD.

Responsável pela Aplicação: Diretor de Compliance, Risco e PLD.

Sanções: Advertência, suspensão, desligamento ou exclusão por justa causa, ou demissão por justa causa, conforme aplicável. A Gestora: **(i)** poderá ainda pleitear indenização pelos eventuais prejuízos suportados, perdas e danos e/ou lucros cessantes, por meio das medidas legais cabíveis; **(ii)** não assume a responsabilidade de Colaboradores que transgridam a lei ou cometam infrações no exercício de suas funções; e **(iii)** pode exercer o direito de regresso em face dos responsáveis, caso venha a ser responsabilizada ou sofra prejuízo de qualquer natureza por atos de seus Colaboradores.

II. Políticas de Confidencialidade

1. Sigilo e Conduta

Todos os Colaboradores deverão ler atentamente e entender o disposto neste Manual, bem como deverão firmar o termo de adesão e de confidencialidade ("Termo de Confidencialidade").

O Termo de Confidencialidade deverá prever que 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 e infralegais, aplicáveis à Gestora e suas atividades.

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 e carteiras geridas pela 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) 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.

A Informação Confidencial não pode ser divulgada, em hipótese alguma, a terceiros não-Colaboradores ou a Colaboradores não autorizados, 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.

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 e/ou administrativas, deverá ser prévia e tempestivamente informada ao Diretor de Compliance, Risco e PLD, 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, 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.

2. *Insider Trading, "Dicas" e Front-running*

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.

É expressamente proibido valer-se das práticas aqui descritas 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, conforme o caso, eventual demissão ou exclusão por justa causa.

III. Políticas de Segurança da Informação e Segurança Cibernética

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 não 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 execução direta das atividades relacionadas à política de segurança da informação e segurança cibernética ficará a cargo do Comitê de Compliance, Risco e PLD, que, em conjunto com a equipe de Tecnologia da Informação serão responsáveis inclusive por sua revisão, realização de testes e treinamento dos Colaboradores, conforme descrito neste Manual.

1. 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: Informações Confidenciais, incluindo informações a respeito de investidores, clientes, Colaboradores e

da própria Gestora, operações e ativos investidos pelas carteiras de valores mobiliários 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: 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; e

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

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.

2. Ações de Prevenção e Proteção

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

A Gestora realiza efetivo controle do acesso a arquivos que contemplem Informações Confidenciais em meio físico, disponibilizando-os somente aos Colaboradores que efetivamente estejam envolvidos 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 o Comitê de Compliance, Risco e PLD 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 não mantém arquivo físico centralizado, sendo cada Colaborador responsável direto 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-drives, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na 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. Neste caso, 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 ou deficiência física), obsceno, pornográfico ou ofensivo é terminantemente proibida.

AÇÕES DE PREVENÇÃO E PROTEÇÃO DE INFORMAÇÕES CONFIDENCIAIS E SEGURANÇA CIBERNÉTICA
Acesso Escalonado do Sistema
O acesso como "administrador" de área de *desktop* é limitado aos usuários aprovados pelo Diretor de Compliance, Risco e PLD 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.
Senha e Login
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. As senhas deverão ser trocadas **semestralmente**, 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.
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.

Acesso Remoto

A Gestora permite o acesso remoto pelos Colaboradores ao e-mail, rede e diretório, conforme requisição por estes e autorização pelo Diretor de Compliance, Risco e PLD.

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 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.

Controle de Acesso

O acesso de pessoas estranhas à Gestora a áreas restritas somente é permitido com a autorização do Diretor de Compliance, Risco e PLD ou do Diretor de Gestão.

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.

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 é responsável por determinar o uso apropriado de *firewalls* (por exemplo, perímetro da rede).

A Gestora mantém proteção atualizada contra *malware* nos seus dispositivos e software antivírus projetado 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 **mensais** 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 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. As informações da Gestora são atualmente objeto de backup **diário** com o uso de computação na nuvem.

3. Monitoramento e Testes

O Comitê de Compliance, Risco e PLD adota as seguintes medidas para monitorar determinados usos de dados e sistemas em um esforço para detectar acessos não autorizados ou outras violações potenciais, em base, no mínimo, **anual**:

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

4. Plano de Identificação e Resposta

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 prontamente. O Diretor de Compliance, Risco e PLD 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 determinará quais clientes ou investidores, se houver, deverão ser contatados com relação eventual à violação.

O Diretor de Compliance, Risco e PLD responderá 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 Diretor de Compliance, Risco e PLD, após a condução de investigação e uma avaliação completa das circunstâncias do incidente.

5. Arquivamento de Informações

Os Colaboradores deverão manter arquivada, pelo prazo regulamentar aplicável, toda e qualquer informação, bem como documentos e extratos 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 e/ou lavagem de dinheiro, bem como todos os documentos e informações exigidos pela Resolução CVM 21, correspondência, interna e externa, papéis de trabalho, relatórios e pareceres relacionados com o exercício de suas funções em conformidade com o inciso IV do artigo 18 e com o artigo 34 da Resolução CVM 21.

IV. 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.

V. Política de Anticorrupção

1. Introdução

A Gestora está sujeita às normas e leis de anticorrupção, incluindo, mas não se limitando, às Normas de Anticorrupção, as quais 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.

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.

2. Definição

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.

(v) 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.

3. Normas de Conduta

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

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.

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, estes têm a obrigação de seguir estritamente a legislação vigente.

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 ao Diretor de Compliance, Risco e PLD imediatamente após sua ocorrência.

VI. Política de Certificação

1. Introdução

A Gestora aderiu e está sujeita às disposições do Código de Certificação, devendo garantir que todos os profissionais elegíveis estejam devidamente certificados.

2. Atividades Elegíveis e Critérios de Identificação.

Tendo em vista a atuação da Gestora como gestora de recursos de terceiros, foi identificado que a Certificação de Gestores ANBIMA ("CGA") e a Certificação de Gestores ANBIMA para Fundos Estruturados ("CGE") são as certificações pertinentes às suas atividades, aplicáveis aos profissionais com alçada/poder discricionário de investimento.

Ademais, para a prestação de serviços de gestão de patrimônio foi identificado que a CGA e a CGE são as certificações pertinentes às suas atividades de gestão profissional dos ativos financeiros integrantes da carteira dos veículos de investimento, com foco individualizado nas necessidades financeiras do investidor. Adicionalmente, ainda poderão ser utilizadas, somente para fins desta atividade, as certificações CFP e CFA.

Nesse sentido, destaca-se ainda que o Código de Certificação determina que, no mínimo, 75% (setenta e cinco por cento) dos profissionais que atuam na gestão

de patrimônio, realizando o contato comercial com o investidor e o assessorando em suas decisões de investimento, devem ser certificados CGA, CGE, CFP ou CFA. Em complemento, a Gestora destaca que as certificações são de cunho pessoal e intransferíveis, bem como seguirão os seguintes prazos, os quais serão monitorados pelo Diretor de Compliance, Risco e PLD, sendo certo que caso o Colaborador esteja exercendo a atividade elegível de CGA ou CGE na Gestora e a certificação não esteja vencida, a partir do vínculo do Colaborador com a Gestora, o prazo de validade da certificação CGA e CGE será indeterminado, enquanto perdurar o seu vínculo com a Gestora e a sua atuação na atividade elegível. Por outro lado, caso o Colaborador não esteja exercendo a atividade elegível da CGA ou CGE na Gestora, a validade da respectiva certificação será de 3 (três) anos, contados da data de aprovação no exame, ou da data em que deixou de exercer a atividade elegível da CGA ou CGE, conforme o caso.

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 de Certificação.

3. Identificação de Profissionais Certificados e Atualização do Banco de Dados

Antes da contratação, admissão ou transferência de área de qualquer Colaborador, o Comitê de Compliance, Risco e PLD 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.

O Diretor de Gestão deverá esclarecer ao Comitê de Compliance, Risco e PLD se Colaboradores que integrarão o departamento técnico envolvido na gestão de recursos terão ou não alçada/poder discricionário de decisão de investimento e com quais produtos cada um dos Colaboradores irá atuar.

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

O Comitê de Compliance, Risco e PLD também deverá checar se Colaboradores que estejam se desligando da Gestora estão indicados no Banco de Dados como profissionais elegíveis/certificados vinculados à Gestora, sendo, para estes, obrigatória a inclusão do desligamento no Banco de Dados.

O Comitê de Compliance, Risco e PLD deve incluir no Banco de Dados as informações cadastrais de todos os Colaboradores que tenham qualquer

certificação ANBIMA, esteja a certificação vencida e/ou em processo de atualização, sendo referida inclusão facultativa somente para estagiários e terceiros contratados.

Todas as atualizações no Banco de Dados devem ocorrer **até o último dia útil do mês subsequente à data do evento que deu causa a atualização**, sendo que a manutenção das informações contidas no Banco de Dados deverá ser objeto de análise e confirmação pelo Comitê de Compliance, Risco e PLD, conforme disposto abaixo.

4. Rotinas de Verificação

Semestralmente, o Comitê de Compliance, Risco e PLD deverá verificar as informações contidas no Banco de Dados, 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 de Certificação.

Ainda, o Diretor de Gestão deverá contatar o Comitê de Compliance, Risco e PLD **prontamente**, sempre que houver algum tipo de alteração nos cargos/funções dos Colaboradores que integram o departamento técnico envolvido na gestão de recursos e/ou com quais produtos cada destes Colaboradores atuarem, confirmando, além disso, 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 pelo Comitê de Compliance, Risco e PLD, 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 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.

5. Processo de Afastamento

Todos os profissionais não certificados ou em processo de certificação, e para os quais haja certificação exigível, nos termos previstos neste Manual, serão imediatamente afastados das atividades elegíveis aplicáveis, até que se certifiquem ou até que o Conselho de Certificação conceda a isenção de obtenção da certificação aplicável.

VII. Vigência e Atualização

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

Histórico das Atualizações		
Data	**Versão**	**Responsável**
02 de abril de 2026	5ª e Atual	Diretor de Compliance, Risco e PLD