POLÍTICA DE

COMPLIANCE E SEGURANÇA DA INFORMAÇÃO

Atualização 23/03/2020

bari.
asset

Política de *Compliance* e Controles Internos

Objetivo

Formalizar os procedimentos para gerenciamento dos riscos de *compliance* e controles internos na Barigui Gestão de Recursos Ltda. ("GESTORA").

A quem se aplica?

Sócios, diretores e funcionários que participem, de forma direta, das atividades diárias e negócios, representando a GESTORA (doravante, "Colaboradores").

Os Colaboradores devem atender às diretrizes e procedimentos estabelecidos nesta Política, informando qualquer irregularidade ao **Diretor de *Compliance* e Risco.**

Responsabilidades

Cabe à GESTORA garantir, por meio de regras, procedimentos e controles internos adequados, o permanente atendimento às normas, políticas e regulamentações vigentes, referentes às diversas modalidades de investimento, à própria atividade e aos seus padrões éticos e profissionais.

Todos devem adotar e cumprir as diretrizes e controles aplicáveis à GESTORA contidas nesta Política, zelando para que todas as normas éticas e legais sejam cumpridas por todos aqueles com quem são mantidas relações de cunho profissional, comunicando imediatamente qualquer violação ao **Diretoria de *Compliance* e Risco.**

Cabe à alta administração da GESTORA:

1-) A responsabilidade pelos controles internos e o gerenciamento dos riscos de *compliance*;

2-) Indicar um diretor estatutário responsável por *compliance* e controles internos, com capacidade técnica e função independente das relacionadas à administração de carteiras de valores mobiliários (ou em qualquer atividade que limite a sua independência, na instituição ou fora dela), devendo tal profissional ter acesso a todas as informações e pessoas no exercício de suas atribuições;

3-) Aprovar, estabelecer e divulgar esta Política; e

4-) Garantir a efetividade do gerenciamento do risco de *compliance*.

O Diretor de *Compliance* e Controles Internos deve:

1-) Auxiliar a alta administração a assegurar a efetividade do Sistema de Controles Internos e *Compliance* da GESTORA, atuando no gerenciamento efetivo de tais atividades no seu dia-a-dia;

2-) Gerenciar o Comitê de *Compliance* e Risco, garantindo seu adequado funcionamento e o registro em ata das decisões tomadas;

3-) Designar o secretário das reuniões do Comitê de *Compliance* e Risco;

4-) Monitorar e exercer os controles e procedimentos necessários ao cumprimento das normas**.**

Todos os Colaboradores devem estar comprometidos com a cultura de *compliance* e reportar imediatamente ao Diretor de *Compliance* e Risco qualquer suspeita e/ou evidência de desconformidade por eles verificada.

É responsabilidade de todos os Colaboradores da GESTORA o cumprimento das normas legais, infralegais e autorregulatórias aplicáveis às suas atividades, bem como de todas as normas internas da GESTORA, devendo comunicar imediatamente a ocorrência de violações e/ou indícios de violação ao **Diretor de *Compliance* e Risco**.

O Diretor de *Compliance* e Risco se reporta apenas à alta administração da GESTORA, tendo autonomia para indagar a respeito de práticas e procedimentos adotados nas suas operações/atividades, e devendo adotar medidas que coíbam ou mitiguem os efeitos nelas porventura reputados inadequados, incorretos e/ou inaplicáveis.

Os controles internos e monitoramentos de conformidade determinados nesta Política são prerrogativa exclusiva dos integrantes da Área de *Compliance* e Controles Internos, sendo exercidos de forma autônoma e independente, com ampla liberdade de discussão e análise dos temas sob sua responsabilidade.

A Área de *Compliance* é formada pelo diretor estatutário responsável e por um analista interno, o qual se dedica com exclusividade ao exercício das atividades de cumprimento de regras, políticas, procedimentos e controles internos, incluindo gestão de riscos e cumprimento das normas relativas ao combate e prevenção à lavagem de dinheiro.

A GESTORA colocará à disposição da Diretoria de *Compliance* e Risco alternativas de atualização, capacitação e treinamento na matéria, as quais deverão ser objeto de aprovação final pelos sócios.

Revisão e Atualização

Esta Política deverá ser revisada a atualizada a cada 2 (dois) anos, ou em prazo inferior, se assim determinado em mudanças legais/regulatórias/autorregulatórias.

Escopo e Atribuições do *Compliance* e Controles Internos

Em matéria de *compliance* e controles internos, o escopo de atuação do Diretor de *Compliance* e Risco abrange:

Temas Normativos

- ✓ Controlar a aderência às novas leis, regulamentações, práticas e diretrizes de autorregulação aplicáveis à GESTORA, e apresentar o resultado de suas verificações no Comitê de *Compliance* e Controles Internos;
- ✓ Controlar e monitorar as licenças legais, registros e certificações necessárias (registros na CVM, na Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais – ANBIMA, e demais entidades aplicáveis), bem como sua renovação/manutenção junto às autoridades competentes;
- ✓ Auxiliar a alta administração da GESTORA no relacionamento com órgãos reguladores e assegurar que as informações requeridas sejam fornecidas no prazo e qualidade requeridos; e
- ✓ Realizar testes internos, revisões e relatórios obrigatórios nas frequências definidas nas políticas e manuais internos, bem como na legislação em vigor.

Boas Práticas

- ✓ Disseminar e promover - junto com a Diretoria da GESTORA - as informações necessárias para o cumprimento das políticas internas e normas legais, infralegais e de autorregulação, bem como exercer seu controle, garantindo que as políticas e manuais pertinentes estejam atualizados e mantidos em diretório acessível a todos que delas devam ter conhecimento;
- ✓ Disponibilizar aos novos Colaboradores as políticas internas aplicáveis, e coletar os termos de ciência e aderência por eles assinados;
- ✓ Estabelecer controles para que todos os Colaboradores da GESTORA que desempenhem funções ligadas à gestão de fundos de investimento ou carteiras administradas atuem com independência e atentem ao devido dever fiduciário para

com seus clientes, e que os interesses comerciais, ou aqueles de seus clientes, não desviem o foco de seu trabalho;

- ✓ Garantir que os controles internos sejam compatíveis com os riscos da GESTORA em suas atividades, bem como efetivos e consistentes com a natureza, complexidade e risco das operações realizadas para o exercício profissional de administração de carteiras de valores mobiliários;
- ✓ Auxiliar a alta administração da GESTORA a assegurar a efetividade desta Política;
- ✓ Analisar informações, indícios ou identificar, administrar e, se necessário, levar o tema para análise e deliberação no Comitê de *Compliance* e Risco, no caso de eventuais conflitos de interesses ou descumprimentos regulatórios e/ou de políticas e normas;
- ✓ Comunicar aos órgãos competentes, nos prazos regulatórios, a respeito de eventuais descumprimentos normativos, de modo a assegurar que todas as informações solicitadas sejam prontamente disponibilizadas;
- ✓ orientar previamente e/ou acompanhar o responsável pela comunicação à imprensa em contatos telefônicos, entrevistas, publicação de artigos ou qualquer outra forma de manifestação de opinião através de veículo público, inclusive na internet.

Governança

- ✓ Aprovar novas políticas internas no Comitê de *Compliance* e Risco, ou a sua revisão, por força da regulamentação ou decisões internas;
- ✓ Aprovar a oferta de novos produtos e prestação de novos serviços pela GESTORA, a partir de *inputs* técnicos do Comitê de Investimento;
- ✓ Atuar para que haja efetividade na segregação física de atividades conflitantes;
- ✓ Apresentar o resultado de seus controles e verificações no Comitê de *Compliance* e Risco;
- ✓ Monitorar e buscar a efetiva aplicação dos documentos de *compliance* e controles internos abaixo listados;
- ✓ Servir como canal para comunicações de desconformidades regulatórias e/ou de temas relacionados ao Código de Ética e Conduta Profissional da GESTORA;
- ✓ Convocar, gerenciar, organizar e secretariar o Comitê de *Compliance* e Controles Internos, registrando suas decisões em atas;
- ✓ O Comitê de *Compliance* e Risco se reunirá bimestralmente, e o Conselho de Ética apenas sob demanda, podendo ambos, ainda, ser convocados sempre que necessário para avaliação de casos de desvio de conduta pessoal e profissional.

Análise e Comunicação aos Órgãos Competentes

Toda desconformidade em temas de conduta pessoal e profissional - e a sua respectiva análise efetuada pelo *Compliance* - deve ser submetida ao Comitê de *Compliance* a Risco

da GESTORA para conclusão e deliberação dos passos a serem dados a respeito.

Nos casos aplicáveis de desvio da norma específica das atividades reguladas, o Diretor de *Compliance* e Risco deve comunicar os respectivos órgãos competentes, nos prazos regulatórios, como seguem:

- ✓ **A CVM deve ser comunicada no prazo máximo de 10 (dez) dias da respectiva ocorrência ou sua identificação ou prazo menor se exigido pela regulamentação;**
- ✓ **O COAF deve ser comunicado no prazo de 24 (vinte e quatro) horas da sua efetiva identificação.**

Documentos de *Compliance* e Controles Internos

O Sistema de *Compliance* e Controles Internos da GESTORA se dá mediante seus documentos internos, que englobam todas as suas políticas, manuais e Código de Ética e Conduta Profissional, além dos seguintes procedimentos e organismos:

Documentos Específicos Disponibilizados no *Website* da GESTORA

Cabe ao Diretor de *Compliance* e Risco preencher o respectivo Formulário de Referência da GESTORA e mantê-lo em seu *website*. Tal formulário deve ser atualizado obrigatoriamente até o dia 31 de março de cada ano**.**

Adicionalmente, cabe ao Diretor de *Compliance* e Risco manter no *website* da GESTORA, em sua versão atualizada, os seguintes documentos:

- ✓ Código de Ética e Conduta Profissional;
- ✓ Política de *Compliance* e Controles Internos;
- ✓ Política de Gestão de Riscos;
- ✓ Política de Investimentos Pessoais e da Empresa;
- ✓ Política de Rateio de Ordens de Investimento;
- ✓ Formulário de Referência da GESTORA;
- ✓ Política de Exercício de Direito de Voto em Assembleias Gerais.

Relatório Anual

Para verificação dos controles internos, sua efetividade e consistência com a natureza, complexidade e riscos das operações realizadas pela GESTORA, é realizado um teste anual de aderência, o qual deve ser formalizado em um relatório formal (modelo no **Anexo I**, e orientação sobre o respectivo conteúdo no **Anexo II**).

O relatório é de responsabilidade do Diretor de *Compliance* e Risco, e, após ratificação pelo Comitê de *Compliance* e Risco, será encaminhado ao Comitê Executivo da GESTORA anualmente, até o último dia útil de **abril** de cada ano (com conteúdo relativo à análise do ano civil imediatamente anterior).

O Relatório Anual fica disponível para consulta da CVM, na sede da GESTORA.

Tal relatório contém:

- ✓ **As conclusões dos exames efetuados relativos aos controles internos e *Compliance*;**
- ✓ **As recomendações a respeito de eventuais deficiências, com o estabelecimento de cronogramas de saneamento, quando for o caso; e**
- ✓ **A manifestação do diretor responsável pela gestão de carteiras de valores mobiliários ou, quando for o caso, pelos diretores responsáveis pela gestão de risco e de *compliance* e controles internos a respeito das deficiências encontradas em verificações anteriores e das medidas planejadas, de acordo com cronograma específico, ou efetivamente adotadas para saná-las.**

Mecanismos Adicionais de *Compliance* e Controles Internos

Além da aplicação das políticas e controle de seus procedimentos em si, são também mecanismos de *Compliance* e controles internos:

- ✓ **A disseminação e o conhecimento** do conteúdo dos termos e dos documentos acima, atestados com a assinatura do Termo de Conhecimento e Aceitação das políticas por todos os Colaboradores (parte integrante do Código de Ética e Conduta Profissional da GESTORA);
- ✓ **Certificações** - Controle da regularidade das certificações pertinentes;
- ✓ **Teste e Relatório de Aderência Anual -** descrito abaixo em tópico específico;
- ✓ **Teste Anual dos Sistemas de Informações -** Conforme descrito na Política de Segurança da Informação, os testes periódicos dos sistemas de informações, em especial para os mantidos em meio eletrônico, efetuados pela Diretoria de *Compliance* e Risco, devem: (i) assegurar que os recursos humanos e computacionais estão adequados ao porte e à área de atuação da GESTORA, (ii) garantir o adequado nível de confidencialidade e acessos às informações confidenciais, (iii) assegurar que os recursos computacionais sejam protegidos contra adulterações e (iv) assegurar que a manutenção de registros permita a realização de auditorias e inspeções;
- ✓ **Implementação de Regras e Guarda de Evidências** – monitorar a adequada implementação de procedimentos necessários para o cumprimento das normas, e das políticas internas, bem como a adequada manutenção de mecanismos de

guarda de evidências que demonstre a sua aplicação;

- ✓ **Salvaguarda de Informações -** O administrador de carteiras de valores mobiliários deve manter, pelo prazo mínimo de 5 (cinco) anos, ou por prazo superior por determinação expressa da CVM, todos os documentos e informações exigidos pela regulação aplicável, bem como toda a correspondência, interna e externa, todos os papéis de trabalho, relatórios e pareceres relacionados com o exercício de suas funções. Os documentos e informações podem ser guardados em meio físico ou eletrônico, admitindo-se a substituição de documentos originais pelas respectivas imagens digitalizadas.

Organismos Relacionados a *Compliance* e Controles Internos

Comitê de *Compliance* e Risco

O Comitê de *Compliance* e Risco é o organismo responsável por **avaliar o descumprimento das normas legais, regulatórias, autorregulatórias e das políticas internas, manuais e procedimentos internos da GESTORA.**

Ademais, cabe ao Comitê de *Compliance* e Risco avaliar, do ponto de vista normativo, a atividade da GESTORA e dos veículos de investimento sob sua responsabilidade, a fim de garantir a aderência à legislação e normas administrativas e autorregulatórias em vigor, bem como aprovar ações de correção nestas matérias, além de:

- ✓ **Avaliar os processos internos da GESTORA do ponto de vista de melhores práticas, bem como avaliar as ocorrências do período;**
- ✓ **Concluir por eventuais apontamentos de situações irregulares à alta administração da GESTORA;**

- ✓ **Analisar eventuais situações ocorridas de desenquadramento de mandato, procedimentos adotados, e recomendações de controle futuro;**
- ✓ **Elaborar e distribuir a Lista Restrita de Ativos fazendo seu acompanhamento e monitoramento; e**
- ✓ **Monitorar mudanças regulatórias e coordenar ajustes e adaptações necessárias na GESTORA e seus produtos.**

Periodicidade: semestralmente ou sob demanda

Participantes: Diretor de Gestão, diretor de *Compliance* e Risco e Diretor Administrativo

Convidados: os demais Colaboradores podem ser convidados, porém, sem direito a voto

Formalização das decisões: atas do Comitê

Política de Certificação

A quem se aplica?

Sócios, diretores, funcionários, prestadores de serviço, terceirizados, consultores e demais pessoas físicas ou jurídicas contratadas ou outras entidades que participem, de forma direta, das atividades diárias e negócios, representando a Barigui Gestão de Recursos Ltda. (respectivamente, "GESTORA" e "Colaboradores"), que desempenhem atividades diretas de **gestão profissional** de carteiras de títulos e valores mobiliários, com alçada de decisão sobre o investimento, desinvestimento e manutenção dos recursos dos recursos dos veículos de investimento a cargo da GESTORA.

Os Colaboradores devem atender às diretrizes e procedimentos estabelecidos nesta Política, informando qualquer irregularidade ao **Diretor de *Compliance* e Risco.**

Responsabilidades

O Diretor de *Compliance* e Risco é responsável pelos controles que garantem o atendimento às demandas relativas à necessidade ou não de certificação dos profissionais da GESTORA.

Revisão e Atualização

Esta política deverá ser revisada a atualizada a cada 2 (dois) anos, ou em prazo inferior, se necessário, em função de mudanças legais/regulatórias/autorregulatórias.

Elegibilidade

A GESTORA desempenha atividades de gestão de carteiras de títulos e valores mobiliários. Segundo a Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais - ANBIMA, o seu "Código de Regulação e Melhores Práticas – Programa de Certificação Continuada" ("Código de Certificação") se aplica também a quaisquer integrantes do conglomerado ou grupo econômico da GESTORA que desempenhem qualquer das atividades disciplinadas pelo Código (*i.e.*, qualquer sociedade controlada, controladora ou sob controle comum com a GESTORA).

Assim sendo, a GESTORA requer dos profissionais elencados acima a Certificação de Gestores ANBIMA (CGA).

Controles

A Área de *Compliance* mantém controle dos Colaboradores da GESTORA com as seguintes informações:

- ✓ dados profissionais;
- ✓ data de admissão;
- ✓ data de desligamento, quando aplicável;
- ✓ atividade exercida;
- ✓ área de atuação;
- ✓ cargo;
- ✓ tipo de gestor, quando aplicável;
- ✓ endereço eletrônico individual;
- ✓ se dispõe de certificação ANBIMA e a sua validade.

O Diretor de *Compliance* e Risco é responsável por verificar que todos os Colaboradores elegíveis à CGA sejam certificados e que as respectivas certificações estejam válidas.

A CGA é válida por prazo indeterminado, desde que o profissional esteja exercendo atividades que dela sejam objeto.

Compete ao Diretor de *Compliance* e Risco garantir que um Colaborador não certificado não exerça função que pressuponha certificação ou que a obtenha nos termos ditados pela ANBIMA. Caso o Colaborador não disponha da certificação aplicável, o Diretoria de *Compliance* e Risco é responsável por manter a documentação formal que evidencie o afastamento do Colaborador das atividades elegíveis à certificação.

Cabe ao Diretor de *Compliance* e Risco monitorar o cumprimento das demais diretrizes estabelecidas no Código de Certificação da ANBIMA.

As certificações pendentes e o afastamento das funções elegíveis devem ser reportadas ao Comitê de *Compliance* e Risco, que deve monitorar a regularização.

Quaisquer outras situações identificadas aplicáveis à matéria devem ser objeto de análise, aprovação, formalização ou eventual assunção de risco no âmbito do Comitê de *Compliance* e Risco.

Admissões de Colaboradores

O **Diretor de *Compliance* e Risco** acompanha as informações sobre novas admissões e transferências internas, e se os novos Colaboradores possuem a respectiva certificação ANBIMA eventualmente aplicável.

Os candidatos a cargos que pressupõem certificação CGA devem ser contratados com certificações válidas. Eventuais exceções deverão ser avaliadas pelo Diretor de *Compliance* e Risco e reportadas ao Comitê de *Compliance* e Risco para controle das respectivas atividades e possível afastamento das funções até a efetiva obtenção da certificação aplicável.

O Diretoria de *Compliance* e Risco deve cadastrar, no site da ANBIMA, o novo funcionário e/ou transferido internamente, o que deve ocorrer no mesmo mês da contratação/transferência. Além disso, deve atualizar seus controles internos.

Licenças e Desligamentos

No caso de licenças e desligamentos, o **Diretor de *Compliance* e Risco** verifica se o Colaborador está vinculado à GESTORA no site da ANBIMA, e, nesse caso, desvincula o profissional, o que deve ocorrer **impreterivelmente** no mesmo mês de licença e/ou desligamento.

Os profissionais em licença não devem continuar vinculados no período em que estiverem de licença. Quando retornarem, deverá ser efetuado o vínculo novamente.

Banco de Dados da ANBIMA

O **Diretor de *Compliance* e Risco** é responsável pela veracidade e manutenção do banco de dados da ANBIMA atualizado.

O controle de admissão, licença e demissão consta na agenda regulatória do Comitê de *Compliance* e Risco, onde são formalizados tais registros, devendo as **eventuais atualizações junto à entidade ocorrer até o último dia do mês subsequente ao evento.**

Código de Ética e Conduta Profissional

O Código de Certificação determina que a GESTORA observe os princípios e padrões de conduta definidos em seu Código de Ética e Conduta Profissional, bem como evidencie a adesão de seus profissionais até o último dia do mês subsequente à sua contratação.

Cabe ao Diretor de *Compliance* e Risco requerer dos novos Colaboradores um Termo de Conhecimento e Adesão ao Código de Ética e Conduta Profissional e das demais políticas da GESTORA.

O **Diretor de *Compliance* e Risco** também é responsável por controlar os termos do Código de Ética e Conduta Profissional e das demais políticas internas da GESTORA, além de verificar e se certificar de que os novos Colaboradores tomem conhecimento dos mesmos dentro do próprio mês de admissão.

Política de Confidencialidade e Segurança da Informação

Objetivo

Estabelecer princípios e diretrizes de proteção das informações no âmbito da Barigui Gestão de Recursos Ltda. ("GESTORA").

A quem se aplica?

Sócios, diretores, funcionários, prestadores de serviço, terceirizados, consultores e demais pessoas físicas ou jurídicas contratadas ou outras entidades, que participem, de forma direta, das atividades diárias e negócios, representando a GESTORA (doravante, "Colaboradores").

Responsabilidades

Os Colaboradores devem atender às diretrizes e procedimentos estabelecidos nesta Política, informando quaisquer irregularidades ao **Diretor de *Compliance* e Risco**, a quem caberá (i) avaliá-las, e (ii) submetê-las ao Comitê de *Compliance* e Risco, o qual decidirá sobre as eventuais medidas cabíveis.

O **Diretor de *Compliance* e Risco** deve garantir o atendimento a esta Política, sendo o responsável na GESTORA por temas de segurança da informação/cibernética.

Revisão e Atualização

Esta Política deverá ser revisada e atualizada a cada 2 (dois) anos, ou em prazo inferior, caso necessário, em função de mudanças legais/regulatórias/autorregulatórias.

Definições

São consideradas "Informações Confidenciais" aquelas não disponíveis ao público, que:

- ✓ **Identifiquem dados pessoais, patrimoniais ou estratégicos;**
- ✓ **Sejam objeto de acordo de confidencialidade celebrado com terceiros;**
- ✓ **Identifiquem ações estratégicas – dos negócios da GESTORA, seus clientes ou dos portfólios sob gestão – cuja divulgação possa prejudicar a gestão dos negócios, clientes e fundos de investimentos a cargo da GESTORA, ou reduzir sua vantagem competitiva;**
- ✓ **Todas as informações técnicas, jurídicas e financeiras, escritas ou arquivadas eletronicamente, que digam respeito às atividades da GESTORA, e que sejam devidamente identificadas como sendo confidenciais, ou que constituam sua propriedade intelectual ou industrial, e não estejam disponíveis, de qualquer outra forma, ao público em geral;**
- ✓ **Sejam assim consideradas em razão de determinação legal, previsão legal, regulamentar e/ou autorregulatória; e que**
- ✓ **O Colaborador utiliza para autenticação de sua identidade (senhas de acesso ou crachás) de uso pessoal e intransferível.**

Na atividade de gestão, a GESTORA considera que o controle do fluxo de informações é o risco mais relevante em termos de controle estratégico para o seu negócio. A mitigação de tal risco se dá através de procedimentos operacionais de segurança, ligados ao uso de equipamentos internos (mitigado através dos contratos/sistemas fornecidos pelos prestadores de serviço), e através de procedimentos internos que parametrizam o comportamento dos Colaboradores, descritos nesta Política.

Não caracteriza descumprimento desta Política a divulgação de Informações Confidenciais mediante prévia autorização do **Diretor de *Compliance* e Risco,** em atendimento a ordens do Poder Judiciário ou autoridade regulatória, administrativa ou legislativa competente, seja em âmbito municipal, estadual ou federal, bem como quando a divulgação se justificar, por força da natureza do contexto da revelação da informação, a advogados, auditores e contrapartes.

Em caso de dúvida, o Colaborador deverá consultar previamente o **Diretor de *Compliance* e Risco** acerca da possibilidade de compartilhamento da Informação Confidencial, a qual deverá se manifestar formalmente sobre o caso.

Disposições Gerais

Os seguintes princípios norteiam a segurança da informação na GESTORA:

Confidencialidade: o acesso à informação deve ser obtido somente por pessoas autorizadas, e quando for de fato necessário;

<u>Disponibilidade</u>: as pessoas autorizadas devem ter acesso à informação sempre que necessário;

<u>Integridade</u>: a informação deve ser mantida em seu estado original, visando a protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

As seguintes diretrizes devem ser seguidas por todos os Colaboradores da GESTORA:

- ✓ As informações confidenciais devem ser tratadas de forma ética e sigilosa, e de acordo com as leis e normas internas vigentes, evitando-se mau uso e exposição indevida;
- ✓ A informação deve ser utilizada de forma transparente, e apenas para a finalidade para a qual foi coletada;
- ✓ A concessão de acessos às informações confidenciais deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades;
- ✓ A identificação de qualquer Colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas;
- ✓ Segregação de instalações, equipamentos e informações comuns, quando aplicável;
- ✓ A senha é utilizada como assinatura eletrônica e deve ser mantida secreta, sendo proibido seu compartilhamento.

Qualquer risco ou ocorrência de falha na confidencialidade e na segurança da informação devem ser reportados ao Diretoria de *Compliance* e Risco.

Processos e Controles

Para assegurar que as informações sejam adequadamente protegidas, a GESTORA definiu os seguintes processos/controles:

Identificação da Informação

O Colaborador que recebe ou prepara uma informação deve identificar a natureza desta, conforme o item a seguir.

Classificação da Informação

Algumas informações podem ser classificadas como “Confidenciais”.

Para tal, devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida

das informações.

Controles para Informações Classificadas como "Confidencial"

O acesso às Informações Confidenciais deve ser controlado.

Sempre que necessário, contratos de confidencialidade da informação devem ser assinados com terceiros, sob supervisão do **Diretor de *Compliance* e Risco**, e, se reputado necessário, da assessoria jurídica da GESTORA.

Salvaguarda da Informação

A informação deve receber proteção adequada em todo o seu ciclo de vida, que compreende a sua geração, manuseio, armazenamento e descarte.

O Colaborador responsável pela informação gerada deve ter conhecimento do tempo regulatório de salvaguarda e gerenciar o seu armazenamento e descarte. Em caso de dúvida, o Colaborador deverá consultar o **Diretor de *Compliance* e Risco**.

O descarte de Informação Confidencial armazenada em meio físico deve ser efetuado utilizando máquina fragmentadora/trituradora de papéis ou incineradora.

Mesa Limpa

Nenhuma Informação Confidencial deve ser deixada à vista nos locais de trabalho dos Colaboradores. Ademais, ao usar uma impressora coletiva, o documento impresso deve ser imediatamente recolhido.

Gestão de Acessos

Os serviços de rede, internet e correio eletrônico disponíveis na GESTORA são de sua propriedade exclusiva, sendo permitido o uso moderado para fins particulares, mediante autorização prévia do **Diretor de *Compliance* e Risco**.

A GESTORA poderá, a qualquer momento, mediante prévia aprovação do Diretor de *Compliance* e Risco:

- ✓ **inspecionar conteúdo e registrar o tipo de uso dos e-mails feitos pelos usuários;**
- ✓ **disponibilizar esses recursos a terceiros, caso entenda necessário;**
- ✓ **solicitar aos usuários justificativas pelo uso efetuado.**

No caso de mudança de área ou desligamento do Colaborador, a respectiva senha de acesso é imediatamente adaptada para compatibilizar/adequar o acesso, ou cancelada em definitivo, visando ao impedimento de acesso não autorizado pelo ex-Colaborador.

Boas Práticas de Utilização

A utilização da rede, internet, e-mail e dispositivos móveis na GESTORA e/ou pelos seus Colaboradores em comunicações de trabalho devem se dar pelas seguintes regras:

- ✓ somente enviar mensagens para as pessoas envolvidas no assunto tratado, certificando-se dos endereços de destino escolhidos;
- ✓ somente imprimir as mensagens quando realmente necessário;
- ✓ ao identificar mensagem com título ou anexo suspeito, certificar-se sobre a segurança em abrí-la, para evitar vírus ou códigos maliciosos;
- ✓ no caso de recebimento de mensagens que contrariem as regras estabelecidas pela GESTORA, **NUNCA** as repassar, alertando o responsável da sua área e do **Diretor de *Compliance* e Risco**, se for o caso;
- ✓ Ao se ausentar do seu local de trabalho, mesmo que temporariamente, bloquear a estação de trabalho;
- ✓ Quando sair de férias ou se ausentar por períodos prolongados, o Colaborador deve utilizar o recurso de ausência temporária de e-mail.

Vedações

É vedado ao usuário:

- ✓ Enviar e-mail ou acessar sites que promovam a veiculação de mensagens, produtos, imagens ou informações que interfiram na execução das atividades profissionais, sendo proibido, sobretudo, conteúdo pornográfico, racista, subversivo ou ofensivo à moral e aos princípios éticos;
- ✓ Divulgar informações ou trocar arquivos com configurações dos equipamentos e de negócios da GESTORA, ou qualquer outra informação sobre a GESTORA, seus negócios, produtos, equipamentos ou Colaboradores, sem prévia aprovação para isso. Em caso de exigência de alguma autoridade ou entidade autorreguladora, solicitar orientação ao **Diretor de *Compliance* e Risco**;
- ✓ Trocar informações que causem quebra de sigilo bancário e/ou possuam caráter confidencial ou estratégico;
- ✓ Prejudicar intencionalmente usuários da internet, mediante desenvolvimento de programas, acessos não autorizados a computadores e alteração de arquivos, programas e dados residentes na rede da GESTORA;
- ✓ Divulgar propaganda ou anunciar produtos ou serviços particulares pelo correio eletrônico da GESTORA;

- ✓ Alterar qualquer configuração técnica dos softwares que comprometam o grau de segurança, ou impeçam/dificultem seu monitoramento pelo **Diretor de *Compliance* e Risco**;
- ✓ Contratar provedores de acesso sem autorização prévia do **Diretor de *Compliance* e Risco**;
- ✓ Redirecionar caixa postal pessoal (e-mail de outros provedores) para a sua caixa postal de correio eletrônico na GESTORA e vice-versa.
- ✓ Fazer cópias (físicas ou eletrônicas) ou imprimir os arquivos utilizados, gerados ou disponíveis na rede e circular em ambientes externos com estes arquivos, salvo se em prol da execução e do desenvolvimento dos negócios e dos interesses da GESTORA. Nestes casos, o Colaborador que estiver na posse e guarda do arquivo será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

Bloqueio de Acesso a Sites

O **Diretor de *Compliance* e Risco***,* juntamente com os responsáveis pelo departamento de Tecnologia da Informação*,* é responsável por monitorar os acessos feitos a sites através de computadores de propriedade da GESTORA, para reporte de eventual mau uso ao Comitê de *Compliance* e Risco, e bloqueio de acesso a sites proibidos.

Sites de Armazenamentos de Arquivos

O acesso a sites de armazenamento de arquivos em "nuvem" é permitido.

Os equipamentos, ferramentas e sistemas concedidos aos Colaboradores devem ser configurados com os controles necessários para cumprir os requerimentos de segurança aplicáveis à GESTORA.

Apenas os Colaboradores devidamente autorizados terão acesso às dependências e sistemas a que estiverem liberados, bem como aos arquivos, diretórios e/ou pastas na rede da GESTORA, mediante segregação física e lógica. Quaisquer exceções deverão ser previamente solicitadas ao o **Diretor de *Compliance* e Risco**, que poderá ou não conceder a exceção.

Gestão de Riscos, Tratamento de Incidentes de Segurança da Informação, Continuidade de Negócio e *Backups*

Os riscos e incidentes de segurança da informação devem ser reportados ao o **Diretor de *Compliance* e Risco**, que adotará as medidas cabíveis.

O plano de contingência e de continuidade dos principais sistemas e serviços deve ser

objeto de testes, visando a reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

No caso de vazamento de informação, ou acesso indevido a informação, o Diretor de *Compliance* e Risco deverá ser imediatamente comunicado para a tomada das medidas cabíveis, variando de simples repreensão pelo acesso, ou mensagem ao destinatário errôneo da mensagem enviada para que apague em definitivo o seu conteúdo, até o estudo e implementação efetiva de providências judiciais, quando e se for o caso, tudo isso sem prejuízo da investigação e eventual punição dos Colaboradores envolvidos, mediante apresentação do caso pelo Diretor de *Compliance* e Risco no Comitê de *Compliance* e Risco.

Testes de Controles

A efetividade desta Política é verificada por meio de testes periódicos dos controles existentes, com intervalos não superiores a 1 (um) ano, sob responsabilidade da **Diretoria de *Compliance* e Controles Internos** e reportados ao Comitê de *Compliance* e Controles Internos.

Os testes devem verificar se:

- ✓ **Os recursos humanos e computacionais são adequados ao porte e às áreas de atuação;**
- ✓ **Há adequado nível de confidencialidade e acessos às informações confidenciais, com identificação de pessoas que tem acesso a estas informações;**
- ✓ **Há segregação física e lógica;**
- ✓ **Os recursos computacionais, de controle de acesso físico e lógico, estão protegidos;**
- ✓ **A manutenção de registros permite a realização de auditorias e inspeções.**

Propriedade Intelectual

Tecnologias, marcas, metodologias e quaisquer informações que pertençam à GESTORA não devem ser utilizadas para fins particulares, nem repassadas a outrem, ainda que tenham sido obtidas ou desenvolvidas pelo próprio Colaborador em seu ambiente de trabalho.

Rastreamento

É permitido o uso pessoal dos equipamentos de informática e de comunicação de propriedade da GESTORA utilizados pelos Colaboradores para a realização das atividades profissionais. Lembrando que, como tais recursos (e-mails, sistemas, computadores,

telefones etc.) pertencem à GESTORA, estes são rastreáveis e sujeitos a monitoramento sem a necessidade de ciência prévia do Colaborador, bem como podem se tornar públicos em caso de auditoria, exigência judicial ou regulatória.

Cybersegurança

Na prestação de seus serviços, a GESTORA obtém e lida com informações sensíveis, não disponíveis ao público em geral, e que podem ocasionar perdas irreparáveis em casos de malversação, negligência ou vazamentos: os riscos potenciais relativos a tais dados envolvem invasões, disseminação errônea ou dolosa, acesso indevido e/ou seu roubo/desvio. O responsável por tais questões na GESTORA é o Diretor de *Compliance* e Risco.

Os Colaboradores deverão observar os seguintes pontos na utilização de equipamentos eletrônicos pertencentes/cedidos pela GESTORA, bem como no acesso à sua rede interna:

- ✓ Os equipamentos deverão ser utilizados com a finalidade primordial de atender aos interesses comerciais da GESTORA, sendo permitida a sua utilização para fins pessoais apenas de forma moderada, com vistas a prevenir invasões, disseminação errônea ou dolosa, acesso indevido e/ou roubo/desvio de informações;

- ✓ A gravação de cópias de arquivos e instalação de programas em computadores da GESTORA deverá respeitar as regras estabelecidas na presente Política, devendo haver a prévia autorização do responsável pelo respectivo departamento da GESTORA, pelo responsável pela área de informática, e, no caso de eventuais dúvidas, a prévia autorização por escrito pelo Diretor de *Compliance* e Controles Internos. Esta medida se destina a evitar a disseminação errônea ou dolosa, acesso indevido e/ou roubo/desvio de informações;

- ✓ *Downloads* podem ser realizados, desde que de forma ponderada, vedados os conteúdos oriundos de sites ou remetentes desconhecidos do Colaborador, maliciosos, pornográficos, racistas, discriminatórios, difamatórios, subversivos, ofensivos a minorias, à moral e/ou aos princípios éticos, assim prevenindo invasões, disseminação errônea ou dolosa e/ou roubo/desvio de informações;

- ✓ O e-mail corporativo da GESTORA é um correio eletrônico corporativo para todos os efeitos legais, especialmente os relacionados aos direitos trabalhistas, sendo sua utilização preferencial voltada para alcançar os fins comerciais aos quais se destina, sendo permitida a utilização pessoal apenas de forma moderada. Tal procedimento tem como objetivo prevenir invasões, disseminação errônea ou dolosa, acesso indevido e/ou roubo/desvio de informações;

- ✓ Os e-mails recebidos pelos Colaboradores da GESTORA, quando abertos, deverão ter seu conteúdo verificado pelo Colaborador, não sendo admitida, em nenhuma hipótese, a manutenção ou arquivamento de mensagens de remetentes desconhecidos do Colaborador, maliciosas, pornográficas, racistas, discriminatórias, difamatórias, subversivas, ofensivas a minorias, à moral e/ou aos princípios éticos, sendo a responsabilidade apurada de forma específica em relação ao destinatário da mensagem. O propósito aqui é evitar invasões, acesso indevido e/ou roubo/desvio de informações;

- ✓ Os computadores, arquivos, e, arquivos de e-mails corporativos poderão ser inspecionados a critério do Diretor de *Compliance* e Risco, a qualquer tempo, independentemente de prévia notificação ao Colaborador, a fim de disseminação errônea ou dolosa, acesso indevido e/ou roubo/desvio de informações;

- ✓ Em regra, os acessos a dispositivos móveis, como pen drives, HDs externos, cartões de memória, estão bloqueados na GESTORA, devendo as eventuais exceções devem ser previamente aprovadas pelo responsável por *Compliance*. Tal aspecto visa a disseminação errônea ou dolosa, acesso indevido e/ou roubo/desvio de informações;

- ✓ Cada Colaborador terá acesso somente a pastas eletrônicas relacionadas à sua área e às pastas comuns a todos os Colaboradores, assim se evitando disseminação errônea ou dolosa, acesso indevido e/ou roubo/desvio de informações;

- ✓ A GESTORA dispõe de *firewall* de segurança nos servidores para acesso à sua rede, visando a manter o ambiente de trabalho disponível e livre de vírus e acessos indesejados. O sistema de prevenção a ataques de vírus é regularmente atualizado. Tais procedimentos têm por objetivo prevenir invasões e acesso indevido de informações;

- ✓ É realizado *backup* de arquivos de forma sistemática diariamente. Os dados de *backup* atualizados são armazenados em nuvem e em local seguro, com monitoramento remoto via *software*, por parte do prestador de serviço de tecnologia da GESTORA;

São adotadas ainda as seguintes medidas preventivas para cada risco acima identificado:

- O histórico de backup é armazenado em disco físico, com redundância que fica fora da rede do escritório;

- Também são utilizados serviços de nuvem para armazenamento de *backup*;

- O escritório possui um *firewall* na entrada da rede filtrando entrada de pacotes;

- É utilizado um sistema de proteção nas estações de trabalho com análise de comportamento de *malwares*, sistema de prevenção de intrusão e sistema de reconhecimento de agentes maliciosos desconhecidos; e

- É utilizado anti-*malware* nas estações de trabalho para evitar ataques de vírus, *ransomware*, *phishing* entre outros.

No que diz respeito à segurança cibernética, o conteúdo desta Política deverá ser atualizado num prazo não superior a 24 (vinte e quatro) meses, quando e se houver mudança regulatória/autorregulatória sobre o tema.

ANEXO I

Modelo de Relatório de Aderência

Ilmos. Srs.

Sócios e Diretores da

BARIGUI GESTÃO DE RECURSOS LTDA

Ref.: Relatório Anual – Instrução CVM nº 558, de [ano]

Prezados Senhores,

Em cumprimento ao disposto no art. 22 da Instrução CVM n.º 558, de 26 de março de 2015 ("ICVM 558"), vimos apresentar a V.Sas. o relatório pertinente às atividades da **[GESTORA]**, ("GESTORA") no ano de [•] ("Relatório").

De acordo com a ICVM 558, o mencionado Relatório contém:

- ✓ As conclusões dos exames efetuados;
- ✓ As recomendações a respeito de eventuais deficiências, com o estabelecimento de cronogramas de saneamento, quando for o caso; e
- ✓ 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 eventuais deficiências encontradas em verificações anteriores e das medidas planejadas, de acordo com cronograma específico, ou efetivamente adotadas para saná-las (cf. art. 22, I, II e III, da ICVM 558).

Este relatório ficará à disposição da Comissão de Valores Mobiliários ("CVM") na sede da GESTORA, para eventuais posteriores checagens, verificações e/ou fiscalizações por parte da CVM.

Além dos aspectos acima, V.Sas. encontrarão também, no corpo do presente Relatório, os resultados do Teste de Aderência determinado na Política de *Compliance* e Controles Internos da GESTORA, e o correspondente parecer final do Diretor *Compliance*

e Controles Internos, que assina o presente documento.

Assim sendo, passamos abaixo à exposição dos elementos pertinentes do presente Relatório.

I. **Conclusão dos Exames Efetuados (ICVM 558, art. 22, I)**

(enumerar detalhadamente por área/ocorrência, com todas as informações pertinentes, incluindo datas da verificação da ocorrência e sua natureza)

II. **Recomendações sobre as Deficiências Encontradas e Cronogramas de Saneamento (ICVM 558, art. 22, II)**

(enumerar detalhadamente por área/ocorrência, com todas as informações pertinentes, incluindo estimativas de datas de acompanhamento e conclusão das soluções)

III. **Manifestações dos Diretores Correspondentes de Gestão e de Risco sobre as Verificações Anteriores e Respectivas Medidas Planejadas (ICVM 558, art. 22, III)**

(enumerar detalhadamente por área/ocorrência, com todas as informações pertinentes, incluindo os resultados esperados e os efetivamente alcançados)

IV. **Parecer Final do Diretor de Risco, *Compliance* e Controles Internos**

(enumerar detalhadamente)

Sendo então o que nos cumpria para o momento, aproveitamos o ensejo desta correspondência para nos colocarmos à disposição de V.Sas. para os eventuais esclarecimentos porventura reputados necessários.

Atenciosamente,

BARIGUI GESTÃO DE RECURSOS LTDA
Diretor de *Compliance* e Risco

ANEXO II

Orientações Gerais sobre o Conteúdo Técnico do Teste de Aderência

A **Diretoria de *Compliance* e Controles Internos** deve estruturar registro e controle **ativo, ao longo do ano,** para composição do Relatório Anual (descrito no Anexo I), ao menos sobre as seguintes matérias relacionadas abaixo.

Tais temas devem – ao longo do ano – ser endereçados e monitorados no Comitê de *Compliance*, Controles Internos e Ética, e, quando necessário, ser objeto de acompanhamento próximo da alta gestão (sócios e diretores) da GESTORA.

Tal controle deve ser feito em planilhas específicas, servindo como ferramenta de *compliance* e controle de risco operacional.

O controle ao longo do ano dos eventos abaixo, e seu registro é uma das obrigações centrais do Comitê de *Compliance*, Controles Internos e Ética.

I. **Conclusão dos Exames Efetuados (ICVM 558, art. 22, I)**

(enumerar detalhadamente por área/ocorrência, com todas as informações pertinentes, incluindo datas da verificação da ocorrência e sua natureza)

→ Deve constar em planilha de controle o registro dos seguintes eventos (ao menos) ocorridos ao longo do ano, suas consequências / perdas e as atitudes corretivas adotadas:

- ✓ **erros operacionais atinentes a operações dos fundos;**
- ✓ **erros relativos a movimentações financeiras de clientes;**
- ✓ **falhas em pagamentos de remuneração de distribuidores ou corretagem de fundos pagas a corretoras ou quaisquer prestadores de serviço;**
- ✓ **desenquadramentos de carteiras, comunicação com administrador e reenquadramento;**
- ✓ **qualquer outro descumprimento de norma legal constatado;**
- ✓ **eventos de liquidez dos fundos;**
- ✓ **falhas operacionais relativas à infraestrutura tecnológica e plano de correção implementado;**
- ✓ **acionamentos do plano de contingência e continuidade de negócios;**
- ✓ **falhas de fornecedores;**
- ✓ **falhas relativas a quaisquer políticas internas ou normas legais e plano de correção implementado;**

- ✓ **mudanças expressivas em parâmetros de liquidez dos fundos;**
- ✓ **eventos relacionados ao gerenciamento de risco, com especial atenção a risco de crédito e liquidez;**
- ✓ **ofícios ou qualquer outro alerta e comunicação recebidos de reguladores, ou processos administrativos junto à CVM, ANBIMA e demais reguladores aplicáveis, ou em alçadas do poder judiciário;**
- ✓ **descumprimento de obrigações relativas à certificação;**
- ✓ **descumprimento de contratos quaisquer;**
- ✓ **quebra de dever de sigilo contratual;**
- ✓ **quaisquer eventos adicionais considerados relevantes pelo *compliance* e que tenham colocado em risco a empresa, seus colaboradores, clientes, carteiras sob gestão ou as boas práticas de mercado.**