AURORA
CAPITAL

POLÍTICA DE *COMPLIANCE* E CONTROLES INTERNOS

AURORA CAPITAL GESTORA DE RECURSOS LTDA.

Agosto-2020

Objetivo

Formalizar os procedimentos para gerenciamento dos riscos de *compliance* e controles internos na Aurora Capital Gestora de Recursos Ltda. ("GESTORA" ou "AURORA").

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").

Os Colaboradores devem atender às diretrizes e procedimentos estabelecidos nesta Política de *Compliance* e Controles Internos ("Política"), informando qualquer irregularidade à Diretora de *Compliance* e de Gestão de Risco, conforme definido no contrato social vigente da AURORA.

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, conforme detalhado adiante.

Todos devem adotar e cumprir as diretrizes e controles aplicáveis à GESTORA contidas nesta Política e nas demais políticas e manuais internos aplicáveis, 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 à Diretora de *Compliance* e de Gestão de Risco.

Revisão e Atualização

Esta Política deverá ser revisada a atualizada a cada 12 (doze) meses, ou em prazo inferior, se assim determinado em mudanças legais, regulatórias e autorregulatórias.

Estrutura de Governança e Mecanismos de *Compliance*

A estrutura de governança da GESTORA é formada fundamentalmente: pela Diretoria de Gestão de Carteira de Valores Mobiliários; pelo Comitê de Investimento e Crédito; pela Diretoria de *Compliance* e de Gestão de Risco; pelo Comitê de *Compliance*, Controles Internos e Ética; e pelo Comitê de Risco.

Diretoria de Gestão de Carteira de Valores Mobiliários

A Diretoria de Gestão de Carteira de Valores Mobiliários é responsável pela elaboração de estudos e análises dos investimentos a serem feitos pela GESTORA, mensurando a atratividade de cada ativo a ser investido, levando tais análises e estudos ao Comitê de Investimento e Crédito, bem como a sua execução, seguindo as diretrizes fixadas nas políticas de investimento previstas em seus regulamentos, conforme as orientações, decisões e/ou restrições estabelecidas pelo Comitê de Investimento e Crédito.

Diretoria de *Compliance* e de Gestão de Risco

A Diretoria de *Compliance* e de Gestão de Risco é responsável por, dentre outras tarefas:

- ✓ Gerenciar o Comitê de *Compliance*, Controles Internos e Ética, garantindo seu adequado funcionamento e o registro em ata das decisões tomadas;
- ✓ Designar o secretário das reuniões do Comitê de *Compliance*, Controles Internos e Ética;
- ✓ Coordenar o processo de *due dilligence* nas companhias alvo dos fundos de investimento em participações sob gestão ("FIPs");
- ✓ Monitorar e exercer os controles e procedimentos necessários ao cumprimento das normas;
- ✓ Realizar, sempre que necessário, o informe de transações suspeitas junto à Unidade de Inteligência Financeira (UIF) ou o reporte negativo anual, nos termos da legislação, caso seja aplicável;
- ✓ Implementar a política de gestão de riscos, planejando a execução e executando os procedimentos definidos pelo Comitê de Risco;
- ✓ Redigir os manuais, procedimentos e regras de risco;
- ✓ Apontar desenquadramentos e aplicar os procedimentos definidos na Política de Gestão de Riscos da GESTORA aos casos fáticos;
- ✓ Produzir relatórios de risco e levá-los ao gestor;
- ✓ Auxiliar o Comitê de Risco em qualquer questão atinente a sua área;
- ✓ 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*, Controles Internos e Ética;
- ✓ Controlar e monitorar as licenças legais, registros e certificações necessárias (registros na Comissão de Valores Mobiliários ("CVM"), Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais ("ANBIMA") e demais aplicáveis), bem como sua renovação/manutenção junto às autoridades;
- ✓ Auxiliar no relacionamento com órgãos reguladores e assegurar que as informações requeridas sejam fornecidas no prazo e qualidade requeridos;
- ✓ Realizar testes internos, revisões e relatórios obrigatórios nas frequências definidas nas políticas e manuais internos, bem como na legislação em vigor;
- ✓ Disseminar e promover - junto com a diretoria da GESTORA - as informações necessárias para o cumprimento das políticas e manuais internos e normas legais, infralegais e de autorregulação, bem como exercer seu controle, garantindo que as

políticas internas e manuais pertinentes estejam atualizados e mantidos em diretório e/ou website, conforme caso, acessível a todos que delas devam ter conhecimento:

- Disponibilizar aos novos Colaboradores as políticas e manuais internos 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;
- Analisar informações, indícios ou identificar, administrar e, se necessário, levar o tema para análise e deliberação no Comitê de *Compliance*, Controles Internos e Ética, no caso de eventuais conflitos de interesses ou descumprimentos regulatórios e de políticas e normas;
- Comunicar aos órgãos competentes, nos prazos regulatórios, a respeito de eventuais descumprimentos normativos.

✓ Aprovar novas políticas e manuais internos, no Comitê de *Compliance*, Controles Internos e Ética, ou a sua revisão, por força da regulamentação ou decisões internas;
✓ Aprovar a estruturação de novos veículos de investimento e prestação de novos serviços pela GESTORA, a partir de *inputs* técnicos do Comitê de Investimento e Crédito;
✓ Atuar para que haja efetividade na segregação física de eventuais atividades conflitantes;
✓ Apresentar o resultado de seus controles e verificações no Comitê de *Compliance*, Controles Internos e Ética;
✓ Monitorar e buscar a efetiva aplicação dos documentos que versem sobre *compliance* e controles internos;
✓ Servir como canal para comunicações de desconformidades regulatórias e/ou de temas relacionados ao Código de Ética e Conduta da GESTORA;
✓ Convocar, gerenciar, organizar e secretariar o Comitê de *Compliance*, Controles Internos e Ética, registrando suas decisões em atas.

Comitê de Investimento e Crédito

Responsabilidades: o Comitê de Investimento e Crédito é o órgão responsável por:

✓ Analisar, ratificar ou alterar o cenário-base de investimentos;
✓ Propor e aprovar estratégias, ativos, instrumentos e modalidades operacionais, emissores, nível de liquidez e mercados passíveis de investimento e seus limites;
✓ Analisar e aprovar, se se limitar:
    - Alocação para emissores recorrentes de renda fixa, no caso de instituições financeiras;

- Estudos sobre as companhias alvo dos FIPs sob gestão;
- Aquisição de ativos emitidos por companhias alvo dos FIPs;
- Propostas específicas de alocação em ativos específicos de emissão corporativa e assemelhados (debêntures, Fundos de Investimento em Direitos Creditórios ("FIDCs"), FIDCs NPs etc.);
- Propostas específicas em crédito estruturado e de dívida típicos de aquisição de FIDCs;
- Operações relativas a ativos imobiliários, créditos e operações relacionadas;
- Demais operações que possam ser consideradas como de crédito privado.

✓ Acompanhar e monitorar a qualidade de crédito dos ativos, emissores e contrapartes, e decidir, se necessário, por ajustar a estratégia de investimento definida inicialmente;
✓ Aprovação de ativos, emissores, instrumentos e modalidades operacionais, nível de liquidez, mercados e limites;
✓ Ratificação de novas contrapartes.

Composição: Diretor de Gestão de Carteira de Valores Mobiliários, conforme definido no contrato social vigente da AURORA, 2 (dois) analistas de crédito e a Diretora de *Compliance* e de Gestão de Risco, que não terá direito de voto, mas terá direito de veto, visando preservar as regras internas e de gestão de risco. Ademais, outros Colaboradores que possam contribuir em suas áreas de especialização podem ser convidados a participar das reuniões, sendo certo que não terão direito a voto.

Periodicidade: mensal, ou sempre que necessário para aprovação de novos ativos ou discussão de mudança de estratégia de investimento.

Decisões: as decisões deverão ter o voto favorável, no mínimo, do Diretor de Gestão de Carteira de Valores Mobiliários, conforme definido no contrato social vigente da AURORA. Dessa forma, as decisões do Comitê de Investimento e Crédito deverão ser tomadas preferencialmente de forma colegiada, pela maioria dos presentes, sendo sempre garantido exclusivamente ao Diretor de Gestão de Carteira de Valores Mobiliários o voto de qualidade e a palavra final em todas as votações. Todas as discussões e deliberações são formalizadas em atas de reunião e arquivadas no acervo físico e digital da AURORA.

Comitê de *Compliance*, Controles Internos e Ética

Responsabilidades: o Comitê de *Compliance*, Controles Internos e Ética é o órgão responsável por, dentre outras tarefas:

✓ Avaliar o descumprimento das normas legais, da autorregulação e das políticas internas, manuais e procedimentos internos;
✓ Avaliar situações de conflitos de interesses graves que possam afetar a imparcialidade dos Colaboradores da GESTORA;
✓ Aplicar as eventuais medidas disciplinares necessárias em casos graves;
✓ 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;
- ✓ 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 aos administradores e diretores da AURORA;
- ✓ Analisar eventuais situações ocorridas de desenquadramento de mandato no mês anterior, 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.

Composição: Diretora de Compliance e de Gestão de Risco e 2 (dois) integrantes do time jurídico.

Periodicidade: o Comitê de *Compliance*, Controles Internos e Ética se reúne de forma ordinária, formalmente, semestralmente. No entanto, dada a estrutura da GESTORA, discussões podem acontecer com mais frequência, de forma que o comitê também poderá ser convocado extraordinariamente, em caso de necessidade ou oportunidade.

Decisões: as decisões do Comitê de *Compliance*, Controles Internos e Ética deverão ter o voto favorável, no mínimo, da Diretora de *Compliance* e de Gestão de Risco. Dessa forma, as decisões do Comitê de *Compliance*, Controles Internos e Ética deverão ser tomadas preferencialmente de forma colegiada, pela maioria dos presentes, sendo sempre garantido exclusivamente à Diretora de *Compliance* e de Gestão de Risco o voto de qualidade e a palavra final em todas as votações. As decisões do Comitê de *Compliance*, Controles Internos e Ética serão formalizadas em ata e arquivadas no acervo físico e digital da AURORA.

Comitê de Risco

Responsabilidades: o Comitê de Risco é o órgão responsável por:

- ✓ Aprovar novos instrumentos, produtos e parâmetros de uma forma geral, sob aspectos de risco, e monitorar os enquadramentos aos parâmetros estabelecidos;
- ✓ Monitoramento e apresentação técnica dos riscos dos veículos de investimento sob responsabilidade da GESTORA, bem como de seus ativos, em linha com as boas práticas de mercado, normas e regulamentações aplicáveis;
- ✓ Análise dos níveis de risco dos veículos de investimento sob responsabilidade da GESTORA em relação a seus limites e estratégias propostos e o uso destes limites;
- ✓ Avaliar os riscos envolvidos no processo de gestão de recursos da GESTORA, que afetam atualmente ou que podem a vir afetar os investimentos por ela geridos;
- ✓ Analisar eventuais situações ocorridas de desenquadramento no mês anterior, risco operacional, e de liquidez, e, discussão de mitigantes e melhorias;

- ✓ Recomendar e fazer implementar medidas corretivas sempre que identificados desenquadramentos aos parâmetros aprovados.

Composição: Diretora de *Compliance* e de Gestão de Risco, 1 (um) analista de risco, 1 (um) assistente jurídico e Diretor de Gestão de Carteira de Valores Mobiliários. Ademais, outros Colaboradores que possam contribuir em suas áreas de especialização podem ser convidados a participar as reuniões, sendo certo que não terão direito a voto.

Periodicidade: o Comitê de Risco se reúne de forma ordinária, formalmente, mensalmente. No entanto, dada a estrutura da GESTORA, discussões podem acontecer com mais frequência, de forma que o comitê também poderá ser convocado extraordinariamente, em caso de necessidade ou oportunidade.

Decisões: as decisões do Comitê de Risco deverão ter o voto favorável, no mínimo, da Diretora de *Compliance* e de Gestão de Risco. Dessa forma, as decisões do Comitê de Risco deverão ser tomadas preferencialmente de forma colegiada, pela maioria dos presentes, sendo sempre garantido exclusivamente à Diretora de *Compliance* e de Gestão de Risco o voto de qualidade e a palavra final em todas as votações. As decisões do Comitê de Risco serão formalizadas em ata e arquivadas.

Garantia de Independência

A Diretoria de *Compliance* e de Gestão de Risco e os Comitês de *Compliance*, Controles Internos e Ética e Risco exercem suas atividades de forma completamente independente das outras áreas da GESTORA e poderão exercer seus poderes e autoridade com relação a qualquer Colaborador.

Mecanismos Adicionais de *Compliance* e Controles Internos

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

- ✓ A disseminação e o conhecimento do conteúdo dos termos e dos documentos internos da GESTORA aplicáveis acima, atestado com a assinatura do Termo de Conhecimento das Políticas por todos os Colaboradores (parte integrante do Código de Ética e Conduta);
- ✓ Controle da regularidade das certificações;
- ✓ Teste e Relatório de Aderência Anual;
- ✓ Teste do Sistema de Informações Anual**:** 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 Diretora de *Compliance* e de Gestão de 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.

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.

O relatório é de responsabilidade da Diretora de *Compliance* e de Gestão de Risco, e, após ratificação pelo Comitê de *Compliance*, Controles Internos e Ética, será encaminhado aos administradores e diretores da AURORA anualmente, até o último dia útil de abril de cada ano (com conteúdo relativo à análise do ano civil imediatamente anterior).

Tal relatório contém, sem se limitar:

- ✓ 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 de Gestão de Carteira de Valores Mobiliários ou, quando for o caso, da Diretora de *Compliance* e de Gestão de Risco a respeito das deficiências encontradas em verificações anteriores e das medidas planejadas, de acordo com cronograma específico, ou efetivamente adotadas para saná-las.

Disposições Gerais e Sanções

Todos os Colaboradores devem estar comprometidos com a cultura de *compliance* e reportar imediatamente à Diretora de *Compliance* e de Gestão de 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 à Diretora de *Compliance* e de Gestão de Risco.

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.

Quando constatada uma violação, o violador será convocado a prestar esclarecimentos ao Comitê de *Compliance*, Controles Internos e Ética. Caberá ao Comitê de *Compliance*, Controles Internos e Ética tomar as medidas necessárias. As sanções decorrentes de uma violação serão definidas pelo Comitê de *Compliance*, Controles Internos e Ética. As sanções que poderão ser aplicadas são: advertência, com impacto no bônus do Colaborador e, no caso de o Colaborador receber mais de 03 (três) advertências, ocorrerá o desligamento ou exclusão por justa causa, no caso de Colaboradores que sejam sócios da Gestora, ou demissão por justa causa, no caso de Colaboradores que sejam empregados da Gestora. Nesse último caso, nos termos do artigo 482 da Consolidação das Leis Trabalhistas – CLT, sem prejuízo do direito da Gestora de pleitear indenização pelos eventuais prejuízos sofridos, perdas e danos e/ou lucros cessantes, por meio de medidas legais.

Política de Certificação

A quem se aplica?

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 geridos pela GESTORA.

Os Colaboradores devem atender às diretrizes e procedimentos estabelecidos nesta Política de Certificação ("Política"), informando qualquer irregularidade à Diretora de *Compliance* e de Gestão de Risco.

Responsabilidades

A Diretora de *Compliance* e de Gestão de Risco é responsável pelos controles que garantem o atendimento as demandas do Código ANBIMA de Regulação e Melhores Práticas para o Programa de Certificação Continuada ("Código de Certificação").

Revisão e Atualização

Esta Política deverá ser revisada a atualizada a cada 12 (doze) meses, ou em prazo inferior, se necessário, em função de mudanças legais/regulatórias ou complementações.

Elegibilidade

A GESTORA desempenha exclusivamente a atividade de gestão de carteiras de títulos e valores mobiliários. Segundo a ANBIMA, o Código de Certificação se aplica também a quaisquer integrantes do seu conglomerado ou grupo econômico que desempenhem qualquer das atividades disciplinadas pelo Código de Certificação (*i.e.*, qualquer sociedade controlada, controladora ou sob controle comum com a GESTORA).

Assim sendo, a GESTORA requer dos Colaboradores elegíveis a Certificação de Gestores ANBIMA ("CGA") ou a sua isenção, observados os termos da autorregulamentação vigente..

Controles

A Diretoria de *Compliance* e Controles Internos 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.

A Diretoria de *Compliance* e Controles Internos é responsável por verificar se todos os Colaboradores elegíveis à CGA estão devidamente certificados e se as respectivas certificações estão válidas.

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

Compete à Diretoria de *Compliance* e Controles Internos 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, a Diretoria de *Compliance* e Controles Internos é responsável por manter a documentação formal que evidencie o afastamento do Colaborador das atividades elegíveis a certificação, vide modelo constante do Anexo II ao presente documento.

Cabe à Diretoria de *Compliance* e Controles Internos monitorar o cumprimento das diretrizes inerentes ao Código de Certificação.

As certificações pendentes e o afastamento das funções elegíveis devem ser reportadas ao Comitê de *Compliance*, Controles Internos e Ética, 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*, Controles Internos e Ética.

Admissões de Colaboradores

A Diretoria de *Compliance* e Controles Internos 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 pela Diretora de *Compliance* e de Gestão de Risco e reportadas ao Comitê de *Compliance*, Controles Internos e Ética para controle das respectivas atividades e possível afastamento das funções até a efetiva obtenção da certificação aplicável.

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

Licenças, Afastamentos e Desligamentos

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

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

Todos os Colaboradores em processo de certificação, e para os quais a certificação seja, de fato, exigível, poderão ser afastados das atividades de gestão de recursos de terceiros até que se certifiquem.

Aos Colaboradores já certificados, caso deixem de ser Colaboradores da GESTORA, deverão assinar documentação pertinente comprovando o afastamento da GESTORA, bem como os Colaboradores em processo de certificação que forem afastados por qualquer dos motivos acima mencionados.

Banco de Dados da ANBIMA

A Diretoria de *Compliance* e Controles Internos é responsável pela veracidade e manutenção do banco de dados da ANBIMA atualizado.

Considerando o porte da GESTORA, semestralmente ou em periodicidade menor, quando necessário, a Diretora de *Compliance* e de Gestão de Risco deverá verificar as informações contidas no banco de dados da ANBIMA, a fim de garantir que todos os Colaboradores certificados/em processo de certificação, conforme aplicável, estejam devidamente identificados.

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

Todas as atualizações no banco de dados da ANBIMA devem ocorrer até o último dia útil do mês subsequente à data do evento que deu causa a atualização, nos termos do Art. 12, §1º, I do Código de Certificação, sendo que a manutenção das informações contidas no banco de dados da ANBIMA deverá ser objeto de análise e confirmação pela Diretora de *Compliance* e de Gestão de Risco.

Treinamento

Serão objeto do treinamento anual de *compliance* assuntos de certificação, incluindo, sem limitação: (i) treinamento direcionado a todos os Colaboradores, descrevendo as certificações aplicáveis à atividade da GESTORA, suas principais características e os profissionais elegíveis; (ii) treinamento direcionado aos membros do departamento técnico envolvidos na atividade de gestão de recursos, reforçando que somente os Colaboradores com CGA podem ter alçada/poder discricionário de decisão de investimento em relação aos ativos integrantes das carteiras sob gestão da GESTORA, devendo os demais buscar aprovação junto ao Diretor de Gestão de Carteira de Valores Mobiliários e/ou ao Comitê de Investimento e Crédito; 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.

Código de Ética e Conduta Profissional

A Política requer 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 à Diretoria de *Compliance* e Controles Internos requerer dos novos Colaboradores um Termo de Conhecimento do Código de Ética e Conduta Profissional e das demais políticas da GESTORA.

A Diretoria de *Compliance* e Controles Internos também é responsável por controlar os termos do Código de Ética e Conduta Profissional e das demais políticas internas da GESTORA, 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 e Segurança Cibernética

Estabelecer princípios e diretrizes de proteção das informações no âmbito da GESTORA.

A quem se aplica?

A todos os Colaboradores.

Responsabilidades

Os Colaboradores devem atender às diretrizes e procedimentos estabelecidos nesta Política de Confidencialidade e Segurança da Informação ("Política"), informando quaisquer irregularidades à Diretora de *Compliance* e de Gestão de Risco, a quem caberá avaliá-las e submetê-las ao Comitê de *Compliance*, Controles Internos e Ética, o qual decidirá sobre eventuais medidas cabíveis.

A Diretora de *Compliance* e de Gestão de Risco deve garantir o atendimento a esta Política, sendo o responsável por temas de segurança da informação e cibernética.

Revisão e Atualização

Esta Política deverá ser revisada e atualizada a cada 12 (doze) meses, ou em prazo inferior, caso necessário, em função de mudanças legais, regulatórias, autorregulatória ou complementações.

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 empresa, seus clientes ou dos portfólios sob gestão – cuja divulgação possa prejudicar a gestão dos negócios, clientes e fundos de investimentos geridos pela 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, constituam propriedade intelectual ou industrial, e não estejam disponíveis, de qualquer outra forma, ao público em geral;
- ✓ Sejam assim consideradas face a determinação legal, previsão legal e/ou regulamentar; 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 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 neste documento.

Não caracteriza descumprimento desta Política a divulgação de Informações Confidenciais mediante prévia autorização da Diretora de *Compliance* e de Gestão de 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 a Diretora de *Compliance* e de Gestão de 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 ele for de fato necessário;
- ✓ Disponibilidade: as pessoas autorizadas devem ter acesso à informação sempre que necessário;
- ✓ Integridade: 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. Desta forma, há a segregação lógica das informações, de modo que e somente os Colaboradores autorizados têm acesso às pastas virtuais respectivas às suas atividades desenvolvidas na GESTORA;
- ✓ 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 à Diretora de *Compliance* e de Gestão de 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 da Diretora de *Compliance* e de Gestão de 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: 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 a Diretora de *Compliance* e de Gestão de Risco.

O descarte de Informação Confidencial armazenada em meio físico deve ser efetuado utilizando máquina fragmentadora 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 da Diretora de *Compliance* e de Gestão de Risco.

A GESTORA poderá, a qualquer momento mediante prévia aprovação da Diretora de *Compliance* e de Gestão de 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 da Diretora de *Compliance* e de Gestão de 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 à Diretora de *Compliance* e de Gestão de 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 pela Diretora de *Compliance* e de Gestão de Risco;
- ✓ Contratar provedores de acesso sem autorização prévia da Diretora de *Compliance* e de Gestão de Risco;
- ✓ Redirecionar caixa postal pessoal (e-mail de outros provedores) para a sua caixa postal de correio eletrônico na GESTORA e vice-versa.

Bloqueio de Acesso a Sites

A Diretora de *Compliance* e de Gestão de Risco, juntamente com os responsáveis pelo departamento de tecnologia da informação, são responsáveis por monitorar os acessos feitos a sites através de computadores de propriedade da GESTORA, para reporte de eventual mau uso ao Comitê de *Compliance*, Controles Internos e Ética 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 à Diretora de *Compliance* e de Gestão de 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 à Diretora de *Compliance* e de Gestão de 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, a Diretora de *Compliance* e de Gestão de Risco deverá ser imediatamente comunicada 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 (se for o caso), 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 pela Diretora de *Compliance* e de Gestão de Risco no Comitê de *Compliance*, Controles Internos e Ética da GESTORA.

O backup de todos os dados e informações da GESTORA é realizado na nuvem diariamente.

Procedimentos de Segurança Cibernética

Identificação e avaliação de riscos (*risk assessment*)

A GESTORA deverá identificar e avaliar os principais riscos cibernéticos aos quais está exposta. O Guia ANBIMA de Segurança Cibernética definiu que os ataques mais comuns de cybercriminals são os seguintes:

- ✓ Malware (vírus, cavalo de troia, spyware e ransomware);
- ✓ Engenharia Social;
- ✓ Pharming;
- ✓ Phishing scam;
- ✓ Vishing;
- ✓ Smishing;
- ✓ Acesso pessoal;
- ✓ Ataques de DDoS e botnets;
- ✓ Invasões (*advanced persistent threats*).

Com a finalidade de se manter resguardada contra estes e outros potenciais ataques, a GESTORA definiu todos os ativos relevantes da instituição, fundamentais a seu funcionamento, criou regras para classificação das informações geradas e avalia continuamente a vulnerabilidade de cada um desses ativos.

A GESTORA levou também em consideração os possíveis impactos financeiros, operacionais e reputacionais em caso de evento de segurança.

Ações de prevenção e proteção

Uma importante regra de prevenção consiste na segregação de acessos a sistemas e dados que a GESTORA adota, conforme já detalhado nas regras internas que tratam de Segurança da Informação.

A GESTORA adota, além disto, regras mínimas na definição de senhas de acesso a dispositivos corporativos, sistemas e rede, em função da relevância do ativo acesso. A GESTORA trabalha com o princípio de que concessão de acesso deve somente ocorrer se os recursos acessados forem relevantes ao usuário.

Os eventos de login e alteração de senhas são auditáveis e rastreáveis. A GESTORA deve criar logs e trilhas de auditoria sempre que os sistemas permitam.

O acesso remoto a arquivos e sistemas internos ou na nuvem tem controles adequados. O acesso ao acervo digital conta com dupla verificação. Quando o Colaborador acessa o office365 para logar, é enviado um código de segurança no seu celular, garantindo a autenticidade.

Outro ponto importante é que, ao concluir novos equipamentos e sistemas em produção, a GESTORA deverá garantir que sejam feitas configurações seguras de seus recursos. Devem ser feitos testes em ambiente de homologação e de prova de conceito antes do envio à produção. A GESTORA conta com recursos anti-malware em estações e servidores de rede, como anti-virus e *firewalls* pessoais. A GESTORA deve, adicionalmente, proibir o acesso a determinados websites e a execução de softwares e/ou aplicações não autorizadas.

É terminantemente proibido que os Colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da GESTORA e circulem em ambientes externos à GESTORA com estes arquivos, uma vez que tais arquivos contêm informações que são consideradas como informações confidenciais. Qualquer exceção à presente regra deverá ser previamente autorizada por escrito pela Diretora de *Compliance* e de Gestão de Risco.

A proibição acima referida não se aplica quando as cópias (físicas ou eletrônicas) ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da GESTORA. Nestes casos, o Colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o

responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

Em consonância com as normas internas acima, os Colaboradores devem se abster de utilizar pen-drivers, disquetes, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na GESTORA.

Para segurança dos perfis de acesso dos Colaboradores, as senhas de acesso dos Colaboradores são parametrizadas conforme regras estabelecidas globalmente.

Dessa forma, o Colaborador pode ser responsabilizado inclusive caso disponibilize a terceiros a senha e login acima referidos, para quaisquer fins.

Cada Colaborador é responsável ainda por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade.

A GESTORA adota também *backup* das informações e dos diversos ativos da instituição, conforme as disposições do presente documento e do plano de continuidade dos negócios da GESTORA.

Os Colaboradores deverão manter arquivada toda e qualquer informação, incluindo informações confidenciais, privilegiadas ou reservadas bem como documentos e extratos que venham a ser necessários para a efetivação satisfatória de possível auditoria ou investigação em torno de possíveis investimentos e/ou clientes suspeitos de corrupção e/ou lavagem de dinheiro, em conformidade com o inciso IV do Artigo 16 da Instrução CVM nº 558/15, em locais seguros, de modo a evitar o acesso de pessoas não autorizadas às informações ali contidas.

Para concluir, pode-se mencionar que as medidas de diligência prévia também são caras à prevenção e proteção dos ativos da GESTORA e devem ser observadas integralmente.

A GESTORA possui mecanismos de todas as ações de proteção implementadas para garantir seu bom funcionamento e efetividade. A GESTORA mantém inventários atualizados de hardware e software, e verifica-os com frequência para identificar elementos estranhos à instituição.

A área responsável da GESTORA deve diligenciar para manter os sistemas operacionais e softwares de aplicação sempre atualizados, instalando as atualizações sempre que forem disponibilizadas.

Deve-se, ademais, realizar trimestralmente testes de invasão externa, phishing, bem como análises de vulnerabilidades na estrutura tecnológica, periodicamente ou sempre que houver mudança significativa em tal estrutura.

Os logs e trilhas de auditoria criados devem ser analisados regularmente pela área responsável, de forma a permitir rápida identificação de ataques, sejam internos ou externos.

Plano de resposta

A área de *compliance* deve, conjuntamente com o departamento de tecnologia da informação, elaborar um plano formal de resposta a ataques virtuais. A GESTORA deverá estabelecer os papeis de cada área em tal plano, prevendo o acionamento de Colaboradores-chave e contatos externos relevantes.

O plano de resposta deverá levar em conta os cenários de ameaças previstos no *risk assessment*. Deve haver critérios para a classificação dos incidentes, por severidade. O plano deve prever, conforme o caso, o processo de retorno às instalações originais após o final do incidente, na hipótese em que as instalações de contingência ou acessos remotos tenham de ser utilizados.

Reciclagem e revisão

O programa de segurança cibernética, que contempla os procedimentos aqui descritos, o plano formal de resposta e demais políticas internas da GESTORA sobre a matéria, deverá ser revisto e atualizado anualmente.

Os grupos de trabalho diretamente envolvidos com qualquer parte do programa devem se manter atualizados, buscando fornecedores especializados, se necessário.

A GESTORA deverá divulgar o programa de segurança cibernética internamente e disseminar a cultura de segurança, alertando sobre os riscos principais e as práticas de segurança.

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 Diretora de *Compliance* e de Gestão de Risco e reportados ao Comitê de *Compliance*, Controles Internos e Ética.

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, bem como podem se tornar públicos em caso de auditoria, exigência judicial ou regulatória.

Termo de Conhecimento

Os Colaboradores devem aderir formalmente a um termo, comprometendo-se a agir de acordo com esta Política.

Os Colaboradores que tenham acesso a Informações Confidenciais ou participem de processo de decisão de investimento devem solicitar à Diretora de *Compliance* e de Gestão de Risco eventuais esclarecimentos sobre o tema de segurança de informação e segurança cibernética.

Política de Seleção e Contratação de Terceiros pela GESTORA, em Nome dos Veículos de Investimento

Objetivo e Aspectos Gerais

Esta Política de Seleção e Contratação de Terceiros pela GESTORA, em Nome dos Veículos de Investimento ("Política") visa registrar o processo de avaliação da AURORA na contratação de terceiros, em nome dos veículos de investimento sob gestão, notadamente corretoras de títulos e valores mobiliários ("Corretoras") e, em determinadas situações, instituições integrantes do sistema de distribuição de valores mobiliários, devidamente habilitadas para a realização de distribuição pública de valores mobiliários, nos mercados primário e secundário ("Instituições Intermediárias"), em cumprimento ao Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros, Capítulo VI – Contratação de Terceiros em Nome dos Fundos de Investimentos.

A AURORA salienta que a seção que trata da Contratação de Corretoras se aplica apenas para os ativos financeiros cuja operação se dá por intermédio de Corretoras.

Sem prejuízo, para a contratação de todo e qualquer terceiro, inclusive eventuais terceiros para as carteiras administradas, a AURORA deverá observar os critérios de qualificação técnica, capacidade operacional, licenças, preço e idoneidade do terceiro contratado. A aferição destas condições será realizada através da análise de documentação, e eventual realização de visitas (*due dilligence*), bem como quaisquer outros procedimentos que sejam julgados necessários para comprovar as qualificações do terceiro contratado.

O contrato escrito a ser celebrado com o terceiro deverá prever, no mínimo, cláusulas que tratam:

- ✓ Das obrigações e deveres das partes envolvidas;
- ✓ Da descrição das atividades que serão contratadas e exercidas por cada uma das partes;
- ✓ Da obrigação de cumprir suas atividades em conformidade com as disposições previstas na regulamentação e autorregulação aplicáveis à atividade; e
- ✓ Que os terceiros contratados devem, no limite de suas atividades, deixar à disposição do contratante todos os documentos e informações exigidos pela regulação em vigor que sejam necessários para a elaboração de documentos e informes periódicos obrigatórios, salvo aqueles considerados confidenciais, nos termos da regulação em vigor.

Quando o contratado tiver acesso a informações sigilosas dos clientes e da GESTORA, deverá ser assinado um contrato com cláusula de confidencialidade que estabeleça multa ou penalidade em caso de quebra de sigilo. O funcionário da empresa terceira que tiver

acesso a informações confidenciais deverá assinar pessoalmente termo de confidencialidade se comprometendo a guardar o sigilo das referidas informações.

A quem se aplica?

A todos os Colaboradores, sobretudo aqueles integrantes das áreas de *compliance* e gestão.

Responsabilidades

Os Colaboradores devem atender às diretrizes e procedimentos estabelecidos nesta Política, informando quaisquer irregularidades à Diretora de *Compliance* e de Gestão de Risco, a quem caberá avaliá-las e submetê-las ao Comitê de *Compliance*, Controles Internos e Ética, o qual decidirá sobre eventuais medidas cabíveis.

A Diretora de *Compliance* e de Gestão de Risco deve garantir o atendimento a esta Política.

Revisão e Atualização

Esta Política deverá ser revisada e atualizada a cada 12 (doze) meses, ou em prazo inferior, caso necessário, em função de mudanças legais, regulatórias, autorregulatória ou complementações.

Contratação de Corretoras

Os critérios para a contratação de terceiros em nome dos veículos de investimento sob gestão – Corretoras -, deve ocorrer em observância ao Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros.

Antes da contratação de uma Corretora a área de gestão de carteira de valores mobiliários da GESTORA deverá aplicar o correspondente questionário modelo ANBIMA, além de verificar se o intermediário está autorizado pelo Banco Central do Brasil, Brasil, Bolsa, Balcão (B3) e CVM a operar e avaliar os seguintes requisitos mínimos: (i) capacidade de execução e habilidades da Corretora em executar operações de curto prazo; (ii) confiabilidade dos sistemas de comunicação e negociação da corretora; (iii) comissões e descontos; e (iv) reputação, saúde financeira da Corretora e de seu grupo econômico.

Após a contratação do terceiro, a GESTORA realizará o monitoramento contínuo das atividades exercidas pelos terceiros contratados, até o término do prazo da contratação.

A GESTORA manterá parâmetros de análise levando em conta os tipos de produtos operados com a corretora, pelas áreas e critérios elencados abaixo:

Área de Gestão de Carteira de Valores Mobiliários

- ✓ Cada gestor e analista faz uma análise por corretora, a qual avaliará a qualidade dos dados informados nos relatórios oferecidos por setor de cobertura. A nota varia de 1 (péssimo) a 6 (ótimo) e, ao final, é constatada uma média para cada corretora;
- ✓ O gestor da AURORA, responsável pela execução das ordens e alocação, faz avaliação da qualidade do serviço de trade; capacidade de atender produtos de menor liquidez e fornecer preço para opções; a qualidade do serviço de Aluguel (BTC) e a qualidade e variedade de eventos relacionados à economia macro. As notas também variam de 1 a 6 e é feita uma média por Corretora;
- ✓ Com a composição das notas fazemos um *ranking* de Corretora, que deve servir de referência para o direcionamento dos trades.

Área de *Compliance*

- ✓ A área de *compliance* registra erros cometidos pelas corretoras e a gravidade do impacto de cada erro. O resultado é analisado e, se considerado inaceitável, pode servir como veto à utilização da Corretora, mesmo que temporariamente;
- ✓ A área de *compliance*, portanto, não faz avaliação quantitativa, mas apenas qualitativa, com viés operacional e, desse modo, avalia qual o risco operacional de se continuar utilizando uma corretora com histórico grande de falhas, caso haja;
- ✓ Mensalmente a área de *compliance* gera um relatório de acompanhamento de gasto de corretagem, que avalia se o orçamento está em linha com o *ranking* definido anteriormente;
- ✓ Semestralmente é realizado uma análise do rebate aplicado por Corretora e o custo fixo para produtos dos mercados organizados. O resultado da análise é discutido em reunião e pode resultar em renegociação da tabela de custos com as corretoras ou, eventualmente, no encerramento da utilização da Corretora.

Contratação de Instituições Intermediárias

No âmbito das ofertas públicas de distribuição de valores mobiliários, nos mercados primário ou secundário, a GESTORA poderá, nos termos da regulamentação vigente, sobretudo a Instrução CVM n° 400, de 29 de dezembro de 2003, conforme alterada, e a Instrução CVM n° 476, de 16 de janeiro de 2009, conforme alterada, contratar, em nome de determinados fundos de investimento sob gestão, Instituições Intermediárias (i.e. Coordenador líder e coordenadores participantes) para distribuição das cotas dos fundos, ou auxiliar o administrador fiduciário de seus fundos na referida contratação.

As áreas de gestão e de *compliance*, quando da contratação das Instituições Intermediárias, deverão observar os critérios de qualificação técnica, capacidade operacional, preço e idoneidade, sendo certo que somente serão contratadas Instituições Intermediárias de primeira linha. A aferição destas condições será realizada através da análise de documentação, sobretudo o questionário de *due dilligence* no padrão da ANBIMA que deverá ser preenchido pelas Instituições Intermediárias, bem como quaisquer outros procedimentos que sejam julgados necessários para comprovar as qualificações do terceiro.

Sem prejuízo do disposto na "Objetivo e Aspectos Gerais" acima, o contrato escrito a ser celebrado com as Instituições Intermediárias deverá prever, no mínimo, cláusulas que tratam:

- ✓ Da qualificação da empresa emissora, da instituição líder e das demais Instituições Intermediárias envolvidas na distribuição, se for o caso;
- ✓ Da assembleia geral extraordinária ou reunião do conselho de administração que autorizou a emissão;
- ✓ Do regime de colocação das cotas;
- ✓ Do total de cotas objeto do contrato, devendo ser mencionada a forma, valor nominal, se houver, preço de emissão e condições de integralização, vantagens e restrições, especificando, inclusive, aquelas decorrentes de eventuais decisões da assembleia ou do conselho de administração que deliberou o aumento;
- ✓ Das condições de revenda das cotas pela instituição líder ou pelas demais Instituições Intermediárias envolvidas na distribuição, no caso de regime de colocação com garantia firme;
- ✓ Da remuneração da instituição líder e demais Instituições Intermediárias envolvidas na distribuição, discriminando as comissões devidas;
- ✓ Da descrição do procedimento adotado para distribuição;
- ✓ Da menção a contratos de estabilização de preços e de garantia de liquidez, se houver;
- ✓ Das obrigações e deveres das partes envolvidas;
- ✓ Da obrigação de cumprir suas atividades em conformidade com as disposições previstas na regulamentação e autorregulação aplicáveis à atividade;
- ✓ Da obrigação das Instituições Intermediárias deixar, no limite de suas atividades, à disposição da AURORA todos os documentos e informações exigidos pela regulação em vigor que sejam necessários para a elaboração de documentos e informes periódicos obrigatórios, salvo aqueles considerados confidenciais, nos termos da regulação em vigor; e
- ✓ Da obrigação de confidencialidade, inclusive com o estabelecimento de multa em caso de quebra de sigilo.

A AURORA manterá cópias de todos os contratos celebrados com as Instituições Intermediárias, documentos de *due diligence* e documentação relativa à prestação de serviços acordadas.

Após a contratação da Instituição Intermediária, a AURORA realizará o monitoramento contínuo das atividades por esta desempenhadas, até o término do prazo da contratação.

O monitoramento será de responsabilidade das diretorias de *compliance* e de gestão.

A análise, para fins de monitoramento, deverá considerar eventuais disparidades na tempestividade e qualidade esperadas.

O processo para monitoramento contínuo do terceiro contratado será conciso e objetivo. Em linhas gerais, as diretorias de *compliance* e de gestão avaliarão o desempenho do terceiro versus a expectativa e metas traçadas quando da sua contratação, a relação custo benefício e o grau de segurança empregado nas suas tarefas.

Na hipótese de serem encontradas não conformidades e ressalvas, a AURORA notificará imediatamente a Instituição Intermediária, para que este sane a questão ou adeque a sua conduta dentro do prazo estabelecido, respeitando, sempre, o contrato celebrado. Caso a Instituição Intermediária não cumpra com os termos exigidos na notificação, a AURORA poderá proceder com a aplicação da cláusula indenizatória eventualmente prevista ou com a descontinuidade dos serviços.

Contratação de Controlador para as Carteiras Administradas

Em consonância com o artigo 10, §2° do Anexo V ao Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros, a AURORA contratará terceiros devidamente habilitados para o apreçamento dos ativos integrantes das carteiras administradas ("Controlador"), haja vista que não desempenha tal atividade.

A AURORA somente contratará Controladores que observem as normas específicas para a atividade de controladoria do Código de Serviços Qualificados e as Regras e Procedimentos ANBIMA para Apreçamento.

As áreas de gestão e de *compliance*, quando da contratação de Controlador, deverão observar os critérios de qualificação técnica, capacidade operacional, preço e idoneidade, sendo certo que somente serão contratados Controladores de primeira linha. A aferição destas condições será realizada através da análise de documentação, sobretudo o questionário de *due dilligence* no padrão da ANBIMA que deverá ser preenchido pelos Controladores, bem como quaisquer outros procedimentos que sejam julgados necessários para comprovar as qualificações do terceiro, incluindo, sem se limitar, a solicitação dos seguintes documentos:

- ✓ Organograma da instituição, demonstrando o nome e as funções dos profissionais responsáveis pelas áreas, caso não conste dos questionários anteriormente mencionados;
- ✓ Procedimentos para Prevenção à Lavagem de Dinheiro;
- ✓ Código de Ética e Conduta;
- ✓ Manual de *Compliance*/Controles Internos;
- ✓ Relação de todas as empresas direta ou indiretamente controladas, bem como das empresas coligadas, quando aplicável;
- ✓ Relação dos principais fornecedores, incluindo site, tipo de serviços ou materiais fornecidos, bem como tempo de relacionamento;
- ✓ Relação dos principais clientes, tipo de operação e tempo de relacionamento;
- ✓ Documentos societários, tais como, Contrato Social/Estatuto Social, Ata da Eleição de Diretoria e Procurações, quando aplicável;

- ✓ Identidade e CPF dos sócios e do diretor ou sócio-gerente;
- ✓ Política de Segurança da Informação, quando aplicável.

A AURORA manterá cópias de todos os contratos celebrados com os Controladores, documentos de *due diligence* e documentação relativa à prestação de serviços acordadas.

Após a contratação do Controlador, a AURORA realizará o monitoramento contínuo das atividades por esta desempenhadas, até o término do prazo da contratação.

O monitoramento será de responsabilidade das diretorias de *compliance* e de gestão.

A análise, para fins de monitoramento, deverá considerar eventuais disparidades na tempestividade e qualidade esperadas.

O processo para monitoramento contínuo do terceiro contratado será conciso e objetivo. Em linhas gerais, as diretorias de *compliance* e de gestão avaliarão o desempenho do terceiro versus a expectativa e metas traçadas quando da sua contratação, a relação custo benefício e o grau de segurança empregado nas suas tarefas.

Na hipótese de serem encontradas não conformidades e ressalvas, a AURORA notificará imediatamente o Controlador, para que este sane a questão ou adeque a sua conduta dentro do prazo estabelecido, respeitando, sempre, o contrato celebrado. Caso o Controlador não cumpra com os termos exigidos na notificação, a AURORA poderá proceder com a aplicação da cláusula indenizatória eventualmente prevista ou com a descontinuidade dos serviços.

Revisão Baseada em Risco

Corretoras

O serviço prestado pelas Corretoras é considerado de baixo risco, pelo fato da Corretora não possuir qualquer tipo de acesso a dados confidenciais, acesso à rede de dados da gestora e o não funcionamento de uma corretora em específico não gera descontinuidade do trabalho operacional da GESTORA. As certificações da Corretora para operar em nome dos fundos de investimento sob gestão indicam que os processos operacionais atendem aos requisitos da norma, significando, portanto, que o risco operacional é controlado.

Não obstante, realizamos a reavaliação constante e análise detalhada da qualidade dos serviços prestados. A queda na qualidade de serviço é analisada rapidamente e pode ser decidido rescindir o contrato entre a GESTORA e a Corretora, temporária ou definitivamente.

As supervisões serão realizadas em periodicidade não superior ao prazo de 36 (trinta e seis meses).

Instituições Intermediárias

Obrigatoriamente, todas as Instituições Intermediárias contratadas pela GESTORA, em nome dos fundos de investimento sob gestão, devem ser aderentes ou associadas aos códigos ANBIMA pertinentes às suas atividades, sendo esta uma condição precedente para a contratação.

Neste sentido, em consonância com as regras emanadas pela autorregulamentação vigente, as Instituições Intermediárias são classificadas como "Baixo Risco".

Ante o exposto, os procedimentos de pós contratação das Instituições Intermediárias, descritos na "Contratação de Instituições Intermediárias", são suficientes para a efetiva supervisão de tais prestadores de serviços.

Não obstante, as supervisões serão realizadas em periodicidade não superior ao prazo de 36 (trinta e seis meses).

Controladores

Obrigatoriamente, todas os Controladores contratados pela GESTORA, em nome das carteiras administradas, devem ser aderentes ou associadas aos códigos ANBIMA pertinentes às suas atividades, sendo esta uma condição precedente para a contratação.

Neste sentido, em consonância com as regras emanadas pela autorregulamentação vigente, os Controladores são classificados como "Baixo Risco".

Ante o exposto, os procedimentos de pós contratação dos Controladores, descritos na "Contratação de Controlador para as Carteiras Administradas", são suficientes para a efetiva supervisão de tais prestadores de serviços.

Não obstante, as supervisões serão realizadas em periodicidade não superior ao prazo de 36 (trinta e seis meses).

Política de Recrutamento e Seleção

A contratação de futuros Colaboradores pela AURORA considerará a qualificação adequada para cada posição a ser ocupada, e avaliará não somente a formação técnica dos candidatos, mas também suas experiências em trabalhos anteriores.

Não serão admitidas na GESTORA as práticas de discriminação, perseguição ou represálias por motivos de idade, raça, cor, religião, sexo, gravidez, nacionalidade, cidadania, opção sexual, deficiência física, estado civil, características genéticas de uma pessoa ou qualquer outra característica protegida por lei.

Especificamente para os Colaboradores envolvidos na área de gestão de carteira de valores mobiliários com alçada para tomada de decisões de investimento e desinvestimento, a contratação do futuro Colaborador pela AURORA estará condicionada à devida certificação do Colaborador, concedida pela ANBIMA, conforme detalhado em seção específica deste documento.

Política de Treinamento Contínuo

A política de treinamento contínuo tem como objetivo estabelecer as regras que orientam o treinamento dos Colaboradores, de forma a torná-los aptos a seguir todas as regras dispostas nas políticas internas da GESTORA. Todos os Colaboradores receberam o devido treinamento acerca de todas as políticas e procedimentos. Assim, serão proporcionados aos Colaboradores uma visão geral das políticas internas da GESTORA, de forma que os mesmos se tornem aptos a exercer suas funções aplicando conjuntamente todas as normas nelas dispostas.

Ainda, com o intuito de promover o constante aperfeiçoamento dos Colaboradores e a melhoria constante das funções dos Colaboradores, cursos de atualização que sejam relacionados às atividades desenvolvidas são incentivados e poderão ser parcialmente patrocinados pela AURORA.

Poderão ser ministradas a todos os Colaboradores da AURORA palestras internas, a fim de dar ciência sobre (i) as políticas adotadas pela GESTORA; (ii) a regulamentação vigente e aplicável aos negócios da AURORA e, ainda, (iii) eventuais fragilidades detectadas, sobretudo para alertar e evitar práticas que possam ferir a regulamentação vigente no exercício das atividades desenvolvidas pela AURORA. Referidas palestras serão de participação obrigatória, comprovada mediante assinatura do Colaborador em lista de presença. Não sendo possível a participação do Colaborador, sua ausência deverá ser justificada à Diretora de *Compliance* e de Gestão de Risco, sendo certo que a ausência deverá ser reposta na data mais próxima possível.

Todo o treinamento interno proposto pela AURORA, além de enfatizar a observância das regras e da relação fiduciária com os clientes, terá como objetivo abordar os procedimentos operacionais da AURORA, especialmente no que diz respeito às informações de natureza confidencial e adoção de posturas éticas e em conformidade com os padrões estabelecidos.

Os treinamentos relacionados ao conteúdo das políticas internas da GESTORA serão realizados, com periodicidade mínima anual, pela Diretora de *Compliance* e de Gestão de Risco sendo obrigatórios a todos os Colaboradores e controlados por lista de presença. Quando do ingresso de um novo Colaborador, a Diretora de *Compliance* e de Gestão de Risco aplicará o devido treinamento de forma individual para o novo Colaborador. A Diretora de *Compliance* e de Gestão de Risco poderá, ainda, conforme achar necessário, promover treinamentos esporádicos visando manter os Colaboradores constantemente atualizados em relação às políticas internas da GESTORA.

Disposições Finais

Dúvidas devem ser esclarecidas junto à Diretora de *Compliance* e de Gestão de Risco.

A área de *compliance* informará oportunamente aos Colaboradores sobre a entrada em vigor de nova versão deste documento e a disponibilizará na página da GESTORA na rede mundial de computadores.

Este documento revoga todas as versões anteriores e passa a vigorar na data de sua aprovação.

Anexo I

Termo de Conhecimento da POLÍTICA DE CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

NOME		
ÁREA	*CARGO*	
DOC. IDENTIDADE No	*TIPO*	*CPF*

Declaro que tenho conhecimento da Política de Confidencialidade e Segurança da Informação e Segurança Cibernética da GESTORA ("Política"), e que estou ciente do seu teor, o qual está diretamente ligado ao exercício de minhas funções.

De acordo com este termo, comprometo-me a:

a) adotar e cumprir as diretrizes indicadas na Política durante a vigência deste Termo e por prazo indeterminado após sua rescisão;

b) comunicar imediatamente à Diretora de *Compliance* e de Gestão de Risco qualquer violação desta Política de que eu venha a ter conhecimento, independentemente de qualquer juízo individual, materialidade ou relevância da violação.

Estou ciente e concordo que meus acessos físicos, lógicos, de voz e de imagem podem ser objeto de monitoramento.

Desde já, aceito incondicionalmente atender e cumprir quaisquer novos itens e condições que possam vir a ser considerados partes integrantes desta Política, sem a necessidade de apor assinatura em novo Termo, bem como, em caso de negligência ou imprudência na aplicação desta Política, tenho total ciência da responsabilidade disciplinar que recairá sobre tal inobservância.

_____, _____ de _____ de 20_____ (local)

_____ Assinatura do Colaborador

Anexo II

Termo de Afastamento

Por meio deste instrumento, eu, _____, inscrito(a) no CPF/MF sob o nº _____, declaro para os devidos fins que, a partir desta data, estou afastado das atividades de gestão de recursos de terceiros prestadas em favor da AURORA por prazo indeterminado:

[ ] ou até que me certifique pela CGA;

[ ] ou caso a diretoria da ANBIMA, nos termos do Art. 17 do Código de Certificação, me dispense da obrigação de realizar o exame CGA;

[ ] já que não tenho alçada/poder discricionário de decisão de investimento no âmbito da atividade de gestão de recursos na AURORA;

[ ] tendo em vista que não sou mais Colaborador da AURORA.

São Paulo, [●] de [●] de [●].

_____

[COLABORADOR]

_____

AURORA CAPITAL GESTORA DE RECURSOS LTDA.

Testemunhas:

1. _____

Nome:

CPF:

2. _____

Nome:

CPF: