STEN GESTÃO PATRIMONIAL LTDA.
("GESTORA")

MANUAL DE REGRAS, PROCEDIMENTOS E CONTROLES INTERNOS
("MANUAL")

JANEIRO/2025

ÍNDICE

1. INTRODUÇÃO

1.1. Objetivo e Aplicabilidade

Estabelecer normas, princípios, conceitos e valores que orientam a conduta de todos aqueles que possuam cargo, função, posição, relação societária, empregatícia, comercial, profissional, contratual ou de confiança ("Colaboradores") com a 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.

1.2. Base Legal

(i) Item 2.7 do Ofício-Circular/CVM/SIN/Nº 05/2014;
(ii) Resolução da Comissão de Valores Mobiliários ("CVM") nº 21, de 25 de fevereiro de 2021, conforme alterada ("Resolução CVM 21/21");
(iii) Resolução da Comissão de Valores Mobiliários ("CVM") nº 175, de 23 de dezembro de 2022, conforme alterada ("Resolução CVM 175/22");
(iv) Código da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais ("ANBIMA") de Ética ("Código de Ética");
(v) Código ANBIMA de Administração e Gestão de Recursos de Terceiros ("Código de AGRT");
(vi) Código ANBIMA de Certificação ("Código ANBIMA de Certificação");
(vii) Lei nº 12.846/13 e Decreto nº 11.129/22, conforme alterada ("Normas de Anticorrupção"); e
(viii) Demais manifestações e ofícios orientadores dos órgãos reguladores e autorregulados aplicáveis às atividades da Gestora.

1.3. Ambiente Regulatório e Termo de Compromisso

Este Manual é parte integrante das regras que regem a relação societária ou de trabalho dos Colaboradores, que, ao receberem o presente Manual, deverão assinar o termo de recebimento e compromisso constante do **Anexo I** do Código de Ética ("Termo de Recebimento e Compromisso"), a fim de demonstrar que aceitam expressamente as normas, princípios, conceitos e valores aqui estabelecidos. Periodicamente, poderá ser requisitado aos Colaboradores que assinem novos Termos de Recebimento e Compromisso, reforçando o conhecimento e concordância com os 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. As principais normas aplicáveis às atividades da Gestora constam no Anexo II do presente Manual.

2. POLÍTICA DE COMPLIANCE

2.1. Introdução

2.1.1. Responsabilidades e Obrigações

A coordenação direta das atividades relacionadas a este Manual é uma atribuição do Colaborador da Gestora indicado como Responsável pelo cumprimento de regras, políticas, procedimentos e controles internos da Gestora ("Diretor de Compliance"), nos termos da Resolução CVM 21/21.

São obrigações da Equipe de Compliance sob a responsabilidade do Diretor de Compliance:

(i) Acompanhar as políticas descritas 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 do Comitê de Compliance 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) 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;
(viii) Encaminhar aos órgãos de administração da Gestora, até o **último dia útil do mês de abril** de cada ano, relatório referente ao ano civil imediatamente anterior à data de entrega, contendo: ***(a)*** as conclusões dos exames efetuados; ***(b)*** as recomendações a respeito de eventuais deficiências, com o estabelecimento de cronogramas de saneamento, quando for o caso; e ***(c)*** a manifestação do diretor responsável pela administração de carteiras de valores mobiliários ou, quando for o caso, pelo diretor responsável pela gestão de risco a respeito das deficiências encontradas em verificações anteriores e das medidas planejadas, de acordo com cronograma específico, ou efetivamente adotadas para saná-las; devendo referido relatório permanecer disponível à CVM na sede da Gestora;
(ix) Definir os princípios éticos a serem observados por todos os Colaboradores, constantes deste Manual ou de outros documentos que vierem a ser produzidos para este fim, elaborando sua revisão periódica;

(x) Promover a ampla divulgação e aplicação dos preceitos éticos no desenvolvimento das atividades de todos os Colaboradores, inclusive por meio dos treinamentos periódicos previstos neste Manual;
(xi) Apreciar todos os casos que cheguem ao seu conhecimento sobre o potencial descumprimento dos preceitos éticos e de compliance previstos neste Manual ou nos demais documentos aqui mencionados, e apreciar e analisar situações não previstas;
(xii) Garantir o sigilo de eventuais denunciantes de delitos ou infrações, mesmo quando estes não solicitarem, exceto nos casos de necessidade de testemunho judicial;
(xiii) Solicitar sempre que necessário, para a análise de suas questões, o apoio da auditoria interna ou externa ou outros assessores profissionais;
(xiv) Aplicar as eventuais sanções aos Colaboradores, conforme definido pelo Comitê de Compliance; e
(xv) 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:

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

O Diretor de Compliance poderá contar, ainda, com outros Colaboradores para as atividades e rotinas de compliance, 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.

Ademais, a Gestora possui também um Comitê de Compliance.

2.1.2. Garantia de Independência

Os Colaboradores da Equipe de Compliance, atuam sob a coordenação do Diretor de Compliance, e todos exercem suas atividades de forma completamente independente das outras áreas da Gestora.

2.1.3. 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, 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, que submeterá para análise em âmbito de Comitê de Compliance o ocorrido.

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, que reportará tal conduta para avaliação no âmbito do Comitê de Compliance. 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 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, o Colaborador deverá informar diretamente aos demais administradores da Gestora.

2.1.4. 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, 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.

Todo conteúdo que está na rede será acessado pela Equipe de Compliance, caso haja necessidade, inclusive arquivos pessoais salvos em cada computador serão acessados caso a Equipe de Compliance julgue necessário. Da mesma forma, mensagens de correio eletrônico de Colaboradores serão gravadas e, quando necessário, interceptadas sem que isto represente invasão da privacidade dos Colaboradores já que se tratam de ferramentas de trabalho disponibilizadas pela Gestora.

Adicionalmente, será realizado um monitoramento **anual**, pela Equipe de Compliance, sobre uma amostragem significativa dos Colaboradores, escolhida aleatoriamente pela Equipe de Compliance, 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.

Ainda, a Equipe de Compliance 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.

O Diretor de Compliance poderá utilizar as informações obtidas em tais monitoramentos para decidir em conjunto e no âmbito de Comitê de Compliance, 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.

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

2.1.5. Sanções ("Enforcement")

Responsável pela Definição: Comitê de Compliance.

Responsável pela Aplicação: Diretor de Compliance.

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.

3. POLÍTICAS DE CONFIDENCIALIDADE

3.1. Sigilo e Conduta

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

Conforme disposto no Termo 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 II** 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) 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.

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, para que esta decida sobre a forma mais adequada para tal revelação, após exaurirem todas as medidas jurídicas apropriadas para evitar a supramencionada revelação.

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

Insider Trading e "Dicas"

Insider Trading significa 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).

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

Front-running

Front-running significa 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.

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

Caso os Colaboradores tenham acesso, por qualquer meio, a Informação Confidencial, deverão levar tal circunstância ao imediato conhecimento do Diretor de Compliance, 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 o Diretor de Compliance anteriormente mencionada.

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

4. POLÍTICAS DE TREINAMENTO

A Gestora possui um processo de integração e treinamento inicial dos seus Colaboradores e um programa de reciclagem contínua dos conhecimentos de tais Colaboradores com relação aos princípios gerais e normas de *Compliance* da Gestora, bem como às principais Leis e normas aplicáveis às suas atividades, conforme preceitua a Resolução CVM nº 21/2021.

Assim que cada Colaborador passa a fazer parte do dia-a-dia da Gestora, antes do início efetivo de suas atividades, este participará de um processo de integração e treinamento onde irá adquirir conhecimento sobre as atividades da Gestora, suas atribuições e normas internas, políticas e códigos, além de informações sobre as principais Leis e normas que regem as atividades da Gestora.

Logo, conforme descrito no presente Manual e no Código de Ética da Gestora, o Colaborador, ao iniciar suas atividades na instituição, receberá as políticas da Gestora.

Ademais, conforme Termo de Recebimento e Compromisso com o Código de Ética, todo Colaborador atesta o recebimento e confere ciência de todas as políticas acima descritas, no ato de seu ingresso na gestora.

Treinamento Contínuo: Em consonância com o disposto no art. 24, III, da Resolução CVM n.º 21/2021, que versa sobre a necessidade de implantação e manutenção de programa de treinamento, a Gestora entende que é fundamental que todos os Colaboradores tenham conhecimento, bem como mantenham-no sempre atualizado, dos seus princípios éticos, aplicáveis as suas atividades.

Neste sentido, em cumprimento a referida norma e aos valores da nossa instituição, a Gestora adota um programa de reciclagem dos seus Colaboradores, com o objetivo de fazer com que os mesmos estejam sempre atualizados sobre os termos e responsabilidades aqui descritos.

O referido programa de reciclagem dos Colaboradores da Gestora, que terá periodicidade mínima anual, consiste, dentre outras atividades, na disponibilidade do Diretor de Compliance para tirar quaisquer dúvidas dos Colaboradores a qualquer momento, com o intuito de manter os Colaboradores sempre em consonância com as regras dos órgãos reguladores e da própria Gestora.

Ademais, em caso de alguma alteração nas políticas da Gestora, devido à exigência de órgãos reguladores ou por quaisquer outros motivos, a gestora poderá realizar um programa de reciclagem para os Colaboradores, com o intuito de fornecer a nova política aos mesmos e também de apresentar as mudanças e os novos pontos abordados por tal política.

Os Colaboradores que possuírem acesso a informações confidenciais, participem do processo de decisão de investimento ou participem do processo de distribuição de cotas de fundos de investimento participarão de treinamentos específicos que abrangem as políticas e procedimentos adotados pela Gestora no sentido de preservar as atividades executadas.

Cumpre salientar que o processo de treinamento inicial e o programa de reciclagem continuada são controlados pelo Diretor de Compliance e exigem o comprometimento total dos Colaboradores quanto a sua assiduidade e dedicação.

Cabe ainda destacar, o disposto na RCVM nº 50, no Art. 7º, C, II, em que o Diretor de PLD deve manter treinamento contínuo para seus colaboradores, específico para Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo.

O treinamento deve ser realizado utilizando-se linguagem clara, acessível e ser compatível com as funções desempenhadas e com a sensibilidade das informações a que têm acesso aqueles que participam do programa. O treinamento terá periodicidade mínima anual.

Programas De Treinamento: Um programa eficaz de treinamento inclui disposições para assegurar que:

a) O treinamento seja contínuo, incorporando eventos atuais e mudanças nos códigos, políticas e produtos da Gestora, bem como Leis e regulamentos que digam respeito a sua atividade; e
b) O treinamento se concentra em instruir os Colaboradores da Gestora quanto às políticas e valores da empresa, dispondo ainda sobre as consequências do descumprimento das mesmas.

9. SEGREGAÇÃO DAS ATIVIDADES

Atualmente, a Gestora desempenha apenas atividades voltadas para a administração de carteiras de valores mobiliários, representada pela gestão de fundos de investimento, sendo tal atividade exaustivamente regulada pela CVM.

A atividade de gestão de recursos exige credenciamento específico e está condicionada a uma série de providências, dentre elas a segregação total de suas atividades de administração de carteiras de valores mobiliários de outras que futuramente possam vir a ser desenvolvidas (com exceção da distribuição de cotas de fundos de investimento dos quais é gestora, conforme regulamentação em vigor) pela Gestora ou empresas controladoras, controladas, ligadas ou coligadas, bem como prestadores de serviços.

Neste sentido, a Gestora, sempre que aplicável, assegurará aos Colaboradores, seus clientes e às autoridades reguladoras, a completa segregação de suas atividades, adotando procedimentos operacionais objetivando a segregação física de instalações entre a Gestora e empresas responsáveis por diferentes atividades prestadas no mercado de capitais.

Todas e quaisquer informações e/ou dados de natureza confidencial (incluindo, sem limitação, todas as informações técnicas, financeiras, operacionais, econômicas, bem como demais informações comerciais) referentes à Gestora, suas atividades e seus clientes e quaisquer cópias ou registros dos mesmos, orais ou escritos, contidos em qualquer meio físico ou eletrônico, que tenham sido direta ou indiretamente fornecidos ou divulgados em razão da atividade de administração de carteiras de valores mobiliários desenvolvida pela Gestora, não deverão ser divulgadas a terceiros sem a prévia e expressa autorização do Diretor de Compliance.

Dessa forma, todos os Colaboradores deverão respeitar as regras estabelecidas neste Manual e guardar o mais completo e absoluto sigilo sobre as informações que venham a ter acesso em razão do exercício de suas atividades.

A Gestora deve exercer suas atividades com lealdade e boa-fé em relação aos seus clientes, evitando práticas que possam ferir a relação fiduciária com eles mantida.

Portanto, quando do exercício de suas atividades, os Colaboradores devem atuar com a máxima lealdade e transparência com os clientes. Isso significa, inclusive, que diante de uma situação de potencial conflito de interesses, a Gestora deverá informar ao cliente que está agindo em conflito de interesses e as fontes desse conflito, sem prejuízo do dever de informar após o surgimento de novos conflitos de interesses.

A coordenação das atividades de administração de carteiras de valores mobiliários é uma atribuição do Diretor de Gestão da Gestora, conforme indicado em seu Formulário de Referência.

5. 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.

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 do Diretor de Compliance, que será a responsável inclusive por sua revisão, realização de testes e treinamento dos Colaboradores, conforme aqui descrito.

5.1. 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: 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; 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.

5.2. Ações de Prevenção e Proteção

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

- 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 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 a Equipe de Compliance 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.

Ademais, fica terminantemente proibido que os Colaboradores discutam ou acessem remotamente Informações Confidenciais.

Qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora, pois pode conter informações restritas e confidenciais mesmo no ambiente interno da Gestora.

A Gestora não mantém arquivo físico centralizado, sendo cada Colaborador responsável direto pela boa conservação, integridade e segurança de quaisquer informações em meio físico que tenha armazenadas consigo.

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 ou deficiência física), obsceno, pornográfico ou ofensivo é terminantemente proibida.

- Acesso Escalonado

O acesso como "administrador" de área de *desktop* é limitado aos usuários aprovados pelo Diretor de Compliance 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 ao Diretor de Compliance.

- 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.

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 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 expressa de Colaboradores autorizados pelos administradores da Gestora ou pelo Diretor de Compliance.

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 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 é responsável por patches regulares nos sistemas da Gestora.

A Gestora mantém e testa regularmente medidas de backup consideradas apropriadas pelo Diretor de Compliance. As informações da Gestora são atualmente objeto de backup

diário com o uso de computação na nuvem.

5.3. Monitoramento e Testes

A Equipe de Compliance 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.

Os monitoramentos acima poderão ser conduzidos conjuntamente com os monitoramentos indicados no item 1.4 deste Manual.

A Equipe de Compliance poderá adotar medidas adicionais para monitorar os sistemas de computação e os procedimentos aqui previstos para avaliar o seu cumprimento e sua eficácia.

5.4. Plano de Identificação e Resposta

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

- Procedimentos de Resposta

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

5.5. Arquivamento de Informações

De acordo com o disposto neste Manual, 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, em conformidade com o inciso IV do Artigo 18 da Resolução CVM 21/21.

5.6. 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 III** 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.

5.7. Revisão da Política

O Diretor de Compliance realizará uma revisão desta Política de Segurança da Informação e Segurança Cibernética **anualmente**, 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.

5.8. 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) fomento de atividades de engajamento social dos Colaboradores.

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.

6. POLÍTICA DE ANTICORRUPÇÃO

6.1. Introdução e Abrangência das Normas de Anticorrupção

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.

6.2. 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.

Ainda pela Lei de Anticorrupção, as sanções previstas para a pessoa jurídica responsabilizada pelos atos ilícitos apresentados anteriormente são:

I. Perdimento dos bens, direitos ou valores que representem vantagem ou proveito direta ou indiretamente obtidos da infração, ressalvado o direito do lesado ou de terceiro de boa-fé;
II. Suspensão ou interdição parcial de suas atividades;
III. Dissolução compulsória da pessoa jurídica;
IV. Proibição de receber incentivos, subsídios, subvenções, doações ou empréstimos de órgãos ou entidades públicas e de instituições financeiras públicas ou controladas pelo poder público, pelo prazo mínimo de 1 (um) e máximo de 5 (cinco) anos.

6.3. Normas de Conduta

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

6.4. Proibição de Doações Eleitorais

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

6.5. 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 o Diretor de Compliance e PLD imediatamente após sua ocorrência.

6.6. Procedimentos e Programa de Integridade

A Gestora utiliza seus melhores esforços para monitorar todos os Colaboradores da instituição, de forma a garantir que os mesmos atuem em observância a Lei de Anticorrupção e sua regulamentação, respeitando e praticando, na medida de suas atividades e possibilidades, os atos referentes ao Programa de Integridade.

Tal monitoramento é fundamental, pois também é responsabilidade de todos os Colaboradores proteger a empresa de atividades de corrupção e suborno, de forma que não serão tolerados comportamentos omissos sobre a questão ou envolvimento nesses tipos de atividade.

Diante disso, constituem parâmetros do Programa de Integridade da Gestora as seguintes medidas:

I. Comprometimento dos sócios da Gestora com o Programa de Integridade;
II. Políticas de conduta e ética que são aplicadas para todos os Colaboradores da Gestora, inclusive a terceiros, quando necessário, vide Código de Ética;
III. Treinamento periódico dos Colaboradores, vide Política de Treinamento e Reciclagem dos Colaboradores;
IV. Registros contábeis que reflitam as transações da Gestora de forma precisa e completa, feitos por empresa especializada externa;
V. Independência dos procedimentos de Compliance;
VI. Fácil comunicação de irregularidades para quaisquer Colaboradores ou terceiros;
VII. Medidas disciplinares executadas contra aqueles que violarem as normas da Gestora, ou cometerem qualquer tipo de infração corruptiva listada acima; e
VIII. Prévia Due Diligence antes de contratação de terceiros.

Ademais, conforme mencionado nas alíneas acima, a Gestora não aceita em hipótese alguma a prática de qualquer das infrações apontadas no capítulo anterior, devendo os seus Colaboradores informar imediatamente ao Diretor de Compliance e PLD, o

conhecimento de qualquer atividade que se enseje na caracterização das infrações da Lei de Anticorrupção.

Por fim, todos os Colaboradores são instruídos a ler essa política e a assinar o "Termo de Recebimento e Compromisso", anexado ao Código de Ética, que traz a hipótese de desligamento imediato da Gestora por justa causa, caso algum dos Colaboradores exerça algum ato de suborno ou de corrupção, conforme dispõe o subitem anterior e a Lei de Anticorrupção.

7. POLÍTICA DE CERTIFICAÇÃO

7.1. Introdução

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

7.2. Atividades Elegíveis e Critérios de Identificação.

Tendo em vista a atuação da Gestora como gestora de recursos de terceiros de classes reguladas pela Instrução CVM 175, de 23 de dezembro de 2022, conforme alterada, a Gestora identificou, segundo o Código ANBIMA de Certificação, que a Certificação de Gestores ANBIMA ("CGA") é a certificação pertinente às suas atividades, sendo a CGA aplicável aos profissionais da Gestora com alçada/poder discricionário de investimento.

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 CGA.

Os profissionais que atuam na Gestão de Patrimônio Financeiro realizando contato comercial com o investidor, assessorando suas decisões de investimento devem deter uma das seguintes certificações: CEA; CFP, CFA III; CGA ou CGE.

Em complemento, a Gestora destaca que as certificações são pessoais e intransferível.

Desse modo, a Gestora assegurará que os Colaboradores que atuem na atividade elegível 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.

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

Antes da contratação, admissão ou transferência de área de qualquer Colaborador, a Equipe de Compliance 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.

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

A Equipe de Compliance 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.

A Equipe de Compliance 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.

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 pela Equipe de Compliance, conforme disposto abaixo.

7.4. Rotinas de Verificação

Mensalmente, a Equipe de Compliance 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 Equipe de Compliance a fim de informá-los, prontamente, caso haja algum tipo de alteração nos cargos e funções dos Colaboradores que integram o departamento técnico envolvido na gestão de recursos e contato com os clientes ou potenciais clientes, confirmando, além disso, todos aqueles Colaboradores que atuem com alçada/poder discricionário de investimento, se for o caso, bem como que possam realizar o contato diretamente junto a investidores, se for o caso.

Colaboradores que não tenham CGA (e que não tenham a isenção 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. Já os Colaboradores que não tenham CEA; CFP, CFA III; CGA ou CGE estão impedidos de assessorar os investidores.

Ademais, no curso das atividades de compliance e fiscalização desempenhadas pela Equipe de Compliance, 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 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 ANBIMA de Certificação, sendo que as análises e eventuais recomendações, se for o caso, deverão ser objeto do relatório anual de compliance.

7.5. Inscrição para Obtenção da Certificação

Os Colaboradores contratados ou que foram transferidos internamente para outra atividade e/ou área, devem se comunicar com a área de Compliance sobre eventuais dúvidas a respeito do processo de certificação.

O profissional deve se inscrever no site de certificação da ANBIMA e escolher a melhor data disponível para agendar a prova. O profissional ficará responsável por todo o processo, desde a sua inscrição, cadastro nos respectivos sites e o pagamento dos custos da certificação.

O Diretor de Compliance acompanhará juntamente com o responsável da área elegível a regularização do profissional.

7.6. 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, §1ª, inciso V do Código ANBIMA de Certificação, imediatamente afastados das atividades elegíveis aplicáveis, até que se certifiquem.

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

7.7. Exceções

Para os casos de exceção ao cumprimento das regras previstas nesta Política, o solicitante deverá apresentar pedido de exceção à área de Compliance com as razões que o fundamentam. A aprovação ficará a critério do Diretor de Compliance.

8. CONFLITOS DE INTERESSE

De forma a evitar possíveis conflitos de interesse, uma vez constatado a incidência ou possibilidade de qualquer conflito, o Diretor de Compliance terá comunicação direta com os administradores e sócios da Gestora para realizar relato dos resultados decorrentes das atividades relacionadas a suas funções, incluindo possíveis irregularidades ou falhas identificadas.

Uma vez que os sócios da Gestora podem dispor de participação societária em outras instituições, sempre que for identificado qualquer potencial conflito de interesses, o Diretor de Compliance convocará o Comitê de Compliance onde os impactos e os mitigadores serão identificados e definidos.

Adicionalmente, a Gestora entende que eventuais acordos e transações com instituições que seus sócios tenham participação societária, encontram-se em potencial conflito de interesses, devendo ser evitadas.

Caso algum acordo ou transação seja considerado a melhor oportunidade para seus cotistas, visando a transparência e ética, os cotistas dos veículos geridos serão sempre previamente informados sobre o potencial conflito de interesses, sendo que tais transações só poderão ocorrer se aprovadas em assembleia de cotistas.

9. CONFLITOS DE INTERESSE – ACORDO DE REMUNERAÇÃO

Na hipótese de existir acordo de remuneração com base na taxa de administração, performance ou gestão, que deve ser paga diretamente pela classe investida a classes investidoras dos fundos de investimento da Gestora, nos termos do inciso XVII do art. 117 da Resolução CVM nº 175/22, o valor das correspondentes parcelas das taxas de administração ou gestão deve ser subtraído e limitado aos valores destinados pela classe investida ao provisionamento ou pagamento das despesas com as referidas taxas.

A Gestora controlará para que o acordo de remuneração não resulte em desconto, abatimento ou redução de taxa de administração, performance, gestão ou qualquer outra taxa devida pela classe investidora à investida dos fundos de investimento sob gestão.

10. DISPOSIÇÕES GERAIS

Em cumprimento ao art. 16, III, da Resolução CVM n.º 21/2021, a presente Política está disponível no endereço eletrônico disponibilizado pela Gestora para tal fim.

Eventuais comunicações para a Área de Compliance devem ser enviadas para o Diretor de *Compliance*.

11. VIGÊNCIA E ATUALIZAÇÃO

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

Histórico das atualizações		
Data	Versão	Responsável
Setembro de 2023	1ª Versão	Diretor de Compliance
Agosto de 2024	2ª Versão	RRZ Consultoria

ANEXO I
PRINCIPAIS NORMATIVOS APLICÁVEIS ÀS ATIVIDADES DA STEN GESTÃO PATRIMONIAL LTDA.

1. Resolução CVM nº 50, de 31 de agosto de 2021;
2. Resolução CVM nº 175, de 23 de dezembro de 2022;
3. Resolução CVM nº 21, de 25 de fevereiro de 2021;
4. Ofício-Circular/CVM/SIN/Nº 05/2014;
5. Código ANBIMA de AGRT;
6. Regras e Procedimentos do AGRT;
7. Código ANBIMA de Certificação;
8. Código ANBIMA de Ética;
9. Lei nº 12.846, de 1º de agosto de 2013;
10. Decreto nº 11.129, de 11 de julho de 2022; e
11. Lei 9.613/98, conforme alterada.