POLÍTICA DE CONTROLES INTERNOS

KAPITALO ALOCAÇÃO GLOBAL GESTÃO DE RECURSOS LTDA.

Janeiro de 2021

Sumário

1. Objetivo

Esta Política de Controles Internos ("Política") tem por objetivo estabelecer regras, procedimentos e descrição dos controles internos a serem observados para o fortalecimento e funcionamento dos sistemas de controles internos da **KAPITALO ALOCAÇÃO GLOBAL GESTÃO DE RECURSOS LTDA.** ("Kapitalo").

As regras e procedimentos aqui descritos visam garantir o permanente atendimento pela Kapitalo e seus colaboradores às normas, políticas e regulamentações vigentes, referentes às diversas modalidades de investimento, à própria atividade de administração de carteiras de valores mobiliários e aos padrões ético e profissional.

Desta forma, estes procedimentos visam mitigar os riscos de acordo com a natureza, complexidade e risco das operações realizadas pela Kapitalo, bem como, disseminar a cultura de controles para garantir o cumprimento da Instrução da Comissão de Valores Mobiliários n.º 558, de 26 de março de 2015, conforme alterada (respectivamente "CVM" e "Instrução CVM n.º 558"), no Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros ("Código ANBIMA de ART") da Associação Brasileira das Entidades dos Mercados Financeiros e de Capitais ("ANBIMA") e no Código ANBIMA de Regulação e Melhores Práticas para o Programa de Certificação Continuada ("Código ANBIMA de Certificação"), bem como das demais normas estabelecidas pelos órgãos reguladores e autorreguladores.

2. Abrangência

Esta Política aplica-se a todos aqueles que possuam cargo, função, posição e/ou relação societária, empregatícia, comercial, profissional, contratual ou de confiança, (independentemente da natureza destas atividades, sejam elas direta, indireta e/ou secundariamente relacionadas com quaisquer atividades fim ou meio) com a Kapitalo ("Colaboradores"), por meio das quais possam ter ou vir a ter acesso a informações confidenciais ou informações privilegiadas de natureza financeira, técnica, comercial, estratégica, negocial ou econômica, dentre outras.

3. Ambiente Regulatório

Esta Política será entregue aos Colaboradores no momento de seu ingresso na Kapitalo conjuntamente com o Código de Ética e 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** ao Código de Ética ("Termo de Recebimento e Compromisso"), estão aceitando expressamente as normas, princípios, conceitos e valores aqui estabelecidos.

Todos os Colaboradores devem se assegurar do perfeito entendimento das leis e normas aplicáveis à Kapitalo bem como do completo conteúdo desta Política.

4. Princípios Gerais

As atividades objeto desta Política devem ser constantemente avaliadas, tomando como referência as boas práticas de governança corporativa. Os controles internos consistem em um processo desenvolvido para garantir que sejam atingidos os objetivos da instituição, nas seguintes categorias:

- Eficiência e efetividade operacional;
- Confiança nos registros de dados e informações;
- Conformidade; e
- Abordagem baseada em risco.

4.1. Diretrizes

Esta Política tem como diretrizes:

- Disseminar a cultura sobre a importância dos controles internos a todos os Colaboradores da Kapitalo;
- Assegurar o cumprimento das normas e regulamentos e aderência às políticas e procedimentos internos;
- Alinhar a estrutura dos controles internos aos riscos e objetivos do negócio;
- Garantir a existência de atribuição de responsabilidades e delegação de autoridade, observada a estrutura hierárquica da Kapitalo;
- Promover a elaboração de relatórios sobre a situação dos controles internos, a serem apreciados e aprovados por alçada competente; e
- Assegurar que o sistema de controles internos seja periodicamente revisado e atualizado de forma a garantir sua efetividade.

5. Governança

5.1. Responsável por Compliance

A atividade de controles internos e de cumprimento das políticas, procedimentos, controles internos e regras estabelecidas pela regulação vigente ("Compliance") é de responsabilidade da Área de Compliance da Kapitalo, cuja gerência é realizada pelo Responsável pelo Compliance, o qual é o diretor estatutário indicado no contato social e no Formulário de Referência da Kapitalo como responsável pelo cumprimento de regras, políticas, procedimentos e controles internos da Kapitalo ("Responsável por Compliance"), que realiza suas atividades com independência e de forma exclusiva, bem como pode exercer seus poderes e autoridade com relação a qualquer Colaborador.

Sem prejuízo das demais atribuições estabelecidas a seguir, o escopo de atuação do Responsável por Compliance também se encontra descrito no Código de Ética da Kapitalo.

I. Implementação e Manutenção do Sistema de Controles Internos

O Responsável por Compliance é o encarregado pela implantação de práticas de negócio eficientes e controles internos adequados e eficazes.

Os controles internos devem ser devidamente documentados pelos responsáveis das áreas de negócio e sua implementação deve tomar como base as disposições das políticas internas e manuais operacionais da Kapitalo.

II. Análise do Sistema de Controles Internos

O Responsável por Compliance é o encarregado pela supervisão e monitoramento dos controles internos da Kapitalo, sendo também responsável pelo atendimento aos órgãos reguladores e autorreguladores, sem prejuízos da atribuição do Comitê Executivo.

III. Avaliação do Sistema de Controles Internos

O Responsável por Compliance é encarregado por promover a avaliação independente das atividades desenvolvidas pelas áreas da Kapitalo, permitindo à aferição da adequação dos controles ao cumprimento das normas e regulamentos.

O processo de aferição é realizado através de um conjunto de exames de aderência nos processos existentes e documentados.

A periodicidade e os exames de aderência a serem realizados são definidos pelo Responsável por Compliance, de acordo com os eventos reportados.

Nesse sentido, serão realizados monitoramentos periódicos a cargo do Responsável por Compliance, sobre uma amostragem significativa dos Colaboradores, escolhida aleatoriamente pelo Responsável por Compliance, para que sejam verificados os arquivos eletrônicos, inclusive e-mails, com o objetivo de verificar possíveis situações de descumprimento às regras contidas na presente Política.

O Responsável por Compliance poderá utilizar as informações obtidas em tais sistemas a fim de apresentá-las ao Comitê de Compliance, o qual deverá decidir sobre eventuais sanções a serem aplicadas aos Colaboradores envolvidos, nos termos do Código de Ética. 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.

IV. Acompanhamento do Sistema de Controles Internos

O Responsável por Compliance é encarregado por acompanhar o resultado dos testes de aderência e supervisionar as atividades de controles internos da Kapitalo. Adicionalmente, o Responsável por Compliance também monitora a qualidade e integridade dos mecanismos de controles internos da Kapitalo, apresentando as recomendações de aprimoramento de políticas, práticas e procedimentos que entender necessárias.

O Responsável por Compliance também tem acesso regular à capacitação e treinamento dos Colaboradores ou futuros Colaboradores, podendo recomendar novos critérios, medidas e políticas, conforme seu discernimento.

Por fim, nos termos do artigo 22 da Instrução CVM n. 558, o Responsável por Compliance também é encarregado de encaminhar aos órgãos de administração da Kapitalo, até o **último dia útil do mês de abril** de cada ano, relatório referente ao ano civil imediatamente anterior à data de entrega, em linha com as exigências previstas na regulamentação aplicável.

Devendo referido relatório ser enviado aos órgãos de administração da Kapitalo e permanecer disponível à CVM na sede da Kapitalo ("Relatório de Controles Internos").

5.2. Comitê de Compliance

Conforme detalhado no Código de Ética, a Kapitalo também conta com um Comitê de Compliance que terá plena autonomia para o exercício de suas funções de supervisão do cumprimento das disposições das políticas internas da Kapitalo, inclusive para a definição e aplicação de sanções. A composição, periodicidade de reunião e forma de registro de decisões do Comitê de Compliance se encontram descritas no Código de Ética da Kapitalo.

5.3. Comitê Executivo

O Comitê Executivo se reúne mensalmente e é o principal fórum de deliberação das Gestoras Kapitalo, conforme termo definido na Política de Conflito de Interesses e Segregação de Atividades.

Compõem o Comitê Executivo o grupo de sócios controladores das Gestoras Kapitalo e, para que as decisões tomem efeito, faz-se necessária a presença e aprovação mínima de 3 (três) dos seus membros. As decisões do Comitê Executivo são registradas por e-mail.

6. Disposições Gerais

Em cumprimento ao art. 14, III, da Instrução CVM n.º 558, a presente Política de Controles Internos está disponível no endereço eletrônico da Kapitalo: http://www.kapitalo.com.br.

Eventuais comunicações para a Área de Compliance devem ser enviadas para compliance@kapitalo.com.br ou pelos canais de Compliance (https://app.compliasset.com/kapitalo-compliance) e Denúncia (https://app.compliasset.com/kapitalo) da gestora.

7. 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, momento o qual a Área de Compliance informará aos Colaboradores dos novos mecanismos de controles internos.

Histórico das atualizações desta Política		
Data	**Versão**	**Responsável**
Janeiro de 2021	1ª	Responsável por Compliance

ANEXO I

POLÍTICA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO

1. Apresentação

A Política de Segurança Cibernética e da Informação da Kapitalo aplica-se a todos os Colaboradores, prestadores de serviços, sistemas, incluindo trabalhos executados externamente ou por terceiros que utilizem o ambiente de processamento da Kapitalo, ou que acesse informações a ela pertencentes. Todo e qualquer usuário de recursos computadorizados da nossa instituição tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática.

2. Objetivo

A Kapitalo reconhece que o comprometimento com os princípios éticos e legais é indispensável para que sejam mantidos uma boa imagem e o alto padrão de confiabilidade de seus negócios e relacionamentos, constituindo tais princípios como a estrutura basilar para seu crescimento a médio e longo prazo dentro dos mercados financeiro e de capitais.

Assim, as políticas da Kapitalo refletem a sua filosofia, seus princípios cotidianos, prioridades e valores básicos para os processos de tomada de decisão de investimento.

A Kapitalo faz sua parte ao contribuir para que os mercados financeiro e de capitais estejam fundados na justiça, solidariedade e confiança para benefício de todos os envolvidos. Dentro desta linha, as Políticas da Kapitalo têm os seguintes objetivos:

a. Assegurar a conformidade com todos os requerimentos e diretrizes legais e regulatórias. É essencial para a Kapitalo que as autoridades regulatórias e de supervisão tenham confiança nas estruturas de Controles Internos e de Compliance da Kapitalo; e
b. Regulamentar a independência e eficiência das regras de Compliance em relação às demais atividades desenvolvidas pela Kapitalo.

Nesse sentido, a Política de Segurança Cibernética e da Informação visa proteger as informações de propriedade e/ou sob guarda da Kapitalo, garantindo que os recursos computacionais e os registros sejam, disponíveis, íntegros, seguros, confidenciais, legais, autênticos e auditáveis, conforme art. 4, §8º, da Instrução CVM n.º 558 e do Código ANBIMA de ART.

3. Segurança Cibernética

Os avanços tecnológicos criam facilidades e possibilitam o uso de novas ferramentas para a atuação das instituições, permitindo agilidade na construção e disponibilização de serviços, aplicação dos meios de comunicação, entre outros avanços. Por outro lado, o aumento do uso de tais ferramentas potencializa o vazamento de informações e os riscos de ataques cibernéticos, ameaçando a confidencialidade, a integralidade e a disponibilidade dos dados e/ou dos sistemas das instituições.

3.1. Identificação de Riscos

As ameaças cibernéticas podem variar de acordo com a natureza, vulnerabilidade, informações ou ativos de cada organização. As consequências para as instituições podem ser significativas em termos operacionais, de risco de imagem, danos financeiros ou perda de vantagem concorrencial, podendo tais danos serem irreparáveis.

Diante desse cenário, os métodos mais comuns de ataques cibernéticos são os seguintes:

- *Malware* – softwares desenvolvidos para corromper computadores e redes:

  - Vírus: software que causa danos a máquina, rede, softwares e banco de dados;
  - Cavalo de Troia: aparece dentro de outro software e cria uma porta para a invasão do computador;
  - *Spyware*: software malicioso para coletar e monitorar o uso de informações; e
  - *Ransomware*: software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.

- Engenharia Social – métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito:

  - *Pharming*: direciona o usuário para um site fraudulento, sem o seu conhecimento;
  - *Phishing*: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;
  - *Vishing*: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;
  - *Smishing*: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais;
  - Acesso pessoal; pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

- Ataques de DDoS (*distributed denial of services*) e *botnets* - ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos *botnets*, o ataque vem de um grande número de computadores infectados utilizados para criar e mandar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.
- Invasões (*advanced persistent threats*) - ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Ainda, além de ataques cibernéticos, a Kapitalo pode estar sujeita a mal funcionalidades dos sistemas utilizados e a atos ou omissões de seus Colaboradores, que podem acarretar na perda e/ou adulteração de dados e Informações Confidenciais.

3.2. Ações de Prevenção e Proteção

Para que se possam prevenir eventuais ataques cibernéticos e vazamento de informações, primeiro deve-se definir quais informações são as de maior sensibilidade para a Kapitalo,

assim como aquelas que teriam o maior impacto financeiro, operacional e reputacional para Kapitalo, em caso de incidente de segurança.

Deste modo, a Kapitalo segrega as informações geradas, aperfeiçoando a implementação de processos e o devido manuseio, armazenamento, transporte e descarte destas informações.

Assim, classifica-se as informações digitais da instituição em 3 (três) classes diferentes, quais sejam:

a) *Green Flag*:
   - Quaisquer informações e/ou dados que a Kapitalo teve acesso ou conhecimento por ser de domínio público ("Informação Pública");
   - Quaisquer informações e/ou dados que não estejam sujeitas a compromissos ou acordos de confidencialidade; ou
   - Quaisquer informações e/ou dados que tenham a obrigatoriedade de divulgação por lei ou autoridade competente.

b) *Yellow Flag*:
   - Quaisquer informações que venham a ter a obrigatoriedade de divulgação por lei ou autoridade competente, mas o termo legal ainda não foi iniciado ou findado (Ex. Data de Divulgação);

c) *Red Flag*:
   - Todas as informações definidas como "Informações Confidenciais", a saber:
   - *know-how*, técnicas, cópias, diagramas, modelos, amostras, programas de computador, informações técnicas, financeiras, estatísticas, logísticas ou relacionadas às estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e/ou dos fundos geridos pela Kapitalo;
   - operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento e carteiras geridas pela Kapitalo; e
   - estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços, bem como informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da Kapitalo e/ou de seus sócios e clientes.

A partir da definição acima, a Kapitalo se empenhará para manter controles, conforme o nível de criticidade das informações e dados, sendo certo de que a prioridade será escalonada na seguinte ordem de relevância: Red Flag, Yellow Flag e Green Flag.

3.3. Propriedade e Disponibilização:

Todos os recursos computacionais e de sistemas disponibilizados para os Colaboradores são de propriedade da Kapitalo. Não é permitida a utilização de notebooks, tablets ou outros hardwares para operações conectadas no servidor da Kapitalo, salvo expressa permissão da Área de Compliance. Tal restrição não se aplica ao Wi-fi "público", que pode ser utilizado pelos colaboradores.

Todos os computadores disponibilizados para os Colaboradores da Kapitalo têm por objetivo o desempenho das atividades profissionais na Kapitalo, não devendo ser utilizados para quaisquer outros fins.

Todo o processo de criação e exclusão de usuários, instalação de softwares e aplicativos, permissões de acesso, entre outras funcionalidades informáticas, devem ser previamente aprovada pela Área de Compliance.

a. A disponibilização e uso dos recursos tecnológicos da Kapitalo respeitam as seguintes regras:

- A cada novo Colaborador, a Área de TI autorizará, mediante solicitação do superior direto do colaborador, conforme orientado pela área em que o colaborador contratado for atuar e anuência da Área de Compliance, a criação de novo usuário e a disponibilização técnica de recursos;
- Todos os equipamentos, softwares e permissões acessos devem ser testados, homologados e autorizados pela TI Kapitalo, mediante supervisão e aprovação da Área de Compliance.
- A Área de TI autorizará, mediante solicitação, a retirada ou substituição do computador disponibilizado para o usuário e comunicará à Área de Compliance o evento;
- Cada computador tem o seu usuário gestor, que é responsável por esse equipamento. O controle das máquinas é de responsabilidade da TI Kapitalo, mediante supervisão e aprovação da Área de Compliance.
- A identificação do usuário é feita através do login e senha, que através do registro de logs utilizado pela Kapitalo é sua assinatura eletrônica no servidor da Kapitalo.
- Será apenas permitida senhas com no mínimo 08 (oito) caracteres alfanuméricos, maiúsculos e minúsculos. A reutilização de senhas obedecerá ao ciclo mínimo de 05 (cinco) vezes.
- Não é recomendada a utilização da mesma senha para projetos e serviços diferentes realizados pela Kapitalo, não devendo ser criada uma senha única padrão para todos os serviços e áreas em que um mesmo Colaborador atue.
- São permitidas apenas 05 (cinco) tentativas máximas de autenticação de senha, sendo todas malsucedidas, será bloqueado o acesso, o qual apenas poderá ser reestabelecido através de solicitação à Área de TI.
- A senha possui validade de 90 (noventa) dias e sua troca será solicitada automaticamente quando da sua expiração.
- Todos os eventos de login e alteração de senhas são auditáveis e rastreáveis, podendo ser solicitados pela Área de Compliance à TI Kapitalo.
- A Área de Compliance e o TI manterão inventários de softwares e usuários utilizados pelos colaboradores da Kapitalo para o exercício de suas atividades, estando esses na rede ou serem web.

b. A implantação e configuração de softwares da Kapitalo respeitam as seguintes regras:

- Todos os softwares, programas básicos (sistema operacional e ferramentas) e componentes físicos são implantados e configurados pela TI Kapitalo, mediante supervisão e aprovação da Área de Compliance.
- É desabilitado aos usuários implantar novos programas ou alterar configurações da rede sem a permissão formalizada da Área de Compliance e do TI.
- É desabilitado ao usuário implantar ou alterar componentes físicos em seus computadores.
- Somente é permitido o uso de equipamentos homologados e devidamente contratados pela Kapitalo.
- A utilização de equipamentos pessoais por terceiros nas instalações da Kapitalo e a conexão destes na rede interna à Internet requer autorização prévia e expressa da Área de Compliance. Os Colaboradores estão autorizados a conectar seus telefones celulares

e computadores pessoais diretamente à rede interna e à Internet, desde que utilizem suas credenciais de acesso.
- A conexão de dispositivos móveis de armazenamento (e.g. USB Drive) somente poderá ser realizada mediante autorização prévia e expressa da Área de Compliance.

c. Demais Proteções dos Recursos Tecnológicos

- Proteção de tela no computador e/ou proteção de ausência (após um tempo de inatividade, o computador bloqueia o sistema, exigindo senha para ser usado novamente).
- Bloqueio de Tela do computador automático por inatividade durante o período de 01 (uma) hora.
- Bloqueio do acesso as portas USB dos computadores para proteção contra vírus e cópia indevida dos dados contidos nos servidores.
-
- Bloqueio de sistemas de gerenciamento de computador à distância que não tenham sido previamente configurados pelo TI da Kapitalo a fim de viabilizar o trabalho remoto dos Colaboradores.

O Colaborador é responsável por todo acesso realizado com a sua autenticação.

A Kapitalo verifica regularmente eventuais desvios às condutas estabelecidas na presente Política por parte dos Colaboradores, por meio (a) do monitoramento, por amostragem, do acesso dos Colaboradores a sites, blogs, fotologs, webmails, entre outros, bem como os e-mails enviados e recebidos; e (b) da 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, a fim de aferir a integridade, autenticidade e auditabilidade das informações e sistemas, conforme 4º, §8º, da Instrução CVM n.º 558.

3.4. Responsabilidades dos Usuários:

O Colaborador é o custodiante dos recursos disponibilizados a ele, devendo este cuidar adequadamente do equipamento.

O Colaborador também deve garantir a integridade física e o seu perfeito funcionamento, seguindo as regras e orientações fornecidas pela Kapitalo.

Ainda, o Colaborador deve adotar um comportamento seguro condizente com a Política, devendo:

- Não compartilhar nem divulgar sua senha a terceiros;
- Não transportar Informações Confidenciais da Kapitalo em qualquer meio (CD, DVD, pendrive, papel, etc.) sem as devidas autorizações e proteções;
- Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas (aviões, restaurantes, encontros sociais, etc.);
- Não abrir mensagens de origem desconhecida, ou links suspeitos mesmo que advindos de origem conhecida;
- Armazenar e proteger adequadamente documentos impressos e arquivos eletrônicos que contêm Informações Confidenciais (conforme definido na Política de Confidencialidade da Kapitalo); e

- Seguir corretamente a política para uso de internet e correio eletrônico estabelecida pela Kapitalo.
- Informar os logins e acessos de sistemas que utiliza para o exercício de sua atividade.

3.4.1. Outras Proteções aos Computadores

- Proteção de tela no computador e/ou proteção de ausência (após um tempo de inatividade, o computador bloqueia o sistema, exigindo senha para ser usado novamente).
- "Log-off" automático por inatividade durante o período de 24 horas.
- Bloqueio do acesso as portas USB dos computadores para proteção contra vírus e cópia indevida dos dados contidos nos servidores.
- Bloqueio do acesso a sites.
- Bloqueio de sistemas de gerenciamento de computador à distância.

3.4.2. Regras do Uso da Internet

O Colaborador é responsável por todo acesso realizado com a sua autenticação.

Quando o usuário se comunicar através de recursos de tecnologia da Kapitalo, este deve sempre resguardar a imagem da Kapitalo, evitando entrar em sites de fontes não seguras, assim como de abrir e-mails pessoais, ou, de fontes não conhecidas.

Caso o usuário, acesse um site com conteúdo indevido por equívoco, deverá fechar a janela de imediato e reportar caso ache necessário.

O usuário é proibido de acessar endereços de internet (sites) que:

- Possam violar direitos de autor, marcas, licenças de programas (softwares) ou patentes existentes.
- Possuam conteúdo pornográfico, relacionado a sexo, exploração infantil ou ao crime de pedofilia.
- Contenham informações que não colaborem para o alcance dos objetivos da Kapitalo.
- Defendam atividades ilegais, menosprezem, depreciem ou incitem o preconceito a determinadas classes como sexo, raça, orientação sexual, religião, nacionalidade, local de nascimento ou deficiência física.
- Possuam origem suspeita ou que não se atenham aos padrões de segurança adequados, assim como possuírem links suspeitos.

O usuário deve garantir que está cumprindo a legislação em relação ao direito autoral, licença de uso e patentes existentes e que o uso do material foi autorizado, no mínimo, pelo gestor da sua área.

É proibido o uso de serviços de mensagem instantânea através dos computadores da Kapitalo, exceto em eventuais situações de uso profissional.

Também se faz expressamente proibido o uso de serviços de download de vídeos, filmes e músicas, através dos computadores da Kapitalo.

3.4.3. Responsabilidades e Forma de Uso de Correio Eletrônico

O Colaborador que utiliza um endereço de correio eletrônico é responsável por todo acesso, conteúdo de mensagens e uso relativos ao seu e-mail, podendo enviar mensagens necessárias para o seu desempenho profissional na Kapitalo.

É proibido criar, copiar ou encaminhar mensagens ou imagens que:

- Contenham declarações difamatórias ou linguagem ofensiva de qualquer natureza;
- Façam parte de correntes de mensagens, independentemente de serem legais ou ilegais;
- Repassem propagandas ou mensagens de alerta sobre qualquer assunto. Havendo situações em que o usuário ache benéfico divulgar o assunto para a Kapitalo, a sugestão deve ser encaminhada para a seu superior direto, que definirá a sua publicação ou não;
- Menosprezem, depreciem ou incitem o preconceito a determinadas classes, como sexo, raça, orientação sexual, idade, religião, nacionalidade, local de nascimento ou deficiência física;
- Possuam informação pornográfica, obscena ou imprópria para um ambiente profissional;
- Sejam susceptíveis de causar qualquer tipo de prejuízo a terceiros;
- Defendam ou possibilitem a realização de atividades ilegais;
- Sejam ou sugiram a formação ou divulgação de correntes de mensagens;
- Possam prejudicar a imagem da Kapitalo; e
- Sejam incoerentes com o Código de Ética da Kapitalo.

É proibido reproduzir qualquer material recebido pelo correio eletrônico ou outro meio, que possa infringir direitos de autor, marca, licença de uso de programas ou patentes existentes, sem que haja autorização expressa do autor do trabalho e da organização.

O Colaborador deve estar ciente que uma mensagem de correio eletrônico da Kapitalo é um documento formal e, portanto, possui as mesmas responsabilidades de um documento convencional em papel timbrado da entidade.

Exceto quando especificamente autorizado para tal, é proibido emitir opinião pessoal, colocando-a em nome da Kapitalo, tanto por vias escritas como por voz.

Deve observar se o endereço do destinatário corresponde realmente ao destinatário desejado. O Colaborador deve ser diligente em relação:

- Aos usuários que receberão a mensagem (Destinatário/ To, Copiado/Cc e Copiado Oculto/Bcc);
- Ao nível de sigilo da informação contida na mensagem;
- Aos anexos da mensagem, enviando os arquivos apenas quando for imprescindível e garantindo a sua confidencialidade;
- Ao uso da opção encaminhar (Forward), verificando se é necessária a manutenção das diversas mensagens anteriores que estão encadeadas.

É recomendável ao Colaborador deixar mensagem de ausência quando for passar um período maior do que 72 (setenta e duas) horas sem acessar seu correio eletrônico. Essa mensagem deve indicar o período de ausência e o endereço do substituto para quem deve ser enviada a mensagem.

4. Monitoramento e Testes de Contingência

O monitoramento dos controles existentes e estabelecidos nessa Política serão realizados e executados pela TI Kapitalo, sob supervisão da Área de Compliance. O referido monitoramento acontecerá de forma contínua.

Os Testes de Contingência serão realizados, no mínimo, anualmente, de modo a permitir que a Kapitalo esteja preparada para a continuação de suas atividades, assim como a mitigar eventuais riscos operacionais ou reputacionais. Outras informações acerca dos Testes de Contingência estão no Plano de Continuidade de Negócios da Kapitalo.

5. Plano de Resposta

Conforme as melhores práticas de mercado, a Kapitalo desenvolveu um Plano de Resposta para indícios, suspeita fundamentada, vazamento de Informações Confidenciais ou outra falha de segurança.

Na hipótese de verificação de uma das hipóteses acima, inclusive em decorrência da ação de criminosos cibernéticos, as providências pertinentes deverão ser iniciadas, devendo cada área responsável agir conforme o disposto na presente Política de Segurança Cibernética ou da Informação.

Estas providências consistem em:

(i) TI Kapitalo:
- Verificação e Auditoria dos Logs;
- Criação de laudo pericial contendo as informações que foram potencialmente vazadas;
- Execução de aplicativos externamente ou em sistemas afetados para eliminar aplicativos indesejados;
- Desinstalação de software;
- Execução de varreduras offline para descobrir quaisquer ameaças adicionais;
- Formatação e reconstrução do sistema operacional;
- Substituição física de dispositivos de armazenamento
- Reconstrução de sistemas e redes;
- Restauração de dados provenientes do backup realizado diariamente; e
- Entre outros.

(ii) Área de Compliance:
- Criação de relatório baseado no laudo pericial elaborado pela Empresa de TI Terceirizada, de forma a constar eventuais consequências reputacionais e jurídicas derivadas dos danos ocasionados pelo incidente de segurança; e
- Em caso de confirmação do incidente de segurança e eventual vazamento de informações confidenciais, elaborar notificação às partes impactadas informando o ocorrido.

(iii) BackOffice:
- Análise de dados perdidos e suas influências frente ao planejamento contábil e aos ativos da Kapitalo.
- Realizar planejamento dos impactos frente ao ocorrido.

Em caso de necessidade, poderá ser contratada empresa especializada no combate ao evento identificado, assim como nas respostas ao eventual dano.

Todo e qualquer incidente ocorrido, assim como os resultados do Plano de Resposta, deverão ser devidamente classificados por nível de severidade, arquivados e documentados pela Área de Compliance, bem como ser formalizado no Relatório de Controles Internos da Kapitalo.

Caso o evento tenha sido causado por algum Colaborador, deverá ser avaliada a sua culpabilidade, nos termos do Código de Ética da Kapitalo.

6. Treinamento

O Responsável por Compliance organizará treinamento **anual** dos Colaboradores com relação às regras e procedimentos acima, sendo que tal treinamento poderá ser realizado em conjunto com o treinamento anual de compliance (conforme estabelecido na Política de Treinamento da Kapitalo)

7. Revisão da Política

O Responsável por Compliance realizará uma revisão desta Política de Segurança da Informação e Segurança Cibernética a cada **24 (vinte e quatro) meses**, para avaliar a eficácia da sua implantação, identificar novos riscos, ativos e processos e reavaliando os riscos residuais. A finalidade de tal revisão será assegurar que os dispositivos aqui previstos permaneçam consistentes com as operações comerciais da Kapitalo e acontecimentos regulatórios relevantes.

ANEXO II

POLÍTICA DE TREINAMENTO

1. Treinamento e Processo de Reciclagem

A Kapitalo possui um processo de treinamento inicial de todos os seus Colaboradores, especialmente aqueles que tenham acesso à Informações Confidenciais (conforme termo definido na Política de Confidencialidade da Kapitalo) 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.

Em até 1 (um) mês após a contratação de cada Colaborador, ele participará de um processo de treinamento em que irá adquirir conhecimento sobre as atividades da Kapitalo e terá oportunidade de esclarecer dúvidas relacionadas a tais princípios e normas.

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

2. Implementação e Conteúdo

A implementação do processo de treinamento inicial e do programa de reciclagem continuada fica sob a responsabilidade do Responsável por 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 da Kapitalo, seus princípios éticos e de conduta, as normas de compliance, as políticas de segregação, quando for o caso, e as demais políticas descritas nesta Política (especialmente aquelas relativas à confidencialidade, segurança das informações, e segurança cibernética e negociações pessoais), bem como aquelas descritas no Código de Ética e na Política de Investimentos Pessoais da Kapitalo 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** do Código de Ética da Kapitalo.

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

ANEXO III

POLÍTICA DE COMBATE A CORRUPÇÃO

1. Objetivo

Seguindo os preceitos da Lei n.º 12.846, de 1º de agosto de 2013, conforme alterada ("Lei de Anticorrupção") bem como os de sua regulação, através do Decreto n.º 8.240, de 18 de março de 2015 ("Decreto n.º 8.240"), o combate à corrupção também é um dever de todos os Colaboradores com a Kapitalo.

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

2. Abrangência da Lei de Anticorrupção

A Lei de Anticorrupção responsabiliza objetivamente as pessoas jurídicas, nos âmbitos administrativo e civil, pelos atos lesivos previstos praticados em seu interesse ou benefício e não exclui a responsabilidade individual de seus dirigentes ou administradores ou de qualquer pessoa natural, autora, coautora ou partícipe do ato ilícito.

Considera-se agente público e, portanto, sujeito à Lei 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 Combate a Corrupção e da Lei de Anticorrupção.

3. Atos Lesivos e Sanções

Na forma da referida lei, entende-se por atos lesivos à administração pública os seguintes:

1) Prometer, oferecer ou dar, direta ou indiretamente, vantagem indevida a agente público, ou a terceira pessoa a ele relacionada;

2) Comprovadamente, financiar, custear, patrocinar ou de qualquer modo subvencionar a prática dos atos ilícitos previstos nesta Lei;

3) Comprovadamente, utilizar-se de interposta pessoa física ou jurídica para ocultar ou dissimular seus reais interesses ou a identidade dos beneficiários dos atos praticados;

4) No tocante a licitações e contratos: frustrar ou fraudar, mediante ajuste, combinação ou qualquer outro expediente, o caráter competitivo de procedimento licitatório público; impedir, perturbar ou fraudar a realização de qualquer ato de procedimento licitatório público; afastar ou procurar afastar licitante, por meio de fraude ou oferecimento de vantagem de qualquer tipo; fraudar licitação pública ou contrato dela decorrente; criar, de modo fraudulento ou irregular, pessoa jurídica para participar de licitação pública ou celebrar contrato administrativo; 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 manipular ou fraudar o equilíbrio econômico-financeiro dos contratos celebrados com a administração pública; e

5) 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.

4. Procedimentos e Programa de Integridade

A Kapitalo utiliza seus melhores esforços para monitorar todos os Colaboradores da instituição, de forma a garantir que os mesmos atuem em observância a Lei de Anticorrupção e sua regulamentação, respeitando e praticando, na medida de suas atividades e possibilidades, os atos referentes ao Programa de Integridade disposto no Decreto n.º 8.240.

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

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

(a) Comprometimento dos sócios da Kapitalo com o Programa de Integridade;
(b) Políticas de conduta e ética que são aplicadas para todos os Colaboradores da Kapitalo, inclusive a terceiros, quando necessário, vide Código de Ética da Kapitalo;
(c) Treinamento periódico dos Colaboradores, vide Política de Treinamento e Reciclagem dos Colaboradores da Kapitalo;
(d) Registros contábeis que reflitam as transações da Kapitalo de forma precisa e completa, feitos por empresa especializada externa;
(e) Independência dos procedimentos de compliance;
(f) Canais de comunicação de irregularidades abertos para quaisquer Colaboradores ou terceiros;

(g) Medidas disciplinares executadas contra aqueles que violarem as normas da Kapitalo, ou cometerem qualquer tipo de infração corruptiva listada acima; e
(h) Prévia análise antes de contratação de terceiros, conforme procedimentos listados no Apêndice I à presente Política.

Ademais, conforme mencionado acima e nas demais políticas, a Kapitalo não aceita em hipótese alguma a prática de qualquer uma das condutas listadas no item 3 acima, devendo os seus Colaboradores informar imediatamente a Área de Compliance, o conhecimento de qualquer atividade que se enseje na caracterização das infrações da Lei de Anticorrupção.

5. Normas de Conduta

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

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

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

Nenhum sócio ou colaborador poderá ser penalizado devido a atraso ou perda de negócios resultantes de sua recusa em pagar ou oferecer suborno a agentes públicos.

6. Proibição de Doações Eleitorais

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

7. Relacionamentos com Agentes Públicos

Quando se fizer necessária a realização de reuniões privadas, desde que não sejam eventos públicos ou organizadas por instituições financeiras e/ou contem com a participação de mais empresas, e audiências ("Audiências") com agentes públicos, sejam elas internas ou externas, a Kapitalo deverá se certificar de empregar a cautela exigida para a ocasião, com o objetivo de se resguardar contra condutas ilícitas no relacionamento com agentes públicos. Dentre os procedimentos adotados, os Colaboradores que estiverem representando a Kapitalo são instruídos a elaborar relatórios de tais Audiências, caso tenha identificado uma conduta por parte do agente público que possa ser considerada pelo Colaborador como irregular ou violadora da Lei de Anticorrupção e os apresentar ao Responsável por Compliance imediatamente após sua ocorrência.

Estão isentos desses procedimentos relacionamentos que ocorram no âmbito particular da vida do colaborador, ex. jantares de família e/ou amigos.

Apêndice I
Procedimentos Anticorrupção para Contratação de Terceiros

O objetivo desse anexo é estabelecer os critérios e orientar quanto aos procedimentos, atitudes e comportamentos a serem adotados nos processos de contratação e acompanhamento de empresas contratadas como prestadoras de serviços ("Terceiros"), com segurança operacional e jurídica, de forma a tornar a Kapitalo em compliance com as normas e regras acerca da matéria.

A Kapitalo poderá deixar de aplicar os procedimentos aqui expostos a seu exclusivo critério, em virtude do porte do prestador, do valor do contrato, do alto renome e/ou do notório conhecimento, uma vez que minimizará os riscos abarcados nessa política com a contratação desses Terceiros.

Para os efeitos deste procedimento, considera-se como Contratação de Terceiros, toda aquela em que a empresa contratada coloca mão de obra ou tecnologia à disposição da Kapitalo, devendo ser orientada pelos seguintes procedimentos:

1) Antes de qualquer contratação, **os Colaboradores da Kapitalo deverão recolher informações e referências sobre o referido Terceiro**, tais como: (i) antigos clientes, inclusive entrando em contato com eles; (ii) pesquisas na rede mundial de computadores sobre notícias negativas acerca do Terceiro; e (iii) entre outras informações desse gênero.

2) Os Terceiros deverão ser legalmente constituídos e ter comprovado idoneidade e capacidade técnico-econômica e administrativo-trabalhista, para assunção das responsabilidades contratuais. De forma a comprovar tal capacidade, antes de qualquer Contratação de Terceiros, **os Colaboradores envolvidos no negócio deverão requisitar o Contrato Social ou Estatuto Social da referida empresa mais atualizado**.

3) **Os Colaboradores envolvidos na contratação também deverão verificar o Cadastro Nacional de Pessoas Jurídicas**, a fim de confirmar as informações contidas no Contrato Social ou Estatuto Social do terceiro.

4) **O início das atividades dos Terceiros deve ficar vinculado à formalização da contratação dos serviços. Nenhum tipo de pagamento pelos serviços prestados poderá ser efetuado antes da celebração do contrato**.

5) Além dos procedimentos acima expostos, as seguintes informações e documentos poderão ser computados para decisão de contratação ou não do terceiro, a saber:

(a) Sócios dos Terceiros;
(b) Idoneidade;
(c) Qualidade dos serviços;
(d) Estrutura; e
(e) Demonstrações Financeiras.

ANEXO IV

POLÍTICA DE CERTIFICAÇÃO E CAPACITAÇÃO

1 Objetivo

Esta Política de Certificação e Capacitação ("Política de Certificação") estabelece as diretrizes para a capacitação da equipe de gestão da Kapitalo com o objetivo de desenvolver competências específicas sobre Gestão de Fundos de Investimento, considerando que a Kapitalo aderiu e está sujeita às disposições do Código ANBIMA de Certificação, devendo garantir que todos os profissionais elegíveis estejam devidamente certificados.

2 Abrangência

Esta Política de Certificação é aplicável aos colaboradores da área de gestão de recursos de terceiros da Kapitalo ("Colaboradores").

3 Vigência

Os procedimentos definidos nesta Política de Certificação entrarão em vigor na data de sua aprovação e serão revisados anualmente, devendo 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.

4 Área Responsável pela Revisão desta Política

O Comitê Executivo será responsável pela revisão desta Política de Certificação.

5 Conceito

Assegurar a observância das normas legais e regulamentares relativas à capacitação de profissionais que desempenham atividades de gestão de recursos de terceiros e possibilitar um desenvolvimento e capacitação especializada aos colaboradores para exercer com excelência o atendimento aos clientes.

6 Diretrizes

6.1. Procedimento adotado para determinar as Atividades Elegíveis:

A Kapitalo considera que todos os profissionais que atuam na área de gestão desempenhando atividades de gestão de recursos e tenham poder decisório de gestão, devem possuir, no mínimo, Certificação de Gestores ANBIMA (CGA), não existindo pré-requisito quanto à formação acadêmica. Em complemento, a Kapitalo destaca que a CGA é certificação pessoal e intransferível.

Os Colaboradores que não tenham CGA (e que não tenham a isenção concedida pelo Conselho de Certificação, nos termos do Art. 17 do Código ANBIMA de Certificação) estão impedidos de ordenar a compra e venda de ativos para os fundos de investimento sob

gestão sem a aprovação prévia do Responsável pela Gestão, tendo em vista que não possuem alçada/poder final de decisão para tanto.

6.2. Procedimentos para identificação de profissionais certificados

6.2.1. Admissão

Durante o processo admissional de um novo profissional será solicitado o preenchimento da Ficha Admissional. Nela o colaborador deverá declarar se possui ou já possuiu alguma certificação da ANBIMA. Em posse dessas informações, o RH informará a Área de Compliance sobre o colaborador e seus dados, incluindo as suas certificações.

Após ser informado sobre a contratação do novo profissional, a Área de Compliance entrará em contato com o responsável pela contratação para entender as atividades que serão desempenhadas pelo novo Colaborador. Em posse dessa informação, a Área de Compliance estipulará a necessidade de o mesmo possuir alguma certificação. Caso seja observado a necessidade, ele será instruído a obtê-la e somente após aprovado nos exames é que poderá assumir as funções relacionadas a tal certificação.

Após à data de início do novo colaborador, o Compliance acessará o Banco de Dados da ANBIMA, e caso o profissional conste no mesmo, será feita a vinculação dele à Kapitalo.

6.2.2. Alteração de Funções e Desligamento

Caso haja novas oportunidades para que o colaborador exerça novas funções, a Área de Compliance irá se certificar de que o ele possuí as certificações necessárias para exercer tais atividades. Caso não as possua, ele deverá obtê-las antes de assumir suas novas responsabilidades.

No momento do desligamento de algum colaborador o Compliance providenciará as devidas alterações junto ao Banco de Dados da ANBIMA.

Os profissionais já certificados, caso deixem de ser Colaboradores da Kapitalo, deverão assinar a documentação prevista no Apêndice I a esta Política de Certificação denominado "Termo de Afastamento", comprovando o seu afastamento da Kapitalo. O mesmo procedimento de assinatura do Apêndice I 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.

6.3. Procedimento para atualização da certificação

A Área de Compliance será responsável por monitorar e notificar os prazos de vencimento da certificação profissional aos profissionais relacionados diretamente à atividade de gestão de recursos de terceiros, para que eles realizem os procedimentos de atualização de sua certificação, antes do seu vencimento. Para isso, a Área de Compliance possuí um controle interno das certificações, com base nas informações do Banco de Dados da ANBIMA, que é atualizado sempre que algum colaborador novo entra ingressa nas empresas do grupo ou algum colaborador adquire alguma certificação.

Ainda, a Área de Compliance deverá, semestralmente, contatar a Área de RH, 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.

A atualização da certificação deve ocorrer antes do vencimento da certificação vigente. Nesse sentido, caso o Colaborador esteja exercendo a atividade elegível de CGA na Kapitalo, conforme acima indicada, e a certificação não esteja vencida a partir do vínculo do Colaborador com a Kapitalo, o prazo de validade da certificação CGA será indeterminado, enquanto perdurar o seu vínculo com a Kapitalo.

6.4. Procedimento para afastamento

Caso seja identificada a situação de um profissional relacionado diretamente à gestão de recursos de terceiros que não possua certificação válida, seja pela não obtenção ou pelo vencimento da certificação, ao Área de Compliance irá notificá-lo, imediatamente, verbalmente e por escrito que está impedido de realizar tais atividades, devendo seu superior imediato designar outras funções, bem como apurar potenciais irregularidades e eventual responsabilização dos envolvidos, inclusive dos superiores do Colaborador, conforme aplicável, e ainda para traçar um plano de adequação.

Nesse sentido, todos os profissionais não certificados ou em processo de certificação, e para os quais a certificação seja exigível, nos termos previstos nesta Política de Certificação, serão, nos termos do art. 9º, §1ª, inciso V do Código de Certificação, imediatamente afastados das atividades elegíveis aplicáveis, até que se certifiquem. O evento será reportado no sistema de Compliance da Kapitalo e as evidências da notificação e da suspensão serão arquivados dentro do sistema.

O profissional poderá voltar a exercer sua função de gestão somente quando obtiver a certificação.

7. Procedimento de atualização no Banco de Dados ANBIMA

A Área de Compliance será responsável por atualizar as informações relativas aos seus profissionais certificados, em processo de certificação, com a certificação vencida, e/ou em processo de atualização da certificação, especialmente no que se refere à contratação, desligamento e área de atuação.

A atualização deverá ser realizada sempre que houver alguma alteração relevante até o último dia do mês subsequente à data de ocorrência do evento, por meio da plataforma disponibilizada pela ANBIMA, nos termos do Art. 12, §1º, I do Código ANBIMA de Certificação, sendo que a manutenção das informações contidas no Banco de Dados deverá ser objeto de análise e confirmação pela Área de Compliance

8. Treinamento

Com o objetivo de assegurar a observância das normas legais e regulamentares relativas à capacitação de profissionais que desempenham atividades de gestão de recursos de terceiros, a presente Política de Certificação será apresentada anualmente aos Colaboradores nos treinamentos internos a respeito das políticas internas.

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

Apêndice I
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 da **KAPITALO ALOCAÇÃO GLOBAL GESTÃO DE RECURSOS LTDA.** ("Kapitalo") por prazo indeterminado:

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

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

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

São Paulo, [•] de [•] de [•].

_____
[COLABORADOR]

_____
KAPITALO ALOCAÇÃO GLOBAL GESTÃO DE RECURSOS LTDA.

Testemunhas:

1._____
Nome:
CPF:

2._____
Nome:
CPF:

(Destacar)