ORGANON CAPITAL GESTÃO DE INVESTIMENTOS LTDA.

MANUAL DE CONTROLES INTERNOS

Versão: 04 – Agosto 2024

ÍNDICE

INTRODUÇÃO

1.1. Sumário

Este Manual de Controles Internos ("Manual"), elaborado em conformidade com o disposto na Resolução CVM nº 21/2021, conforme alterada ("CVM 21"), demais orientações da CVM, no Código ANBIMA de Administração e Gestão de Recursos de Terceiros ("Código ANBIMA de AGRT") e suas respectivas regra e procedimentos do Código ANBIMA AGRT e Deveres Básicos ("RP Deveres Básicos ANBIMA"), bem como o Código ANBIMA de Certificação ("Código ANBIMA de Certificação"), tem por objetivo estabelecer normas, princípios, conceitos e valores que orientam a conduta de todos aqueles que possuam cargo, função, posição, relação societária, empregatícia, comercial, profissional, contratual ou de confiança ("Colaboradores") com a **Organon Capital Gestão de Investimentos Ltda.** ("Gestora"), tanto na sua atuação interna quanto na comunicação com os diversos públicos.

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

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

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

A Gestora mantém versões atualizadas do presente Manual em seu website (www.organoncapital.com.br), juntamente com os seguintes documentos: (i) Formulário de Referência, conforme Anexo E da CVM 21/2021; (ii) Política de Gestão de Risco; (iii) Política de Rateio e Divisão de Ordens; e (iv) Política de Exercício de Direito de Voto.

Ademais, este Manual de Controles Internos ficará disponível em um diretório específico da rede interna (nuvem) da Gestora sendo de fácil acesso a todos colaboradores o acesso para consulta.

A Gestora manterá armazenado todos os arquivos eletronicamente, pertinentes a este Manual e aos processos descritos nas políticas que contemplam este Manual, pelo prazo mínimo de 05 (cinco) anos, conforme legislação vigente.

1.2. Aplicabilidade do Manual

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

1.3. Ambiente Regulatório

Este Manual é parte integrante das regras que regem a relação societária ou de trabalho dos Colaboradores, os quais, ao assinar o termo de recebimento e compromisso constante do **Anexo I** a este Manual ("Termo de Recebimento e Compromisso"), estão aceitando expressamente as normas, princípios, conceitos e valores aqui estabelecidos.

Todos os Colaboradores devem se assegurar do perfeito entendimento das leis e normas aplicáveis à Gestora bem como do completo conteúdo deste Manual. Para melhor referência dos Colaboradores, as principais normas aplicáveis às atividades da Gestora foram apontadas no **Anexo IV** do presente Manual.

1.4. Termo de Compromisso

Todo Colaborador, ao receber este Manual, firmará o Termo de Recebimento e Compromisso. Por meio desse documento, o Colaborador reconhece e confirma seu conhecimento e concordância com os termos deste Manual e com as normas, princípios, conceitos e valores aqui contidos; comprometendo-se a zelar pela aplicação das normas de Compliance e princípios nele expostos. Periodicamente, poderá ser requisitado aos Colaboradores que assinem novos Termos de Recebimento e Compromisso, reforçando o conhecimento e concordância com os termos deste Manual.

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

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

POLÍTICA DE COMPLIANCE

1. Introdução

1.1 Responsabilidades e Obrigações

A coordenação direta das atividades relacionadas a este Manual é uma atribuição do diretor estatutário da Gestora indicado como diretor responsável pelo cumprimento de regras, políticas, procedimentos e controles internos da Gestora, bem como pelo cumprimento normas de prevenção e combate à lavagem de dinheiro, ao financiamento do terrorismo e da proliferação de armas de destruição em massa ("Diretor de Compliance, Risco e PLD"), nos termos da CVM 21/2021 e da Resolução CVM nº 50/2021, conforme alterada ("CVM 50/2021"), de acordo com as diretrizes do Código Anbima de Administração e Gestão de Recursos de Terceiros ("Código ANBIMA de AGRT") e suas respectivas Regras e Procedimentos de Deveres Básicos ("RP Deveres Básicos ANBIMA").

São obrigações do Diretor de Compliance, Risco e PLD:

(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 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 Comissão de Valores Mobiliários ("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 à Alta 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; 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.

Todo e qualquer Colaborador que souber de informações ou situações em andamento, que possam afetar os interesses da Gestora, gerar conflitos ou, ainda, se revelarem contrárias aos termos previstos neste Manual, deverá informar o Diretor de Compliance, Risco e PLD, para que sejam tomadas as providências cabíveis.

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

Os Colaboradores que desempenharem as atividades de risco e *compliance* formarão a Área de Compliance e Risco, sob a coordenação do Diretor de Compliance, Risco e PLD, sendo certo que a Área de Compliance e Risco exerce suas atividades de forma completamente independente das outras áreas da Gestora e poderá exercer seus poderes e autoridade com relação a qualquer Colaborador.

Em cumprimento ao Inciso III do Artigo 16 da Resolução CVM nº 21/21, a presente Política de Compliance vigente e suas alterações, estarão sempre disponíveis para consulta no seguinte endereço eletrônico: https://www.organoncapital.com.br/empresa.

1.2 Comitê de Compliance e Risco

O Comitê de Compliance e Risco tem como composição mínima o Diretor de Compliance, Risco e PLD, os colaboradores da área e o Diretor de Investimentos e é realizado, no mínimo, anualmente.
Todas as decisões e deliberações do Comitê de Compliance e Risco são registradas em ata ou e-mail.

A Área de Compliance e Risco atua segregada da área de Gestão, de forma independente e com autonomia.

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.

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

Mesmo que haja apenas a suspeita de uma potencial situação de conflito ou ocorrência de uma ação que vá afetar os interesses da Gestora, o Colaborador deverá seguir essa mesma orientação. Esta é a maneira mais transparente e objetiva para consolidar os valores da cultura empresarial da Gestora e reforçar os seus princípios éticos.

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

1.4 Acompanhamento das Políticas descritas neste Manual

Mediante ocorrência de descumprimento, suspeita ou indício de descumprimento de quaisquer das regras estabelecidas neste Manual, no Código de Ética, assim como nas demais Políticas da Gestora ou quaisquer outros documentos aplicáveis às atividades da Gestora, que cheguem ao conhecimento do Diretor de Compliance, Risco e PLD, de acordo com os procedimentos estabelecidos neste Manual, o Diretor de Compliance, Risco e PLD utilizará os registros e sistemas de monitoramento eletrônico referidos neste Manual para verificar a conduta dos Colaboradores envolvidos.

Caso haja necessidade, todo conteúdo que está na rede será acessado pelo Diretor de Compliance, Risco e PLD, inclusive arquivos pessoais salvos em cada computador serão acessados caso o Diretor de Compliance, Risco e PLD julgue necessário. Da mesma forma, mensagens de correio eletrônico e ligações telefônicas de Colaboradores serão gravadas e, quando necessário, interceptadas e escutadas, sem que isto represente invasão da privacidade dos Colaboradores já que são ferramentas de trabalho disponibilizadas pela Gestora.

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

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

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

1.5 Sanções (“*Enforcement*”)

A eventual aplicação de sanções decorrentes do descumprimento dos princípios estabelecidos neste Manual é de responsabilidade do Diretor de Compliance, Risco e PLD, conforme por este definido, garantido ao Colaborador, contudo, amplo direito de defesa. As sanções poderão ser aplicadas, sem prejuízos do direito da Gestora de pleitear indenização pelos eventuais prejuízos suportados, perdas e danos e/ou lucros cessantes, por meio das medidas legais cabíveis, sempre que aplicáveis.

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

1.6 Dever de Reportar

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

1.7 Vigência e Atualizações

A Política de Compliance entra em vigor na data de sua publicação e permanece vigente devendo ser mantido atualizado. Deverá ser revista por prazo não superior a 24 (vinte e quatro) meses ou em prazo inferior se exigido pela regulação 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.

2. Políticas de Confidencialidade

2.1. Sigilo e Conduta

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

Todos os Colaboradores deverão ler atentamente e entender o disposto neste Manual, bem como deverão firmar o termo de confidencialidade, conforme modelo constante no Anexo II ("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 IV 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:

a) *Know-how*, técnicas, cópias, diagramas, modelos, amostras, programas de computador;
b) Informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e dos fundos geridos pela Gestora;
c) Operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento geridos pela Gestora;

d) Estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços;
e) 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;
f) Informações a respeito de resultados financeiros antes da publicação dos balanços, balancetes e/ou demonstrações financeiras dos fundos de investimento;
g) Transações realizadas e que ainda não tenham sido divulgadas publicamente; e
h) 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, 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.

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, 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 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.

2.2. Vedações - Negociação Com Uso Indevido De Informação Privilegiada

De acordo com a Resolução CVM 175, de 23 de dezembro de 2022 (“Resolução CVM 175”) é vedada negociação com uso indevido de informação privilegiada, na utilização de informação relevante ainda não divulgada, por qualquer pessoa que a ela tenha tido acesso, com a finalidade de auferir vantagem, para si ou para outrem, mediante negociação de cotas em mercados organizados.

Para fins de caracterização do ilícito, presume-se que:

a) A pessoa que negociou cotas dispondo de informação relevante ainda não divulgada fez uso de tal informação na referida negociação;
b) Os diretores do gestor que participam de decisões relacionadas à gestão da carteira de ativos têm acesso a toda informação relevante ainda não divulgada a respeito do fundo;
c) O diretor do administrador que é responsável pelo fundo, no âmbito de sua esfera de atuação, tem acesso a informações relevantes ainda não divulgadas a respeito do fundo;
d) Os cotistas que participem das decisões relacionadas à gestão da carteira de ativos têm acesso a toda informação relevante ainda não divulgada a respeito da classe da

qual são cotistas;

e) As pessoas listadas nos incisos b, c e d, bem como aqueles que tenham relação comercial, profissional ou de confiança com o fundo, ao terem tido acesso à informação relevante ainda não divulgada ao mercado, sabem que se trata de informação privilegiada; e
f) O prestador de serviços que se afasta ou é afastado do fundo dispondo de informação relevante e ainda não divulgada se vale de tal informação caso negocie cotas no período de 3 (três) meses contados do seu afastamento.

As presunções para fins de caracterização do ilícito, devem:

a) Ser relativas e devem ser analisadas em conjunto com outros elementos que indiquem se o ilícito previsto no caput foi ou não, de fato, praticado; e
b) Podem, se for o caso, ser utilizadas de forma combinada.
c) A proibição não se aplica a subscrições de novas cotas, sem prejuízo da incidência das regras que dispõem sobre a divulgação de informações no contexto da emissão e distribuição de cotas.

2.3. Vigência e Atualizações

A Política de Confidencialidade entra em vigor na data de sua publicação e permanece vigente devendo ser mantido atualizado. Deverá ser revista por prazo não superior a 24 (vinte e quatro) meses ou em prazo inferior se exigido pela regulação 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.

3. Políticas de Conflito de Interesses e Segregação das Atividades

3.1. Objetivo e Definição

A Gestora desempenha exclusivamente atividades voltadas para a administração de carteiras de valores mobiliários e distribuição de fundos sob gestão própria, representada pela gestão e distribuição de fundos de investimento, as quais são exaustivamente reguladas pela CVM.

Tal atividade exige credenciamento específico e está condicionada a uma série de providências, dentre elas a segregação total de suas atividades de outras que futuramente possam vir a ser desenvolvidas 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 segregação de suas atividades, adotando procedimentos operacionais objetivando a segregação física de instalações, bem como a segregação lógica, garantindo inclusive a correta e segregada utilização de equipamentos e informações 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, desenvolvidas pela Gestora, não deverão ser divulgadas a terceiros sem a prévia e expressa autorização do Diretor de Compliance, Risco e PLD.

Neste sentido, todos os Colaboradores deverão respeitar as regras e segregações 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. Para tanto, cada Colaborador, ao firmar o Termo de Compromisso, atesta expressamente que está de acordo com as regras aqui estabelecidas e, por meio da assinatura do Termo de Confidencialidade, abstém-se de divulgar informações confidenciais que venha a ter acesso.

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 e fundos sob gestão própria são atribuições dos diretores estatutários da Gestora, conforme indicados em seu Formulário de Referência (“Diretor de Investimentos”) e (“Diretor de Distribuição”).

No âmbito das regulamentações aplicáveis à administração de carteiras, observadas as regras de cumulação descritas nas normas internas específicas aplicáveis às atividades de administração de carteiras, os Diretores Estatutários da Gestora têm suas responsabilidades atribuídas, conforme abaixo:

- para o cumprimento das atividades de administração de carteiras de títulos e

valores mobiliários, nos termos do artigo 4º, inciso III, da Resolução CVM nº 21/21, é atribuída responsabilidades da diretoria estatutária para o cumprimento das atividades de Gestão de Recursos, nomeada como Diretoria de Gestão de Recursos de Terceiros;

- para cumprimento das regras, procedimentos e controles internos (Diretoria de Compliance, Risco e PLD) nos termos do artigo 4º, inciso VI, da Resolução CVM nº 21/21, no caso acumula a responsabilidade pela gestão dos riscos nos termos do artigo 4º, inciso V, da Resolução CVM nº 21/21; e
- para cumprimento da diretoria estatutária com responsabilidade quanto à prevenção e combate à lavagem de dinheiro, nos termos da Resolução CVM nº 50/21, artigo 8º, que é cumulada pelo Diretor de Compliance, Risco e PLD.

A Gestora manterá seu cadastro atualizado dos Diretores nomeados como responsáveis, nos cadastros da CVM e ANBIMA, providenciando as alterações, de imediato, observando os prazos estabelecidos na regulamentação vigente e que os respectivos diretores responsáveis pela administração de carteiras de valores mobiliários, na categoria gestor de recursos, sejam autorizados pela CVM para prestar tais serviços e que, mantenham a condição de credenciados, em consonância com a regulamentação vigente.

3.2. Conflito de Interesses

Conflitos de interesse são situações decorrentes do desempenho das funções de determinado Colaborador, nas quais os interesses pessoais de tal Colaborador possam ser divergentes ou conflitantes com os interesses da Gestora e/ou entre os interesses diferentes de dois ou mais de seus clientes, para quem a Gestora tem um dever para cada um ("Conflito de Interesses").

O Colaborador tem o dever de agir com boa-fé e de acordo com os interesses dos investidores com o intuito de não ferir a relação fiduciária com o cliente. Para tal, o Colaborador deverá estar atento para uma possível situação de conflito de interesses, e sempre que tal situação ocorrer deverá informar, imediatamente, o Diretor de Compliance, Risco e PLD sobre sua existência e abster-se de consumar o ato ou omissão originador do Conflito de Interesse até decisão em contrário.

Em razão das atividades atualmente desempenhadas pela Gestora, conforme indicado no item anterior, a Gestora entende não existir qualquer conflito de interesses potencial ou efetivo a ser aqui tratado.

3.3. Vigência e Atualizações

A Política de Conflito de Interesses e Segregação das atividades, entra em vigor na data de sua publicação e permanece vigente devendo ser mantido atualizado. Deverá

ser revista por prazo não superior a 24 (vinte e quatro) meses ou em prazo inferior se exigido pela regulação 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.

4. Políticas de Treinamento

4.1 Treinamento e Processo de Reciclagem

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

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

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

4.2 Implementação e Conteúdo

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

Tanto o processo de treinamento inicial quanto o programa de reciclagem deverão abordar as atividades da Gestora, seus princípios éticos e de conduta, as normas de *compliance*, as políticas de segregação, quando for o caso, e as demais políticas descritas neste Manual (especialmente aquelas relativas à confidencialidade, segurança das informações, segurança cibernética e negociações pessoais), bem como as penalidades aplicáveis aos Colaboradores decorrentes do descumprimento de tais regras, além das principais leis e normas aplicáveis às referidas atividades, constantes do Anexo IV deste Manual.

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

5 Políticas de Segurança e Segurança Cibernética

Em atenção aos dispositivos da Resolução CVM nº 21/21, do Código ANBIMA de Administração e Gestão de Recursos de Terceiros, do Guia ANBIMA de Cibersegurança e da Lei Geral de Proteção de Dados Pessoais - Lei nº 13.709/2018, a Gestora formaliza por meio desta política os mecanismos de segurança da informação e segurança cibernética com a finalidade de assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados, bem como visa o processo de preservação e legalidade das informações.

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

As instalações da Gestora são protegidas por controles de entrada apropriados para assegurar a segurança dos Colaboradores e proteger o sigilo, a integridade e a disponibilidade da informação.

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

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

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

5.1 Ativos De Informação

A Gestora considera como ativos de informação todas as informações, disponíveis em qualquer meio, utilizadas ou manipuladas nas operações da empresa, bem como todos os sistemas, equipamentos e instalações onde estas informações são manuseadas ou armazenadas.

As informações podem ser apresentadas nas mais distintas formas escritas, faladas, transmitidas, digitadas, armazenadas ou processadas em qualquer equipamento, papel, telefone, programa de computador, base de dados ou outro meio existente. Seja qual for o estado ou o meio do qual a informação seja apresentada ou compartilhada, ela

deverá estar sempre protegida adequadamente, de acordo com as normas definidas neste documento.

5.2 Classificação Da Informação

As informações são classificadas de maneira a serem adequadamente protegidas quanto ao seu acesso e uso, sendo que, para aquelas consideradas de alta criticidade, são necessárias medidas especiais de tratamento. A classificação das informações deverá seguir a seguinte ordem:

(i) Pública: É uma informação da Gestora ou de seus clientes com linguagem e formato dedicado à divulgação ao público em geral, sendo seu caráter informativo, comercial ou promocional. É destinada ao público externo ou ocorre devido ao cumprimento de legislação vigente que exija publicidade.

(ii) Interna: É uma informação da Gestora que ela não tem interesse em divulgar, onde o acesso por parte de indivíduos externos à empresa deve ser evitado. Caso esta informação seja acessada indevidamente, poderá causar danos à imagem da organização, porém, não com a mesma magnitude de uma informação confidencial. Pode ser acessada sem restrições por todos os empregados e terceiros contratados da Gestora.

(iii) Confidencial: É uma informação crítica para os negócios da Gestora ou de seus clientes. A divulgação não autorizada dessa informação pode causar impactos de ordem financeira, de imagem, operacional ou, ainda, sanções administrativas, civis e criminais à Gestora ou aos seus clientes. É sempre restrita a um grupo específico de pessoas, podendo ser este composto por empregados, clientes e/ou fornecedores.

(iv) Privilegiada: É a informação relevante ainda não divulgada publicamente e que seja obtida de forma privilegiada (em decorrência da relação profissional ou pessoal mantida com um cliente, com pessoas vinculadas a empresas analisadas ou investidas ou com terceiros). As informações privilegiadas devem ser mantidas em sigilo por todos que a elas tiverem acesso, seja em decorrência do exercício da atividade profissional ou de relacionamento pessoal.

(v) Restrita: É toda informação que pode ser acessada somente por usuários da Gestora explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização.

Nenhuma informação interna, confidencial, privilegiada e restrita pode ou deve ser discutida por qualquer colaborador ou terceiro contratado pela Gestora, em locais inapropriados, como lugares públicos ou fechados, na presença de terceiros ou pessoas não diretamente relacionadas ao assunto, ou adiante daqueles sem autorização para

conhecimento dessas informações. Há impacto negativo e relevante na situação de vazamento desse tipo de informação.

Qualquer informação sobre a Gestora, ou de qualquer natureza relativa às atividades da Gestora e aos sócios, obtida em decorrência do desempenho das atividades normais dos Colaboradores, só poderá ser fornecida ao público, mídia ou a demais órgãos caso autorizado pelo Compliance.

A gestão dessas informações é realizada através de um processo de melhoria contínua, partindo dos seguintes mecanismos de supervisão:

(i) Classificação de informações: conforme mencionado no acima o acesso é restringido e são reforçados os mecanismos de controle e segurança de acordo com a criticidade e sensibilidade de cada dado;

(ii) Equipamentos e Estrutura: Os equipamentos utilizados para o desenvolvimento das atividades da Gestora devem estar sempre atualizados, regra que inclui sistema operacional, antivírus e firewalls, garantindo assim maior proteção às informações neles inseridas. Ainda os cuidados se estendem também à infraestrutura onde são armazenados os dados: que possuem cópias de segurança (backups) atualizadas periodicamente;

(iii) Armazenamento de Dados e Computação em Nuvem: Os serviços de armazenamento de dados e computação em nuvem que contratamos passam por uma seleção interna rígida que avalia a necessidade da terceirização do serviço em questão e a confiabilidade técnica do fornecedor analisado, a fim de garantir que ele possua as qualificações de segurança necessárias;

(iv) Gerenciamento de Acesso: Os acessos dados são restringidos a menor permissão e privilégio possíveis, possuindo a Gestora a capacidade para monitorar e registrar o acesso a dados classificados como dados pessoais e/ou sensíveis sendo exigida a mesma garantia de seus colaboradores e terceiros contratados, conforme Lei Geral de Proteção de Dados (Lei nº 13.709); e

(v) Capacitação e Atualização: Os colaboradores e os terceiros contratados passam por treinamentos periódicos referentes à prevenção e resposta à incidentes, bem como de melhores práticas de segurança da informação e cibernética, sendo realizadas ainda, avaliações buscando atingir o maior comprometimento de todos os nossos colaboradores.

Toda a informação coletada, gerada ou desenvolvida por qualquer colaborador e terceiro contratado constitui como ativo e propriedade intelectual da Gestora. Independente da forma apresentada, compartilhada ou armazenada, todas as informações devem ser utilizadas para uma finalidade específica e justificável, coberta pelos princípios desta Política.

Os princípios básicos da segurança da informação são:

(i) Confidencialidade: garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas;

(ii) Integridade: garantir que as informações sejam mantidas íntegras, sem modificações indevidas (acidentais ou propositais);

(iii) Disponibilidade: garantir que as informações estejam disponíveis a todas as pessoas autorizadas a tratá-las.

Outras características são: irrefutabilidade, autenticação e o controle de acesso. Os benefícios são evidentes ao reduzir os riscos com vazamentos, fraudes, erros, uso indevido, sabotagens, roubo de informações e diversos outros problemas que possam comprometer esses princípios básicos.

5.3 Contratação de Serviços de Processamento e Armazenamento de Dados em Nuvem

A Gestora irá verificar a capacidade e o potencial prestador de serviço, na contratação de serviços de processamento e armazenamento de dados em nuvem, incluindo, no mínimo:

(i) O acesso da Gestora aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;

(ii) A confidencialidade, a integridade, a disponibilidade e a recuperação das informações e dados processados ou armazenados pelo prestador de serviço;

(iii) A sua aderência a cerificações exigidas pela Gestora ou reguladores para a prestação do serviço a ser contratado, caso aplicável;

(iv) O provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

(v) A identificação e a segregação dos dados dos clientes, funcionários, colaboradores ou terceiros relevantes por meio de controles físicos ou lógicos;

(vi) A qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes, funcionários, colaboradores e terceiros relevantes.

Adicionalmente, a Gestora poderá utilizar o questionário de due diligence para contratação de serviço de processamento e armazenamento de dados e de computação em nuvem, no país ou no exterior, disponibilizado no site da ANBIMA.

5.4 Identificação de Riscos (*risk assessment*)

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

- 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 mobiliários sob sua gestão, e as comunicações internas e externas (por exemplo: correspondências eletrônicas e físicas);
- Sistemas: informações sobre os sistemas utilizados pela Gestora e as tecnologias desenvolvidas internamente e por terceiros, suas ameaças possíveis e sua vulnerabilidade;
- Processos e Controles: processos e controles internos que sejam parte da rotina das áreas de negócio da Gestora; e
- 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:

- *Malware* – softwares desenvolvidos para corromper computadores e redes (tais como: Vírus, Cavalo de Troia, *Spyware* e *Ransomware*);
- Engenharia social – métodos de manipulação para obter informações confidenciais (*Pharming*, *Phishing*, *Vishing*, *Smishing*, e *Acesso Pessoal*);
- Ataques de DDoS (*distributed denial of services*) e *botnets*: ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição;
- Invasões (*advanced persistent threats*): ataques realizados por invasores sofisticados utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Não se imitando aos riscos citados acima, a Gestora relaciona todos os processos e ativos relevantes, em seu processo de avaliação de riscos, incluindo equipamentos, sistemas e dados, necessários ao adequado funcionamento das atividades exercidas pela Gestora, de modo a identificar suas vulnerabilidades e possíveis cenários de ameaça.

Os possíveis impactos dependem ainda da rápida detecção e resposta após a identificação do ataque. Uma vez definidos os riscos, ações de prevenção e proteção deverão ser tomadas de acordo com esta política e conforme orientação do Diretor de Compliance, Risco e PLD.

A avaliação dos riscos e as ações de prevenção inerentes às atividades desempenhadas pela Gestora estão descritas no Anexo VI do presente Manual.

Com base no acima e, no que aplicável, no Plano de Contingência e Continuidade dos Negócios da Gestora, há a avaliação e definição do 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.

Por fim, a Gestora está devidamente preparada para a realização de atividades de maneira emergencial por meio de trabalho home office, em caso de indisponibilidade da sede, todos os colaboradores conseguem desempenhar suas atividades de maneira remota com acesso a nuvem da Gestora.

5.5 Ações de Prevenção e Proteção

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 disponibilizando-os somente aos Colaboradores que efetivamente estejam evolvidos no projeto que demanda o seu conhecimento e análise.

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

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

A troca de informações entre os Colaboradores da Gestora deve sempre se pautar no conceito de que o receptor deve ser alguém que necessita receber tais informações para o desempenho de suas atividades e que não está sujeito a nenhuma barreira que

impeça o recebimento daquela informação. Em caso de dúvida a Área de Compliance e Risco deve ser acionada previamente à revelação.

Neste sentido, os Colaboradores não deverão, em qualquer hipótese, deixar em suas respectivas estações de trabalho ou em outro espaço físico da Gestora qualquer documento que contenha Informação Confidencial durante a ausência do respectivo usuário, principalmente após o encerramento do expediente.

Cada Colaborador será responsável direto pela boa conservação, integridade e segurança de quaisquer informações em meio físico que tenha armazenadas consigo.

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.

A Gestora mantém arquivo em nuvem e 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.

A Gestora poderá utilizar o questionário de diligência para contratação de serviço de processamento e armazenamento de dados e de computação em nuvem, no país ou no exterior, disponibilizado no site da ANBIMA, quando aplicável.

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 disseminação 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.

Conforme estabelecido pela Gestora, todos os Colaboradores contratados que tenham vínculo com a Gestora, independente da forma de contratação, devem assinar, de forma manual ou eletrônica, o Termo de Confidencialidade, constante no Anexo II deste Manual, comprometendo-se a observar integralmente os termos desta Política de Segurança e Segurança Cibernética.

Estão dispensados de assinar o Termo de Confidencialidade os terceiros contratados que estejam enquadrados em prestadores de serviços contratados em nome dos veículos de investimentos (corretoras de títulos e valores mobiliários), que em seu contrato de prestação de serviço haja uma cláusula de confidencialidade, conforme estabelecido na política Credenciamento Política de Contratação de Terceiros.

A Gestora possui uma Política de Confidencialidade e a Política de Conflitos de Interesses e Segregação das atividades, reafirmam e tratam o compromisso da Gestora com os princípios da ética, transparência, segurança e respeito, com o adequado gerenciamento, acesso e preservação das informações confidenciais e privilegiadas de sua propriedade ou sob a guarda da Gestora.

A Política de Confidencialidade e a Política de Conflitos de Interesses e Segregação das atividades, são integrantes a esse Manual, conforme descritas nos Capítulos 2 e 3, porém são independentes e integrantes a esta Política de Segurança e Segurança Cibernética e nela todos os colaboradores e terceiros contratados possam verificar com maior detalhamento o tema abordado.

- Acesso Escalonado do Sistema

O acesso como “administrador” de área de desktop é limitado aos sócios e 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, periodicamente, conforme aviso fornecido pelo responsável pela área de informática.

Dessa forma, o Colaborador pode ser responsabilizado inclusive caso disponibilize intencionalmente 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 não 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 de forma escalonada, no que se refere a rede, diretório e e-mail, para os sócios e usuários autorizados.

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 expressa de Colaboradores autorizados pelos administradores da Gestora.

O acesso ao Data-Center é restrito aos sócios da Gestora.

Tendo em vista que a utilização de computadores, telefones, internet, e-mail e demais aparelhos se destina exclusivamente para fins profissionais, como ferramenta para o desempenho das atividades dos Colaboradores, a Gestora monitora a utilização de tais meios.

- *Firewall, Software*, Varreduras e *Backup*

A Gestora utiliza *hardwares* de *firewall* com estrutura de redundância, projetados 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 periódicas 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.

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.

5.6 Monitoramento e Testes

o Diretor de Compliance, Risco e PLD (ou pessoa por ele incumbida) tem as seguintes medidas e ferramentas disponíveis para monitorar determinados usos de dados e sistemas em um esforço para detectar acessos não autorizados ou outras violações potenciais, em base, no mínimo:

(i) Monitoramento, por amostragem, do acesso dos Colaboradores a sites, blogs, fotologs, webmails, entre outros, bem como os e-mails enviados e recebidos;
(ii) Monitoramento, por amostragem, das ligações telefônicas dos Colaboradores pertencentes às equipes de atendimento a clientes, distribuidores e mesa de operações, realizadas ou recebidas por meio das linhas telefônicas disponibilizadas pela Gestora para a atividade profissional desses Colaboradores; e
(iii) Verificação, por amostragem, das informações de acesso ao espaço do

escritório, a desktops, pastas e sistemas, de forma a avaliar sua aderência às regras de restrição de acesso e escalonamento.

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

Desta forma, ao realizar os procedimentos acima descritos, o Diretor de Compliance, Risco e PLD identificará, caso existam, Colaboradores detentores de informações confidenciais para responsabilização, em caso de vazamento.

Os testes de contingência serão realizados anualmente, de modo a permitir que a Gestora esteja preparada para a continuação de suas atividades, assim como a mitigar eventuais riscos operacionais ou reputacionais. Outras informações acerca dos testes de contingência estão descritas no documento Plano de Continuidade de Negócios. O documento possui maior detalhamento sobre o tema abordado.

5.7 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 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, poderão 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.

- Procedimentos de Resposta

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 responderá pelas 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.

5.8 Compromisso em Relação a Dados Pessoais

Todos os Dados Pessoais que a Gestora mantiver contato, seja como controladora ou operadora perante a classificação da Lei Geral de Proteção de Dados (Lei nº 13.709) serão classificadas como Informação Confidencial e deverão obedecer às premissas da Política de LGPD da Gestora. Todo Dado Pessoal que não tiver embasamento legal para ser tratado ou armazenado deverá ser excluído.

Os critérios próprios, as regras e procedimentos que tratem da privacidade e dos dados pessoais a que a Gestora tenha acesso, está descrito em um documento independente, porém integrante a esta Política de Segurança e Segurança Cibernética e nela todos os colaboradores e terceiros contratados possam verificar com maior detalhamento o tema abordado.

Qualquer solicitação em relação ao tratamento de dados pessoais ou de informações específicas relacionadas ao tratamento de dados pessoais, se faz necessário o envio um e-mail para leandro.neves@organoncapital.com.br.

5.9 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.

5.10 Propriedade Intelectual

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 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.

5.11 Treinamento

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

5.12 Divulgação

A Política de Segurança e Segurança Cibernética, normas e procedimentos relativos ao tratamento dos ativos de informação e/ou dados sigilosos será divulgada a todos os Colaboradores contratados que tenham vínculo com a Gestora, independente da forma de contratação, com o propósito de desenvolver e manter uma efetiva conscientização de segurança, assim como promover o seu fiel cumprimento. A presente Política será divulgada por intermédio de mensagem eletrônica (e-mail), assim como estará disponível em um diretório interno da Gestora, com total acesso a todos os colaboradores.

5.13 Revisão da Política

O Diretor de Compliance, Risco e PLD realizará uma revisão desta Política de Segurança da Informação e Segurança Cibernética, em prazo não superior a 24 (vinte e quatro) meses ou em prazo inferior sempre que necessário ou na ocorrência de algum fato relevante ou evento motive sua revisão antecipada, 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.

6 Vantagens, Benefícios e Presentes

6.1 Vantagens e Benefícios proibidos

Os Colaboradores não devem, direta ou indiretamente, nem para si nem para terceiros, solicitar, aceitar ou admitir dinheiro, benefícios, favores, presentes, promessas ou quaisquer outras vantagens que possam influenciar o desempenho de suas funções ou como recompensa por ato ou omissão decorrente de seu trabalho.

Os Colaboradores somente poderão aceitar, presentes, refeições ou outros benefícios, sem prévia autorização do Diretor de Compliance, Risco e PLD, nos seguintes casos:

(a) Refeição, que não possua valor suficientemente alto a ponto de influenciar o bom desempenho das funções do Colaborador;
(b) Material publicitário ou promocional até um valor de USD100 (cem dólares americanos) distribuídos no curso normal dos negócios;
(c) Qualquer presente ou benefício com valor não superior a USD100 (cem dólares americanos) habitualmente oferecidos na ocasião de um aniversário ou outra ocasião semelhante, que não seja incomum;
(d) Qualquer presente ou benefício com valor de até USD100 (cem dólares americanos);
(e) Presente da família ou amigos não ligados com os deveres e responsabilidades profissionais.

Caso o benefício ou presente não se enquadrar nos dispostos acima, o Colaborador somente poderá aceitá-lo mediante prévia autorização do Diretor de Compliance, Risco e PLD.

6.2 *Soft Dollar*

Em termos gerais, *Soft Dollar* pode ser definido como sendo o benefício econômico, de natureza não pecuniária, eventualmente concedido à Gestora por corretoras de títulos e valores mobiliários ou outros fornecedores (“Fornecedores”), em contraprestação ao direcionamento de transações dos fundos de investimento geridos pela Gestora, para fins de auxílio no processo de tomada de decisões de investimento em relação aos respectivos fundos.

Tais benefícios não devem apresentar caráter pecuniário e devem ser utilizados pelos representantes da Gestora exclusivamente em benefício dos clientes, como ferramentas de auxílio da avaliação, seleção e decisão de investimento e suporte à gestão dos fundos de investimento geridos pela Gestora.

A Gestora não deverá selecionar seus Fornecedores considerando somente os benefícios recebidos por meio de acordos de *Soft Dollar*, mas deverá levar em consideração, primordialmente, a eficiência, produtividade ou menores custos oferecidos por tais Fornecedores.

A Gestora, por meio de seus representantes, deverá observar os seguintes princípios e regras de conduta ao firmar acordos de *Soft Dollar*:

(i) Colocar os interesses dos clientes acima de seus próprios interesses;
(ii) Definir de boa-fé se os valores pagos pelos clientes e, consequentemente, repassados aos Fornecedores, são razoáveis em relação aos serviços de execução de ordens ou outros benefícios que esteja recebendo;
(iii) Ter a certeza de que o benefício recebido auxiliará diretamente no processo de tomada de decisões de investimento em relação ao veículo que gerou tal benefício, devendo alocar os custos do serviço recebido de acordo com seu uso, se o benefício apresentar natureza mista;
(iv) Divulgar amplamente a clientes, potenciais clientes e ao mercado os critérios e políticas adotadas com relação às práticas de *Soft Dollar*, bem como os potenciais conflitos de interesses oriundos da adoção de tais práticas;
(v) Cumprir com seu dever de lealdade, transparência e fidúcia com os clientes;
(vi) Transferir à carteira dos clientes qualquer benefício ou vantagem que possa alcançar em decorrência de sua condição de Gestora de carteira de valores mobiliários, conforme disposto no Artigo 20, inciso II da CVM 50/2021.

Os acordos de *Soft Dollar* devem ser transparentes e mantidos por documento escrito. A Gestora deverá manter registros dos benefícios recebidos, identificando, se possível, a capacidade de contribuírem diretamente para o processo de tomada de decisões de investimento, visando comprovar o racional que levou a firmar tais acordos de *Soft Dollar*.

Ao contratar os serviços de execução de ordens, a Gestora não buscará somente o menor custo, mas o melhor custo-benefício, em linha com os critérios de *best execution* estabelecidos no mercado internacional, devendo ser capaz de justificar e comprovar que os valores pagos aos Fornecedores com que tenha contratado *Soft Dollar* são favoráveis aos fundos de investimento sob sua gestão comparativamente a outras corretoras, considerados para tanto não apenas os custos aplicáveis, mas também a qualidade dos serviços oferecidos, que compreendem maior eficiência na execução de transações, condições de segurança, melhores plataformas de negociação,

atendimento diferenciado, provimento de serviço de análise de ações e qualidade técnica dos materiais correspondentes, disponibilização de sistemas de informação, entre outros.

Caso o benefício seja considerado de uso misto, os custos deverão ser alocados de forma razoável, de acordo com a utilização correspondente.

Quaisquer benefícios não relacionados ao processo de tomada de decisão de investimentos, tais como pagamento de despesas de escritório, viagens, entretenimento, entre outros, não devem ser objeto de acordos de *Soft Dollar*.

Os acordos de *Soft Dollar* não devem gerar qualquer vínculo de exclusividade ou de obrigação de execução de volume mínimo de transações os Fornecedores, devendo a Gestora manter a todo tempo total independência para selecionar e executar com quaisquer Fornecedores operações em nome dos fundos de investimento sob gestão, sempre de acordo as melhores condições para seus clientes.

7 Política de Sustentabilidade

A Gestora adota 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) incentivo à utilização de meios de transporte alternativos ou de menor impacto ambiental por seus Colaboradores, como transportes coletivos, caronas ou bicicletas.

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

Apesar da Gestora adotar práticas e ações sustentáveis para minimizar eventuais impactos ambientais, esclarecemos que a Gestora não possuem fundos de investimentos que interagem a fundos com questões ESG e/ou Fundos Investimentos Sustentáveis (“IS”), conforme diretrizes determinadas no documento Regras e Procedimentos para Investimentos em Ativos Sustentáveis, vinculadas ao Código de Administração e Gestão Recursos de Terceiros (“Código AGRT”).

8 Política de Anticorrupção

8.1 Introdução

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

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

8.2 Abrangência das Normas de Anticorrupção

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

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

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

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

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

8.3 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.

8.4 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.

8.5 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, podendo realizar doações, desde que respeitadas as normas de Anticorrupção.

8.6 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 um dos seus Diretores, 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.

8.7 Vigência e Atualizações

A Política Anticorrupção entra em vigor na data de sua publicação e permanece vigente devendo ser mantido atualizado. Deverá ser revista por prazo não superior a 24 (vinte e quatro) meses ou em prazo inferior se exigido pela regulação 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.

POLÍTICA DE CERTIFICAÇÃO

1.1. Introdução

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

Os profissionais certificados devem estar em conformidade com os requisitos descritos abaixo:

- Possuir reputação ilibada;
- Exercer suas atividades com boa-fé, transparência, diligência e lealdade;
- Agir de acordo com as normas de conduta ética e profissional;
- Cumprir suas obrigações, devendo empregar, no exercício de suas atividades, o cuidado que toda pessoa prudente e diligente costuma dispensar à administração de seus próprios negócios, respondendo por quaisquer infrações ou irregularidades que venham a ser cometidas;
- Preservar as informações reservadas ou privilegiadas que lhes tenham sido confiadas em virtude do exercício de suas atividades, a menos que a sua divulgação seja exigida por lei ou tenha sido expressamente autorizada;
- Manter elevados padrões éticos, adotar práticas transparentes nas negociações com o mercado e proibir práticas caracterizadoras de concorrência desleal e de condições não equitativas;
- Não permitir a intermediação de investimentos ilegais e não participar de qualquer negócio que envolva fraude ou corrupção, manipulação ou distorção de preços, declarações falsas ou lesão aos direitos de investidores;
- Ser diligente e não contribuir para a veiculação ou circulação de notícias ou de informações inverídicas ou imprecisas sobre o mercado financeiro e de capitais;
- Zelar para que não sejam dadas informações imprecisas a respeito das atividades que é capaz de prestar, bem como com relação a suas qualificações, seus títulos acadêmicos e experiência profissional; e
- Cumpram com o disposto neste Código e nos Códigos ANBIMA das Atividades Elegíveis as quais exerçam, como o Código de Administração e Gestão de Recursos de Terceiros.

1.2. Atividades Elegíveis e Critérios de Identificação.

Tendo em vista a atuação da Gestora como gestora de recursos de terceiros e distribuidora de fundos sob gestão própria, foi identificado, segundo o Código ANBIMA de Certificação, que a Certificação de Gestores ANBIMA ("CGA") e Certificação Profissional ANBIMA Série 20 ("CPA 20) são as certificações pertinentes às suas atividades, sendo a CGA aplicável aos profissionais da Gestora com alçada/poder discricionário de investimento e o CPA 20 aplicável aos profissionais da Gestora que atuem na distribuição de investimento junto a investidores.

No que se refere à atividade de investimento, 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 Investimentos, ou seja, o Colaborador que tenha, de fato, alçada/poder discricionário de investimentos, é elegível à CGA.

A Gestora assegurará que os Colaboradores que atuem nas atividades elegíveis participem do procedimento de atualização de suas respectivas certificações, de modo que a certificação obtida esteja devidamente atualizada dentro dos prazos estabelecidos neste Manual e nos termos previstos no Código ANBIMA de Certificação.

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

Contratação

Antes da contratação, admissão ou transferência de área de qualquer Colaborador, o Diretor 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 da Gestora.

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

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

Alteração de Funções

Ainda, o Diretor de Investimentos deverá contatar e informar o Diretor de Compliance, Risco e PLD sempre que houver algum tipo de alteração nos cargos e funções dos Colaboradores que integram a Equipe de Gestão, confirmando, ainda, todos aqueles Colaboradores que atuem com alçada/poder discricionário de investimento, se for o caso.

Desligamento

O Diretor de Compliance, Risco e PLD 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.

Prazo 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 Código ANBIMA de Certificação, sendo que a manutenção das informações contidas no Banco de Dados deverá ser objeto de análise e confirmação pelo Diretor de Compliance, Risco e PLD, conforme disposto abaixo.

Vedação

A Gestora não atua com colaboradores, com ou sem certificações ANBIMA, que tenham:

- Sido inabilitados para o exercício de cargo em instituições financeiras e demais entidades autorizadas a funcionar pelo Banco Central do Brasil, pela Comissão de Valores Mobiliários, pela Superintendência Nacional de Previdência Complementar ou pela Superintendência de Seguros Privados;
- Sua autorização para o exercício da atividade suspensa, cassada ou cancelada;
- Ter sofrido punição definitiva, nos últimos 5 (cinco) anos, em decorrência de sua atuação como administrador ou estar inabilitado ou suspenso para o exercício do cargo em instituições financeiras.

1.4. Rotinas de Verificação

Periodicamente, o Diretor de Compliance, Risco e PLD 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.

Colaboradores que não tenham CGA (e que não tenham a isenção concedida pelo Conselho de Certificação, nos termos 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 Investimentos, tendo em vista que não possuem alçada/poder final de decisão para tanto.

Colaboradores que que não tenham CPA 20 (e que não tenham a isenção concedida pelo Conselho de Certificação, nos termos Código ANBIMA de Certificação) estão impedidos atuar na distribuição de produtos de investimento junto a investidores.

Ademais, no curso das atividades de compliance e fiscalização desempenhadas pelo Diretor de Compliance, Risco e PLD, caso seja verificada qualquer irregularidade com as funções exercidas por Colaborador indicando, 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 avaliados os procedimentos e rotinas de verificação para cumprimento do Código de Certificação, sendo que as análises e eventuais recomendações, se for o caso, deverão ser objeto do relatório anual de compliance.

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

1.5. Processo de Afastamento

Todos os profissionais não certificados ou em processo de certificação, e para os quais a certificação seja exigível, nos termos previstos neste Manual, serão, nos termos do 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 a este Manual denominado “Termo de Afastamento” (Anexo V), comprovando o seu afastamento da Gestora. O mesmo procedimento de assinatura do Anexo 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.

1.6. Vigência e Atualização

Esta Política entra em vigor na data de sua publicação e permanece vigente devendo ser mantida atualizada. Deverá ser revista, conforme as melhores práticas de mercado, por prazo não superior a 24 (vinte e quatro) meses ou em prazo inferior se exigido pela regulação 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.

Na ocorrência de alteração/atualização desta Política, a Gestora registrará esta sua nova versão nos documentos do SSM da ANBIMA.

ANEXO I
TERMO DE RECEBIMENTO E COMPROMISSO

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

(i) Ter recebido, na presente data, o Manual de Controles Internos, Código de Ética e Política de Investimentos Pessoais atualizado da **ORGANON CAPITAL GESTÃO DE INVESTIMENTOS LTDA.** ("Gestora");
(ii) Ter lido, sanado todas as minhas dúvidas e entendido integralmente as disposições constantes no Manual;
(iii) Estar ciente de que o Manual como um todo passa a fazer parte dos meus deveres como Colaborador da Gestora, incorporando-se às demais regras internas adotadas pela Gestora; e
(iv) Estar ciente do meu compromisso de comunicar o Diretor de Compliance, Risco e PLD da Gestora qualquer situação que chegue ao meu conhecimento que esteja em desacordo com as regras definidas neste Manual.

[local], [data].

_____

[**COLABORADOR**]

ANEXO II
TERMO DE CONFIDENCIALIDADE

Por meio deste instrumento eu, _____, inscrito no CPF sob o nº _____, doravante denominado Colaborador, e **ORGANON CAPITAL GESTÃO DE INVESTIMENTOS LTDA.** ("Gestora").

Resolvem as partes, para fim de preservação de informações pessoais e profissionais dos clientes e da Gestora, celebrar o presente termo de confidencialidade ("Termo"), que deve ser regido de acordo com as cláusulas que seguem:

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

a) *Know-how,* técnicas, cópias, diagramas, modelos, amostras, programas de computador;
b) Informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes, dos clubes, fundos de investimento geridos pela Gestora;
c) Operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os clubes, fundos de investimento geridos pela GESTORA;
d) Informações estratégicas ou mercadológicas e outras, de qualquer natureza, obtidas junto a sócios, sócios-diretores, funcionários, *trainees* ou estagiários da Gestora ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral, incluindo alterações societárias (fusões, cisões e incorporações), informações sobre compra e venda de empresas, títulos ou valores mobiliários, inclusive ofertas iniciais de ações (*IPO*), projetos e qualquer outro fato que seja de conhecimento em decorrência do âmbito de atuação da Gestora e que ainda não foi devidamente levado à público;
e) Informações a respeito de resultados financeiros antes da publicação dos balanços e balancetes dos fundos;
f) Transações realizadas e que ainda não tenham sido divulgadas publicamente; e
g) Outras informações obtidas junto a sócios, diretores, funcionários, *trainees* ou estagiários da Gestora ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.

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

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

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

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

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

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

4. O Colaborador reconhece e toma ciência que:

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

todos os documentos permanecer em poder e sob a custódia da Gestora, salvo se em virtude de interesses da Gestora for necessário que o Colaborador mantenha guarda de tais documentos ou de suas cópias fora das instalações da Gestora;

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

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

5. Ocorrendo a hipótese do Colaborador ser requisitado por autoridades brasileiras ou estrangeiras (em perguntas orais, interrogatórios, pedidos de informação ou documentos, notificações, citações ou intimações, e investigações de qualquer natureza) a divulgar qualquer Informação Confidencial a que teve acesso, o Colaborador deverá notificar imediatamente a Gestora, permitindo que a Gestora procure a medida judicial cabível para atender ou evitar a revelação.

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

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

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

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

Assim, estando de acordo com as condições acima mencionadas, assinam o presente em 02 (duas) vias de igual teor e forma, para um só efeito produzirem, na presença das testemunhas abaixo assinadas.

[local], [data].

_____

[COLABORADOR]

_____

ORGANON CAPITAL GESTÃO DE INVESTIMENTOS LTDA.

Testemunhas:

1._____
Nome:
CPF:

2._____
Nome:
CPF:

ANEXO III
DECLARAÇÃO DE INVESTIMENTOS

Através deste instrumento eu, _____, inscrito no CPF sob o nº _____, declaro, para os devidos fins, ter observado integralmente, no período de [__.__.____] a [__.__.____], a Política de Investimentos Pessoais estabelecida no Manual de Controles Internos, Código de Ética e Política de Investimentos Pessoais da **ORGANON CAPITAL GESTÃO DE INVESTIMENTOS LTDA.** ("GESTORA"), do qual tomei conhecimento e com o qual concordei.

Declaro ainda que, nesta data: (i) meu nível de endividamento pessoal encontra-se plenamente de acordo com minha remuneração e com meu patrimônio; (ii) os extratos que acompanham esta declaração e a listagem abaixo são a expressão fiel e integral dos investimentos que detenho nos mercados financeiro e de capitais que estejam sujeitos a restrições de acordo com a Política de Investimentos Pessoais descrita no Manual; e (iii) a presente declaração faz parte das políticas adotadas pela GESTORA em estrito cumprimento ao disposto na Instrução CVM nº 21/2021.

Ativo	Valor

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

[local], [data].

_____

[**COLABORADOR**]

ANEXO IV

PRINCIPAIS NORMATIVOS APLICÁVEIS ÀS

ATIVIDADES DA ORGANON CAPITAL GESTÃO DE INVESTIMENTOS LTDA.

1. Resolução CVM Nº 50/2021.
2. Resolução CVM 175/22.
3. Resolução CVM Nº 21/2021.
4. Código ANBIMA de Administração e Gestão de Recursos de Terceiros.
5. Código de Certificação.
6. Lei 9.613/98, conforme alterada redação dada pela Lei 12.683/12

Data Base: agosto de 2024

ANEXO V
TERMO DE AFASTAMENTO

Por meio deste instrumento, eu, _____, inscrito(a) no CPF sob o nº _____, declaro para os devidos fins que, a partir desta data, estou afastado das atividades de gestão de recursos de terceiros da **ORGANON CAPITAL GESTÃO DE INVESTIMENTOS LTDA.** ("GESTORA") por prazo indeterminado:

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

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

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

São Paulo, [---] de [---] de [---].

_____

[COLABORADOR]

_____

ORGANON CAPITAL GESTÃO DE INVESTIMENTOS LTDA.

Testemunhas:

1._____
Nome:
CPF:

2._____
Nome:
CPF:

ANEXO VI

No exercício de suas atividades, a Gestora se utiliza primordialmente dos processos e ativos da organização identificados.

Para cada processo/ativo identificado, o Compliance avaliará o risco quanto à ameaça cibernética e à segurança da informação e seu impacto na organização, caso o evento de risco se realize, definindo, assim, as correspondentes ações de prevenção e proteção, conforme mapeamento abaixo:

Processo		**Grau**	**Impacto**			**Ações de**
	Ameaças	**de Exposição**				**Prevenção e Proteção**
Ativo			Financeiro	Reputação	Operacional	
Sistemas na "Nuvem"	Malware	ALTO	MEDIO	MEDIO	ALTO	Firewall/antivírus/sistema operacional atualizados, backups diários, provedores de serviço na nuvem de boa reputação; uso de códigos/iniciais e não nomes dos clientes; sistemas com login/perfil de acesso; controle de acesso centralizado e conforme Inventário de Informações; logs de acessos e trilha de auditoria.
	Ataques DDoS	BAIXO	BAIXO	BAIXO	MEDIO	
	Invasões	MEDIO	MEDIO	MEDIO	ALTO	
Servidor de Arquivos – Informações Gerais/Documentos	Malware	ALTO	MEDIO	MEDIO	ALTO	Firewall/antivírus/sistema operacional atualizados, backups diários, provedores de serviço na nuvem de boa reputação; controle de acesso centralizado e conforme Inventário de Informações; logs de acessos e trilha de auditoria.
	Ataques DDoS	BAIXO	BAIXO	BAIXO	MEDIO	
	Invasões	MEDIO	MEDIO	ALTO	ALTO	
Contratos e documentos físicos com identificação de qualquer Pessoa Física/Terceiro Contratado/Colaboradores no escritório	Engenharia Social					Código de Ética e Conduta e Regras e Procedimento de Compliance (treinamento e prática) Política de Mesa Limpa / armazenamento seguro Destruição de documentos segura
	Invasão de e-mails	BAIXO	BAIXO	ALTO	BAIXO	Acesso restrito ao escritório / segurança Acessos restrito à informação na nuvem conforme controle de acessos definidos
Trading	Engenharia Social					Provedores de e-mail de boa reputação; uso de

	Invasão de e-mails	MEDIO	BAIXO	MEDIO	BAIXO	códigos e contas no *trading*
Comunicação geral (e-mail e telefone)	Engenharia Social					Provedores de e-mail de boa reputação; uso de nomes abreviados, iniciais ou primeiro nome na comunicação
	Invasão de e-mails	MEDIO	BAIXO	MEDIO	BAIXO	
Contratação de Serviços em Nuvem no país e no exterior	Engenharia Social Malwares Ataques DDoS Invasões (*Advanted Persist Threats*)	CRÍTICO	ALTO	ALTO	ALTO	Seguir as diretrizes emanadas no documento Regras e Procedimentos de Deveres Básicos – ANBIMA, integrante ao Código AGRT. Questionário DD Cibersegurança, quando aplicável.