MANUAL DE REGRAS, PROCEDIMENTOS E CONTROLES INTERNOS

VALORA
INVESTIMENTOS

12.2023

Sumário

1. Objetivo e Aplicabilidade

O presente Manual de Regras, Procedimentos e Controles Internos ("Manual") do "Grupo Valora" visa estabelecer princípios, conceitos, bem como consolidar as regras, procedimentos e controles internos adotados.

O Diretor de Compliance, Risco e PLD é o responsável pela implementação do Manual, incluindo uma revisão anual dos processos e procedimentos, manutenção e atualização. O Diretor de Compliance, Risco e PLD é também responsável por verificar se as Políticas descritas neste Manual estão sendo na prática verificadas, executadas e as evidências necessárias para sua comprovação corretamente registradas.

Este Manual aplica-se a todos os colaboradores da "Colaboradores", assim entendidos como aqueles que possuam cargo, função, posição, relação societária, empregatícia, comercial, profissional, contratual ou de confiança com as Gestoras.

Ademais, **anualmente** e quando ingressar na instituição, os Colaboradores devem assinar o termo de recebimento e adesão ao Manual, conforme **Anexo A**.

2. Ambiente Legal

Todos os Colaboradores devem se assegurar do perfeito entendimento das leis e normas aplicáveis às Gestoras bem como do completo conteúdo deste Manual. São as principais normas aplicáveis às atividades das Gestoras:

(i) Resolução da Comissão de Valores Mobiliários ("CVM") nº 21, de 25 de Fevereiro de 2021, conforme alterada ("Resolução CVM nº 21");
(ii) Ofício-Circular/CVM/SIN/Nº 05/2014;
(iii) Código da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais ("ANBIMA") de Ética ("Código ANBIMA de Ética");
(iv) Código de Administração de Recursos de Terceiros ("Código de ART");
(v) Código de Certificação ("Código de Certificação");
(vi) Lei nº 12.846/13 e Decreto nº 11.129/22, conforme alterada ("Normas de Anticorrupção");
(vii) Resolução CVM nº 50, de 31 de agosto de 2021 ("Resolução CVM nº 50");
(viii) Lei 9.613/98, conforme alterada;
(ix) Instrução CVM nº 555, de 17 de dezembro de 2014, conforme alterada ("Instrução CVM 555");
(x) Instrução CVM nº 578, de 30 de agosto de 2016, conforme alterada ("Instrução CVM 578");

(xi) Instrução CVM nº 472, de 31 de outubro de 2008, conforme alterada ("Instrução CVM 472");
(xii) Instrução CVM nº 356, de 17 de dezembro de 2001, conforme alterada ("Instrução CVM 356"); e
(xiii) Demais manifestações e ofícios orientadores dos órgãos reguladores e autorregulados aplicáveis às atividades das Gestoras.

3. Princípios e Diretrizes

3.1 Orgãos de Governança

3.1.1 – Departamento de Compliance e Risco

O Departamento de Compliance e Risco será liderado pelo Diretor de Risco e Compliance. Seus principais objetivos são (i) avaliar controles internos, exposição a riscos e cumprimento de leis e regulamentos aplicáveis, (ii) monitorar investigações relacionadas a questões de ética e conflitos de interesses, (iii) aprovar e atualizar periodicamente as Políticas e Diretrizes internas e (iv) desenvolver programas de cultura de Compliance abrangendo desde a alta Administração até os demais Colaboradores das Gestoras.

3.1.3 – Comitê de Gestão de Renda Fixa

O Comitê de Gestão de Renda Fixa é composto por toda equipe de gestão de renda fixa e é realizado semanalmente, onde são discutidos os temas abaixo listados, identificando os pontos de atenção e planos de ação:

i. As estratégias de cada carteira;
ii. Enquadramentos;
iii. Liquidez;
iv. Desempenho de cada ativo; e
v. Fluxo de caixa dos fundos.

Na análise de novos ativos para investimento, a equipe de gestão realiza um check-list de suas elegibilidades. Caso o ativo não satisfaça algum dos critérios elencados, será descartado. Caso contrário, o ativo será encaminhado para a Área de Crédito que efetuará uma análise profunda.

3.1.4 – Comitê de Investimentos de Renda Fixa

O Comitê é realizado semanalmente ou por demanda, e é responsável pela aprovação de novos limites, renovações/manutenção dos limites vigentes, acompanhamento do risco das carteiras e dos ativos investidos. Todas as deliberações são registradas em Ata.
Abaixo seguem os tópicos abordados:

i. Análise de Crédito dos Ativos;
ii. Liquidez dos ativos que compõem a carteira dos fundos;
iii. Deliberação de crédito para investimento em novos ativos;
iv. Volatilidade da carteira dos fundos;
v. Limites de risco por emitente;
vi. Concentração por ativo;
vii. Concentrações dos passivos dos fundos;
viii. Exposição dos Fundos da Valora Gestão de Investimentos nos Fundos investidos

O Comitê é composto por no mínimo 4 (quatro) membros seniores da Gestão, obrigatoriamente um com certificação de gestão, além do Gerente de Crédito e do Diretor de Risco e Compliance.

3.1.4 – Comitê de Produtos Estruturados de Renda Fixa

O Comitê é realizado por demanda, e é responsável pela aprovação de novos produtos. Todas as deliberações são registradas em Ata.
Abaixo seguem os tópicos abordados:

i. Estratégias de Investimento dos fundos;
ii. Liquidez dos ativos que compõem a carteira dos fundos;
iii. Avaliação da área de Crédito;
iv. Avaliação da área de Compliance;
v. Deliberação de crédito para investimento em novos ativos;
vi. Volatilidade da carteira dos fundos;
vii. Limites de risco por emitente;

O Comitê é composto por no mínimo 4 (quatro) membros seniores da Gestão, obrigatoriamente um com certificação de gestão, além do Diretor de Risco e Compliance.

3.1.5 – Comitê de Investimentos Imobiliário

O Comitê é realizado por demanda, e é responsável pela aprovação de novos produtos, acompanhamento do risco das carteiras e dos ativos investidos. Todas as deliberações são registradas em Ata.
Abaixo seguem os tópicos abordados:

i. Estratégias de investimento dos fundos;
ii. Evolução dos resultados de captação dos fundos;
iii. Deliberação de crédito para investimento em novos ativos;
iv. Limites de risco por emitente/devedor;
v. Concentração por ativo;
vi. Exposição dos Fundos da Valora Gestão de Investimentos nos Fundos investidos

O Comitê é composto por: no mínimo 4 (quatro) membros seniores da Gestão, obrigatoriamente um com certificação de gestão, além do Diretor de Risco e Compliance.

3.1.5 – Comitê de Investimentos Agro

O Comitê é realizado por demanda, e é responsável pela aprovação de novos produtos, acompanhamento do risco das carteiras e dos ativos investidos. Todas as deliberações são registradas em Ata.

Abaixo seguem os tópicos abordados:

i. Estratégias de investimento dos fundos;
ii. Evolução dos resultados de captação dos fundos;
iii. Deliberação de crédito para investimento em novos ativos;
iv. Limites de risco por emitente/devedor;
v. Concentração por ativo;
vi. Exposição dos Fundos da Valora Gestão de Investimentos nos Fundos investidos

O Comitê é composto por: no mínimo 4 (quatro) membros seniores da Gestão, obrigatoriamente um com certificação de gestão, além do Diretor de Risco e Compliance.

3.1.6 – Comitê de Investimentos Infra

O Comitê é realizado por demanda, e é responsável pela aprovação de novos produtos, acompanhamento do risco das carteiras e dos ativos investidos. Todas as deliberações são registradas em Ata.

Abaixo seguem os tópicos abordados:

i. Estratégias de investimento dos fundos;
ii. Evolução dos resultados de captação dos fundos;
iii. Deliberação de crédito para investimento em novos ativos;
iv. Limites de risco por emitente/devedor;
v. Concentração por ativo;
vi. Exposição dos Fundos da Valora Gestão de Investimentos nos Fundos investidos

O Comitê é composto por: no mínimo 4 (quatro) membros seniores da Gestão, obrigatoriamente um com certificação de gestão, além do Diretor de Risco e Compliance.

3.2 Segurança da Informação e Segurança Cibernética

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

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

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

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

A execução direta das atividades relacionadas à política de segurança da informação e segurança cibernética ficará a cargo da Equipe de Compliance, Risco e PLD que, em conjunto com a equipe de Tecnologia da Informação serão, responsáveis inclusive por sua revisão, realização de testes e treinamento dos Colaboradores, conforme descrito neste Manual.

3.2.1 Identificação de Riscos (*risk assessment*)

No âmbito de suas atividades, as Gestoras identificaram os seguintes principais riscos internos e externos que precisam de proteção:

(i) Dados e Informações: Informações Confidenciais, incluindo informações a respeito de investidores, clientes, Colaboradores e das próprias Gestoras, operações e ativos investidos pelas carteiras de valores mobiliários sob sua gestão, e as comunicações internas e externas (por exemplo: correspondências eletrônicas e físicas);
(ii) Sistemas: Informações sobre os sistemas utilizados pelas Gestoras e as tecnologias desenvolvidas internamente e por terceiros, suas ameaças possíveis e sua vulnerabilidade;
(iii) Processos e Controles: Processos e controles internos que sejam parte da rotina das áreas de negócio das Gestoras; e
(iv) Governança da Gestão de Risco: Eficácia da gestão de risco pelas Gestoras quanto às ameaças e planos de ação, de contingência e de continuidade de negócios.

Ademais, no que se refere especificamente à segurança cibernética, as Gestoras identificaram as seguintes principais ameaças, nos termos inclusive do Guia de Cibersegurança da ANBIMA:

(i) *Malware* – softwares desenvolvidos para corromper computadores e redes (tais como: Vírus, Cavalo de Troia, *Spyware* e *Ransomware*);
(ii) Engenharia social – métodos de manipulação para obter informações confidenciais (*Pharming*, *Phishing*, *Vishing*, *Smishing*, e *Acesso Pessoal*);
(iii) Ataques de DDoS (*distributed denial of services*) e *botnets*: ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; e
(iv) Invasões (*advanced 8ersistente threats*): ataques realizados por invasores sofisticados utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

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

3.2.2 Ações de Prevenção e Proteção

Após a identificação dos riscos, o Grupo Valora adota as medidas a seguir descritas para proteger Informações Confidenciais e sistemas.

- Regra Geral de Conduta

O Grupo Valora realiza efetivo controle do acesso a arquivos que contemplem Informações Confidenciais em meio físico, disponibilizando-os somente aos Colaboradores que efetivamente estejam envolvidos no projeto que demanda o seu conhecimento e análise.

Os Colaboradores são orientados para que façam apenas em situação de exceção cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede do Grupo Valora e circulem em ambientes externos ao Grupo Valora com estes arquivos, uma vez que tais arquivos contêm informações que são consideradas confidenciais.

A troca de informações entre os Colaboradores do Grupo Valora deve sempre se pautar no conceito de que o receptor deve ser alguém que necessita receber tais informações para o desempenho de suas atividades e que não está sujeito a nenhuma barreira que impeça o recebimento daquela informação. Em caso de dúvida a Equipe de Compliance, Risco e PLD deve ser acionada previamente à revelação.

Neste sentido, os Colaboradores não deverão, em qualquer hipótese, deixar em suas respectivas estações de trabalho ou em outro espaço físico do Grupo Valora qualquer documento que contenha Informação Confidencial durante a ausência do respectivo usuário, principalmente

após o encerramento do expediente.

Qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora, pois pode conter informações restritas e confidenciais mesmo no ambiente interno do Grupo Valora.

O Grupo Valora não mantém arquivo físico centralizado, sendo cada Colaborador responsável direto pela boa conservação, integridade e segurança de quaisquer Informações Confidenciais que estejam em meio físico sob a sua guarda.

O descarte de Informações Confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. Os documentos físicos que contenham Informações Confidenciais ou de suas cópias deverão ser triturados e descartados imediatamente após seu uso de maneira a evitar sua recuperação ou leitura.

Em consonância com as normas internas acima, os Colaboradores devem se abster de utilizar pen-drives, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade no Grupo Valora.

O envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é também terminantemente proibido, bem como o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam difamar a imagem e afetar a reputação do Grupo Valora.

O recebimento de e-mails muitas vezes não depende do próprio Colaborador, mas espera-se bom senso de todos para, se possível, evitar receber mensagens com as características descritas previamente. Neste caso, o Colaborador deve apagá-las imediatamente, de modo que estas permaneçam o menor tempo possível nos computadores do Grupo Valora.

A visualização de *sites*, *blogs*, *fotologs*, *webmails*, entre outros, que contenham conteúdo discriminatório, preconceituoso (sobre origem, etnia, religião, classe social, opinião política, idade, sexo ou deficiência física), obsceno, pornográfico ou ofensivo é terminantemente proibida.

AÇÕES DE PREVENÇÃO E PROTEÇÃO DE INFORMAÇÕES CONFIDENCIAIS E SEGURANÇA CIBERNÉTICA
Acesso Escalonado do Sistema
O acesso como “administrador” de área de *desktop* é limitado aos usuários aprovados pelo Diretor de Compliance, Risco e PLD e, com isso, serão determinados privilégios/credenciais e níveis de acesso de usuários apropriados para os Colaboradores.

O Grupo Valora mantém diferentes níveis de acesso a pastas e arquivos eletrônicos de acordo com as funções e senioridade dos Colaboradores. As combinações de *login* e senha são utilizadas para autenticar as pessoas autorizadas e conferir acesso à parte da rede do Grupo Valora necessária ao exercício de suas atividades.

A implantação destes controles é projetada para limitar a vulnerabilidade dos sistemas do Grupo Valora em caso de violação.

Senha e Login

A senha e *login* para acesso aos dados contidos em todos os computadores, bem como nos e-mails que também possam ser acessados via webmail, devem ser conhecidas somente pelo respectivo usuário do computador e são pessoais e intransferíveis, não devendo ser divulgadas para quaisquer terceiros. As senhas deverão ser trocadas **semestralmente**, conforme aviso automático, programado no e-mail pela área de informática.

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

Uso de Equipamentos e Sistemas

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

A utilização dos ativos e sistemas do Grupo Valora, incluindo computadores, telefones, internet, e-mail e demais aparelhos se destina prioritariamente a fins profissionais. O uso indiscriminado destes para fins pessoais deve ser evitado e nunca deve ser prioridade em relação a qualquer utilização profissional.

Todo Colaborador deve ser cuidadoso na utilização do seu próprio equipamento e sistemas e zelar pela boa utilização dos demais. Caso algum Colaborador identifique a má conservação, uso indevido ou inadequado de qualquer ativo ou sistemas deve comunicar o Diretor de Compliance, Risco e PLD.

Acesso Remoto

O Grupo Valora permite o acesso remoto pelos Colaboradores ao e-mail, rede e diretório, conforme requisição por estes e autorização pelo responsável da área.

Controle de Acesso

O acesso de pessoas estranhas ao Grupo Valora a áreas restritas somente é permitido com a autorização expressa de Colaboradores autorizados pelos administradores da respectiva Gestora.

Tendo em vista que a utilização de computadores, telefones, internet, e-mail e demais aparelhos se destina exclusivamente para fins profissionais, como ferramenta para o desempenho das atividades dos Colaboradores, as Gestoras monitoram a utilização de

tais meios.
Firewall, Software*, Varreduras e *Backup
As Gestoras utilizam um *hardware* de *firewall* projetado para evitar e detectar conexões não autorizadas e incursões maliciosas. O Diretor de Compliance, Risco e PLD é responsável por determinar o uso apropriado de *firewalls* (por exemplo, perímetro da rede). As Gestoras mantém proteção atualizada contra *malware* nos seus dispositivos e software antivírus projetado para detectar, evitar e, quando possível, limpar programas conhecidos que afetem de forma maliciosa os sistemas da empresa (por exemplo, *vírus*, *worms*, *spyware*). Serão conduzidas varreduras **diárias** para detectar e limpar qualquer programa que venha a obter acesso a um dispositivo na rede das Gestoras. As Gestoras utilizam um plano de manutenção projetado para guardar os seus dispositivos e *softwares* contra vulnerabilidades com o uso de varreduras e patches. O Diretor de Compliance, Risco e PLD é responsável por patches regulares nos sistemas das Gestoras. As Gestoras mantém e testa regularmente medidas de backup consideradas apropriadas pelo Diretor de Compliance, Risco e PLD. As informações das Gestoras são atualmente objeto de backup **diário** com o uso de computação na nuvem.

3.3 Monitoramento e Testes

A Equipe de Compliance, Risco e PLD adota as seguintes medidas para monitorar determinados usos de dados e sistemas em um esforço para detectar acessos não autorizados ou outras violações potenciais, em base, no mínimo, **anual**:

(i) Monitoramento, por amostragem, do acesso dos Colaboradores a sites, blogs, fotologs, webmails, entre outros, bem como os e-mails enviados e recebidos; e

(ii) Verificação, por amostragem, das informações de acesso ao espaço do escritório, a desktops, pastas e sistemas, de forma a avaliar sua aderência às regras de restrição de acesso e escalonamento.

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

3.4 Plano de Identificação e Resposta

- Identificação de Suspeitas

Qualquer suspeita de infecção, acesso não autorizado, outro comprometimento da rede ou dos dispositivos das Gestoras (incluindo qualquer violação efetiva ou potencial), ou ainda no caso de vazamento de quaisquer Informações Confidenciais, mesmo que de forma involuntária, deverá ser informada ao Diretor de Compliance, Risco e PLD prontamente. O Diretor de Compliance, Risco e PLD determinará quais membros da administração das Gestoras e, se aplicável, de agências reguladoras e de segurança pública, deverão ser notificados.

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

- Procedimentos de Resposta

O Diretor de Compliance, Risco e PLD responderá a qualquer informação de suspeita de infecção, acesso não autorizado ou outro comprometimento da rede ou dos dispositivos das Gestoras de acordo com os critérios abaixo:

(i) Avaliação do tipo de incidente ocorrido (por exemplo, infecção de *malware*, intrusão da rede, furto de identidade), as informações acessadas e a medida da respectiva perda;
(ii) Identificação de quais sistemas, se houver, devem ser desconectados ou de outra forma desabilitados;
(iii) Determinação dos papéis e responsabilidades do pessoal apropriado;
(iv) Avaliação da necessidade de recuperação e/ou restauração de eventuais serviços que tenham sido prejudicados;
(v) Avaliação da necessidade de notificação de todas as partes internas e externas apropriadas (por exemplo, clientes ou investidores afetados, segurança pública);
(vi) Avaliação da necessidade de publicação do fato ao mercado, nos termos da regulamentação vigente, (por exemplo: em sendo Informações Confidenciais de fundo de investimento sob gestão das Gestoras, a fim de garantir a ampla disseminação e tratamento equânime da Informação Confidencial);
(vii) Determinação do responsável (ou seja, às Gestoras ou o cliente ou investidor afetado) que arcará com as perdas decorrentes do incidente. A definição ficará a cargo do Diretor de Compliance, Risco e PLD, após a condução de investigação e uma avaliação completa das circunstâncias do incidente.

3.5 Arquivamento de Informações

Os Colaboradores deverão manter arquivada, pelo prazo regulamentar aplicável, toda e qualquer informação, bem como documentos e extratos que venham a ser necessários para a efetivação satisfatória de possível auditoria ou investigação em torno de possíveis investimentos e/ou clientes suspeitos de corrupção e/ou lavagem de dinheiro, bem como todos os documentos e informações exigidos pela Resolução CVM nº 21, correspondência, interna e externa, papéis de

trabalho, relatórios e pareceres relacionados com o exercício de suas funções em conformidade com o inciso IV do Artigo 18 e com o Artigo 34 da Resolução CVM nº 21.

4. Propriedade Intelectual

O Grupo Valora é detentor dos direitos de propriedade de quaisquer materiais, produtos ou serviços que sejam criados durante a jornada regular de trabalho e/ou que tenham sido produzidos fazendo-se o uso de ativos ou recursos da Instituição.

Qualquer pessoa que voluntariamente malversar, furtar, ou se apropriar de maneira fraudulenta de qualquer quantia, recurso financeiro ou ativo de valor pertencente ao Grupo Valora, ficará sujeito, além das sanções disciplinares, aos rigores da legislação aplicável.

Os Colaboradores não poderão bloquear o uso ou o acesso de quaisquer materiais, produtos ou serviços sujeitos à propriedade intelectual, inclusive e através de criação de senhas.

Todo e qualquer arquivo físico ou eletrônico gravado na rede corporativa é de propriedade exclusiva do Grupo Valora.

5. Lei Geral de Proteção de Dados (LGPD) – lei 13.709/2018

A VALORA GESTÃO DE INVESTMENTOS assume o compromisso perante seus clientes, usuários e demais partes interessadas, de cumprir e zelar pelos princípios da Lei nº 13.709/2018, zelando pela privacidade e segurança das informações coletadas dos usuários que utilizam nossos serviços. Agimos, assim, na qualidade de controlador dos dados pessoais dos usuários e estamos sujeitos às disposições da Lei federal n.º 13.709/2018 (Lei Geral de Proteção de Dados – LGPD).

Tratamos apenas os dados pessoais enquanto forem necessários e adequados para as finalidades que embasam a coleta, sempre observando as bases legais do tratamento.
Nosso so de Privacidade pode ser acessado no link:
AVISO-DE-PRIVACID
ADE-Valora-Invest.p

Em caso de dúvidas podem ser esclarecidas por meio do e-mail: dpo@valorainvest.com.br ou pelo fone: + 55 11 3016-0906

6. Sigilo – Confidencialidade de Informações

Confidencialidade é um princípio fundamental para o Grupo Valora, aplicável a quaisquer informações não públicas, no que diz respeito ao Grupo Valora e às informações recebidas de um cliente ou fornecedor para um propósito comercial expresso.

O Grupo Valora resguarda o sigilo e a privacidade das informações pessoais e financeiras de seus clientes, tratando todas as informações fornecidas por seus clientes como sigilosas, não sendo, portanto, permitida sua transmissão a terceiros, salvo mediante expressa e prévia anuência do cliente.

Os Colaboradores do Grupo Valora devem resguardar o sigilo e a confidencialidade das informações relativas aos clientes, obtidas no desenvolvimento das atividades relacionadas ao Grupo Valora. O sigilo e a confidencialidade devem ser mantidos mesmo após o rompimento do vínculo, por qualquer motivo, com a Valora. A não observância da confidencialidade estará sujeita à apuração de responsabilidades nas esferas cível e criminal.

Todas as informações, documentos, cópias e extratos gerados nas atividades do Grupo Valora são de propriedade do Grupo Valora e deverão permanecer única e exclusivamente com ao Grupo Valora. Os Colaboradores, no término de sua relação com ao Grupo Valora, devolverão ao Grupo Valora todos os originais e todas as cópias de quaisquer documentos recebidos ou adquiridos durante a relação mantida com ao Grupo Valora, bem como todos os arquivos, correspondências e/ou outras comunicações recebidas, mantidas e/ou elaboradas durante a respectiva relação com ao Grupo Valora.

Qualquer divulgação de informações a autoridades governamentais em virtude de decisões judiciais, arbitrais ou administrativas que envolva, direta ou indiretamente, as atividades desenvolvidas pelo Grupo Valora, deverá ser prévia e tempestivamente comunicada ao Oficial de Compliance responsável pela aplicação deste Código, para que este decida sobre a forma mais adequada para tal divulgação.

Tendo em vista a alta especialização da atividade desenvolvida pelo Grupo Valora, assim como os princípios que regem o mercado de valores mobiliários, é absolutamente vedada a revelação de carteiras e estratégias de investimento de todo e qualquer produto analisado, administrado e/ou gerido pelo Grupo Valora a qualquer não colaborador, seja da imprensa, de círculo pessoal de convívio, de ligação imediata de parentesco ou de estado civil. A não observância deste item estará sujeita à apuração de responsabilidades nas esferas cível e criminal.

Informações sobre o Grupo Valora devem ser transmitidas apenas se vierem a favorecer a um fim legítimo do Grupo Valora. A transmissão destas informações deve ser efetuada com o entendimento expresso de que as mesmas são confidenciais e devem ser utilizadas exclusivamente para o objeto restrito para o qual foram recebidas ou concedidas. Salvo instrução legal em contrário, informação confidencial só poderá ser usada para fins profissionais e sob nenhuma deverá ser utilizada para obtenção de quaisquer vantagens pessoais.

Adicionalmente, é proibida a divulgação desse tipo de informação para terceiros ou profissionais não envolvidos e/ou autorizados a recebê-la.

Todos os Colaboradores são responsáveis pela guarda de documentos relativos às suas atividades, devendo, portanto, assegurar que informações confidenciais não sejam expostas a outros profissionais ou a terceiros em trânsito no Grupo Valora em períodos de ausência de seu local físico de trabalho.

O Grupo Valora adota normas de proteção de informações confidenciais de clientes e tem como política de não fornecer e nem divulgar quaisquer informações a respeito de contas, investimentos, valores, volumes e dados cadastrais de seus clientes a terceiros, salvo se houver determinação do Poder Judiciário.

Sendo assim, o Colaborador tem o compromisso de não divulgar a terceiros, direta ou indiretamente, durante o período em que estiver prestando serviços ao Grupo Valora e após o seu término, quaisquer informações confidenciais ou documentos por ele elaborados no desempenho de suas funções, devendo mantê-las sob o mais absoluto sigilo.

O descumprimento às exigências relacionadas à confidencialidade das informações está sujeita às penalidades civis e criminais, multas e prisão, podendo ainda ser impostas sanções administrativas a critério da Diretoria do Grupo Valora.

Toda e qualquer informação financeira que diz respeito ao Grupo Valora é confidencial, a não ser que tenha sido objeto de divulgação através de relatórios publicados em jornais ou outros veículos de comunicação.

Excetua-se ao caso acima quando este tipo de informação é requisitado por órgão regulador ou com prévia aprovação do Comitê de Ética.

7. Informação Privilegiada (“Insider Information”)

É vedado o uso ou a divulgação de informação privilegiada por qualquer profissional ligado ao Grupo Valora, seja por atuação em benefício próprio ou de terceiros. As violações às exigências relacionadas ao uso de informações privilegiadas estarão sujeitas às penalidades civis e criminais, multas e prisão, podendo ainda ser impostas sanções administrativas a critério da Diretoria do Grupo Valora.

Considera-se informação privilegiada qualquer informação relevante a respeito de qualquer sociedade ou negócio que envolva o Grupo Valora, que não tenha sido divulgada publicamente e que seja obtida de forma privilegiada, em decorrência da relação profissional ou pessoal mantida com um cliente, com colaboradores de empresas analisadas ou investidas ou com terceiros.

São exemplos de informações privilegiadas: informações verbais ou documentadas a respeito de resultados operacionais de empresas, alterações societárias (fusões, cisões e incorporações), informações sobre compra e venda de empresas, títulos ou valores mobiliários, e, ainda, qualquer informação que seja objeto de um acordo de confidencialidade firmado pelo Grupo Valora com terceiros.

As informações privilegiadas devem ser mantidas em sigilo por todos que a elas tiverem acesso, seja em decorrência do exercício da atividade profissional ou de relacionamento pessoal.

Quem tiver acesso a uma informação privilegiada deverá divulgá-la imediatamente ao Oficial de Compliance que é responsável pela aplicação deste Código, não devendo divulgá-la a ninguém, nem mesmo a outros Colaboradores, profissionais de mercado, amigos e parentes, e nem a utilizar, em benefício próprio ou de terceiros.

O Oficial de Compliance irá analisar a suposta informação privilegiada a ele divulgada pelo Colaborador e, caso entenda que tal informação possa realmente ser classificada como tal, irá informar aos gestores de todos os produtos geridos pelo Grupo Valora que tais produtos estão proibidos de negociar ações ou quaisquer outros títulos de companhias cujos valores possam ser afetados pela divulgação de tal informação privilegiada. Quando o Oficial de Compliance responsável pela aplicação deste Código entender que tal informação privilegiada não mais poderá afetar os valores das ações e/ou títulos das companhias em questão, ele informará imediatamente a todos os gestores de produtos geridos pelo Grupo Valora que tais ações e/ou títulos estão liberados para negociação por tais produtos.

Caso haja dúvida sobre o caráter privilegiado da informação, aquele que a ela teve acesso deve imediatamente relatar tal fato ao Oficial de Compliance responsável pela aplicação deste Código. Todo aquele que tiver acesso a uma informação privilegiada deverá restringir ao máximo a circulação de documentos e arquivos que contenham essa informação.

Existem normas que vedam a compra, venda, recomendação ou outros tipos de transferência de títulos e valores mobiliários em situações de conhecimento privilegiado de informações, isto é, que não sejam de domínio público, sobre o emissor desses títulos.

Essas normas também proíbem a revelação dessas informações a terceiros que possam comercializar tais títulos. As consequências da utilização de “informações privilegiadas” podem ser graves tanto para o Colaborador quanto para o Grupo Valora.

Os Colaboradores que tenham acesso às informações privilegiadas e àquelas que ainda não tenham sido divulgadas ao público investidor devem garantir o sigilo das mesmas, exceto quando necessária à condução dos negócios da Instituição e, ainda, somente caso não haja motivos ou indícios para presumir que o receptor da informação a utilizará erroneamente.

As violações às exigências relacionadas ao uso de informações privilegiadas estarão sujeitas às penalidades civis e criminais, multas e prisão, podendo ainda ser impostas sanções administrativas a critério da Diretoria do Grupo Valora.

8. Treinamentos

Todos os novos Colaboradores do Grupo Valora participam de um treinamento de compliance online. Além disso, são entregues cópias do Código de Ética e Conduta e da Política de Investimentos Pessoais, bem como, dois termos de adesão, atestando leitura e compreensão destas regras e comprometimento em cumpri-las.

Anualmente ou sempre que houver alteração na norma vigente, é realizado um novo treinamento de reciclagem com os Colaboradores.

9. Processos e Controles

9.1 Agenda Regulatória

As Gestoras dentre suas atribuições, possuem a obrigação de encaminhar aos órgãos reguladores e autorreguladores informações e documentos com base nas atividades exercidas =. Segue abaixo a periodicidade para envio de tais informações:

Organismo	Regra	Tema	Exigência	Prazo
COAF	Lei 9.613 – Art.11 inciso II	Lavagem de Dinheiro	Comunicar operações que possam conter indícios de crimes de lavagem de dinheiro.	24 horas
COAF/CVM	Lei 9.613 – Art.11 III e ICVM 301 Art. 7A	Lavagem de Dinheiro	Comunicar anualmente através do SISCOAF ou sistema disponível na CVM a não ocorrência de transações inconsistentes – Declaração Negativa.	Até o último dia útil de Janeiro.
CVM	Instrução 558 – Art. 15 II	Formulário de Referência	Envio anual do formulário com as informações atualizadas.	Até o dia 31 de Março de cada ano

ANBIMA	Código de Fundos de Investimentos – Art.40 e Deliberação 65	Suitability	Envio do Laudo de Suitability contendo as informações relativas ao ano civil anterior.	Até último dia útil de Março

Ademais, a Associação Brasileira do Mercado Financeiro e de Capitais (ANBIMA) elaborou o documento "Guia de Prazo dos Códigos" que pode ser baixado através do site da associação, no qual consta a relação de todas as informações que precisam ser encaminhadas pelas instituições participantes de seus códigos de autorregulação.

9.2 Matriz de Risco

A Matriz de Risco é elaborada pelos responsáveis de cada área justamente por conhecer os riscos dos processos no qual está inserido e é atualizada anualmente.
Com base no levantamento dos responsáveis, o Oficial de Risco e Compliance consolida as informações e elabora um relatório com os problemas identificados, ações necessárias e prazos para a regularização.

Este relatório é apresentado ao Comitê de Compliance e ao Administrador de Carteiras responsável pelas Gestoras para ciência, assinatura e providências das ações a serem tomadas. Este relatório é arquivado digitalmente em local específico da rede com acesso limitado ao Oficial de Risco e Compliance e ao Administrador responsável junto à CVM no seguinte diretório: M:\invest\09.Apoio Operacional\01.Compliance\Controles Internos\Matriz de Risco.

9.3 Processo de Boletagem e Aprovação

A boletagem do ativo engloba um processo anterior que é a aprovação do ativo em um Comitê onde além do tipo de ativo também é deliberado o limite global e/ou individual para alocação da equipe de Gestão conforme mandato de cada fundo.

Após esta aprovação, o Oficial de Risco e Compliance formaliza em ata a deliberação dos limites dos ativos e atualiza a planilha de limites de ativos aprovados.

Com base na deliberação, a equipe de Gestão solicita à equipe de Backoffice o cadastro do(s) ativo(s) junto ao Administrador dos nossos fundos bem como o cadastramento de passivo no Administrador do(s) fundo(s) investido(s).

Após a confirmação por parte do Backoffice de que não há qualquer pendência cadastral, a equipe de Gestão está apta para envio, por e-mail, das operações a serem executadas para os fundos conforme aprovado no Comitê.

A equipe de Backoffice, com base na planilha de limites aprovados, verifica se a operação enviada pela equipe de Gestão está em conformidade. Caso haja alguma inconsistência, a equipe de Backoffice verifica junto à equipe de Gestão e com o Oficial de Risco e Compliance sobre a divergência.

Após sanada a dúvida, a operação poderá seguir ou não para execução e liquidação junto ao Administrador do fundo.

9.4 Controles de Compliance

É de responsabilidade da área de Compliance, no início de cada ano, elaborar um cronograma dos controles que serão executados dentro do ano, a fim de verificar a efetividade dos processos adotados pelas áreas dentro do Grupo Valora.

O processo de verificação é fragmentado em 4 fases, sendo elas:

1° fase: Mapeamento das informações que serão analisadas, levando em consideração o risco perante as regras regulatórias;
2° fase: Criação de monitoramento e execução das análises (Amostrais);
3°fase: Elaboração de um relatório consolidado contendo os pontos de deficiências identificados, bem como o plano de ação a ser executado;
4° fase: Acompanhamento do plano de ação junto as Áreas responsáveis pelo tratamento.

Processo	Periodicidade	Ação
Normas Regulatórias	Por demanda	Acompanhar as leis e instruções emitidas pelos órgãos reguladores quanto às atividades realizadas pelo Grupo Valora. Para as novas instruções e atualizações, realizar uma análise para verificar o impacto nas Gestoras e as possíveis mudanças.
Bloqueio Carteira	Mensal	No 5 ° dia útil de cada mês, bloquear no site da CVM a carteira dos fundos de investimentos.
Autorização Compra de Ativos	Por demanda	Receber da área de Gestão, para análise, os dados dos ativos a serem adquiridos. Após aprovação, transmitir ao backoffice a ordem de compra.
Verificação de Ativos	Por demanda	Acompanhar a relação dos ativos aprovados em Comitê e o seu vencimento. Quando necessário agendar reunião parta atualizar a relação dos ativos e seus limites.
Gestão de Ativos	Mensal	Acompanhamento das carteiras com o objetivo de verificar a adequação dos fundos aos seus regulamentos, políticas de investimentos do Grupo Valora e legislação pertinente. Informar os gestores possíveis casos de desenquadramento.

Certificação	Por demanda	Atualização do banco de dados ANBIMA, após admissão/desligamento de Colaboradores.
	Trimestral	A área de compliance acessa o banco de dados ANBIMA para efetuar atualizações, inclusões e consultas aos prazos de certificação.
Cadastro dos Cotistas	Semestral	I. Analisar o processo de coleta da informação; II. As análises nos sistemas RISC e E-Guardian (identificar possíveis deficiências); III. Análise Amostral dos Cotistas (+/- 5) a. verificar se o cliente possui todos os documentos mínimos; b. a conformidade das informações fornecidas; c. a evidência do processo de KYC; d. o armazenamento e validade dos documentos.
Ordem	Trimestral	Verificar a efetividade do processo: a. Ordem do cotista (e-mail) b. Verificação de compatibilidade do fundo versus perfil de risco; c. Armazenamento das informações.
Prevenção à Lavagem de dinheiro	Mensal	I. Acompanhar o Sistema E-guardian e tratar os alertas identificados; II. Verificação de Mídias,listas restritivas e lista PEP a fim de verificar se algum cotista da gestora está na relação
	Trimestral	I. Verificar os controles adotados internamente e a efetividade do sistema E-guardian; II. Realizar uma análise amostral dos cotistas e testar o processo de PLD.
Suitability	Semestral	I. Verificação do questionário preenchido a fim de identificar se o perfil definido está em conformidade com as respostas; II. Verificar se o fundo aplicável é compatível ao perfil de risco do investidor; III. Caso aplicável, verificar se o cliente possui um termo de recusa e/ou desenquadramento; IV. Verificar se o processo de comunicação com o cliente no momento da definição do perfil e, em casos de desenquadamento; V. Verificar os processos de vedação de recomendar produtos e ordenação de operação, bem como o controle para verificar possíveis desenquadramentos; VI. Verificar o processo de controles internos executado pela área de relacionamento junto ao cliente;
Plano de Continuidade	Semestral	Realização de testes de: I. Nobreak: Verificar se as informações do servidor principal estão sendo transmitidas corretamente para o secundário;

Treinamento		II. Ambiente Alternativo: Se dirigir até o local e testar os sistemas e gerar evidências dos testes; III. Acesso via VPN: Testar o acesso remoto e gerar evidências do acesso aos sistemas.
	Anual	Treinamento/Reciclagem dos funcionários sobre os seguintes temas: I. Prevenção à Lavagem de Dinheiro e Know Your Client; II. Processo de Suitability; III. Segurança da Informação

9.5 Controles de Risco

A Área de Risco monitora através de controles internos, além do risco pré-trade, os processos listados abaixo:

Processo	Periodicidade	Ação
Enquadramento das carteiras	Semanal	Verificar os limites de exposições por ativo em relação ao patrimônio do fundo.
Gerenciamento do Risco de Liquidez	Semanal	Verificar a liquidez do fundo em relação ao cumprimento das obrigações de pagamentos das despesas e resgate solicitados.
Grau de Dispersão de Cotas	Semanal	Verificar a exposição do maior cotista dentro de cada fundo aberto.
Concentração dos Cotistas	Semanal	Verificar a pulverização de cotistas dentro de cada fundo aberto.
Concentração dos Distribuidores	Semanal	Verificar a concentração dos distribuidores dentro de cada fundo aberto.
Maior Resgate Esperado	Semanal	Verificar o track record do maior resgate sofrido por cada fundo aberto.
Matriz de Risco	Anual	Consolidar o mapeamento feito pelos responsáveis pelas respectivas áreas acerca dos riscos identificados por eles.

Um relatório consolidado é gerado periodicamente com os indicadores acima e encaminhado para a área de Gestão, Diretor Responsável junto à CVM e ao Oficial de Compliance.

A Matriz de Risco é consolidada pelo Oficial de Risco e Compliance para elaboração de um relatório anual que é apresentado ao Comitê de Compliance e o diretor responsável pela administração de carteiras perante a CVM para ciência e providências das ações a serem tomadas para regularização dos apontamentos.

9.6 Controles de Gestão

A Área de Gestão é a responsável pela busca de novos ativos, monitoramento, gerenciamento de caixa das carteiras, compra, venda e alocação de acordo com a legislação vigente e em consonância com os mandatos de cada fundo gerido pelo Grupo Valora. A Gestão também compila o material gerado pela Área de Crédito e prepara apresentação para que seja submetido ao Comitê de Investimentos e Produtos.

Processo	Periodicidade	Ação
Validação da Carteira	Diariamente	É realizado o batimento dos ativos, despesas, caixa disponível e validação da cota dos fundos.
Alocação da Carteira	Por demanda	Enviar operações para alocação e gerenciamento de caixa dos fundos conforme política de liquidez.
Acompanhamento de Carteiras	Mensalmente	Acompanhamento qualitativo e quantitativo dos ativos durante o período de investimentos, reuniões presenciais e/ou conferências telefônicas junto aos emissores dos ativos adquiridos.
Participação em Assembleias	Por demanda	Participação em assembleias quando a matéria tratar de alterações estruturais dos fundos investidos.
Carta Mensal	Mensalmente	Elaborar relatórios mensais com panorama do mercado e comportamento das carteiras para os clientes e distribuidores.

9.7 Controles de BackOffice

A Área de Backoffice é responsável pela execução das operações e tem o dever fiduciário sobre as atividades listadas abaixo:

Processo	Periodicidade	Ação
Boletagem de Operação	Diariamente	Registro das operações na plataforma do administrador para devida liquidação.
Validação da Carteira	Diariamente	É realizado um confronto entre o extrato Cetip e as informações extraídas do site do Administrador.
Liquidação de Operações	Por demanda	Acompanhar as liquidações das operações boletadas junto às contrapartes.
Fluxo de Caixa dos Fundos	Semanalmente	Levantamento de todos os resgates e despesas a serem liquidadas no intervalo de 1 semana e providenciar caixa necessário para cumprimento das obrigações.
Controle de Rebate	Mensal	Calcular os valores dos rebates de cada distribuidor, encaminhar a memória de cálculo para respectivamente e ordenar os pagamentos junto ao Administrador dos fundos.

10. Política de Certificação

a. Introdução

As Gestoras aderiram e estão sujeita às disposições do Código de Certificação, devendo garantir que todos os profissionais elegíveis estejam devidamente certificados.

b. Atividades Elegíveis e Critérios de Identificação.

Tendo em vista a atuação das Gestoras como gestoras de recursos de terceiros e distribuidoras dos seus próprios fundos sob gestão, foi identificado que a CGA e a CGE são as certificações pertinentes às suas atividades, aplicáveis aos profissionais com alçada/poder discricionário de investimento, bem como que a CPA-20 é a certificação pertinente para os Colaboradores que realizam a distribuição dos fundos de investimento diretamente junto a investidores.

Nesse sentido, apenas o Colaborador com poder para realizar a distribuição dos fundos de investimento diretamente junto a investidores é elegível ao CPA-20, ao passo que, somente o Colaborador com poder final para ordenar a compra ou venda de posições, sem a necessidade de aprovação prévia do Diretor de Gestão, ou seja, o Colaborador que tenha, de fato, alçada/poder discricionário de investimentos, é elegível à CGA e CGE, a depender do investimento gerido, uma vez que a CGA é a certificação aplicável aos profissionais que atuam em carteiras administradas, fundo de renda fixa, fundo de ações, fundo multimercado, fundo cambial e/ou fundos de índice e a CGE é aplicável aos profissionais que atuam em fundo de investimento em participações, fundo de investimento em direitos creditórios não padronizados, fundo de índice, fundo de investimento em direitos creditórios, fundo de investimento em cotas de fundos de investimento em direitos creditórios e/ou fundo de investimento imobiliário.

Em complemento, as Gestoras destacam que as certificações são de cunho pessoal e intransferíveis, bem como seguirão os seguintes prazos, os quais serão monitorados pelo Diretor de Compliance, Risco e PLD, sendo certo que caso o Colaborador esteja exercendo a atividade elegível de CGA ou CGE nas Gestoras e a certificação não esteja vencida, a partir do vínculo do Colaborador com as Gestoras, o prazo de validade da certificação CGA e CGE será indeterminado, enquanto perdurar o seu vínculo com as Gestoras e a sua atuação na atividade elegível. Por outro lado, caso o Colaborador não esteja exercendo a atividade elegível da CGA ou CGE na Gestora, a validade da respectiva certificação será de 3 (três) anos, contados da data de aprovação no exame, ou da data em que deixou de exercer a atividade elegível da CGA ou CGE, conforme o caso.

Não obstante o acima, estão dispensados da obtenção da CPA-10, CPA-20 e CEA para o exercício das atividades elegíveis a estas certificações os Colaboradores que atuarem como planejadores

financeiros que possuem CFP enquanto mantiverem a condição de profissionais certificados pelo IBCPF.

Com relação ao Colaborador certificado pela CPA-20 que se vincular as Gestoras para exercer atividade elegível, e desde que a sua certificação não esteja vencida na data do vínculo, terá o prazo de vencimento de sua certificação equivalente a 5 (cinco) anos, contados a partir da data da aprovação no exame ou da conclusão do procedimento de atualização, conforme o caso. Por outro lado, caso o Colaborador não esteja exercendo a atividade elegível de CPA-20 na Gestora, a validade da certificação será de até 3 (três) anos, contados da data de aprovação no exame ou da conclusão do procedimento de atualização, conforme o caso, ou, ainda, no caso de o Colaborador já ter atuado na atividade elegível anteriormente, o prazo será contado a partir da data de desligamento comunicada à ANBIMA, respeitado o prazo máximo de 5 (cinco) anos.

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

c. Identificação de Profissionais Certificados e Atualização do Banco de Dados

Antes da contratação, admissão ou transferência de área de qualquer Colaborador, a Equipe de Compliance, Risco e PLD deverá solicitar esclarecimentos ou confirmar junto ao supervisor direto do potencial Colaborador o cargo e as funções a serem desempenhadas, avaliando a necessidade de certificação, bem como verificar no Banco de Dados se o Colaborador possui alguma certificação ANBIMA, uma vez que, em caso positivo, as Gestoras deverão inserir o Colaborador no Banco de Dados.

O Diretor de Gestão deverá esclarecer à Equipe de Compliance, Risco e PLD se Colaboradores que integrarão o departamento técnico envolvido na gestão de recursos terão ou não alçada/poder discricionário de decisão de investimento e com quais produtos cada um dos Colaboradores irão atuar, bem como se Colaboradores que integrarão o departamento técnico envolvido na distribuição poderão realizar a distribuição dos fundos de investimento diretamente junto a investidores.

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

A Equipe de Compliance, Risco e PLD também deverá checar se Colaboradores que estejam se desligando das Gestoras estão indicados no Banco de Dados como profissionais elegíveis/certificados vinculados à Gestora, sendo, para estes, obrigatória a inclusão do desligamento no Banco de Dados.

A Equipe de Compliance, Risco e PLD deve incluir no Banco de Dados as informações cadastrais de todos os Colaboradores que tenham qualquer certificação ANBIMA, esteja a certificação vencida e/ou em processo de atualização, sendo referida inclusão facultativa somente para estagiários e terceiros contratados.

Todas as atualizações no Banco de Dados devem ocorrer **até o último dia útil do mês subsequente à data do evento que deu causa a atualização**, sendo que a manutenção das informações contidas no Banco de Dados deverá ser objeto de análise e confirmação pela Equipe de Compliance, Risco e PLD, conforme disposto abaixo.

d. Rotinas de Verificação

Semestralmente, a Equipe de Compliance, Risco e PLD deverá verificar as informações contidas no Banco de Dados, a fim de garantir que todos os profissionais certificados/em processo de certificação, conforme aplicável, estejam devidamente identificados, bem como se as certificações estão dentro dos prazos de validade estabelecidos no Código de Certificação.

Ainda, o Diretor de Gestão deverá contatar a Equipe de Compliance, Risco e PLD **prontamente**, sempre que houver algum tipo de alteração nos cargos/funções dos Colaboradores que integram o departamento técnico envolvido na gestão de recursos e/ou com quais produtos cada destes Colaboradores atuarem, confirmando, além disso, todos aqueles Colaboradores que atuem com alçada/poder discricionário de investimento, se for o caso.

Colaboradores que não tenham CPA-20 estão impedidos de realizar a distribuição dos fundos de investimento diretamente junto a investidores, assim como aqueles que não tenham, bem como aqueles que não tenha, CGA ou CGE, conforme aplicável (e que não tenham a isenção concedida pelo Conselho de Certificação), estão impedidos de ordenar a compra e venda de ativos sem a aprovação prévia do Diretor de Gestão, tendo em vista que não possuem alçada/poder final de decisão para tanto.

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

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

e. Processo de Afastamento

Todos os profissionais não certificados ou em processo de certificação, e para os quais haja certificação exigível, nos termos previstos neste Manual, serão imediatamente afastados das atividades elegíveis aplicáveis, até que se certifiquem ou até que o Conselho de Certificação conceda a isenção de obtenção da certificação aplicável, devendo para tanto assinar a documentação prevista no **Anexo B** a este Manual, comprovando o seu afastamento da Gestora.

11. Considerações Finais

Todas as dúvidas sobre as diretrizes deste Manual podem ser esclarecidas com o Oficial de Compliance no telefone abaixo:

(11) 3016 0906

12. Quadros de Aprovação e de Controle de Manutenção da Política

Data Atualização	Responsável	Aprovação
12/04/2022	MP	DP
01/11/2021	MP	DP
19/12/2017	MP	DP
04/12/2023	MP	DP

13. ANEXO A

Termo de Recebimento e Adesão – Manual de Regras, Procedimentos e Controles Internos

Eu, _____, portador da Cédula de Identidade n°_____, inscrito no CPF _____, declaro para os devidos fins que:

(i) Recebi o Manual de Compliance da Valora Gestão de Investimentos, li e compreendi o seu conteúdo, bem como me comprometo a observar integralmente seus termos e condições.

(ii) Nos casos de condutas inadequadas, inclusive de terceiros, devo comunicar imediatamente meu superior imediato ou o Oficial de Compliance.

São Paulo, [•] de [•] de [•].

_____

Assinatura

14. ANEXO B

TERMO DE AFASTAMENTO

Por meio deste instrumento, eu, _____, inscrito(a) no CPF/ME sob o nº _____, declaro para os devidos fins que, a partir desta data, estou afastado das atividades de alçada/poder final de decisão de investimentos e/ou desinvestimentos dos fundos sob gestão da **[DENOMINAÇÃO DA SOCIEDADE DO GRUPO VALORA]**, inscrita no CNPJ sob o nº. [==] ("GESTORA") por prazo indeterminado:

[[ ] até que me certifique pela CGA e CGE;

[ ] até que o Conselho de Certificação me conceda a isenção de obtenção da CGA e CGE.

[[ ] até que me certifique pela CGA;

[ ] até que o Conselho de Certificação me conceda a isenção de obtenção da CGA;

[[ ] até que me certifique pela CGE; ou

[ ] até que o Conselho de Certificação me conceda a isenção de obtenção da CGE.]

[ ] até que me certifique pela CPA-20, no caso das atividades de distribuição dos fundos de investimento diretamente junto a investidores.

São Paulo, [---] de [---] de [---].

_____
[COLABORADOR]

_____
[DENOMINAÇÃO DA SOCIEDADE DO GRUPO VALORA]

Testemunhas:

1._____
Nome:
CPF/ME:

2._____
Nome:
CPF/ME: