



MANUAL DE REGRAS, PROCEDIMENTOS E CONTROLES INTERNOS

Rev. 04/2024

Versão 03

Índice

INTRODUÇÃO	3
ABRANGÊNCIA	3
OBJETIVOS DA ÁREA DE COMPLIANCE E CONTROLES INTERNOS	3
GOVERNANÇA	4
SEGREGAÇÃO DE ATIVIDADES	6
SEGURANÇA DA INFORMAÇÃO	6
REGRAS E PROCEDIMENTOS DE CONTROLES INTERNOS	9
CONSEQUÊNCIAS DO DESCUMPRIMENTO DAS POLÍTICAS E PROCEDIMENTOS	11
PROGRAMA DE TREINAMENTO DE COLABORADORES	12
DISPOSIÇÕES GERAIS	12
APROVAÇÃO, VIGÊNCIA E ATUALIZAÇÃO	12

INTRODUÇÃO

O presente Manual de Regras, Procedimentos e Controles Internos (“**Manual**”) tem a finalidade de reunir as regras, procedimentos e controles internos que regem o funcionamento e o desenvolvimento das atividades da SIG Capital Gestão de Recursos Ltda. (“**SIG Capital**”) e a conduta dos sócios, diretores, funcionários, estagiários e jovens aprendizes (“**Colaborador**” e em conjunto como os “**Colaboradores**”).

Este Manual foi elaborado em conformidade com as instruções CVM nº 21/2021, nº 175/2022, e alterações posteriores, ao Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros (“**Código de Administração de Recursos**”) e demais políticas e regulamentações vigentes, referentes às diversas modalidades de investimento, à própria atividade de Gestão de Recursos e aos padrões ético e profissional.

ABRANGÊNCIA

Os princípios e regras deste Manual devem ser observados por todos os Colaboradores que venham, de maneira direta ou indireta, trabalhar para a SIG Capital.

Todos os Colaboradores, Diretores e Sócios, obrigando-se a conhecer o inteiro teor deste Manual e cumpri-lo integralmente, estado este disponibilizado no site da empresa para livre consulta www.sigasset.com

Os Colaboradores também deverão frequentar os cursos internos e externos determinados pela Dir.de Risco e Compliance a fim de se mantrem atualizados quanto às melhores práticas e políticas de gestão de recursos aplicáveis à SIG Capital.

OBJETIVOS DA ÁREA DE COMPLIANCE E CONTROLES INTERNOS

Os principais objetivos da área de *Compliance* da SIG Capital são:

- (a) o permanente atendimento às normas, políticas e regulamentações vigentes, referentes às diversas modalidades de investimento, à própria atividade de gestão de recursos de terceiros (“**Gestão de Recursos**”) e aos padrões ético e profissional;
- (b) a atuação com imparcialidade dos Colaboradores;
- (c) o conhecimento pelos Colaboradores do Código de Ética e Conduta Profissional da SIG Capital, das normas aplicáveis, das políticas previstas na regulação e legislação vigente, bem como das disposições deste Manual;
- (d) a identificação, a administração e a eliminação de eventuais conflitos de interesses que possam afetar a imparcialidade dos Colaboradores que desempenham funções ligadas à gestão de recursos;
- (e) o estabelecimento de mecanismos para:
 - Assegurar a segregação das atividades desenvolvidas pela SIG Capital;

- Mitigar as ocorrências de erro operacional;
- Prevenção à lavagem de dinheiro e combate ao terrorismo;
- Efetividade no atendimento das exigências e solicitações dos órgãos reguladores e fiscalizadores; e
- Coordenação de ações de treinamento relacionados a Compliance, Controles Internos, PLD e Segurança da Informação.

A área de *Compliance* atua de forma autônoma e independente, se reportando apenas ao Diretor de *Compliance* indicado na Comissão de Valores Mobiliários, conforme o disposto no inciso IV, art. 4º, da RES 21 e no art. 11 do Código de Administração de Recursos.

GOVERNANÇA

A área de *Compliance* da SIG Capital está sob a responsabilidade da Diretoria de *Compliance* e sua implementação e controle, sob responsabilidade desta área.

Ainda, os assuntos relacionados a área de *Compliance* da SIG Capital poderão ser levados para conhecimento e eventuais deliberações do Comitê de Risco e *Compliance*.

Principais atribuições do Diretor de *Compliance*

O Diretor de *Compliance*, que exerce suas funções com plena independência, não estando sujeito a qualquer ingerência por parte de quaisquer outras áreas de atuação da Sig Capital, incluindo aquelas correlatas à atividade de Gestão de Recursos (“**Áreas de Atuação**”), é responsável pela implementação dos procedimentos previstos neste Manual. Os controles internos devem ser efetivos e consistentes com a natureza, complexidade e risco das operações realizadas pela SIG Capital.

São atribuições do Diretor de Risco e *Compliance*, sem prejuízo das demais descritas neste Manual:

- (a) Supervisão e manutenção das políticas e procedimentos a serem cumpridos pelos Colaboradores, de acordo com as regras estabelecidas;
- (b) Suporte a todas as Áreas de Atuação da SIG Capital no que concerne a esclarecimentos dos controles e do disposto neste Manual e nas demais normas internas da SIG Capital;
- (c) Acompanhamento da conformidade das atividades da SIG Capital com as normas regulamentares (externas e internas, inclusive, mas não exclusivamente, conforme estabelecidas neste Manual) em vigor;
- (d) A avaliação periódica de controles internos contemplando:
 - Conclusões acerca de exames efetuados;
 - Recomendações acerca de eventuais deficiências, com cronogramas de saneamento; e
 - Manifestação do Diretor de *Compliance* a respeito das deficiências encontradas em verificações anteriores e das medidas planejadas, de acordo com o cronograma proposto, ou efetivamente

adotadas para saná-las.

Principais atribuições do Comitê de Risco e *Compliance*

A SIG Capital também dispõe de Comitê de Risco e *Compliance*, onde são tratados os assuntos relativos à mensuração e controles dos diversos riscos envolvidos na operação de gestão, assim como os temas referentes ao *Compliance*, sempre que necessário.

São atribuições do Comitê de Risco e *Compliance*:

- (a) Definir os princípios éticos a serem observados por todos os Colaboradores da SIG Capital, constantes deste Manual ou de outros documentos que vierem a ser produzidos para este fim, elaborando sua revisão periódica;
- (b) Promover a ampla divulgação e aplicação dos preceitos éticos no desenvolvimento das atividades de todos os Colaboradores da SIG Capital;
- (c) Apreciar todos os casos que cheguem ao seu conhecimento sobre o descumprimento dos preceitos éticos e de *Compliance* previstos neste Manual ou nos demais documentos aqui mencionados, além de apreciar e analisar situações não previstas;
- (d) Garantir o sigilo de eventuais denunciadores de delitos ou infrações, mesmo quando estes não solicitarem, exceto nos casos de necessidade de testemunho judicial ou em manifestação em processo administrativo;
- (e) Tratar todos os assuntos que cheguem ao seu conhecimento dentro do mais absoluto sigilo e preservando os interesses e a imagem institucional e corporativa da SIG Capital, como também dos Colaboradores envolvidos;
- (f) Definir e aplicar eventuais sanções aos Colaboradores;
- (g) Analisar situações que possam ser caracterizadas como “conflitos de interesse” pessoais e profissionais.
- (h) Definir a periodicidade e os exames de aderência nos processos existentes a serem realizados, sempre respeitando os prazos estabelecidos pelas normas e regulamentos e documentando tal processo de aferição.

O Comitê de Risco e *Compliance* contará com: (i) 2 (dois) membros fixos, ambos sócios participantes direta ou indiretamente da SIG Capital, com profundo conhecimento e vivência em mercado de capitais, operações financeiras, atividades bancárias e em *Real Estate*, (ii) os diretores da SIG Capital, incluindo necessariamente o Diretor de Risco, Diretor de *Compliance* e o Diretor Administrador de Carteira, e (iii) podendo, conforme o caso, contar com demais profissionais do time da SIG Capital, ou mesmo, contratar profissional independente para auxílio em matérias específicas de cunho técnico. As deliberações serão registradas em ata.

Ainda, cabe ressaltar que o Comitê de Risco e *Compliance* é soberano em relação às matérias relativas à gestão de Risco e *Compliance*.

Formulário de Referência

A SIG Capital deverá enviar à CVM, até o dia 31 de março de cada ano, seu respectivo Formulário de Referência, por meio de sistema eletrônico disponível na página da CVM na rede mundial de computadores, cujo conteúdo

deve refletir o Anexo 17-E da Res 21.

SEGREGAÇÃO DE ATIVIDADES

A SIG Capital adota a prática de segregação lógica e funcional de atividades entre as suas Áreas de Atuação com a finalidade de (i) prevenir o uso impróprio de informações confidenciais, relevantes e/ou não públicas e que possam ter impacto no preço de um ativo a ser adquirido pelos fundos de investimentos (“Informação Confidencial” e “Fundo”) sob sua gestão, bem como (ii) mitigar quaisquer situações de conflitos de interesse.

Além da segregação de atividades entre as Áreas de Atuação, a SIG Capital também compreende como importante segregar e proteger as suas atividades e informações (físicas e lógicas) das atividades e informações das demais empresas que compartilham o mesmo espaço comercial, prevenindo, com isso, potenciais conflitos de interesse que causem prejuízos para elas, seus cotistas e a própria SIG Capital.

Com o intuito de assegurar a completa segregação, os seguintes procedimentos operacionais serão adotados:

Espaço Físico

A atividade de Gestão de Recursos é desenvolvida segregada das demais atividades desenvolvidas pelas empresas que compartilham o mesmo espaço comercial que a SIG Capital.

O acesso, bem como a permanência na área segregada é destinada à atividade de Gestão de Recursos é restrito a pessoas autorizadas, notadamente, seus Colaboradores. O acesso à referida área, que se dá por meio de controle de acesso, somente é possível por essas pessoas, sendo certo que a circulação é totalmente restrita e controlada

A eventual autorização de entrada de pessoa não registrada no sistema de controle de acesso é previamente informada à área de *Compliance*.

Controle de acesso a arquivos eletrônicos

Os arquivos eletrônicos são mantidos em áreas lógicas dos servidores de arquivos e estão segregadas por Área de Atuação.

Para manutenção e controle da segregação entre as Áreas de Atuação, as solicitações de acesso são realizadas pela área de Tecnologia da Informação que é prestada por um terceiro contratado (“área de TI”).

Além disso, são implementados controles de acesso aos recursos computacionais, como por exemplo, restrição de uso das unidades de armazenamento removíveis limitado aos respectivos Colaboradores de cada Área de Atuação.

SEGURANÇA DA INFORMAÇÃO

A segurança da informação (“**Segurança da Informação**”) é compatível com o porte, o perfil de risco e o modelo de negócio da SIG Capital, com a natureza das suas operações e a complexidade dos seus produtos, serviços, atividades e processos, e com a sensibilidade dos dados e das informações sob sua responsabilidade.

Todas as informações produzidas e utilizadas internamente pelos Colaboradores devem ser consideradas como ativos que tem valor para a SIG Capital e se constituem em vantagem competitiva.

A proteção dessas informações e a preservação de sua confidencialidade é responsabilidade e obrigação de todos os Colaboradores e uma prioridade para a SIG Capital.

Princípios Gerais de Segurança da Informação

Os Princípios Gerais de Segurança da Informação (“**Princípios Gerais**”) valorizados pela SIG Capital são a Integridade, a Disponibilidade e a Proteção.

A utilização dos ativos e sistemas da SIG Capital, incluindo computadores, telefones, internet, e-mail e demais aparelhos se destina prioritariamente a fins profissionais. Seu uso indiscriminado para fins pessoais deve ser evitado e nunca deve ser prioridade em relação a qualquer utilização profissional.

Os sistemas corporativos e o e-mail corporativo são gravados e ficam registrados nos servidores, disponíveis para eventuais inspeções do Diretor de *Compliance*.

O envio ou repasse por e-mail ou outros meios de comunicação de material que contenha conteúdo discriminatório, preconceituoso, obsceno ou ofensivo é também terminantemente proibido, bem como o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam denegrir a imagem e afetar a reputação da SIG Capital ou de seus Colaboradores.

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. Na eventualidade do recebimento de mensagens com as características acima descritas, o Colaborador deve apagá-las imediatamente, de modo que estas permaneçam o menor tempo possível nos servidores e computadores da SIG Capital.

Diretrizes de Segurança da Informação

- (a) Respeitar a propriedade intelectual da SIG Capital e cumprir as leis e normas que regulamentam a propriedade intelectual no que se refere às informações de propriedade ou controladas pela SIG Capital;
- (b) Não discutir questões confidenciais de trabalho, presencialmente ou por telefone, em ambientes públicos;
- (c) Utilizar as ferramentas disponibilizadas pela SIG Capital, inclusive as contas de correio eletrônico e os acessos disponibilizados à internet, exclusivamente para o exercício de sua atividade profissional;
- (d) Não manter informações confidenciais impressas à vista em estações de trabalho, salas de reunião ou qualquer outro ambiente do escritório ou fora dele, e armazenar as informações de maneira adequada e protegida;

- (e) Não fornecer ou emprestar a terceiros as senhas que lhe forem confiadas, e não transportar ou retirar informações da SIG Capital através de correio eletrônico, transferência eletrônica de dados, arquivos ou qualquer tipo de ferramenta capaz de transportar documentos eletrônicos, registros, dados e informações;
- (f) Não executar tentativas de violação de acessos a instalações, sistemas, equipamentos (servidores e microcomputadores) informações e documentos;
- (g) Não instalar softwares e sistemas na rede de computadores da SIG Capital sem autorização;
- (h) Não utilizar os acessos disponibilizados à internet para navegação em sites não relacionados às suas atividades na SIG Capital; e
- (i) Ter responsabilidade sobre as informações e compreender ameaças externas que possam afetar sua segurança, como vírus de computador, interceptação de mensagens eletrônicas e telefônicas, sequestro de informações, arquivos de origem desconhecida e ferramentas de *phishing* utilizadas para cometer fraudes, e notificar a área de TI em caso de suspeita.

Testes Periódicos de Segurança para os Sistemas de Informação

A SIG Capital deve assegurar a existência de testes periódicos de segurança para os sistemas de informação, em especial para os mantidos em meio eletrônico.

São exemplos de alguns dos testes conduzidos:

- (a) Documentação e homologação do ambiente de tecnologia da informação (“TI”), que envolve o mapeamento das licenças, serviços de TI, parque de informática, centro de processamento de dados, *firewalls* e sistemas de antivírus e e-mail;
- (b) Topologia da rede, incluindo a rede interna, a rede externa, os serviços de nuvem, a rede wireless e o sistema de contingência;
- (c) Instalação de correções e atualizações no código para os sistemas de computador administrados;
- (d) Simulação de casos de desastre, em que os servidores de produção são desligados e os Colaboradores acessam a rede através do sistema de contingência.

Manutenção de Arquivos

A SIG Capital 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 instrução ICVM nº 21, bem como toda a correspondência, papéis de trabalho, relatórios e pareceres relacionados com o exercício de suas funções, além de um arquivo segregado documentando as operações em que tenha sido contraparte dos Fundos. Os documentos e informações podem ser guardados em meio físico ou eletrônico, sendo de responsabilidade da Diretoria de cada área garantir o arquivo dos documentos.

Monitoramento dos Sistemas de Comunicação

Os Colaboradores devem ter ciência de que os e-mails enviados e recebidos, as ligações telefônicas e outros sistemas de informação poderão ser monitorados e gravados pela SIG Capital.

O Diretor de *Compliance*, no exercício de suas funções pode realizar inspeções das comunicações eletrônicas e telefônicas, sobre uma amostragem dos Colaboradores, escolhida aleatoriamente, independentemente da suspeita ou ocorrência de quaisquer descumprimentos das regras estabelecidas nos normativos internos da SIG Capital.

O monitoramento realizado pelo Diretor de *Compliance* tem o propósito de verificar a aderência dos Colaboradores às disposições estabelecidas nos manuais e políticas internas da SIG Capital, e não representa uma invasão de privacidade.

Os registros obtidos pelo Diretor de *Compliance* através do monitoramento podem ser utilizados para detecção de violações dos normativos internos da SIG Capital, e servir como evidência em processos administrativos e legais.

REGRAS E PROCEDIMENTOS DE CONTROLES INTERNOS

Além supervisionar o cumprimento pelos Colaboradores das obrigações que lhes são atribuídas neste Manual e nas demais normas internas que regem a SIG Capital, a área de *Compliance* é responsável pela atualização e pelo monitoramento do cumprimento deste Manual e das demais normas internas que regem a SIG Capital, bem como, pelo treinamento dos Colaboradores necessário à sua observância.

Tendo em vista o estabelecido neste Manual, cada Diretoria é responsável pela fiscalização e monitoramento das políticas e dos procedimentos aplicáveis a cada área reportando as infrações ao *Compliance*, quando identificado descumprimento cabendo às respectivas Diretorias:

- (a) Fiscalizar os atos praticados pelos Colaboradores da SIG Capital, verificando o cumprimento de seus deveres legais, estatutários e nos termos do presente Manual e demais políticas aos quais estes ou a SIG Capital venha a aderir;
- (b) Esclarecer as eventuais dúvidas e questionamentos apresentados pelos Colaboradores com relação ao cumprimento das políticas e dos procedimentos estabelecidos neste Manual;
- (c) Adotar as providências necessárias tendo em vista o recebimento das comunicações e notificações enviadas pelos Colaboradores, conforme o estabelecido neste Manual;
- (d) Solicitar ao responsável pela área de TI da SIG Capital o resgate de qualquer comunicação emitida e/ou recebida via e-mail que considere relevante para o exercício de suas funções;
- (e) Verificar a ocorrência do descumprimento pelos referidos Colaboradores nas previsões contida neste Manual;
- (f) Monitorar as informações relacionadas às operações e transações armazenadas nos sistemas informatizados e de comunicação disponibilizados pela SIG Capital (“**Dados Operacionais**”) para o desenvolvimento de suas atividades;

- (g) Planejar trabalhos de auditorias, com relação aos Dados Operacionais, visando à identificação de irregularidades ou oportunidades de melhorias dos procedimentos estabelecidos neste Manual e demais normativos internos; e
- (h) Aplicar as penalidades previstas para o descumprimento das políticas e procedimentos estabelecidos, de acordo com os termos e condições constantes do Código de Ética e Norma Profissionais da SIG Capital.

Caso um Colaborador tome conhecimento de prática de atividades em discordância com as políticas e procedimentos estabelecidos no presente Manual, e/ou de não observância, eventual ou reiterada, das políticas e procedimentos aqui estabelecidos, tal Colaborador deverá reportar a irregularidade e/ou não observância de procedimentos a área de *Compliance*.

A omissão em reportar atividades irregulares e/ou a não observância das regras deste Manual será considerada como cumplicidade à mesma, sujeitando o Colaborador à aplicação das penalidades previstas no Código de Ética e Conduta Profissional da SIG Capital.

Atendimento de solicitações dos Órgãos Reguladores, Autorreguladores, Fiscalizadores e Ministério Público

A área de *Compliance* centraliza a recepção dos ofícios ou comunicações encaminhadas pelos órgãos reguladores, autorreguladores, fiscalizadores e Ministério Público.

Avaliação da prioridade e das áreas envolvidas:

- Identificar os prazos exigidos pelo regulador/fiscalizador;
- Identificar as áreas que serão responsáveis por fornecer os dados/informações que serão enviados/publicados; e
- Estabelecer com tais áreas um planejamento para fornecimento dos dados/informações necessárias (escopo, definição das atividades, duração, qualidade, pessoas envolvidas).

Encaminhamento para os responsáveis:

- Comunicar as áreas envolvidas e definir cronograma para retorno do posicionamento, compatível com a data exigida pelo regulador ou fiscalizador; e
- Registrar os apontamentos na nuvem, para controle de ocorrências de erro operacional.

Controle de prazos:

- Com base na data-limite para envio/publicação das informações, estabelecer um cronograma reverso, ou seja, definir datas (prazos) para obtenção e manipulação dos dados, geração das informações, conferência, análise, validação, formatação e aprovação, visando o cumprimento dos prazos determinados pelos órgãos demandantes. Este cronograma deve ser validado com as áreas envolvidas e divulgado com antecedência a cada período de atualização das informações;
- Dentro do cronograma definido para atendimento aos prazos exigidos, solicitar posicionamento das áreas envolvidas quanto ao atendimento da solicitação;

- Efetuar o acompanhamento (monitoramento e controle) da execução do que foi planejado/acordado com as áreas e dos respectivos prazos, realizando reuniões de ponto de controle com os envolvidos, visando identificar eventuais atrasos no cronograma e, caso necessário, efetuar as devidas correções no processo para que o prazo possa ser atendido; e

Elaboração das respostas

- Cabe a cada área elaborar as repostas à solicitação. Caso a solicitação envolva mais de uma área, a área de *Compliance* deverá consolidar as informações para o atendimento à solicitação final;
- Quando for o caso, a área responsável deverá apresentar as evidências exigidas pelo órgão regulador e/ou pelo *Compliance*;
- Avaliar a efetividade das respostas das áreas em relação à solicitação, solicitando correções e/ou detalhamentos; e
- Quando houver necessidade, solicitar prorrogação de prazo junto aos órgãos demandantes.

Formalização da resposta

- Preparar memorando de encaminhamento das respostas ou de evidências às solicitações dos órgãos demandantes;
- Validar o memorando com a Diretoria e áreas envolvidas;
- Encaminhar a resposta ao órgão demandante, utilizando o canal definido na solicitação;
- Armazenar a solicitação, memorando de resposta e evidências em área específica da rede local; e

Controle do Risco Operacional

O controle do risco operacional consiste em perdas decorrentes de falhas, deficiências ou inadequação dos processos internos da SIG Capital envolvendo tanto pessoas quanto sistemas (“Risco Operacional”).

Os procedimentos adotados para mitigar o Risco Operacional estão descritos na Política de Gestão de Riscos.

Prevenção a Lavagem de Dinheiro e Combate ao Terrorismo

As diretrizes relativas à Prevenção a Lavagem de Dinheiro e Combate ao Terrorismo estão devidamente descritas numa política elaborada especificamente para este fim, cujo Termo de Adesão é obrigatório a todos os Colaboradores da SIG Capital.

CONSEQUÊNCIAS DO DESCUMPRIMENTO DAS POLÍTICAS E PROCEDIMENTOS

O descumprimento das disposições legais ou regulamentares internas pode acarretar sanções disciplinares, no caso de Colaboradores da SIG Capital ou o encerramento do relacionamento comercial, no caso de parceiros, fornecedores ou prestadores de serviços. As situações que representem violação ao estabelecido neste Manual e demais normas internas que regem a SIG Capital, são analisadas pela área de *Compliance*, que recomenda as medidas disciplinares cabíveis conforme descritas no Código de Ética e Conduta Profissional da SIG Capital para deliberação do Diretor de *Compliance*.

PROGRAMA DE TREINAMENTO DE COLABORADORES

Uma vez que o Colaborador inicie o seu vínculo formal com a SIG Capital, ele irá adquirir conhecimento sobre as atividades da SIG Capital, suas atribuições e normas internas, políticas e códigos, além de informações sobre as principais Leis e normas que regem as atividades da SIG Capital, conforme preceitua a ICVM nº 21.

Ademais, em caso de alguma alteração nas políticas da SIG Capital, devido à exigência de órgãos reguladores ou por quaisquer outros motivos, a gestora poderá realizar um programa de reciclagem para os Colaboradores, com o intuito de fornecer a nova política aos estes e de apresentar as mudanças e os novos pontos abordados por tal política.

DISPOSIÇÕES GERAIS

Em cumprimento ao art. 16, III, da ICVM nº 21, a presente Política está disponível no endereço eletrônico disponibilizado pela SIG Capital. www.sigasset.com

APROVAÇÃO, VIGÊNCIA E ATUALIZAÇÃO

Esta Política foi aprovado pela Diretoria de Compliance em abril de 2024, e será revisado periodicamente pela equipe de Compliance. Serão utilizadas como base para sua atualização as legislações, instruções normativas, regulamentações e melhores práticas vigentes na data da sua revisão.

Versão	Data	Elaborado / Modificado por:	Aprovado por:
v.03	04/2024	Dir. Risco e Compliance	Dir. Risco e Compliance