Manual de Controles Internos e de *Compliance*

Grupo Portofino

Versão 6.0 – Agosto de 2025

ÍNDICE

1.	**Introdução**	**4**
1.1.	**Sumário**	**4**
1.2.	**Interpretação**	**5**
1.3.	**Aplicabilidade do Manual**	**6**
1.4.	**Ambiente Regulatório**	**6**
1.5.	**Termo de Compromisso**	**6**
2.	**POLÍTICA DE COMPLIANCE**	**8**
2.1.	**Introdução**	**8**
2.2.	**Responsabilidades e Obrigações**	**8**
2.3.	**Diretor de Risco e Compliance**	**8**
2.4.	**Comitê de Compliance**	**10**
2.5.	**Área de Compliance e Responsabilidades**	**10**
2.6.	**Garantia de Independência**	**12**
2.7.	**Dúvidas ou ações contrárias aos princípios e normas do Manual**	**12**
2.8.	**Revisão de Compliance**	**13**
2.9.	**Sistema de Gerenciamento de Compliance**	**14**
3.	**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**	**14**
3.1.	**Introdução**	**14**
3.2.	**Confidencialidade**	**15**
3.3.	**Identificação de Riscos (risk assessment)**	**17**
3.4.	**Controles de Acesso a Informações Confidenciais**	**17**
3.5.	**Barreira de Controle de Informações**	**18**
3.6.	**Identificação dos Detentores da Informação, Manutenção de Registros e Logs**	**20**
3.7.	**Proteção da Base de Dados**	**21**
3.8.	**Vazamento de Informações Confidenciais**	**21**
3.9.	**Procedimentos de Resposta**	**21**
3.10.	**Testes e Treinamento de Segurança da Informação**	**22**
3.11.	**Divulgação de Fatos Relevantes**	**22**
4.	**POLÍTICA DE SEGURANÇA CIBERNÉTICA**	**23**
4.1.	**Objetivo**	**23**
4.2.	**Princípios**	**24**
4.3.	**Responsabilidade pela Segurança Cibernética**	**24**
4.4.	**Demais Atribuições**	**25**
4.5.	**Identificação/Avaliação de Riscos (Risk Assessment)**	**25**
4.6.	**Ações de Prevenção e Proteção**	**26**
4.7.	**Procedimentos de Segurança Cibernética de Terceiros**	**29**
4.8.	**Monitoramento e Testes**	**29**
4.9.	**Plano de Resposta a Incidente**	**30**

4.10. Procedimento em Caso de Incidente 30
4.11. Propriedade Intelectual 31
4.12. Reciclagem e Revisão 31
5. POLÍTICAS DE TREINAMENTO 31
5.1. Treinamento e Processo de Reciclagem 31
5.2. Implementação e Conteúdo 32
6. POLÍTICA DE SUSTENTABILIDADE 32
7. POLÍTICA DE ANTICORRUPÇÃO 33
7.1. Introdução 33
7.2. Abrangência das Normas de Anticorrupção 33
7.3. Definição 33
7.4. Normas de Conduta 34
7.5. Proibição de Doações Eleitorais 35
7.6. Relacionamentos com Agentes Públicos 35
8. POLÍTICA DE CERTIFICAÇÃO 35
8.1. Introdução 35
8.2. Atividades Elegíveis e Critérios de Identificação 35
8.3. Identificação de Profissionais Certificados e Atualização do Banco de Dados da ANBIMA 36
8.4. Rotinas de Verificação 36
8.5. Processo de Afastamento 37
ANEXO I – TERMO DE RECEBIMENTO E COMPROMISSO AO MANUAL DE CONTROLES INTERNOS E DE COMPLIANCE DO GRUPO PORTOFINO 39
ANEXO II – TERMO DE CONFIDENCIALIDADE 40
ANEXO III – PRINCIPAIS NORMATIVOS APLICÁVEIS ÀS ATIVIDADES DO GRUPO PORTOFINO 43
ANEXO IV - TERMO DE AFASTAMENTO 44
ANEXO V – TERMO DE PROPRIEDADE INTELECTUAL A POLÍTICA DE SEGURANÇA DA INFORMAÇÃOI E CIBERNETICA DO GRUPO PORTOFINO. 45

1. Introdução

Este documento foi elaborado com base em diretrizes comuns às gestoras Portofino Gestão de Recursos Ltda. ("PMFO Gestão"), PMFO Esportes e Entretenimento Gestão de Recursos Ltda. ("PMFO Esportes"), e PMFO Internacional Gestão de Recursos Ltda. ("PMFO Internacional") todas integrantes do Grupo Portofino (em conjunto, denominadas como "Grupo Portofino" ou "Gestoras", e, individualmente, cada uma delas como "Gestora", conforme o contexto aplicável). Sempre que aplicável, as disposições aqui estabelecidas serão adaptadas para refletir as particularidades operacionais, regulatórias e comerciais de cada Gestora, de acordo com seu escopo de atuação e os produtos sob sua administração. Nos trechos em que não for possível adotar diretrizes uniformes, as referências serão feitas de forma individualizada à Gestora correspondente.

Cumpre esclarecer que:

- PMFO Gestão é uma gestora de recursos especializada na gestão de fundos de investimento financeiro, notadamente por meio fundos de investimento exclusivos, bem como carteiras administradas, tendo como foco a atividade de gestão de patrimônio de clientes que sejam investidores qualificados e profissionais.

- PMFO Esportes é uma gestora de recursos especializada na gestão de recursos, notadamente por meio de carteiras administradas, de investidores que sejam atletas de alta performance, artistas e empresários atuantes nos segmentos de esportes, artes e entretenimento, bem como na realização de acompanhamento e gerenciamento (concierge) da estrutura patrimonial e financeira de tais clientes.

- PMFO Internacional é uma gestora de recursos com atuação especializada na gestão de fundos de investimentos e carteiras administradas constituídos no exterior.

1.1. Sumário

Este Manual de Regras, Procedimentos e Controles Internos ("Manual"), elaborado em conformidade com o disposto no item 2.7 do Ofício-Circular/CVM/SIN/Nº 05/2014, na Resolução CVM nº 21, de 25 de fevereiro de 2021, conforme alterada ("Resolução CVM nº 21"), Resolução CVM nº 175, de 23 de dezembro de 2022, conforme alterada ("Resolução CVM 175") e seus Anexos Normativos, demais orientações da Comissão de Valores Mobiliários ("CVM"), no Código Anbima de Autorregulação para Administração e Gestão de Recursos de Terceiros ("Código de ART"), no Código ANBIMA de Ética ("Código ANBIMA de Ética") e nas Regras e Procedimentos de Administração e Gestão de Recursos de Terceiros ("Regras e Procedimentos ANBIMA"), 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 o Grupo Portofino, tanto na sua atuação interna quanto na comunicação com os diversos públicos.

Na busca incessante da satisfação dos clientes, as Gestoras atuam 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 as Gestoras assume nos mercados em que atua.

As Gestoras 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.

As Gestoras mantêm versões atualizadas no website do Grupo Portofino (www.portofinomultifamilyoffice.com.br) dos seguintes documentos: (i) Formulário de Referência, conforme Anexo E da Resolução CVM nº 21; (ii) Política de Gestão de Risco; (iii) Política de Rateio e Divisão de Ordens; (iv) Manual de Regras, Procedimentos e Controles Internos; (v) Manual de Ética; (vi) Política de Investimentos Pessoais; e (vii) Política de Exercício de Direito de Voto.

O website do Grupo Portofino deverá disponibilizar também os seguintes documentos e informações relativos aos fundos sob gestão, conforme exigido pela regulamentação em vigor:

Documento ou Informação[1]	**Base Legal**
Regulamento anexos e apêndices atualizados	Art. 47, Parte Geral, Resolução CVM 175
Descrição da tributação aplicável ao fundo e/ou classe	Art. 47, Parte Geral, Resolução CVM 175
As informações periódicas e eventuais de cada fundo e/ou Classe	Art. 61, Parte Geral, Resolução CVM 175
Fatos Relevantes	Art. 64, §2º, Parte Geral, Resolução CVM 175
Convocação da assembleia de cotistas geral do fundo de investimento e especial das classes e subclasses	Art. 72, Parte Geral da Resolução CVM 175
Demonstração de desempenho dos Fundos de Investimento Financeiros	Art. 13 do Anexo I (FIFs), Resolução CVM 175
Lâmina dos Fundos de Investimento Financeiros	Art. 13 do Anexo I (FIFs), Resolução CVM 175
Identificação dos Prestadores de Serviço contratados	Art. 48, inciso I, Resolução CVM 175
Política de Voto	Art. 13 do Anexo I (FIFs), Resolução CVM 175

1.2. Interpretação

Para fins de interpretação dos dispositivos previstos deste Manual, exceto se expressamente disposto de forma contrária: (a) os termos utilizados deste Manual terão o significado

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

atribuído na Resolução CVM 175; (b) as referências a Fundos abrangem as Classes e Subclasses, se houver; (c) as referências a regulamento abrangem os anexos e apêndices, se houver, observado o disposto na Resolução CVM 175; e (d) as referências às Classes abrangem os Fundos ainda não adaptados à Resolução CVM 175.

O disposto nesta Política será aplicável às Gestoras apenas na medida em que sua atuação, os produtos sob sua gestão, suas teses de investimento, mandatos específicos e situações operacionais estejam abrangidos pelos regramentos descritos. Caso alguma Gestora não administre veículos ou ativos específicos sujeitos a uma ou mais regras, estas deverão ser consideradas inaplicáveis à Gestora em questão.

1.3. Aplicabilidade do Manual

Sem prejuízo da aplicabilidade regulatória deste Manual para as Gestoras, as demais empresas do Grupo Portofino também se sujeitarão ao conteúdo deste, no que aplicável e condizente com a realidade de cada empresa não regulada.

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

1.4. 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 ao Grupo Portofino bem como do completo conteúdo deste Manual. Para melhor referência dos Colaboradores, as principais normas aplicáveis às atividades das Gestoras foram apontadas no Anexo III do presente Manual.

1.5. 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 das Gestoras, deverá ser levado para apreciação do Diretor de Risco e Compliance

da respectiva Gestora, abaixo definido, e/ou do Comitê de Compliance de acordo com os procedimentos estabelecidos neste Manual. Competirá ao Comitê de Compliance definir 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 Risco e Compliance da respectiva Gestora e/ou o Comitê de Compliance sobre violações ou possíveis violações dos princípios e normas aqui dispostos, de maneira a preservar os interesses dos clientes das Gestoras, bem como zelar pela reputação da empresa. Caso a violação ou suspeita de violação recaia sobre o próprio Diretor de Risco e Compliance da respectiva Gestora e/ou membros do Comitê de Compliance da respectiva Gestora , o Colaborador deverá informar diretamente aos demais administradores do Grupo Portofino.

2. POLÍTICA DE COMPLIANCE

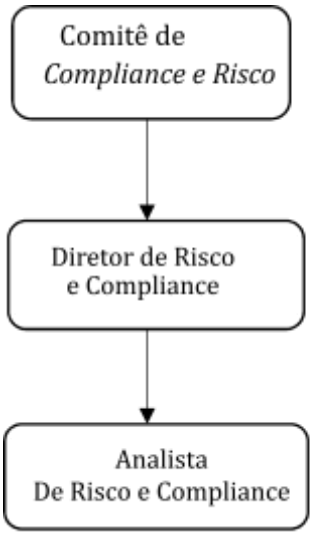
2.1. Introdução

2.2. Responsabilidades e Obrigações

As Áreas de Compliance das Gestoras são responsáveis pela elaboração e manutenção dos Programas de Compliance, sob responsabilidade final e coordenação direta dos diretores estatutários das Gestoras indicados como diretores responsáveis pelo cumprimento de regras, políticas, procedimentos e controles internos das Gestoras ("Diretor de Risco e Compliance"), nos termos da Resolução CVM nº 21, que inclui a revisão e atualização periódica destas Políticas e demais políticas e manuais das Gestoras, bem como a implementação de controles internos e testes de aderência para monitorar a efetividade das políticas e, ainda, a realização de treinamentos aos colaboradores.

O Programa de *Compliance* das Gestoras foram desenvolvidos com vistas a dar cumprimento às obrigações estabelecidas na Resolução CVM nº 21, nos códigos e regras de autorregulação da ANBIMA pertinentes, inclusive o Código de ART e as Regras e Procedimentos ANBIMA, bem como demais atos normativos aplicáveis, dentre outras melhores práticas nacionais e internacionais.

As Áreas de *Compliance* são as principais responsáveis pela disseminação e supervisão das regras, controles e procedimentos internos das Gestoras, visando mitigar os riscos operacionais, regulatórios, reputacionais e legais de sua atividade. Segue abaixo organograma da Área de *Compliance*:



2.3. Diretor de Risco e Compliance

Nos termos da Resolução CVM nº 21, o Diretor de Risco e *Compliance* das Gestoras, reporta-se diretamente apenas ao Comitê de *Compliance* da respectiva Gestora em que é Diretor, com plena autoridade sobre a implementação do Programa de *Compliance* da respectiva Gestora.

O Diretor de Risco e *Compliance* é um dos administradores da Gestora, na forma do seu contrato social, cada Gestora do Grupo Portofino consta com um Diretor de Risco e *Compliance*. Ademais, a parte mais substancial de sua remuneração é garantida, de formam totalmente independente da performance dos fundos ou carteiras administradas, conforme aplicável, como mais uma maneira de garantir sua independência. O mesmo ocorre com os demais recursos humanos que integram a Área de *Compliance* de cada Gestora do Grupo Portofino, no que tange à forma de remuneração.

São obrigações do Diretor de Risco e *Compliance*, no âmbito desta Política:

(i) Atender prontamente todos os Colaboradores;

(ii) Identificar possíveis condutas contrárias a lei, regulação, autorregulação, políticas e manuais da respectiva Gestora em que exerce função de Diretor;

(iii) Acompanhar as políticas descritas neste Manual;

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

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

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

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

(viii) Encaminhar aos órgãos de administração da respectiva 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 do Grupo Portofino;

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

(x) Promover a ampla divulgação e aplicação dos preceitos éticos no desenvolvimento das atividades de todos os Colaboradores, inclusive por meio dos treinamentos periódicos previstos neste Manual;

(xi) Apreciar todos os casos que cheguem ao seu conhecimento sobre o potencial

descumprimento dos preceitos éticos e de compliance previstos neste Manual ou nos demais documentos aqui mencionados, e apreciar e analisar situações não previstas;

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

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

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

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

- Investimentos pessoais;
- Transações financeiras com clientes fora do âmbito da respectiva 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 do Grupo Portofino que souberem de informações ou situações em andamento que possam afetar os interesses das Gestoras, gerar conflitos ou, ainda, se revelarem contrárias aos termos previstos nesta Política, deverá informar ao Diretor de Risco e *Compliance* e/ou ao Comite de *Compliance* respectiva Gestora em que é Colaborador , para que sejam tomadas as providências cabíveis.

Ainda, cabe ao Diretor de Risco e *Compliance da* no âmbito de sua função na Gestora analisar situações que possam ser caracterizadas como "conflitos de interesse" pessoais e profissionais e eventuais condutas descritas no Manual de Ética, respeitada as competências do Comitê de Compliance da respectiva Gestora, acompanhar o resultado dos testes de aderência e supervisionar as atividades de controles internos desta.

2.4. Comitê de Compliance

Cada Gestora do Grupo Portofino conta com um Comitê de *Compliance* para assessorar sobre as questões de *Compliance* da Gestora e que tem autonomia para o exercício das suas funções. É composto pelo Diretor de Risco e *Compliance*, que atua como Coordenador do Comitê, pelo Diretor de Gestão e por um profissional da Área de *Compliance*. As regras e competências do Comitê de Compliance da Gestora estão definidas no Regimento de Comitê Internos da Gestora.

2.5. Área de Compliance e Responsabilidades

As seguintes atividades são de responsabilidade primária da Área de *Compliance*, no âmbito de

sua Gestora:

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

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

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

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

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

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

(vii) Manutenção e atualização de agenda regulatória contendo todos os prazos emanados de normas regulatórias e autorregulatórias, devendo usar sistemas eletrônicos ou planilhas para tanto; Realização de testes periódicos a fim de monitorar e avaliar a efetividade das políticas estabelecidas na Política e dos sistemas e controles da respectiva Gestora, sugerindo e acompanhando as ações de melhorias decorrentes de tais testes, podendo utilizar- se de sistema eletrônico próprio para tanto;

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

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

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

(xi) Interação com os órgãos reguladores e autorreguladores em nome da respectiva Gestora, bem como o atendimento a fiscalizações e supervisões de órgãos reguladores e autorreguladores, auditorias terceirizadas e *due dilligence*, fazendo a interface entre as solicitações destes e as áreas internas da respectiva Gestora, respeitadas as regras dispostas no Manual de Ética do Grupo Portofino;

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

ocorrência e eventual comunicação ao COAF;

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

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

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

(xvi) Estabelecer controles adicionais para gestão de Carteiras Administradas, conforme aplicável, sobretudo no que tange às regras de contratação de terceiros estabelecidas na Resolução CVM nº 21, no Código de ART e regras complementares e demais normas aplicáveis;

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

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

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

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

Sempre que entender necessário ou conveniente, o Diretor de Risco e *Compliance* da respectiva Gestora poderá levar qualquer assunto de sua competência para apreciação ou deliberação pelo Comitê de *Compliance*.

2.6. Garantia de Independência

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

2.7. 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 das Gestoras, 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 Risco e Compliance e/ou o

Comitê de Compliance da Gestora aplicável, para obtenção de orientação mais adequada.

Mesmo que haja apenas a suspeita de potencial situação de conflito ou ocorrência de uma ação que vá afetar os interesses das Gestoras, o Colaborador deverá seguir essa mesma orientação. Esta é a maneira mais transparente e objetiva para consolidar os valores da cultura empresarial do Grupo Portofino 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 Risco e Compliance e/ou do Comitê de Compliance, das Gestoras, 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 das Gestoras, 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 Risco e Compliance e/ou ao Comitê de Compliance, exclusivamente por meio de e-mail.

2.8. Revisão de Compliance

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

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

Adicionalmente, será realizado um monitoramento **semestral**, a cargo do Diretor de Risco e Compliance, de cada Gestora do Grupo Portofino, sobre uma amostragem significativa dos Colaboradores, escolhida aleatoriamente pelo Diretor de Risco e Compliance, para que sejam verificados os arquivos eletrônicos, inclusive e-mails, com o objetivo de verificar possíveis situações de descumprimento às regras contidas no presente Manual.

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

O Grupo Portofino realizará inspeções com periodicidade **trimestral**, a cargo do Diretor de Risco e Compliance de cada Gestora, com base em sistemas de monitoramento eletrônico, independentemente da ocorrência de descumprimento ou suspeita ou indício de descumprimento de quaisquer das regras estabelecidas neste Manual ou aplicáveis às atividades do Grupo Portofino, sendo tal inspeção realizada de forma aleatória.

Adicionalmente, os Diretores de Risco e Compliance, no âmbito de suas Gestoras, deverão ainda verificar rotineiramente os níveis de controles internos e *compliance* junto a todas as áreas das suas Gestoras, com o objetivo de promover ações para esclarecer e regularizar eventuais desconformidades. Analisará também os controles previstos neste Manual, bem como em outras políticas do Grupo Portofino, propondo a criação de novos controles e melhorias naqueles considerados deficientes, monitorando as respectivas correções.

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

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

Como resultado da revisão anual, a Área de *Compliance,* de cada Gestora do Grupo Portofino, deverá elaborar relatório de conclusões de controles internos de que trata o artigo 25 da Resolução CVM nº 21, sob condução e responsabilidade final do Diretor de Risco e Compliance no âmbito de suas Gestoras.

2.9. Sistema de Gerenciamento de Compliance

As Gestoras utilizam um sistema para gestão de *Compliance* denominado Compliasset. Tal sistema disponibiliza uma agenda de atividades regulatórias atualizada, controles internos e testes de aderência para cumprimento das normas de regulação e autorregulação aplicáveis às Gestoras.

O sistema possui, ainda, uma biblioteca digital para armazenamento de documentos e registro de eventos. Portanto, os registros e arquivamentos a cargo da Área de *Compliance* poderão ser realizados no referido sistema, a critério da Área de *Compliance*.

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

3. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

3.1. Introdução

A Política de Segurança da Informação ("Política") do Grupo Portofino têm por razão o

adequado gerenciamento das informações de posse temporária ou de propriedade das Gestoras. Assim, deverá ser seguida por todos os seus Colaboradores (conforme definidos no Manual de Ética), independentemente do nível hierárquico ou função na instituição, bem como de vínculo empregatício ou prestação de serviços.

A responsabilidade em relação à segurança da informação deve ser comunicada no início do vínculo com as Gestoras, devendo os Colaboradores assinar o Termo de Responsabilidade e Confidencialidade, de acordo com o Anexo II desta Política.

A Área de *Compliance* realizará a revisão e atualização desta Política anualmente ou sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do Diretor de Risco e *Compliance* e/ou do Comitê de Investimentos.

3.2. Confidencialidade

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

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

Conforme disposto no Termo de Responsabilidade e Confidencialidade, nenhuma Informação Confidencial, conforme abaixo definido, deve, em qualquer hipótese, ser divulgada fora do ambiente do Grupo Portofino. Fica vedada qualquer divulgação, no âmbito pessoal ou profissional, que não esteja em acordo com as normas legais (especialmente, mas não de forma limitada, aquelas indicadas no **Anexo III** deste Manual) e de *compliance* do Grupo Portofino.

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 o Grupo Portofino, sobre as empresas pertencentes ao seu conglomerado, seus sócios e clientes, aqui também contemplados os próprios veículos sob gestão das Gestoras, incluindo:

1. *Know-how*, técnicas, cópias, diagramas, modelos, amostras, programas de computador;
2. Informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e dos veículos geridos pelas Gestoras;
3. Operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os veículos de investimento e carteiras geridas pelas Gestoras;
4. Estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços;
5. Informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades das Gestoras 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 das Gestoras e que ainda não foi devidamente levado à público;

6. Informações a respeito de resultados financeiros antes da publicação dos balanços, balancetes e/ou demonstrações financeiras dos fundos de investimento e classes respectivas;
7. Transações realizadas e que ainda não tenham sido divulgadas publicamente; e
8. Outras informações obtidas junto a sócios, diretores, funcionários, *trainees*, estagiários ou jovens aprendizes das Gestoras ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.

Sem prejuízo da colaboração das Gestoras 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 Risco e Compliance, 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 das Gestoras, 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 as Gestoras, 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 Risco e Compliance, indicando, além disso, a fonte da Informação Confidencial assim obtida. Tal dever de comunicação também será aplicável nos casos em que a Informação Confidencial seja conhecida de forma acidental,

em virtude de comentários casuais ou por negligência ou indiscrição das pessoas obrigadas a guardar segredo. Os Colaboradores que, desta forma, acessarem a Informação Confidencial, deverão abster-se de fazer qualquer uso dela ou comunicá-la a terceiros, exceto quanto à comunicação ao Diretor de Risco e Compliance anteriormente mencionada.

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

3.3. Identificação de Riscos (risk assessment)

No âmbito de suas atividades, as Gestoras identificaram 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 das próprias Gestoras, operações e ativos investidos pelas carteiras de valores miliários sob sua gestão, e as comunicações internas e externas (por exemplo: correspondências eletrônicas e físicas);
- Sistemas: informações sobre os sistemas utilizados pelas Gestoras 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 das Gestoras; e
- Governança da Gestão de Risco: a eficácia da gestão de risco pelas Gestoras quanto às ameaças e planos de ação, de contingência e de continuidade de negócios.

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

3.4. Controles de Acesso a Informações Confidenciais

Todo acesso a diretórios e sistemas de informações das Gestoras devem ser controlado. Somente poderão acessar tais diretórios e sistemas de informação os Colaboradores previamente autorizados pelo Diretor de Risco e Compliance, no âmbito da Gestora em que exerce função, observado o disposto na Política de Segurança Cibernética.

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

- Garantia de que o nível de acesso concedido ao Colaborador é adequado ao seu perfil; e
- Cancelamento imediato do acesso concedido a Colaboradores desligados, afastados ou que tenham sua função alterada nas Gestoras.

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

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

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

3.5. Barreira de Controle de Informações

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

O *file server* do Grupo Portofino é acessado pelos Colaboradores mediante *login* com usuário e senha próprios, tendo os usuários permissões diferenciadas de acordo com as funções e atividades desempenhadas por cada profissional. Dessa forma, os diferentes níveis de permissão viabilizam melhor controle de acesso e de reprodução dos dados e arquivos pelos profissionais do Grupo Portofino.

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

- Os Colaboradores devem evitar circular em ambientes externos ao Grupo Portofino com cópias (físicas ou digitais) de arquivos contendo Informações Confidenciais, devendo essas cópias ser mantidas através de senha de acesso;
- O descarte de Informações Confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação, sempre com a orientação do superior hierárquico;
- As informações que possibilitem a identificação de um cliente das Gestoras devem se limitar a arquivos de acesso restrito e apenas poderão ser copiadas ou impressas se forem para o atendimento dos interesses das Gestoras ou do próprio cliente;
- Os Colaboradores devem estar atentos a eventos externos que possam comprometer o sigilo das informações das Gestoras, como, por exemplo, vírus de computador, fraudes, entre outros;
- Assuntos confidenciais não devem ser discutidos em ambientes públicos ou locais considerados expostos;
- A troca de informações entre os Colaboradores do Grupo Portofino 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;

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

  Qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora, pois pode conter informações restritas e confidenciais mesmo no ambiente interno do Grupo Portofino. As Gestoras não mantêm arquivo físico centralizado, sendo cada Colaborador responsável direto pela boa conservação, integridade e segurança de quaisquer informações em meio físico que tenha armazenadas consigo;
- Os Colaboradores devem se abster de utilizar pen-drivers, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade nas Gestoras. É proibida a conexão de equipamentos na rede das Gestoras que não estejam previamente autorizados pela área de informática e pelos administradores das Gestoras.

O Grupo Portofino possui uma rede de acesso à internet exclusiva para eventuais terceiros que visitem o escritório do Grupo Portofino, fortalecendo, assim, a estrutura geral das redes do Grupo Portofino contra-ataques cibernéticos.

- Acesso Escalonado do Sistema

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

As Gestoras mantêm 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 das Gestoras necessária ao exercício de suas atividades.

A implantação destes controles é projetada para limitar a vulnerabilidade dos sistemas das Gestoras em caso de violação

- 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.

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 Risco e Compliance.

- Acesso Remoto

As Gestoras permitem o acesso remoto pelos Colaboradores, de acordo com a seguinte regra: a todos os Colaboradores, conforme requisição por estes e autorização pelo Diretor de Risco e

Compliance, no que se refere ao acesso ao e-mail, a rede e ao diretório.

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

- Controle de Acesso

O acesso de pessoas estranhas ao Grupo Portofino a áreas restritas somente é permitido com a autorização expressa de Colaboradores autorizados pelos administradores do Grupo Portofino.

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, o Grupo Portofino monitora a utilização de tais meios.

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

Conforme acima exposto, será atribuído a cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo os usuários (*login*) individuais de Colaboradores internos de responsabilidade do próprio. Assim, é possível realizar a identificação dos detentores da informação para eventual responsabilização, se for o caso.

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

O Grupo Portofino informa, ainda, que poderá tomar as seguintes medidas:

- tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial ou por determinação do Diretor de Risco e Compliance;
- realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;
- instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso;
- Monitoramento, por amostragem, do acesso dos Colaboradores a sites, blogs, fotologs, webmails, entre outros, bem como os e-mails enviados e recebidos;
- Monitoramento, por amostragem, das ligações telefônicas dos seus Colaboradores realizadas ou recebidas por meio das linhas telefônicas disponibilizadas pelas Gestoras para a atividade profissional de cada Colaborador, especialmente, mas não se limitando, às ligações da equipe de atendimento e da mesa de operação das Gestoras; e
- 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 Risco e Compliance poderá adotar medidas adicionais para monitorar os sistemas de computação e os procedimentos aqui previstos para avaliar o seu cumprimento e sua eficácia.

O não cumprimento dos requisitos previstos nesta Política acarretará violação às regras internas do Grupo Portofino e sujeitará o usuário às sanções administrativas e legais cabíveis, observado o disposto no Manual de Ética do Grupo Portofino. Para fins de ilustração, segue uma lista não exaustiva de eventuais exemplos que podem ocasionar sanções:

- uso ilegal de software;
- introdução (intencional ou não) de vírus de informática;
- tentativas de acesso não autorizado a dados e sistemas; ou
- divulgação de informações sensíveis do Grupo Portofino.

3.7. Proteção da Base de Dados

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

Todos os registros eletrônicos realizados pelas Gestoras deverão ser mantidos e estar disponíveis para atender os prazos legais e regulatórios praticados pelos órgãos reguladores locais e de jurisdições que as Gestoras atuem em mercado regulado.

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

3.8. Vazamento de Informações Confidenciais

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

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

3.9. Procedimentos de Resposta

Conforme acima destacado, o Diretor de Risco e Compliance discutirá com o Comitê de Compliance acerca de eventual resposta a qualquer informação de suspeita de infecção, acesso não autorizado ou outro comprometimento da rede ou dos dispositivos das Gestoras 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 e carteira administrada sob gestão das Gestoras, a fim de garantir a ampla disseminação e tratamento equânime da Informação Confidencial);

(vii) Determinação do responsável (ou seja, as Gestoras ou o cliente ou investidor afetado) que arcará com as perdas decorrentes do incidente. A definição ficará a cargo do Comitê de Compliance, após a condução de investigação e uma avaliação completa das circunstâncias do incidente.

3.10. Testes e Treinamento de Segurança da Informação

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

O treinamento sobre segurança de informação fará parte do treinamento inicial e periódico das Gestoras, conforme previsto na Política de Treinamento do Grupo Portofino, o qual deverá considerar, dentre outros, assegurar que todos os Colaboradores tenham conhecimento dos procedimentos e das obrigações aqui previstos, assim como minimizar a ocorrência de incidentes de segurança em função de problemas no uso, desvio de informações, fraudes e na interpretação das normas e procedimentos.

3.11. **Divulgação de Fatos Relevantes**

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

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

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

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

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

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

O Grupo Portofino deverá disponibilizar os fatos relevantes relativos aos fundos sob sua gestão em seu *website*.

4. POLÍTICA DE SEGURANÇA CIBERNÉTICA

4.1. Objetivo

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

A Política segue práticas de mercado, bem como está de acordo com as leis, regulamentação e autorregulação aplicáveis. A presente Política deve ser divulgada a todos os Colaboradores e disponibilizada na intranet, de forma que seu conteúdo possa ser consultado a qualquer momento.

No que se refere à segurança cibernética, as Gestoras identificaram as seguintes principais

ameaças em relação as suas atividades, 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.

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

4.2. Princípios

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

Os processos de segurança de dados e da informação das Gestoras devem assegurar:

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

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

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

4.3. Responsabilidade pela Segurança Cibernética

A equipe de Tecnologia da Informação ("T.I"), em conjunto com o Diretor de Risco e *Compliance*, sendo a principal responsável dentro das Gestoras para tratar e responder questões de segurança cibernética ("Responsável pela Segurança Cibernética"), bem como por implementar as regras e normas aqui estabelecidas e a sua revisão.

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

- Testar a eficácia dos controles utilizados e informar à Diretoria os riscos residuais;
- Acordar com a Diretoria o nível de serviço que será prestado por terceiros contratados e os procedimentos de resposta aos incidentes;
- Configurar os equipamentos e sistemas concedidos aos Colaboradores com todos os controles necessários para cumprir os requerimentos de segurança aqui estabelecidos, bem como definir e assegurar a segregação das funções administrativas a fim de restringir poderes de cada indivíduo e reduzir o número de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações;
- Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio;
- Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção das Gestoras em processos de mudança, sendo ideal a proteção contratual para controle e responsabilização no caso de uso de terceiros;
- Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento das Gestoras, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos das Gestoras;
- Promover a conscientização dos Colaboradores em relação à relevância da segurança da informação para o negócio das Gestoras, mediante treinamentos.

Na ocorrência de qualquer incidente envolvendo risco cibernético, todo e qualquer Colaborador que perceba ou desconfie de tal incidente deverá imediatamente informar o Responsável por Segurança Cibernética, que poderá convocar reunião do Comitê de *Compliance*.

4.4. Demais Atribuições

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

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

4.5. Identificação/Avaliação de Riscos (Risk Assessment)

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

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

Todos os requisitos de segurança da informação e segurança cibernética, incluindo a necessidade de planos de contingência, deverão ser previamente identificados na fase de levantamento de escopo de um projeto ou sistema, e documentados, implantados e testados durante a fase de execução.

Segue abaixo uma lista não exaustiva de alguns riscos de segurança cibernética identificados, na avaliação inicial:

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

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

4.6. Ações de Prevenção e Proteção

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

Internet, E-mail e Computadores

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

As Gestoras utilizam os serviços do WatchGuard, companhia líder do mercado em segurança de redes corporativas, para se proteger de ameaças cibernéticas. A ferramenta de *firewall* da WatchGuard realiza o bloqueio de sites com conteúdo inadequado, conserva a largura de banda da rede e protege contra sites mal-intencionados, vírus, spam, tentativas de *phishing*, *malwares*, *ransomwares* e violação de dados. O firewall gerencia todas as redes das Gestoras, evitando a perda de dados e detectando se informações sensíveis estão tentando deixar sua rede, por qualquer meio.

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

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

- Os equipamentos e computadores disponibilizados aos Colaboradores devem ser utilizados com a finalidade de atender aos interesses comerciais legítimos das Gestoras e sob nenhuma hipótese servirão de instrumento à discriminação em virtude de raça, religião, cor, origem, idade, sexo, incapacidade física e mental ou de qualquer outra forma não autorizada expressamente em lei.
- A utilização de equipamentos é permitida para fins particulares relevantes, sendo expressamente proibida a divulgação de mensagens com conteúdo religioso, racial, pornográfico ou político no âmbito das Gestoras.
- A instalação de cópias de arquivos de qualquer extensão, obtido de forma gratuita ou remunerada, em computadores das Gestoras, depende de autorização do Responsável pela Segurança Cibernética e do Diretor de Risco e *Compliance* e deverá observar os direitos de propriedade intelectual pertinentes, tais como *copyright*, licenças e patentes.
- As mensagens enviadas ou recebidas através do correio eletrônico corporativo (*e- mails* corporativos), seus respectivos anexos, e a navegação através da rede mundial de computadores (*internet*) através de equipamentos das Gestoras poderão ser monitoradas.
- Os *e-mails* corporativos recebidos pelos Colaboradores, quando abertos, deverão ter sua adequação às regras desta Política imediatamente verificada. Não será admitida, sob qualquer hipótese, a manutenção ou arquivamento de mensagens de conteúdo ofensivo, discriminatório, pornográfico ou vexatório, sendo a responsabilidade apurada de forma específica em relação ao destinatário da mensagem.
- Nos equipamentos e computadores disponibilizados pelas Gestoras não é recomendado o uso de e-mails públicos (*webmails*) ou qualquer outro tipo de correio eletrônico que não seja o correio corporativo das Gestoras. Fica também proibido a utilização de programas de conversas eletrônicas (CHATs) externos, gratuitos ou não, salvo para fins comerciais.

Senhas

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

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

É proibido o compartilhamento de *login* para funções de administração de sistemas. A área de Recursos Humanos do Grupo Portofino é a responsável pela emissão e pelo controle dos documentos físicos de identidade dos Colaboradores.

Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.

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

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

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

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

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

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

Monitoramento Telefônico

As conversas telefônicas originadas ou recebidas das Gestoras são gravadas e armazenadas em mídia para eventual consulta posterior (de modo que o conteúdo possa ser usado para fins de esclarecimento de questões relacionadas a esta Política, inclusive no âmbito judicial).

Conforme descrito na Política de Segurança da Informação, as Gestoras poderão realizar, a seu exclusivo critério, o monitoramento, por amostragem, das ligações telefônicas dos seus Colaboradores realizadas ou recebidas por meio das linhas telefônicas disponibilizadas pelas Gestoras para a atividade profissional de cada Colaborador, especialmente, mas não se limitando, às ligações da equipe de atendimento e da mesa de operação das Gestoras.

4.7. Procedimentos de Segurança Cibernética de Terceiros

Os Colaboradores externos do Grupo Portofino, dentre os quais os seus fornecedores, prestadores de serviços e parceiros, também podem representar uma fonte significativa de riscos de cibersegurança. A computação em nuvem pode ser considerada como uma forma de contratação de serviço de terceiros e, assim como as demais contratações de Colaboradores externos, envolve determinados riscos que devem ser levados em conta pelo Grupo Portofino, demandando certos cuidados proporcionais a esta identificação de ameaças.

4.8. Monitoramento e Testes

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

O ambiente de TI do Grupo Portofino será monitorado, por meio de indicadores e geração de históricos:

(i) do uso da capacidade instalada da rede e dos equipamentos; (ii) tempo de resposta no acesso à internet e aos sistemas críticos das Gestoras; (iii) de períodos de indisponibilidade no acesso à internet e aos sistemas críticos das Gestoras; (iv) de incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante); e (v) das atividade de todos os Colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros).

Para garantir as regras mencionadas nesta Política, as Gestoras deverão:

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

- Realizar, a qualquer tempo, inspeção física nas máquinas de hardware, se mantido servidor físico;
- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso; e
- Testar a vulnerabilidade e penetração do website do Grupo Portofino, bem como de todo e qualquer sistema eletrônico desenvolvido internamente pelo Grupo Portofino, a cada 24 (vinte e quatro) meses.

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

4.9. Plano de Resposta a Incidente

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

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

4.10. Procedimento em Caso de Incidente

Uma vez que o Responsável pela Segurança Cibernética tenha sido acionado devido a um potencial incidente, este deverá observar os procedimentos descritos no item 2.9 da Política de Segurança da Informação, respeitadas as peculiaridades no processo de recuperação e retomada abaixo descrito:

Recuperação

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

Também deverá ser avaliado o impacto do incidente nos diversos riscos (mercado, crédito, operacional, dentre outros) e, caso necessário, tomar as devidas ações, tais como manifestação pública na mídia, enquanto a Diretoria verificará se todas as informações necessárias ao portfólio estão seguras e a área de Gestão definirá se decisões de investimento são requeridas. Quaisquer dados faltando ou corrompidos, ou problemas identificados por Colaboradores das Gestoras, devem ser comunicados à Diretoria. Colaboradores externos relevantes deverão ser mantidos atualizados.

Retomada

Tal fase refere-se ao período de transição do retorno ao modo normal de operação e pode incluir a análise de projetos, como voltar ao *full compliance*, reconstrução de eventuais sistemas

e eventuais mudanças e medidas de prevenção. A Área de *Compliance* deverá registrar o histórico em local adequado, como o sistema de gerenciamento Compliasset.

4.11. Propriedade Intelectual

Todos os documentos e arquivos, incluindo, sem limitação, aqueles produzidos, modificados, adaptados ou obtidos pelos Colaboradores, relacionados, direta ou indiretamente, com suas atividades profissionais junto às Gestoras, tais como minutas de contrato, memorandos, cartas, fac-símiles, apresentações a clientes, e-mails, correspondências eletrônicas, arquivos e sistemas computadorizados, planilhas, fórmulas, planos de ação, bem como modelos de avaliação, análise e gestão, em qualquer formato, são e permanecerão sendo propriedade exclusiva das Gestoras, 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 das Gestoras, sendo vedado ao Colaborador, inclusive, apropriar-se de quaisquer desses documentos e arquivos após seu desligamento das Gestoras, salvo se autorizado expressamente pelas Gestoras e ressalvado o disposto abaixo.

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

4.12. Reciclagem e Revisão

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

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

O Responsável pela Segurança Cibernética, em conjunto com a área de *Compliance*, realizará a revisão e atualização desta Política a cada 12 (doze) meses, ou em prazo inferior sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do Diretor de Risco e *Compliance*.

5. POLÍTICAS DE TREINAMENTO

5.1. Treinamento e Processo de Reciclagem

O Grupo Portofino 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 do Grupo Portofino e terá oportunidade de esclarecer dúvidas relacionadas a tais princípios e normas.

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

5.2. Implementação e Conteúdo

A implementação do processo de treinamento inicial e do programa de reciclagem continuada fica sob a responsabilidade da Área de Compliance 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 do Grupo Portofino, seus princípios éticos e de conduta, as normas de *compliance*, as políticas de segregação, quando for o caso, e as demais políticas descritas nesta Manual (especialmente aquelas relativas à confidencialidade, segurança das informações, segurança cibernética e conflitos de interesse), bem como aquelas descritas no Manual de Ética e na Política de Investimentos Pessoais do Grupo Portofino e, ainda, as penalidades aplicáveis aos Colaboradores decorrentes do descumprimento de tais regras, além das principais leis e normas aplicáveis às referidas atividades, constantes do **Anexo III** deste Manual.

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

6. POLÍTICA DE SUSTENTABILIDADE

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

Além disso, as Gestoras incentivam 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.

7. POLÍTICA DE ANTICORRUPÇÃO

7.1. Introdução

O Grupo Portofino está sujeita às leis e normas de anticorrupção, incluindo, mas não se limitando, à Lei nº 12.846/13 e Decreto nº 11.129/25 ("Normas de Anticorrupção").

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

7.2. 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.

7.3. 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.

7.4. Normas de Conduta

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

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

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

Nenhum sócio ou colaborador poderá ser penalizado devido a atraso ou perda de negócios

resultantes de sua recusa em pagar ou oferecer suborno a agentes públicos.

7.5. Proibição de Doações Eleitorais

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

7.6. Relacionamentos com Agentes Públicos

Quando se fizer necessária a realização de reuniões e audiências ("Audiências") com agentes públicos, sejam elas internas ou externas, as Gestoras serão representadas por, ao menos, 2 (dois) Colaboradores, que deverão se certificar de empregar a cautela exigida para a ocasião, com o objetivo de resguardar as Gestoras contra condutas ilícitas no relacionamento com agentes públicos. Dentre os procedimentos adotados, os Colaboradores que estiverem representando as Gestoras deverão elaborar relatórios de tais Audiências, e os apresentar ao Diretor de Risco e Compliance responsável imediatamente após sua ocorrência.

8. POLÍTICA DE CERTIFICAÇÃO

8.1. Introdução

O Grupo Portofino está sujeita às disposições do Regras e Procedimentos de Administração e Gestão de Recursos de Terceiros, inclusive às regras aplicáveis ao tema de certificação ("Regras e Procedimentos de Certificação ANBIMA"), devendo garantir que todos os profissionais elegíveis estejam devidamente certificados.

8.2. Atividades Elegíveis e Critérios de Identificação

Tendo em vista a atuação das Gestoras como gestoras de recursos de terceiros, foi identificado, que a a CGA e a CGE são as certificações pertinentes às suas atividades, aplicáveis aos profissionais com alçada/poder discricionário de investimento..

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

Nesse sentido, para as Gestoras que atuam com gestão de patrimônio, destaca-se ainda que o Regras e Procedimentos de Certificação Anbima determina que, no mínimo, 75% (setenta e cinco por cento) dos profissionais que atuam na gestão de patrimônio, realizando o contato comercial com o investidor e o assessorando em suas decisões de investimento, devem ser certificados CEA, CGA, CGE, CFP ou CFA.

Nesse sentido, somente o Colaborador com poder final para ordenar a compra ou venda de posições, sem a necessidade de aprovação prévia do Diretor de Gestão, ou seja, o Colaborador que tenha, de fato, alçada/poder discricionário de investimentos, é elegível à CGA e CGE, a

depender do investimento gerido, uma vez que a CGA é a certificação aplicável aos profissionais que atuam em carteiras administradas, fundos de investimento financeiros e/ou fundos de índice e a CGE é aplicável aos profissionais que atuam em fundo de investimento em participações, fundo de índice, fundo de investimento em direitos creditórios e/ou fundo de investimento imobiliário.

Em complemento, as Gestoras destacam que as certificações são de cunho pessoal e intransferíveis. Observado que, a partir de 02 de janeiro de 2026, as Gestoras deverão manter, no mínimo 2 (dois) profissionais certificados, conforme detalhado adiante.

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

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

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

Antes da contratação, admissão ou transferência de área de qualquer Colaborador, o Diretor de Risco e Compliance, no âmbito de sua Gestora, 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 respectiva Gestora deverão inserir o Colaborador no Banco de Dados do Grupo Portofino.

O Diretor de Gestão deverá esclarecer ao Diretor de Risco e Compliance, no âmbito de sua Gestora, 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 Risco e Compliance deverá solicitar a comprovação da certificação pertinente ou sua isenção, se aplicável, anteriormente ao ingresso do novo Colaborador.

O Diretor de Risco e Compliance também deverá checar se Colaboradores que estejam se desligando da respectiva Gestora estão indicados no Banco de Dados da ANBIMA como profissionais elegíveis/certificados vinculados ao Grupo Portofino.

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

8.4. Rotinas de Verificação

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

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

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

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

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

Por fim, serão objeto do treinamento **anual** de compliance assuntos de certificação, incluindo, sem limitação: (i) treinamento direcionado a todos os Colaboradores, descrevendo as certificações aplicáveis à atividade das Gestoras, 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 ou CGE podem ter alçada/poder discricionário de decisão de investimento em relação aos ativos integrantes das carteiras sob gestão do Grupo Portofino, devendo os demais buscar aprovação junto o Diretor de Gestão responsável; (iii) treinamento direcionado aos Colaboradores das áreas de Compliance e de Risco, para que os mesmos tenham o conhecimento necessário para operar no Banco de Dados da ANBIMA e realizar as rotinas de verificação necessárias.

8.5. 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 das Regras e Procedimentos de Certificação ANBIMA, imediatamente afastados das atividades elegíveis aplicáveis, até que se certifiquem.

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

DISPOSIÇÕES GERAIS

Em cumprimento ao artigo 16, III, da Resolução CVM nº 21, a presente Política está disponível no endereço eletrônico do Grupo Portofino: www.portofinomultifamilyoffice.com.br.

VIGÊNCIA E ATUALIZAÇÃO

Esta política será revisada anualmente e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterada a qualquer tempo em razão de circunstâncias que demandem tal providência.

ANEXO I – TERMO DE RECEBIMENTO E COMPROMISSO AO MANUAL DE CONTROLES INTERNOS E DE COMPLIANCE DO GRUPO PORTOFINO

Pelo presente Termo de Recebimento e Compromisso, [**nome do novo Colaborador, nacionalidade, estado civil, profissão, identidade, CPF, residência**] ("Aderente"), na qualidade de [**cargo**] da [**nome e CNPJ da empresa**], empresa do grupo [**indicar Gestora do Grupo Portofino**], sociedade limitada com sede na Cidade e Estado de São Paulo, na Rua Leopoldo Couto Magalhães Jr., 758, conjuntos 111 e 112, Itaim Bibi, CEP 04542-000, inscrita no CNPJ/ME sob o nº [=] ("Gestora") a qual faz parte do Grupo Portofino ("Grupo Portofino"), se compromete e adere conforme abaixo:

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

II. O Aderente declara, neste ato, estar ciente de que o Manual como um todo passa a fazer parte dos seus deveres como Colaborador do Grupo Portofino, incorporando-se às demais regras internas adotadas pelo Grupo Portofino.

III. O Aderente também declara, neste ato, que recebeu, leu e compreendeu todas as demais políticas do Grupo Portofino, bem como recebeu o treinamento de integração inicial, momento no qual lhe foi explicado todas as principais normas e regras do Grupo Portofino.

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

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

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

VII. O Aderente se declara ciente do seu compromisso de comunicar o Diretor de Risco e Compliance e/ou o Comitê de Compliance das empresas do Grupo Portofino acerca de qualquer situação que chegue ao seu conhecimento que esteja em desacordo com as regras definidas neste Manual.

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

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

[CIDADE], [DATA].

[COLABORADOR]

ANEXO II – TERMO DE CONFIDENCIALIDADE

Por meio deste instrumento eu, [**nome do novo Colaborador, nacionalidade, estado civil, profissão, identidade, CPF, residência**], doravante denominado Colaborador, da [**nome e CNPJ da empresa**], empresa do grupo [**indicar Gestora do Grupo Portofino**]**,** sociedade limitada com sede na Cidade e Estado de São Paulo, na Rua Leopoldo Couto Magalhães Jr., 758, conjuntos 111 e 112, Itaim Bibi, CEP 04542-000, inscrita no CNPJ/ME sob o nº [=] ("Gestora") a qual faz parte do Grupo Portofino ("Grupo Portofino").

Resolvem as partes, para fim de preservação de informações pessoais e profissionais dos clientes e do Grupo Portofino 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 as empresas do Grupo Portofino, seus sócios e clientes, aqui também contemplados os próprios veículos sob gestão, 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 e carteiras geridas pela Gestora;
   c) Operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os clubes, fundos de investimento e carteiras geridas pela Gestora;
   d) Informações estratégicas ou mercadológicas e outras, de qualquer natureza, obtidas junto a sócios, sócios-diretores, funcionários, *trainees* ou estagiários das empresas do Grupo Portofino 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 das empresas do Grupo Portofino 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 e classes respectivas;
   f) Transações realizadas e que ainda não tenham sido divulgadas publicamente; e
   g) Outras informações obtidas junto a sócios, diretores, funcionários, *trainees* ou estagiários das empresas do Grupo Portofino 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 nas empresas do Grupo Portofino, comprometendo-se, portanto, a não divulgar tais Informações Confidenciais para quaisquer fins, Colaboradores não autorizados, mídia, ou pessoas estranhas às empresas do Grupo Portofino, 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 no Grupo Portofino, se comprometendo, ainda a não utilizar, praticar ou divulgar Informações Confidenciais, "*Insider Trading*", "Dicas" e "*Front Running*", seja atuando em benefício próprio, das empresas do Grupo Portofino ou de terceiros.

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

3. O Colaborador entende que a revelação não autorizada de qualquer Informação Confidencial pode acarretar prejuízos irreparáveis, ficando deste já o Colaborador obrigado a indenizar as empresas do Grupo Portofino, 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 nas empresas do Grupo Portofino são e permanecerão sendo propriedade exclusiva do empresas do Grupo Portofino 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 no Grupo Portofino, devendo todos os documentos permanecer em poder e sob a custódia das empresas do Grupo Portofino, salvo se em virtude de interesses do Grupo Portofino for necessário que o Colaborador mantenha guarda de tais documentos ou de suas cópias fora das instalações das empresas do Grupo Portofino;

(ii) Em caso de rescisão do contrato individual de trabalho, desligamento ou exclusão do Colaborador, o Colaborador deverá restituir imediatamente ao Grupo Portofino 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 do Grupo Portofino, 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 as empresas do Grupo Portofino, permitindo que o Grupo Portofino procure a medida judicial cabível para atender ou evitar a revelação.

   5.1. Caso o Grupo Portofino 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 ao Grupo Portofino 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 o Grupo Portofino, 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 do Grupo Portofino.

Assim, por estarem assim justas e contratadas, assinam o presente instrumento eletronicamente, nos termos do artigo 10 da Medida Provisória nº 2200-2, de 24 de agosto de 2001, cuja validade não será questionada.

[CIDADE], [DATA].

[COLABORADOR]

[EMPRESA]

ANEXO III – PRINCIPAIS NORMATIVOS APLICÁVEIS ÀS ATIVIDADES DO GRUPO PORTOFINO

1. Resolução CVM Nº 50/21
2. Resolução CVM Nº 21/21
3. Ofício-Circular/CVM/SIN/Nº 05/2014
4. Resolução CVM nº 175, de 23 de dezembro de 2022, conforme alterada e seus Anexos Normativos
5. Código Anbima de Autorregulação para Administração e Gestão de Recursos de Terceiros
6. Regras e Procedimentos de Administração e Gestão de Recursos de Terceiros
7. Código ANBIMA de Ética
8. Código ANBIMA de Certificação
9. Lei 9.613/98, conforme alterada
10. Demais manifestações e ofícios orientadores dos órgãos reguladores e autorregulados aplicáveis às atividades da Gestora

ANEXO IV - TERMO DE AFASTAMENTO

Por meio deste instrumento, eu,_____, inscrito(a) no CPF/ME sob o nº_____, declaro para os devidos fins que, a partir desta data, estou afastado das atividades de [gestão de recursos de terceiros / distribuição] da [**indicar Gestora do Grupo Portofino**], inscrita no CNPJ/ME sob o nº. [=] ("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 me conceda a isenção de obtenção da CGA;

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

São Paulo, [---] de [---] de [---].

[COLABORADOR]

[**indicar Gestora do Grupo Portofino**],

Testemunhas:

1._____
CPF/ME:

2._____ Nome:
Nome:
CPF/ME:

ANEXO V – TERMO DE PROPRIEDADE INTELECTUAL A POLÍTICA DE SEGURANÇA DA INFORMAÇÃOI E CIBERNETICA DO GRUPO PORTOFINO.

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

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

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

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

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

[•], [•] de [•] de [•].

[COLABORADOR]