MANUAL DE *COMPLIANCE*, REGRAS, PROCEDIMENTOS E CONTROLES INTERNOS

2024/6

Curitiba/PR

VERSÕES

Versão	Data	Responsável	Aprovação
2020/1	20/07/2020	Diretor de Risco, Compliance e PLDFT	Comitê de Compliance
2020/2	08/10/2020	Diretor de Risco, Compliance e PLDFT	Comitê de Compliance
2021/3	29/10/2021	Diretor de Risco, Compliance e PLDFT	Comitê de Compliance
2022/4	15/02/2022	Diretor de Risco, Compliance e PLDFT	Comitê de Compliance
2023/5	30/03/2023	Diretor de Risco, Compliance e PLDFT	Comitê de Compliance
2024/6	19/04/2024	Diretor de Risco, Compliance e PLDFT	Comitê de Compliance

Sumário

1. INTRODUÇÃO

O Manual de *Compliance*, Regras, Procedimentos e Controles Internos visa estabelecer as orientações aptas a garantir, por intermédio dos Controles Internos adequados, o atendimento integral e ininterrupto às normas, políticas e regulamentações vigentes, mas não se limitando a isto. Visa, também, a transparência na condução dos negócios, a salvaguarda da confidencialidade das informações outorgadas pelos clientes, obliterar o conflito de agência entre os diversos atores da SIGA, evitar ganhos pessoais indevidos por meio da criação de condições artificiais de mercado ou da manipulação e uso de informação privilegiada, combater o ilícito da lavagem de dinheiro e, finalmente, disseminar na cultura organizacional, por meio de treinamento e educação, os valores do *Compliance*.

Este Manual, ademais, teve seu desenvolvimento voltado ao cumprimento das obrigações objetivadas por Instruções e Resoluções da Comissão de Valores Mobiliários, em especial as Resoluções CVM n. 19/2021, 21/2021, n. 35/2021, n. 50/2021, pela legislação aplicável e demais práticas nacionais e internacionais aplicadas à política de *Compliance*.

O presente instrumento tem como objetivo estabelecer os procedimentos adotados pela estrutura organizacional da SIGA. Conforme previsto no artigo 33 da Resolução CVM nº 21/2021, a estrutura da SIGA é composta por duas diretorias, capitaneadas por profissionais aptos e competentes, nomeados em ata de reunião de sócios.

Essas diretorias e seus respectivos colaboradores estão distribuídas da seguinte forma:

1. Diretoria de Gestão e Distribuição; e
2. Diretoria de Gestão de Risco, *Compliance* e Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo (PLDFT).

Para efeito de nomenclatura nos documentos da SIGA, o Diretor de Gestão e Distribuição, que responde pela área Comercial, também pode ser citado como Diretor de Gestão e/ou Diretor de Distribuição. Da mesma forma, quando mencionada a Diretoria de Gestão e Distribuição também pode ser citada como Diretoria de Gestão, e/ou Diretoria de Distribuição.

Ainda para efeito de nomenclatura dos documentos da SIGA, o Diretor de Risco, *Compliance* e PLDFT, que responde pelos Controles Internos, também pode ser citado como Diretor de Risco, Diretor de *Compliance* e/ou Diretor de PLDFT. Da mesma forma a

Diretoria de Risco, *Compliance* e PLDFT também pode ser citada ainda como Diretoria de Risco, Diretoria de *Compliance* e/ou Diretoria de PLDFT.

2. DEFINIÇÕES GERAIS

As definições aqui utilizadas condizem com as indicadas pela ANBIMA, quais sejam:

i. Aderentes: instituições que aderem ao Código de Certificação e se vinculam à Associação por meio contratual, ficando sujeitas às regras específicas deste Código;

ii. Administração de Recursos de Terceiros: atividades de Administração Fiduciária, Gestão de Recursos de Terceiros e Gestão de Patrimônio Financeiro, conforme definidas no Código;

iii. Administração Fiduciária: conjunto de serviços relacionados direta ou indiretamente ao funcionamento e à manutenção do Fundo, desempenhado por pessoa jurídica autorizada pela Comissão de Valores Mobiliários;

iv. Agente Autônomo de Investimento ou AAI: pessoa natural ou jurídica registrada na Comissão de Valores Mobiliários, conforme Regulação vigente;

v. ANBIMA ou Associação: Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais;

vi. Associada ou Filiada: instituições que se associam à ANBIMA e passam a ter vínculo associativo, ficando sujeitas a todas as regras de autorregulação da Associação;

vii. Atividades Elegíveis: atividades de Distribuição de Produtos de Investimento, Gestão de Recursos de Terceiros e Gestão de Patrimônio Financeiro;

viii. Ativos Financeiros: bens e direitos de qualquer natureza, valores mobiliários e ativos financeiros definidos pela Comissão de Valores Mobiliários e/ou pelo Banco Central do Brasil;

ix. Banco de Dados: conjunto de informações cadastrais enviadas para a ANBIMA pelas Instituições Participantes que são armazenadas de forma estruturada;

x. Canais Digitais: canais digitais ou eletrônicos utilizados na Distribuição de Produtos de Investimento que servem como instrumentos remotos, não

possuindo contato presencial entre a Instituição Participante e o investidor ou potencial investidor;

xi. Carta de Recomendação: documento expedido pela Supervisão de Mercados e aceito pela Instituição Participante que contém as medidas a serem adotadas a fim de sanar a(s) infração(ões) de pequeno potencial de dano e de fácil reparabilidade cometida(s) pelas Instituições Participantes, conforme previsto no Código dos Processos;

xii. Carteira Administrada: carteira administrada regulada pela Resolução CVM 21/21 de 25 de fevereiro de 2021, e suas alterações posteriores;

xiii. CEA: certificação ANBIMA para especialistas em investimentos;

xiv. CFA: certificação Chartered Financial Analyst, oferecida pelo CFA Institute USA;

xv. CFG: certificação ANBIMA de fundamentos em Gestão;

xvi. CFP®: Certified Financial Planner, oferecida pela Planejar;

xvii. CGA: certificação de Gestores ANBIMA;

xviii. CGE: certificação de Gestores ANBIMA para Fundos estruturados;

xix. Código de Distribuição: Código ANBIMA de Regulação e Melhores Práticas para Distribuição de Produtos de Investimento;

xx. Código de Recursos de Terceiros: Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros;

xxi. Código dos Processos: Código ANBIMA dos Processos de Regulação e Melhores Práticas;

xxii. Código: Código ANBIMA de Regulação e Melhores Práticas para o Programa de Certificação Continuada;

xxiii. Comissão de Acompanhamento: Organismo de Supervisão com competências definidas conforme disposto nesse Código;

xxiv. Conglomerado ou Grupo Econômico: conjunto de entidades controladoras diretas ou indiretas, controladas, coligadas ou submetidas a controle comum;

xxv. Conselho de Ética: conselho de ética da ANBIMA eleito nos termos do estatuto social disponível no site da Associação na internet;

xxvi. Conselho de Regulação e Melhores Práticas: Organismo de Supervisão com competências definidas conforme disposto no Código;

xxvii. CPA-10: certificação profissional ANBIMA série 10;

xxviii. CPA-20: certificação profissional ANBIMA série 20;

xxix. Diretoria: diretoria da ANBIMA eleita nos termos do estatuto social disponível no site da Associação na internet;

xxx. Distribuição de Produtos de Investimento: (i) oferta de Produtos de Investimento de forma individual ou coletiva, resultando ou não em aplicação de recursos, assim como a aceitação de pedido de aplicação por meio de agências bancárias, plataformas de atendimento, centrais de atendimento, canais digitais ou eletrônicos, ou qualquer outro canal estabelecido para esse fim; e (ii) atividades acessórias oferecidas aos investidores, tais como manutenção do portfólio de investimentos e fornecimento de informações periódicas acerca dos investimentos realizados;

xxxi. FII: Fundos de Investimento Imobiliários regulados pela Instrução CVM nº 472, de 31 de outubro de 2008, e suas alterações posteriores;

xxxii. Fundo 555: Fundo de Investimento regulado pela instrução CVM nº 555, de 17 de dezembro de 2014, e suas alterações posteriores;

xxxiii. Fundo de Índice: Fundos de Índice de Mercado regulados pela Instrução CVM nº 359, de 22 de janeiro de 2002, e suas alterações posteriores;

xxxiv. Fundo de Investimento ou Fundo: comunhão de recursos, constituído sob a forma de condomínio, destinada à aplicação em Ativos Financeiros e Ativos Imobiliários, caso aplicável;

xxxv. Gestão de Patrimônio Financeiro: gestão profissional dos Ativos Financeiros integrantes da carteira dos Veículos de Investimento, com foco individualizado nas necessidades financeiras do investidor e desempenhada por pessoa jurídica autorizada pela Comissão de Valores Mobiliários;

xxxvi. Gestão de Recursos de Terceiros ou Gestão: gestão profissional dos Ativos Financeiros e Imobiliários, caso aplicável, integrantes da carteira dos Veículos de Investimento, desempenhada por pessoa jurídica autorizada pela Comissão de Valores Mobiliários;

xxxvii. Instituições Participantes: instituições Associadas à ANBIMA ou as instituições Aderentes a este Código;

xxxviii. Lei 13.709: Lei nº 13.709, de 14 de agosto de 2018, Lei geral de proteção de dados;

xxxix. Organismos de Supervisão: em conjunto, Conselho de Regulação e Melhores Práticas, Comissão de Acompanhamento e Supervisão de Mercados;

xl. Plataformas de Atendimento: toda e qualquer forma de atendimento ao investidor pelas Instituições Participantes, inclusive por meio de canais digitais e telefônico, em que os profissionais desempenhem a Distribuição de Produtos de Investimento;

xli. Produtos de Investimento: valores mobiliários e Ativos Financeiros regulados pela Comissão de Valores Mobiliários e pelo Banco Central do Brasil;

xlii. Profissional Aprovado: profissional que atinge o índice mínimo estabelecido para aprovação no exame de certificação ou que tenha obtido dispensa de realização do exame CFG, CGA ou CGE, e que não esteja vinculado a nenhuma Instituição Participante;

xliii. Profissional Certificado: profissional que atinge o índice mínimo estabelecido para aprovação no exame de certificação ou que tenha obtido dispensa de realização do exame CFG, CGA ou CGE, e que, cumulativamente, esteja vinculado a uma Instituição Participante;

xliv. Programa Detalhado: documento disponível no site da ANBIMA na internet que reúne todos os assuntos que serão exigidos nos exames de certificação, assim como a proporção de cada um deles;

xlv. Regulação: normas legais e infralegais que abrangem as Atividades Elegíveis;

xlvi. Supervisão de Mercados: Organismo de Supervisão com competências definidas conforme disposto nesse Código;

xlvii. Termo de Compromisso: instrumento pelo qual a Instituição Participante compromete-se perante a ANBIMA a cessar e corrigir os atos que possam caracterizar indícios de irregularidades em face deste Código; e

xlviii. Veículos de investimento: Fundos e Carteiras Administradas constituídos localmente com o objetivo de investir recursos obtidos junto a um ou mais investidores.

3. ABRANGÊNCIA

Este Manual é aplicável aos administradores, colaboradores, estagiários, terceirizados e operadores envolvidos com negócios e atividades da SIGA, bem como aos sócios da gestora.

4. IMPLEMENTAÇÃO E REVISÃO

A implementação deste Manual se dará de forma imediata, após a aprovação da Diretoria e será revisado, no mínimo, anualmente, ou em qualquer tempo que lhe possa agregar valor, de acordo com a relevância, para que seja garantida a sua adequação.

O planejamento de *Compliance* e Controles Internos é efetuado anualmente, com o objetivo de revisar e atualizar todos os procedimentos, códigos, manuais e políticas da SIGA. Essa atividade coincidirá com a entrega do Relatório Anual de Controles Internos e Cumprimento da Resolução CVM nº 21/2021, no prazo legal.

Em caso de mudanças significativas nos negócios ou na regulação, planos devem ser alterados. Deficiências de controles internos detectadas devem ser relatadas para as áreas responsáveis por tais controles e reportadas ao Comitê de *Compliance*.

Revisões extraordinárias destes procedimentos, códigos, manuais e políticas poderão ocorrer em caso de situações imprevistas e/ou mudanças significativas e repentinas, também com vistas a apurar a permanência da conformidade.

5. RESPONSABILIDADE

Compete ao Diretor de Risco, *Compliance* e PLDFT a gestão e a aplicação deste Manual e das Políticas aqui constantes.

Esta Diretoria é responsável, ainda, por adotar os procedimentos formais de controle verificáveis, que se relacionam à obtenção e manutenção ou dispensa e isenções pertinentes aos profissionais da SIGA, conforme determinação da ANBIMA.

O Controle exercido pela Diretoria de Risco, *Compliance* e PLDFT, ainda, inclui a verificação de funcionamento adequado da admissão e desligamento de colaboradores, bem como a sua atualização junto ao sistema da Anbima.

Existe, ainda, a responsabilidade de monitorar o prazo de vencimento da certificação dos Colaboradores elegíveis.

Ressalta-se, ainda, que este documento não detalha, necessariamente, todas as situações passíveis de ocorrência no dia a dia dos negócios. Quaisquer dúvidas deverão ser remetidas ao Diretor de Risco, *Compliance* e PLDFT.

6. ENDEREÇO ELETRÔNICO

Em respeito ao artigo 14 da Resolução CVM nº 21/2021, este documento estará disponível no site da SIGA (www.sigafinance.com.br).

7. RISCOS DE *COMPLIANCE*

O Risco de *Compliance* deriva de falhas no cumprimento de leis, normas, regulação e boas práticas de mercado, que governam a conduta de um negócio específico. Sua inobservância pode ocasionar multas, advertências, suspensão e até inabilitação para o exercício da atividade, dependendo da gravidade da infração.

A Diretoria de Risco, *Compliance* e PLDFT tem a função de identificar, regulamentar e combater as práticas que possam apresentar riscos legais, de *compliance* ou de imagem à SIGA. Assistirá, ainda, a essa Diretoria, a tomar decisões e aconselhar sobre a execução de tarefas.

Cabe ressaltar que esta identificação e avaliação de riscos é um componente importante na função da Diretoria de Risco, *Compliance* e PLDFT, mas não tem caráter deontológico. O papel mais importante da área é o assessoramento e aconselhamento do setor negocial, com o escopo de auxiliar no desenvolvimento de procedimentos, controles e monitoramentos.

Os riscos específicos serão analisados pela Diretoria de Risco, *Compliance* e PLDFT, tendo como base a seguinte matriz 5x5:

Probabilidade/Impacto	Zero	Leve	Médio	Grave	Gravíssimo
Quase Certa	Risco Moderado	Risco Elevado	Risco Extremo	Risco Extremo	Risco Extremo
Alta	Risco Moderado	Risco Elevado	Risco Elevado	Risco Extremo	Risco Extremo
Média	Risco Baixo	Risco Moderado	Risco Elevado	Risco Extremo	Risco Extremo
Baixa	Risco Baixo	Risco Moderado	Risco Moderado	Risco Elevado	Risco Extremo
Rara	Risco Baixo	Risco Baixo	Risco Moderado	Risco Elevado	Risco Elevado

No mínimo anualmente a avaliação de riscos e atualizações serão submetidas à aprovação do Comitê de *Compliance*, que deliberará pela sua aprovação ou necessidade de reformulação.

8. ESTRUTURA DE CONTROLES INTERNOS E TRATAMENTO DE RISCOS

A estrutura adotada deve garantir a efetividade dos Controles Internos nas atividades desenvolvidas, em seus sistemas de informações financeiras, operacionais e gerenciais e no cumprimento das normas regulamentares, internas e legais.

Os Controles Internos devem ser um processo integrado, efetuado pela Diretoria e colaboradores, estruturado para enfrentar os riscos apresentados e fornecer a segurança necessária para subsidiar a missão da SIGA.

Esse processo visa alcançar os seguintes objetivos:

i. Execução ordenada, ética, econômica, eficiente e eficaz das operações;
ii. Cumprimento das leis e regulamentos aplicáveis;
iii. Cumprimento das responsabilidades de prestação de contas; e
iv. Garantia de uso correto dos recursos para evitar perdas e danos.

Para tanto, a SIGA se utiliza do modelo das Três Linhas de Defesa. Neste interim, a estrutura de Controles Internos será dividida da seguinte forma:

a. Primeira Linha: Área de Negócios. Gerencia e detém propriedade sobre os riscos.
b. Segunda Linha: Controles Internos. Supervisão dos riscos, definição da estratégia e estrutura de gerenciamento de riscos. Coordenação dos limites operacionais, monitoramento das funções da primeira linha.
c. Terceira Linha: Funções que fornecem avaliações independentes da estrutura de gerenciamento de riscos.

Pode-se exemplificar o modelo das linhas de defesa adotado pela SIGA com base no seguinte organograma[1]:

No exercício da função de controle, a existência de erros e riscos potenciais devem ser devidamente identificados, reportados, controlados e monitorados, de forma preventiva ou corretiva, além de serem utilizados como instrumentos na gestão de risco.

8.1. Identificação, Classificação e Tratamento de Riscos

[1] Organograma disponível no manual: Declaração de Posicionamento do IIA: As Três Linhas de Defesa no Gerenciamento Eficaz de Riscos e Controles. São Paulo: IIA, 2013. Disponível em: < http://www.planejamento.gov.br/assuntos/empresas-estatais/palestras-e-apresentacoes/2-complemento-papeis-das-areas-de-gestao-de-riscos-controles-internos-e-auditoria-interna.pdf>. Acesso em 28 fev. 2020.

A Diretoria de Risco, *Compliance* e PLDFT é responsável pelo mapeamento de processos, identificação de riscos intrínsecos ou marginais, classificação e monitoramento, sempre visando o controle e a mitigação destes.

Ademais, todos os colaboradores deverão passar, periodicamente, por treinamentos condizentes com o tema, quais seja, Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo (PLDFT), *Compliance*, Código de Ética e Conduta, Segurança de Dados, entre outros assuntos que a SIGA julgar importantes.

8.2. Canais de Comunicação

A SIGA proporciona, nos moldes exigidos pela Resolução nº 3.056/2002 do Conselho Monetário Nacional (CNM), que modificou o artigo 2º da Resolução nº 2.554/1998 do mesmo órgão, canais de comunicação que assegurem aos colaboradores, segundo o correspondente nível de atuação, o acesso a confiáveis, tempestivas e compreensíveis informações consideradas relevantes para suas tarefas e responsabilidades.

Além disso, realiza testes periódicos de segurança para os sistemas de informações, em especial para os mantidos em meio eletrônico.

9. CONTROLES INTERNOS, *COMPLIANCE*, CONDUTA E ÉTICA

A Diretoria de Risco, *Compliance* e PLDFT (2ª Linha de Defesa) possui atribuições relacionadas à linha de defesa da SIGA e tem como responsabilidade apoiar a entidade na condução de um programa de *Compliance*, que consiste na avaliação da conformidade com as leis, regulamentações, procedimentos, códigos, manuais e políticas da SIGA, observando os altos padrões de integridade, de conduta e de ética.

Esta divisão em Três Linhas de Defesa tem como objetivo o amparo à entidade no cumprimento dos temas relacionados à conduta, à integridade, Leis, Regulamentos, Conflitos de Agência, Ética, Conduta Concorrencial e Anticorrupção.

Para os temas de prevenção à lavagem de dinheiro e ao financiamento do terrorismo, a Diretoria tem a responsabilidade de avaliação da conformidade com as Leis e Regulações, ou seja, avaliar a aderência e efetividade dos procedimentos adotados pela SIGA.

9.1. Funções, Responsabilidades e Atribuições da Diretoria de Risco, *Compliance* e PLDFT

Dentre outras, as responsabilidades e atribuições da Diretoria de Risco, *Compliance* e PLDFT da SIGA podem ser exemplificadas pelo seguinte rol não taxativo:

i. Formular regulamentos e normas internas.
ii. Monitorar e implementar mecanismos de controles internos.
iii. Realizar testes de conformidade em transações, procedimentos e informações de registro.
iv. Criar plano de continuidade dos negócios.
v. Proceder pesquisas diárias de leis e regras aplicáveis às atividades da SIGA relacionadas à *Compliance* e controles internos.
vi. Analisar os controles descritos nos demais documentos internos, propor a criação de novos controles, aprimorar aqueles considerados ineficientes e monitorar a correção de quaisquer deficiências.
vii. Subsidiar as áreas no cumprimento dos temas relacionados à conduta/integridade, controles regulatórios, gestão, conflito de interesses, ética, conduta corporativa e concorrencial.
viii. Mapear as atividades das dependências, áreas, produtos e serviços relacionados às Leis, Regulamentos e demais obrigações de *Compliance*.
ix. Assegurar que todos os *stakeholders* estejam agindo em conformidade com o Manual de *Compliance*, Regras, Procedimentos e Controles Internos e com o Código de Ética e Conduta firmados pela entidade.
x. Desenvolver, em conjunto com as demais áreas da SIGA, meios para garantir o acesso a informações confiáveis, oportunas, compreensíveis e relevantes pelos colaboradores, de acordo com os respectivos níveis de atividade.
xi. Determinar a segregação apropriada de tarefas e a separação de responsabilidades, orientando o controle das atividades, a fim de se evitar conflitos de interesse.

A principal função da Diretoria de Risco, *Compliance* e PLDFT é apoiar as áreas da SIGA quanto ao esclarecimento de todos os controles e regulamentos internos, bem como monitorar a conformidade das transações e atividades da entidade, de acordo com as normas regulatórias (internas e externas) em vigor.

A Diretoria de Risco, *Compliance* e PLDFT será responsável, também, pelas seguintes funções:

i. Esclarecer quaisquer dúvidas sobre as regras e termos deste e de quaisquer outros procedimentos, códigos, manuais e políticas da SIGA, sempre que solicitado por algum colaborador.

ii. Autorizar, ou não, investimentos pessoais de colaboradores da SIGA e de seus familiares.

iii. Atualizar o presente documento, no mínimo, anualmente e/ou na superveniência de norma ou lei nova que interfira nas disposições aqui expostas. Assim como, quando o Diretor de Risco, *Compliance* e PLDFT entender conveniente.

iv. Zelar para que os colaboradores da SIGA pautem suas condutas pelo cumprimento integral das regras e a estrita observância dos termos do presente documento, bem como dos demais procedimentos, códigos, manuais e políticas da SIGA.

v. Investigar e analisar situações de descumprimento ao presente documento e definir as ações e sanções que deverão ser tomadas e aplicadas.

vi. Investigar e analisar os casos não previstos no presente documento e definir as ações que deverão ser tomadas.

vii. Promover treinamentos relacionados à prevenção e combate à lavagem de dinheiro.

viii. Autorizar a divulgação de material publicitário e a comunicação de colaboradores com a imprensa, nos termos deste documento.

ix. Arquivar e verificar os relatórios de investigação e os pareceres sobre os clientes, com relação à Política de *Know Your Customer* (KYC).

x. Aplicar as medidas disciplinares cabíveis.

xi. Acompanhar o cumprimento das diretrizes estabelecidas nos procedimentos, códigos, manuais e políticas internas da SIGA.

xii. Avaliar os riscos associados às atividades realizadas pelos diretores e demais colaboradores.

xiii. Prestar suporte a todos os colaboradores em relação ao conteúdo dos procedimentos, códigos, manuais e políticas internas da SIGA.

xiv. Aprimorar os mecanismos de controle interno, objetivando a minimização de potenciais riscos.

xv. Verificar e analisar quaisquer situações que possam resultar em conflitos de interesse e/ou descumprimento de qualquer das normas dispostas nos procedimentos, códigos, manuais e políticas internas da entidade.

As funções do Diretor de Risco, *Compliance* e PLDFT, responsável por liderar e supervisionar esta Diretoria da entidade, serão executadas por Diretor apto e competente, nomeado em Ata de Reunião de Sócios.

9.2. Funções do Diretor de Risco, *Compliance* e PLDFT

O Diretor de Risco, *Compliance* e PLDFT deverá prestar suporte a todas as áreas da SIGA, tanto no que diz respeito aos esclarecimentos de todos os controles e regulamentos internos, bem como ao acompanhamento de conformidade das operações e atividades às normas regulamentadoras. Deverá definir planos de ação, monitorar o cumprimento de prazos e o nível de excelência dos serviços efetuados e assegurar a pronta correção de quaisquer desvios identificados.

O Diretor de Risco, *Compliance* e PLDFT não atua e é impedido de atuar em quaisquer outras áreas comerciais da SIGA, de modo que as suas atribuições não sofram qualquer tipo de conflito de interesses.

Ainda, são atribuições, conjunta ou separadamente, do Diretor de Risco, *Compliance* e PLDFT e do *BackOffice*, sem prejuízo de outras, as seguintes tarefas:

i. Propiciar o amplo conhecimento e execução dos valores éticos nas ações de todos os colaboradores.

ii. Analisar todas as situações acerca do não cumprimento dos procedimentos e valores éticos estabelecidos nos documentos da SIGA, assim como avaliar as demais situações que não foram previstas nas políticas internas da entidade.

iii. Assegurar o sigilo de identidade de possíveis delatores de crimes ou infrações, mesmo sem solicitação expressa, salvo nas situações de testemunho judicial.

iv. Solicitar a tomada das devidas providências nos casos de caracterização de conflitos de interesse.

v. Propor estudos para eventuais mudanças estruturais que permitam a implementação ou garantia de cumprimento do conceito de segregação das atividades.

vi. Diligenciar, no mínimo anualmente, se os colaboradores-chave, em especial os sócios controladores e os diretores estão envolvidos em processos administrativos de órgãos reguladores, criminais, de qualquer natureza, ou ainda outros processos que possam trazer contingências para a SIGA e que, portanto, tornem sua divulgação pública necessária, nos termos da Resolução CVM 21/21 de 25 de fevereiro de 2021.

vii. Confirmar, por meio do CVMWEB, entre os dias 1º e 31 de março de cada ano, que as informações contidas no formulário cadastral da SIGA, conforme previsto na Resolução CVM nº 51/2021 continuam válidas, bem como atualizar o cadastro em caso de alteração de quaisquer dados.

viii. Para cumprimento da Resolução CVM nº 21/2021, as Diretorias deverão, em conjunto, enviar Formulário de Referência, por meio de sistema eletrônico da CVM, até o dia 31 de março de cada ano.

Na execução das atividades sob sua responsabilidade, poderá se utilizar de sistemas eletrônicos e/ou serviços de advogados ou firmas de consultoria de *Compliance* para suporte e auxílio em suas funções.

9.3. Funções, Responsabilidades e Atribuições da Diretoria de Gestão e Distribuição

A principal função da Diretoria de Gestão e Distribuição é comandar as áreas comerciais da SIGA quanto à gestão dos Fundos geridos pela entidade e a distribuição destes produtos.

Dentre outras, as responsabilidades e atribuições da Diretoria de Gestão e Distribuição da SIGA podem ser exemplificadas pelo seguinte rol não taxativo:

i. Implementar e manter política escrita de gestão de riscos que permita o monitoramento, a mensuração e o ajuste permanentes dos riscos inerentes a cada uma das carteiras de valores mobiliários.
ii. Executar os procedimentos necessários à identificação e ao acompanhamento da exposição aos riscos de crédito, de mercado, de liquidez, de concentração, de contraparte, de operacionais e de desenquadramento, entre outros que sejam relevantes para as carteiras de valores mobiliários.
iii. Revisar, constantemente se as técnicas, os instrumentos e a estrutura utilizados para a implementação dos procedimentos citados no item ii estão adequados.
iv. Criar plano de monitoramento dos limites de exposição a riscos das carteiras administradas e dos Fundos de Investimentos que não tenham, respectivamente, no contrato e nos documentos do Fundo, limites expressos.
v. Manter organograma dos cargos das pessoas envolvidas na gestão de riscos e respectivas atribuições e prerrogativas e, se for o caso, o nome do terceiro contratado para monitorar e mensurar os riscos inerentes a cada uma das carteiras de valores mobiliários.
vi. Definir com que frequência e quais pessoas devem receber relatório da exposição ao risco de cada carteira de valores mobiliários sob gestão.
vii. Estabelecer a frequência com que a política deve ser revista e avaliada, devendo ser, no mínimo, suficiente para atender aos objetivos.
viii. Coordenar a distribuição dos Fundos geridos pela entidade.

A Diretoria de Gestão e Distribuição será responsável, também, pelas seguintes funções:

i. Originar os produtos que a entidade irá gerir e ofertar aos seus investidores;
ii. Relacionamento com investidores;
iii. Cumprir a Política de *Suitabibility*;
iv. Estabelecer e implementar as políticas comerciais da entidade; e
v. Representar a entidade perante o mercado, órgãos públicos, reguladores e a mídia.

9.4. Funções do Diretor de Gestão e Distribuição

Cabe ao Diretor de Gestão e Distribuição, a gestão de uma carteira de valores mobiliários, incluindo a aplicação de recursos financeiros no mercado de valores mobiliários por conta do investidor.

Deve adotar política de gerenciamento de riscos consistente e passível de verificação, que é efetivamente levada em conta no processo de tomada de decisões de investimento.

Além disso, deve respeitar política de gerenciamento de riscos compatível com a política de investimentos que pretende perseguir.

O administrador de carteiras de valores mobiliários, pessoa jurídica, pode atuar na distribuição de cotas de Fundos de Investimentos de que seja administrador ou gestor, desde que observe as seguintes normas específicas da CVM:

i. Normas de cadastro de clientes, de conduta e de pagamento e recebimento de valores aplicáveis à intermediação de operações realizadas com valores mobiliários em mercados regulamentados de valores mobiliários.
ii. Normas que dispõem sobre o dever de verificação da adequação dos produtos, serviços e operações ao perfil do cliente.
iii. Normas que dispõem sobre a identificação, o cadastro, o registro, as operações, a comunicação, os limites e a responsabilidade administrativa referentes aos crimes de lavagem ou ocultação de bens, direitos e valores.
iv. Normas que dispõem sobre a troca de informações entre distribuidor e administrador de Fundos de Investimentos.

10. SEGREGAÇÃO ESTRUTURAL, FÍSICA E DE FUNÇÕES

O Diretor de Risco, *Compliance* e PLDFT atua em funções de supervisão, controle e jurídico, em área segregada daquelas utilizadas para a operacionalização dos negócios da SIGA. É considerado profissional *behind all barriers*, na forma das melhores práticas vigentes, sob quem recai o dever legal de zelar pela perfeita segregação de atividades da entidade.

A SIGA atua com a premissa de que a Diretoria de Risco, *Compliance* e PLDFT deve ser completamente independente, de modo que não haja interferência no trabalho por esta desenvolvido.

A segregação funcional da Diretoria de Risco, *Compliance* e PLDFT e demais órgãos da entidade é garantida pela SIGA, de forma a fornecer ao Diretor de Risco, *Compliance* e PLDFT meios para que possa agir de modo independente, fiscalizar qualquer tipo de conduta imprópria e com poderes para vedar a realização de determinados negócios.

10.1. Comitê de *Compliance*

O Comitê de *Compliance* será formado por três membros, tendo como presidente, obrigatoriamente, o Diretor de Risco, *Compliance* e PLDFT. No caso de impedimento deste, o Comitê especialmente instituído será presidido pelo Diretor de Gestão e Distribuição ou outra pessoa a ser designada em assembleia de sócios devidamente convocada. Os demais membros serão escolhidos em conjunto pelos demais diretores e/ou administradores da entidade.

Competirá ao Comitê de *Compliance,* sempre que instado, ou em suas reuniões semestrais:

i. Aprovar a política de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo (PLDFT).
ii. Aprovar início de relacionamento e manutenção de relacionamento com Pessoas Politicamente Expostas (PPE).
iii. Analisar os relatórios de *Compliance* e decidir pela comunicação aos órgãos competentes sobre os clientes enquadrados como Sensíveis.
iv. Analisar as demandas levadas para deliberação nas reuniões do Comitê de *Compliance*, emitindo pareceres e decisões de acordo com os procedimentos, códigos, manuais e políticas da SIGA e com a legislação aplicável.
v. Zelar pela política de prevenção aos crimes de lavagem de dinheiro e ao financiamento do terrorismo, descrita neste documento.
vi. Demais atribuições previstas pelos procedimentos, manuais, códigos e políticas da SIGA.

Todas as deliberações serão registradas em ata, que poderão ser redigidas em formato de sumário, e que deverão ser assinadas por todos os presentes.

11. GOVERNANÇA

A SIGA preza pela prevenção e remediação de qualquer caso de conflito de interesses. Desta forma, os órgãos da entidade são independentes entre si, de modo que previna o conflito de agência. Para tanto, conta com diversas políticas neste sentido.

11.1. *Chinese Wall*

A Resolução CVM nº 21/2021 impõe a segregação da atividade de administração de carteiras de valores mobiliários das demais atividades exercidas pela pessoa jurídica.

Entende-se tal segregação pelo conjunto de procedimentos internos adotados com o objetivo de impedir o acesso e o fluxo de informações confidenciais, sigilosas e privilegiadas entre setores alheios à atividade de administração de carteiras de valores mobiliários, de forma a evitar vazamento de informações, conflito de interesses ou quaisquer das práticas vedadas pela Resolução CVM nº 62/2022 ou pela Lei nº 6.385/1976.

Para tanto, a área de administração de carteiras de valores mobiliários da SIGA deverá estar em um ambiente físico isolado, com acesso exclusivo para os colaboradores que a integram, respeitando todos os níveis de segregação a seguir:

a. Segregação de Atividades e Funções: O primeiro nível de segregação refere-se às diferenças funcionais de atuação e autoridades definidas para cada um dos colaboradores.
b. Segregação Física: A área de c*ompliance* é segregada das áreas de análise e gestão. Além disso, a área financeira, administrativa e pagamentos é separada das áreas de *compliance* e análise.
c. Segregação de Acessos a Documentos: Controle de acessos a documentos e segregação física com acesso restrito aos documentos de cadastro de clientes e de colaboradores, prevenção de informações confidenciais por todos os colaboradores.

Na sede da SIGA, além dos espaços destinados a Recepção, Copa, Banheiros, Sala de Reuniões, existem salas segregadas para as áreas de Gestão e Distribuição e para a área de Risco, *Compliance* e PLDFT.

11.2. Conflitos de Interesses

Extensivamente às regras de segregação, tendo em vista a grande preocupação da entidade em adotar a mais rígida política de identificação, eliminação e mitigação de quaisquer conflitos de agência, inclusive no que se refere a partes relacionadas. Para tanto, a SIGA conta com as seguintes obrigatoriedades.

11.2.1 Atividades de Colaboradores Alheias à SIGA

Todos os colaboradores com participações em outras entidades, que deterem mais de 10%, direta ou indiretamente, de participação, bem como se ocuparem cargos de diretoria ou conselhos, tendo influência significativa na tomada de decisões, deverão declarar à SIGA tais fatos.

São consideradas transações com partes relacionadas a transferência de recursos, bens, serviços ou obrigações entre pessoas físicas ou jurídicas definidas no parágrafo acima, independentemente de haver ou não um valor pecuniário atribuído à transação.

O conflito de interesses, neste caso, irrompe quando uma parte relacionada se encontra envolvida em processo decisório, ou de assessoramento, que tenha o condão de resultar em um ganho para si, para algum familiar, ou para terceiro com o qual esteja envolvido, ou ainda que possa interferir na sua capacidade de julgamento isento, em qualquer caso, desde que em detrimento dos interesses da SIGA e dos clientes.

Os colaboradores da SIGA, em regra, não poderão ter atuação funcional relevante em outras atividades, exceto como conselheiros em entidade cujos objetivos sociais não sejam conflitantes com a entidade. Ademais, estas atividades somente poderão ser realizadas se aprovadas, por ata, pelo Comitê de *Compliance*, desde que não conflitem de nenhuma maneira com a SIGA.

Estes colaboradores, ainda, deverão assinar um termo de responsabilidade, assumindo o dever de observação das regras de conflitos de interesses, informações confidenciais e

privilegiadas, e todas as demais regras dispostas nos manuais da SIGA, sob pena de desligamento e multas relevantes, sem prejuízo de indenização por perdas e danos e processos judiciais criminais e administrativos.

Estas atividades restritas não poderão ser exercidas dentro do estabelecimento da SIGA e nem com os equipamentos (notebooks) de propriedade da entidade. É vedado o salvamento de quaisquer arquivos estranhos à SIGA nas pastas físicas e virtuais do servidor da entidade.

Neste sentido, a SIGA demonstrará publicamente, na forma da regulamentação aplicável, qualquer tipo de conflito, potencial ou material, que seja decorrente desta situação, da seguinte maneira:

a. Regulamento ou documentação acessória do veículo de investimento.
b. Questionários de *due diligence* de prestadores de serviços.
c. Formulário de referência.

11.2.2. Identificação de Conflito de Interesses

No caso da SIGA, também podem ser consideradas como situações envolvendo conflitos de interesses aquelas nas quais os objetivos pessoais dos tomadores de decisão, por qualquer razão, não estejam alinhados aos objetivos da entidade e de seus clientes.

Na hipótese de mera suspeita de conflitos de interesses nas atividades extra laborais dos colaboradores, inclusive sócios, diretores e administradores, os envolvidos serão chamados a comparecer em reunião extraordinária do comitê de *Compliance*, que ouvirá este sujeito e deliberará se:

(i) Não há conflito de interesses;
(ii) Há conflito de interesses e, portanto, deverá deixar de praticar determinada atividade;
(iii) Há conflito de interesses e será desligado da SIGA;
(iv) Sem prejuízo, o colaborador poderá ser afastado das operações em andamento, ou do próprio trabalho, por prazo definido pelo comitê.

Qualquer suspeita deverá ser objeto de denúncia à diretoria de compliance ou ao administrador da entidade, quando aquele for impedido para deliberar.

O Diretor de Risco, *Compliance* e PLDFT é o responsável por identificar qualquer outra situação que possa gerar conflito de interesses. Nesta hipótese, a depender do tipo, risco e materialidade do conflito, o Diretor de Risco, *Compliance* e PLDFT deverá proceder à instauração de alguma(s) das seguintes medidas:

i. Vedar a operação.
ii. Estabelecer barreiras de informação, com o objetivo de isolamento da circulação de dados.
iii. Retirar da operação e afastar o(s) colaborador(es) que tenha(m) relação com o conflito.
iv. Informar a investidores e ao mercado.
v. Aprovar previamente a deliberação em assembleias dos demais titulares de ativos investidos.

Caso qualquer colaborador note que pode haver ou suspeite haver potenciais conflitos de interesses, deverá comunicar o fato imediatamente ao Diretor de *Compliance*, seu superior ou ao administrador.

Na hipótese descrita acima, adicionalmente, o colaborador deverá:

(i) Interromper qualquer ação sob sua responsabilidade que possa resultar ou agravar eventual Conflito de Interesses, seja ele aparente ou concreto; e

(ii) Não utilizar sua influência pessoal para incentivar a Companhia a dar andamento em processos internos que possam estar influenciados por Conflito de Interesses, seja ele aparente ou concreto.

11.2.3. Declaração de Conflito de Interesses

A SIGA reconhece que se encontra em situação de potencial conflito de interesse ao atuar junto a player ou grupo econômico, que mesmo não sendo parte relacionada, em que seus colaboradores tenham, de alguma forma, atuado nos últimos 5 (cinco) anos.

Qualquer colaborador ou prestador de serviços deverá declarar, por escrito, eventuais situações passíveis de gerar conflito de interesses.

A declaração será devida, cumulativamente:

i. Na data da admissão;
ii. Na ocorrência de fato superveniente que altere o anteriormente declarado;
iii. A cada período de 12 meses.

Eventualmente, se uma transação onde exista conflito de interesse ou potencial para conflito de interesse for autorizada pelo Comitê de *Compliance*, a SIGA deverá divulgá-la como informação relevante nos documentos aplicáveis e em seu website, detalhando o tipo de relação e de transação realizada, fornecendo detalhes suficientes para identificação das Partes Relacionadas e de quaisquer condições essenciais, ou não estritamente comutativas, inerentes às transações em questão.

12. POLÍTICA DE CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO

12.1. Objetivo e a Quem se Aplica

A Política de Confidencialidade e Segurança da Informação objetiva concretizar princípios e diretrizes de proteção das informações.

Aplica-se a todos os colaboradores, prestadores de serviços, à Diretoria e sócios.

12.2. Definições

A SIGA segrega e classifica as informações, tratadas, armazenadas ou transferidas, de acordo com sua natureza. Elas podem ser:

(a) Públicas: Informação de acesso livre, disponibilizada em sites ou meios de comunicação.
(b) Internas: À Procedimentos operacionais, que podem ser acessados de forma irrestrita pelos colaboradores. Quaisquer solicitações de transmissão destas

informações a terceiros dependerão de anuência prévia do titular e de aval fundamentado da Diretoria de Risco, *Compliance* e PLDFT.

(c) Confidenciais: São todas aquelas informações sobre clientes, ativos, composição de carteira, estudos e análises, aquelas que identifiquem dados pessoais ou patrimoniais de clientes, sejam objetos de acordo de confidencialidade celebrado com terceiros, identifiquem ações estratégicas cuja divulgação possa prejudicar a gestão dos negócios ou reduzir sua vantagem competitiva. Estes dados somente serão compartilhados com os colaboradores que necessitem, de maneira irremediável, das informações para exercerem as suas funções (princípio do *need to know*). Quaisquer solicitações de transmissão destas informações a terceiros dependerão de anuência prévia do titular e de aval fundamentado da Diretoria de Risco, *Compliance* e PLDFT.

(d) Sigilosas: Informações de conhecimento único da Diretoria, relativas a, geralmente, planos de negócio ou posicionamento.

Todos os tratamentos, armazenamentos ou transferência de dados irão obedecer estritamente às determinações da Lei nº 13.709/2018, Lei Geral da Proteção de Dados (LGPD). Além disso, cada classificação de informações terá diretórios segregados, cujo acesso será concedido apenas a profissionais autorizados, por escrito, além de toda uma estrutura cibernética de proteção de dados, inclusive em respeito à LGPD.

Serão oferecidos, periodicamente, treinamentos e cursos aos colaboradores sobre as questões de proteção de dados, conforme descrito capítulo 14 deste manual.

12.3. Diretrizes

As diretrizes a seguir dispostas são vinculantes e obrigatórias a todos os colaboradores:

(i) 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.

(ii) A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada.

(iii) 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.

(iv) A identificação de qualquer colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas.

(v) Segregação de instalações, equipamentos e informações comuns, quando aplicável.

(vi) A senha é utilizada como assinatura eletrônica e deve ser mantida secreta, sendo proibido seu compartilhamento.

(vii) Qualquer risco ou ocorrência de falha na confidencialidade e na segurança da informação devem ser reportados ao Diretor de Risco, *Compliance* e PLDFT. No caso de impedimento deste, deverá ser reportada ao Diretor de Gestão e Distribuição ou outra pessoa a ser designada em assembleia de sócios devidamente convocada.

12.4. Controles e Barreiras

Com o objetivo de se assegurar o cumprimento das políticas de confidencialidade e segurança da informação, serão adotados, entre outros, os seguintes pontos preventivos:

(i) Identificação e Classificação da Informação: O colaborador que receber ou tratar uma informação deverá classificá-la em uma dentre as quatro definições expostas neste documento, de acordo com as necessidades dos negócios e os possíveis impactos no caso de utilização indevida.

(ii) Gestão de Informações Confidenciais: As informações confidenciais deverão ser identificadas desta maneira em qualquer meio de comunicação (e-mails, memorandos, documentos, arquivos físicos ou eletrônicos). As informações confidenciais serão salvas em HD externo segregado ou dispositivo de armazenamento em nuvem, com limitação e senhas de acesso. Os e-mails serão protegidos. Eventual documento disponibilizado a terceiros deve indicar a sua qualificação e editada com marca d´água ou carimbo especial.

(iii) Salvaguarda da Informação: Toda informação terá o ciclo de vida definido pelas seguintes etapas: geração, manuseio, armazenamento e descarte. O tempo de cada uma das etapas deverá ser de conhecimento do colaborador, que terá a liberdade de

consultar a Diretoria de Risco, C*ompliance* e PLDFT em caso de eventuais dúvidas. Por fim, o descarte deverá ser feito por técnico de Tecnologia da Informação (TI), que não poderá ter acesso às informações e, portanto, será acompanhado durante o processo. Em caso de documentos em papel, estes deverão ser incinerados ou fragmentados.

(iv) Controle de Acessos: Os acessos físicos e digitais dos documentos serão rastreados, a fim de garantir a possibilidade de auditoria, que poderá identificar individualmente cada colaborador que acessou as informações.

(v) Quaisquer riscos e incidentes deverão ser, imediatamente, reportados ao Diretor de Risco, *Compliance* e PLDFT. O plano de contingência e de continuidade dos sistemas e serviços implantados deverá ser testado semestralmente, com o objetivo de se minorar quaisquer riscos de perda de informações, confidencialidade, integridade e disponibilidade da documentação, assim como o *backup*.

(vi) Teste de Controle: O responsável pela TI deverá, periodicamente, efetuar testes que assegurarão que os recursos estarão: a.) adequados ao porte e às áreas de atuação; b.) adequados ao nível de confidencialidade; c.) segregados físicos e logicamente; d.) os recursos computacionais estarão protegidos e assegurados de que a sua manutenção permita a realização de auditorias e inspeções.

Todos os quais estas normas são aplicáveis, deverão assinar formalmente, termo obrigando-se a atuar de acordo com estas políticas, sob pena de sanções.

A SIGA, ainda, disponibilizará treinamentos obrigatórios a todos que participem ou tenham acesso às informações confidenciais.

Por fim, em respeito aos artigos 22 e 23 da Resolução CVM nº 19/2021, os documentos e informações exigidos pela CVM serão mantidos pelo prazo mínimo de cinco anos, salvo por determinação expressa em sentido contrário pelo órgão, bem como toda a correspondência, interna e externa, todos os papéis de trabalho, cálculos que fundamentaram a cobrança de taxa de performance de seus clientes classificados como investidores profissionais, quando for o caso, relatórios e pareceres relacionados com o exercício de suas atividades e os estudos e análises que fundamentaram as orientações, recomendações ou aconselhamentos.

Todos os e-mails e arquivos serão armazenados em um *file server* com altos padrões de segurança e ética, possibilitando controle de acesso e rastreamento de uso dos arquivos por usuário, o que garante a preservação de informações confidenciais e a restrição de acesso aos arquivos sensíveis.

O *file server*, que fica hospedado internamente, também possui, como medida de segurança adicional, um sistema de cópia incremental para um repositório na nuvem com periodicidade semanal.

Toda a base de dados conta com a realização de *backups* simultâneos que ficam armazenados na nuvem e que permitem, em caso de falhas operacionais, recuperação de dados e arquivos.

O *file server* é acessado, pelos colaboradores, mediante *login* com usuário e senha próprios, tendo os usuários permissões diferenciadas de acordo com as funções e atividades desempenhadas por cada profissional.

Os diferentes níveis de permissão viabilizam melhor controle de acesso e de reprodução dos dados e arquivos pelos profissionais. De forma não taxativa, as seguintes condutas devem ser observadas:

(i) Os colaboradores devem evitar circular em ambientes externos à SIGA com cópias (físicas ou digitais) de arquivos contendo informações confidenciais, devendo essas cópias ser mantidas com senha de acesso.

(ii) O descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação, sempre com a orientação do superior hierárquico.

(iii) As informações que possibilitem a identificação de um cliente da SIGA devem se limitar a arquivos de acesso restrito e apenas poderão ser copiadas ou impressas se forem para o atendimento dos interesses da entidade ou do próprio cliente.

(iv) Os colaboradores devem estar atentos a eventos externos que possam comprometer o sigilo das informações da SIGA, como, por exemplo, vírus de computador, fraudes, entre outros.

(v) Assuntos confidenciais não devem ser discutidos em ambientes públicos ou locais considerados expostos.

12.5. Segurança Cibernética

A SIGA identificará e avaliará os principais riscos cibernéticos aos quais está exposta. Levará, como parâmetro inicial, como ataques mais prováveis:

(i) *Malware* (vírus, cavalo de Troia, *spyware* e *ransomware*);
(ii) Engenharia Social;
(iii) *Pharming*;
(iv) *Phishing scam*;
(v) *Vishing*;
(vi) *Smishing*;
(vii) Acesso pessoal;
(viii) Ataques de DDoS e botnets;
(ix) Invasões (*advanced persistent threats*).

Para avaliar as ameaças e vulnerabilidades, serão realizadas varreduras internas/externas de cada ativo de rede, em busca de possíveis problemas de segurança, e eventual correção.

A principal regra de proteção consiste na segregação de acessos a sistemas e dados, conforme já detalhado neste documento.

A SIGA adotará, além disto, regras mínimas na definição de senhas de acesso a dispositivos corporativos, sistemas e rede, em função da relevância do ativo acesso.

A entidade trabalha com o princípio de que concessão de acesso deve somente ocorrer se os recursos acessados forem relevantes ao usuário.

A senha e *login* para acesso aos dados contidos em todos os computadores, bem como a conta de e-mail acessada via *webmail* devem ser conhecidas pelo respectivo usuário destes dispositivos. Estas senhas são pessoais e intransferíveis, não podendo ser divulgadas para quaisquer terceiros.

O acesso a informações confidenciais é limitado a determinados colaboradores cuja necessidade é justificada.

Arquivos eletrônicos são protegidos com senhas de acesso ou outros controles estabelecidos dentro dos sistemas computacionais, o que garante o acesso somente a pessoas autorizadas.

Todo conteúdo que está na rede pode ser acessado pela área Diretoria de Risco, *Compliance* e PLDFT e pelo Comitê de *Compliance* caso haja necessidade.

Arquivos pessoais salvos em cada computador poderão ser acessados caso o Comitê de *Compliance* julgue necessário.

A confidencialidade dessas informações deve ser respeitada e seu conteúdo será divulgado somente se determinado por decisão judicial. Para segurança dos perfis de acesso dos colaboradores, as senhas de acesso são parametrizadas conforme regras estabelecidas globalmente, bem como criptografadas. Desta forma, o colaborador poderá ser responsabilizado caso disponibilize a terceiros as senhas acima referidas para quaisquer fins.

O acesso remoto a arquivos e sistemas internos ou na nuvem terão controles adequados, de acordo com o técnico de TI.

Outro ponto importante é que, ao adquirir novos equipamentos e sistemas em produção, a SIGA 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 SIGA conta com recursos *anti-malware* em estações e servidores de rede, como antivírus e *firewalls* e *firewalls* locais em cada um desses equipamentos, bem como, *firewall* interno a rede e *firewall* UTM de borda, o qual contempla todos os serviços de ips/ids, *antispyware*, antivírus de *gateway*, filtro de aplicações e filtro de conteúdo.

A SIGA deverá, adicionalmente, proibir o acesso a determinados *websites* e a execução de *softwares* e/ou aplicações não autorizadas. A utilização dos ativos da entidade, incluindo computadores, telefones, internet, programas de mensagem instantânea, e-mail e demais aparelhos se destina a fins profissionais.

O uso indiscriminado destes para fins pessoais deve ser evitado, e nunca deve ser prioridade em relação a qualquer utilização profissional. A SIGA poderá gravar ligações telefônicas e históricos de navegação dos colaboradores.

A visualização de sites ou páginas que contenham conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é terminantemente proibida, estando o colaborador que o fizer sujeito aos processos e sanções determinados no Código de Ética e Conduta da SIGA.

Programas instalados nos computadores, principalmente via Internet (*downloads*), sejam de utilização profissional ou para fins pessoais devem obter autorização prévia do Diretor de Compliance.

Não é permitida a instalação de nenhum *software* ilegal ou que possuam direitos autorais protegidos. Somente arquivos sob licenciamento "GPL"[2] ou com o consentimento expresso do respectivo autor poderão ser gravados, mediante autorização prévia do responsável pela TI.

A instalação de novos *softwares*, com a respectiva licença, deve também ser comunicada previamente ao responsável pela TI.

O responsável pela TI, em conjunto com o Diretor de Risco, *Compliance* e PLDFT, são os principais responsáveis para tratar e responder questões de segurança cibernética, bem como por implementar as regras e normas aqui estabelecidas e a sua revisão.

Os deveres e responsabilidades dos responsáveis podem ser exemplificados pelo seguinte rol não taxativo:

(i) Testar a eficácia dos controles utilizados e informar à Diretoria os riscos residuais.

(ii) Acordar com a Diretoria o nível de serviço que será prestado por terceiros contratados e os procedimentos de resposta aos incidentes.

(iii) Configurar os equipamentos e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança aqui estabelecidos, bem como definir e assegurar a segregação das funções administrativas a fim de restringir poderes de cada indivíduo e reduzir o número de pessoas que possam excluir os *logs* e trilhas de auditoria das suas próprias ações.

(iv) Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.

(v) Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da SIGA em processos de mudança, sendo ideal a proteção contratual para controle e responsabilização no caso de uso de terceiros.

(vi) Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da SIGA, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da entidade.

(vii) Promover a conscientização dos colaboradores em relação à relevância da segurança da informação para o negócio da SIGA, mediante treinamentos.

[2] (http://www.gnu.org/licenses/gpl.html)

Na ocorrência de qualquer incidente envolvendo risco cibernético, todo e qualquer colaborador que perceba ou desconfie de tal incidente deverá imediatamente informar o Diretor de Risco, *Compliance* e PLDFT, que poderá convocar reunião do Comitê de *Compliance*. No caso de impedimento deste, o Comitê será instaurado pelo Diretor de Gestão e Distribuição ou outra pessoa a ser designada em assembleia de sócios devidamente convocada.

Ainda, uma vez que cada colaborador possui um login e senha personalíssimos, o acesso a qualquer documento e pasta ficará registrado no sistema, com o ID do usuário e data e horário de acesso, para eventual responsabilização em caso de vazamento.

12.6. Testes de Segurança

A SIGA realizará testes de segurança para os sistemas de informações anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

Os testes de segurança englobarão, mas não se limitarão, a análises de vulnerabilidade física e eletrônica, revisão e teste de códigos, transações sintéticas, testes de intrusão e análises dos registros eletrônicos.

Ainda, o treinamento sobre segurança de informação fará parte do treinamento inicial e contínuo da entidade, conforme previsto na Política de Treinamento descrita neste documento, que deverá assegurar que todos os colaboradores tenham conhecimento dos procedimentos e das obrigações aqui previstos, assim como minimizar a ocorrência de incidentes de segurança em função de problemas no uso, desvio de informações, fraudes e na interpretação das normas e procedimentos.

13. PREVENÇÃO À LAVAGEM DE DINHEIRO E FINANCIAMENTO AO TERRORISMO (PLDFT)

Na forma estabelecida pela Resolução CVM nº 50/2021, a SIGA segue os padrões determinados e possui mecanismos de PLDFT. A essência do processo, mas não se limitando a ela, é a seguinte:

i. Ciência de quem é a outra parte, a origem e finalidade de seu patrimônio.
ii. Análise do emissor e dos ativos investidos.
iii. Validar as informações cadastrais e mantê-las atualizadas, para continuamente conhecer os colaboradores, prestadores de serviços e clientes ativos, incluindo procedimentos de verificação, coleta, validação e atualização de informações cadastrais.
iv. Aplicar verificações das informações cadastrais proporcionais ao risco de utilização de seus serviços para a lavagem de dinheiro e o financiamento do terrorismo.
v. Acompanhar veementemente as atualizações Legais, autorregulamentadoras, e as melhores práticas internacionais, entre outras, como as Recomendações do Grupo de Ação Financeira (GAFI) e ofícios da CVM.
vi. Enviar informações relevantes exigidas pela Unidade de Inteligência Financeira (UIF/COAF).
vii. Monitorar as operações de forma permanente visando a perfectibilização do *Know Your Customer* (KYC).
viii. Empreender todos os esforços para se identificar quem são os beneficiários finais das operações.
ix. Utilizar-se da *Risk Based Analysis*.
x. Classificar os clientes por grau de risco.
xi. Acompanhar de maneira rigorosa a evolução do relacionamento com o cliente, descrevendo as eventuais medidas adotadas na avaliação interna de risco.
xii. Implantar todos as diretrizes descritas na Resolução CVM nº 50/2021.

A Política de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo (PLDFT) será vinculante a todos os colaboradores e prestadores de serviços.

A abordagem de risco, ainda, será feita levando-se em consideração os seguintes pontos:

i. Risco País.
ii. Risco do serviço de gestão de veículos de investimento.
iii. Risco do investidor.
iv. Risco de atividade/profissão do cliente.
v. Risco pelo tipo de serviços ou produtos contratados.

vi. Medição e controle de situações de alto risco; todos baseados no *Guidance on a Risk Based Approach for Managing Money Laundering*[3], elaborado pelo *The Wolfsberg Group*.

vii. O nível de ativos a serem depositados pelo cliente ou tamanho específico das transações realizadas.

viii. Nível de regulação ou supervisão ou regime de governo a que está sujeito o cliente.

ix. A regularidade ou duração do relacionamento entre a SIGA e o cliente. Relacionamentos de longo prazo, que envolvem contatos frequentes, podem apresentar menor risco sob a perspectiva de lavagem de dinheiro ou financiamento ao terrorismo.

x. A familiaridade da SIGA sobre uma jurisdição, incluindo conhecimento de leis locais, regulamentos e regras, bem como a estrutura e extensão da supervisão regulatória.

xi. O uso, por cliente, de veículos corporativos intermediários, ou outras estruturas que não possuam clareza em sua razão de ser ou que desnecessariamente aumentem a complexidade de análise, ou que de qualquer outra forma reduzam a transparência para a SIGA.

Dentro deste contexto, a SIGA, na hipótese de ocorrência de alguma das situações acima previstas, envidará seus melhores esforços para efetuar diligências no sentido de:

i. Estender sua análise a grupos econômicos e partes relacionadas.

ii. Manter cadastro atualizado no Sistema de Controle de Atividades Financeiras (SISCOAF)[4].

iii. Reportar, no prazo de 24 horas, ao Conselho de Controle de Atividades Financeiros (COAF), quaisquer operações suspeitas, nos termos dos artigos 10 e 11 da Lei nº 9.613/1998.

iv. Registrar, em janeiro de cada ano, declarações negativas, na hipótese de não identificação de operação suspeita, no período anterior.

[3] Disponível em: https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/wolfsberg-standards/15.%20Wolfsberg_RBA_Guidance_%282006%29.pdf

[4] http://www.fazenda.gov.br/orgaos/coaf/arquivos/sistema/manual-cadastro.pdf

A estrutura organizacional para a PLDFT será formada por estrutura autônoma e independente das áreas de negócios, abrangendo:

i. Quadro funcional devidamente treinado e atualizado, podendo ser contratada auditoria externa;
ii. O responsável pela Política, que será o Diretor de Risco, *Compliance* e PLDFT;
iii. Comitê de *Compliance*, que se reunirá com periodicidade, no mínimo, semestral.

Todas as informações que tratam de indícios, suspeitas de lavagem de dinheiro e financiamento ao terrorismo são de caráter confidencial, não devendo, em hipótese alguma, serem disponibilizadas a terceiros.

As comunicações de casos suspeitos que tratam a Circular do Banco Central do Brasil, nº 3.978/2020 não devem ser levadas ao conhecimento do cliente envolvido. Os colaboradores da área de *Compliance*, dentro de suas responsabilidades e suas funções, estão autorizados a participar do processo de identificação e reporte para o envio e uso exclusivo dos órgãos reguladores no âmbito de análise e investigação.

Os procedimentos acima estão melhor detalhados na Política de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo (PLDFT), disponível no site da SIGA (www.sigafinance.com.br).

14. PROCEDIMENTO DE *CONHECIMENTO DOS CLIENTES E TERCEIROS E AQUISIÇÃO DE ATIVOS*

Conhecer as Contrapartes é uma das principais exigências para que a SIGA possua práticas operacionais sólidas e seguras.

O conhecimento adequado do cliente minimiza as possibilidades de entrada de capital originário de atividades ilícitas ou criminosas na entidade. Desde a fase da prospecção, o responsável deve estar atento não só às suas metas quantitativas, mas também, às qualitativas, buscando clientes que se enquadrem na estratégia operacional da SIGA.

O Diretor de Gestão e Distribuição, caso essas funções sejam acumuladas pelo mesmo profissional nos moldes previstos, em especial, no art. 33 da Resolução CVM nº 21/2021, ou qualquer outro colaborador devidamente autorizado que ofertar os produtos da SIGA,

deve expor a presente política como um diferencial do mais alto grau de governança, demonstrando sempre positivamente a importância dos procedimentos adotados.

Este colaborador é responsável pelo completo preenchimento do formulário de *Know Your Customer* (KYC) descrevendo todas as informações sobre o cliente que estão em seu domínio, devendo, ainda, empreender esforços adicionais em buscar as informações que, por acaso desconheça e atentar-se para as questões relevantes, fazendo a diligência necessária para prevenção aos crimes e ilícitos abrangidos por esta Política.

A identificação dos clientes deverá abranger procuradores (no caso em que o cliente indicar a figura por meio de procuração com poderes específicos) e, no caso de Pessoa Jurídica, seus sócios, controladores e empresas integrantes do mesmo grupo ou conglomerado, além dos beneficiários finais, que são todas as Pessoas Naturais participantes da organização societária.

A qualidade do preenchimento dos formulários de KYC deve ser observado por todos os envolvidos, sendo de responsabilidade do Diretor de Gestão e Distribuição a clareza, objetividade e integridade das informações descritas neste relatório.

A SIGA adotará uma forte política de KYC, para determinar o nível de risco de cada cliente, verificar a sua adequação às características e especificidades dos negócios que administram, bem como seu enquadramento na cultura da entidade. O principal escopo destes esforços será a prevenção de que eventual cliente utilize os mecanismos oferecidos pela SIGA para atividades ilegais ou impróprias.

Em adição, a SIGA busca, independentemente de manter ou não relacionamento comercial direto com determinado cliente, busca avaliar, quando cabível, previamente ao início de suas atividades, se querem manter relação negocial com os prestadores de serviço dos fundos de investimento e/ou das carteiras administradas (procedimento conheça seu prestador de serviço), considerando, sobretudo, o risco de LD/FTP.

Ressalte-se que os procedimentos previstos neste capítulo são, também, aplicáveis às diligências para contratação de terceiros não credenciados à CVM e para a aquisição de ativos para integrar as carteiras dos Fundos da SIGA.

14.1 Identificação do Cliente, Contraparte e Emissor de Ativos

O cliente deverá sempre ser identificado antes do firmamento do contrato e da operação. Na recusa deste em repassar à SIGA as informações requeridas, haverá a rejeição de seu investimento.

Os procedimentos cadastrais terão ampla divulgação, com o objetivo de minorar os riscos legais, em especial aqueles relacionados com a PLDFT.

A documentação mínima a ser apresentada pelos clientes Pessoas Naturais será a seguinte:

i. Nome Completo, Estado Civil e Regime de Bens, se houver;
ii. Nacionalidade;
iii. Profissão;
iv. Declaração de Renda Média;
v. RG e CPF;
vi. Comprovante de Endereço;
vii. Informação sobre Pessoa Politicamente Exposta (PPE);
viii. Referências Comerciais;
ix. Questionário de Análise do Perfil de Investidor (API);
x. Comprovante de renda e D.I.R.P.F.
xi. Formulários Preenchidos

E para clientes Pessoa Jurídica:

i. Denominação ou Razão Social;
ii. CNPJ/MF e NIRE da Junta Comercial na qual seu ato constitutivo se encontra arquivado;
iii. Atos constitutivos, Contratos Sociais ou Estatuto Social em vigor, devidamente consolidado;
iv. Ano de Eleição dos representantes legais – os quais deverão apresentar toda a documentação descrita no que tange aos investidores Pessoas Naturais;
v. Comprovante de Endereço;
vi. Descrição detalhada das atividades e forma de operação da sociedade;
vii. Referência Comercial;

viii. Questionário de Análise do Perfil de Investidor (API);
ix. Balanço Patrimonial e DRE do ano anterior;
x. Formulários Preenchidos.

Os clientes relacionados com comércio ou referências de procedência duvidosa ou cuja receita atribuída ao negócio seja incompatível ou que não condisser com o objeto social da Pessoa Jurídica deverão ser rejeitados.

A análise deverá identificar o organograma de controle societário dos clientes Pessoa Jurídica, bem como seus beneficiários finais. Na hipótese de ser sociedade de capital aberto, sem identificação de seus acionistas, deverão ser apresentados os boletins de subscrição de ações existentes, certidão simplificada da Junta Comercial emitida há menos de 30 dias e identificação da diretoria.

A análise poderá ser realizada de forma mais branda, caso o investidor venha a adquirir quotas por intermédio ou conta e ordem de gestora ou administradora terceira, devidamente habilitada pela CVM, que possua e demonstre a realização de controles internos.

14.2 Procedimentos de Análise

Todo processo de análise do cliente deve ser documentado internamente por meio de formulários próprios. Antes da aprovação de qualquer contrato, deverão ser realizadas pesquisas minuciosas sobre os clientes no mínimo dos seguintes sites:

i. Google;
ii. Receita Federal;
iii. SERASA
iv. Órgãos Públicos;
v. Site dos Tribunais Regionais Federais (todos);
vi. Tribunal Estadual de Domicílio do Cliente e Grandes Centros;
vii. Supremo Tribunal de Justiça (STJ);
viii. Supremo Tribunal Federal (STF);
ix. Sites do Banco Central (BC), Comissão de Valores Mobiliários (CVM), Superintendência de Seguros Privados (SUSEP), entre outros.

Caso haja a identificação de que, dentro da cadeia de relacionamentos ou organograma societário, exista confirmação ou indícios de participação de empresa que funcione em paraísos fiscais, deverá ser procedida verificação detalhada pela Diretoria de Risco, *Compliance* e PLDFT para certificação de que não exista indícios de práticas que possam caracterizar crimes.

Após o preenchimento do formulário KYC, este deverá ser enviado por e-mail à Diretoria de Risco, *Compliance* e PLDFT, com as informações mínimas necessárias para a adequada análise.

Complementarmente, além das informações encaminhadas à Diretoria de Risco, *Compliance* e PLDFT antes do início do relacionamento com os clientes, deve-se observar os requerimentos de identificação cadastral exigidos para cada tipo de cliente, abrangendo todos os envolvidos até a completa identificação dos beneficiários finais.

As revisões das análises deverão ocorrer em conformidade com nível de risco observado em relação ao processo e ainda em função de operações ou situações que demonstrem alteração do nível de risco apresentado pelo cliente.

As fichas cadastrais devem apresentar assinatura do gestor responsável e do Diretor de Risco, *Compliance* e PLDFT.

Destaca-se a responsabilidade estabelecida pelo Artigo 64 da Lei 8.383/1991:

> *Art. 64 - Responderão como co-autores de crime de falsidade o gerente e o administrador de instituição financeira ou assemelhada que concorrerem para que seja aberta conta ou movimentados recursos sob nome: I - falso; II - de pessoa física ou de pessoa jurídica inexistente; III - de pessoa jurídica liquidada de fato ou sem representação regular.*

Quaisquer situações consideradas atípicas ou suspeitas devem ser comunicadas diretamente ao Diretor de Risco, *Compliance* e PLDFT, para que este efetue análise. Na hipótese de dúvida da Diretoria de Risco, *Compliance* e PLDFT, o contrato será rejeitado.

14.3 Pessoa Politicamente Exposta (PPE)

Cabe ressaltar, ainda, a obrigatoriedade legal de identificar e monitorar de forma mais diligente os clientes que se enquadrarem como Pessoa Politicamente Exposta (PPE). É considerada Pessoa Politicamente Exposta (PPE), aquelas enquadradas no conceito da Circular nº 3.978/2020 do Banco Central do Brasil, as pessoas que se declaram PPE por meio de campo próprio na Ficha Cadastral da SIGA e aquelas apontadas em listas públicas ou privadas pesquisadas pela Diretoria de Risco, *Compliance* e PLDFT.

Desta forma, quando do cadastramento de cliente PPE, é essencial que seja assinalado nos sistemas da SIGA, com destaque, esta condição. A Diretoria de Risco, *Compliance* e PLDFT fará as checagens habituais feitas a clientes, sendo necessário monitoramento especial para estes clientes.

Vale lembrar que os clientes que sejam representantes, familiares ou pessoas do relacionamento próximo de PPE também devem ser assim consideradas e, em função disso, serão monitoradas de forma especial.

14.4 Categorias de Risco dos Clientes

A SIGA categoriza os clientes entre três categorias de risco: Alta; Média; e Baixa, a depender das informações coletadas no momento da abertura do cadastro. Levará em consideração as qualificações de risco apontadas ao longo deste instrumento.

Considerando a diferença dos produtos geridos e distribuídos pela SIGA, haverá duas matrizes de análise de riso.

Para Fundos distribuídos para Investidores Qualificados, considerando o alto valor do Ticket Mínimo:

Valores Investidos junto à SIGA	Clientes sem Fator de Risco	Clientes com Fatores de Risco	Pessoas Politicamente Expostas
Mais de R$ 3.000.000,00	Alto	Alto	Alto

Entre R$ 2.000.000,00 e R$ 3.000.000,00	Médio	Alto	Alto
Entre R$ 800.000,00 e R$ 2.000.000,00	Baixo	Alto	Alto
Entre 0 e R$ 800.000,00	Baixo	Médio	Alto

Para Fundos distribuídos a investidores de varejo:

Valores Investidos junto à SIGA	Clientes sem Fator de Risco	Clientes com Fatores de Risco	Pessoas Politicamente Expostas
Mais de R$ 1.500.000,00	Alto	Alto	Alto
Entre R$ 500.000,00 e R$ 1.500.000,00	Médio	Alto	Alto
Entre R$ 300.000,00 e R$ 500.000,00	Baixo	Alto	Alto
Entre 0 e R$ 300.000,00	Baixo	Médio	Alto

A depender do fator de risco, entretanto, e conforme o disposto neste Manual, o cliente poderá ser considerado de alto risco em qualquer hipótese ou ter seu contrato rejeitado, em respeito ao princípio da precaução.

A área Comercial será a responsável por coletar as primeiras informações, que as repassará ao Diretor de Risco, *Compliance* e PLDFT, que deverá classificar o cliente conforme os riscos.

14.5 Da Atuação da Diretoria de Risco, *Compliance* e PLDFT

Para garantir o cumprimento das rígidas práticas de administração de risco, desde o início do relacionamento, os clientes passam pela análise da Diretoria de Risco, *Compliance* e PLDFT para verificar as informações prestadas e obter dados adicionais.

Tendo em vista as questões relacionadas na Política de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo (PLDFT), é possível haver necessidade de esclarecimentos em função do desenvolvimento da pesquisa ou avaliação da documentação. O objetivo desse procedimento é identificar eventuais indícios de práticas de lavagem de dinheiro ou financiamento ao terrorismo por parte do cliente e das demais pessoas jurídicas e físicas envolvidas direta ou indiretamente na operação proposta ou, ainda, em acontecimentos anteriores.

Nesta senda, a Diretoria de Risco, *Compliance* e PLDFT irá analisar as informações cadastrais, financeiras ou não, fornecidas pelo cliente por meio da área Comercial. Também analisará a existência de processos judiciais e administrativos em que o cliente figura como parte, sua natureza jurídica e resultados.

Observará, ainda, a pesquisa de apontamentos negativos na mídia e listas restritivas disponíveis de maneira a determinar se o relacionamento com o cliente pode acarretar quaisquer riscos ao programa geral de *Compliance* da SIGA e a quaisquer políticas de PLDFT.

O processo terá início quando a Diretoria de Risco, *Compliance* e PLDFT receber da Diretoria de Gestão e Distribuição todas as informações necessárias, incluindo o relatório e parecer inicial sobre a classificação de risco do cliente. A Diretoria de Risco, *Compliance* e PLDFT terá até sete dias úteis para emitir seu parecer.

Será feita a revisão periódica de todos os dados e pesquisas, a fim de atualização dos dados e riscos do cliente.

A Diretoria de Risco, *Compliance* e PLDFT embasará seus pareceres da seguinte forma:

i. Aprovado: Clientes que não apresentaram quaisquer restrições vinculadas à lavagem de dinheiro, corrupção ou condutas relacionadas ou financiamento ao terrorismo. Prazo de monitoramento: a cada dois anos a contar da data da primeira análise.

ii. Aprovado com Ressalvas: Clientes enquadrados na condição de PPE, clientes enquadrados na condição de pessoas relacionadas com PPE e clientes que possuem restrições de natureza leve não ligadas aos crimes de lavagem de dinheiro, corrupção

ou condutas relacionadas devem ser monitoradas com maior diligência e habitualidade. Prazo de monitoramento: semestral, a contar da data detecção da restrição, bem como marcação como cliente PPE ou sensível nos controles.

iii. Em processo de aprovação: Status temporário aguardando justificativa, informação complementar ou documento.

iv. Rejeitado: Clientes que possuem restrições relevantes relacionadas aos crimes de lavagem de dinheiro, financiamento ao terrorismo, corrupção e/ou condutas em desacordo com as políticas, manuais e códigos da SIGA. Acompanhamento: fica a cargo do Comitê de *Compliance* a definição do tratamento de cada situação. Até a definição final, o cliente ficará na condição de inativo no cadastro, impossibilitando o início de relacionamento e de qualquer operação.

O Parecer do Diretor de Risco, *Compliance* e PLDFT será dado em algum destes sentidos:

i. Em caso de aprovação, o contrato poderá ser firmado com o cliente.

ii. Em caso de Aprovação com Ressalvas o processo será remetido ao Comitê de *Compliance*, que emitirá parecer final sobre a rejeição ou aprovação do cliente (que terá monitoramento diferenciado em qualquer dos casos).

iii. Em caso de rejeição, o contrato não será firmado.

14.6. Das Restrições

Para efeitos de monitoramento anteriormente mencionados, serão levadas em consideração as seguintes espécies de restrição:

(i) Restrições Leves: São as restrições não ligadas aos crimes de lavagem de dinheiro, corrupção, tráfico de drogas e de armas e/ou condutas relacionadas com esses crimes.

(ii) Restrições Relevantes: São as restrições ligadas aos crimes de lavagem de dinheiro, corrupção, fraudes, tráfico de drogas e de armas, financiamento ao terrorismo e/ou condutas relacionadas com esses crimes.

14.7. Aprovação dos Clientes

Todos os clientes passam por uma classificação interna para caracterizar seu potencial de risco que possa gerar maior ou menor exposição, de acordo com a natureza de suas atividades, demandando mais ou menos diligência conforme avaliação contínua de seu relacionamento e nível de suscetibilidade ao envolvimento em crimes de lavagem de dinheiro e financiamento ao terrorismo.

A Diretoria de Risco, *Compliance* e PLDFT avaliará o nível de risco do cliente quando efetuar as análises iniciais, e de reavaliação, com foco em possíveis práticas de lavagem de dinheiro e financiamento ao terrorismo, descritas anteriormente. Os resultados da análise, registrados no sistema restrito da SIGA, permitem que o cliente seja adequadamente classificado para monitoramento, quando for observada qualquer situação que enseje acompanhamento de suas movimentações. Assim, quando classificado como "Aprovado com Ressalvas" e/ou Alto Risco, ele também deverá ser classificado conforme a lista abaixo no sistema de acompanhamento e monitoramento de PLDFT:

i. Pessoa Politicamente Exposta (PPE);
ii. Lista Restritiva;
iii. Lista de Sanções;
iv. Especial Atenção (para todos os clientes Aprovados com Ressalvas);
v. Não residente no Brasil;
vi. Apontado na Lei Anticorrupção;
vii. Apontado em Mídia; e
viii. Grandes Fortunas.

Para os clientes classificados como "Aprovado com Ressalvas", de acordo com a gravidade dos apontamentos identificados, a Diretoria de Risco, *Compliance* e PLDFT gerará dossiê com a informação relativa à situação que os classifiquem como tal. Esse dossiê deverá ser levado ao conhecimento do Comitê de *Compliance* para deliberação sobre eventuais medidas a serem adotadas em relação ao cliente.

Para fins de Aprovação com Ressalvas, serão especialmente levados em consideração os clientes que:

i. Apresentem características, no que se refere às partes envolvidas, valores, formas de realização e instrumentos utilizados ou que, pela falta de fundamento econômico ou legal, indiquem risco de ocorrência de crimes de lavagem de dinheiro e financiamento ao terrorismo.
ii. Mantém relacionamento e operações com Pessoa Politicamente Exposta (PPE) de nacionalidade brasileira ou estrangeira.
iii. Apresentem indícios de burla aos procedimentos de identificação e registro.
iv. Realizem operações que dificultem a identificação do beneficiário final.
v. Sejam oriundas ou destinadas a países ou territórios que aplicam insuficientemente as recomendações do Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo (GAFI/FATF).
vi. Não seja possível manter atualizadas as suas informações cadastrais.
vii. Pessoas Naturais e Jurídicas cujo ramo de atividades esteja na lista abaixo:
    a. Partidos Políticos;
    b. Turismo;
    c. Joalheria;
    d. Jogos e Entretenimentos;
    e. Motéis/Hotéis;
    f. Restaurantes;
    g. Agências de Câmbio;
    h. Objetos de Arte;
    i. Academias de Ginástica;
    j. Fundações;
    k. Armas e munições;
    l. Transportadores de Valores;
    m. Supermercados;
    n. Empresas cujo beneficiário fiscal seja domiciliado/sediado em paraísos fiscais;

Este rol não é taxativo e quaisquer outras atividades que, devido a sua natureza, são mais prováveis de serem usadas para lavagem de dinheiro e financiamento ao terrorismo, poderão e deverão ser investigadas como alto risco.

Considerará alto risco, ainda, cliente que tenha conexões com estas atividades.

14.8. Outras Situações de Risco

Todas as situações que o colaborador da SIGA, guiado pelo bom senso, pela boa-fé e pela probidade, entender que haja ou que possa haver indícios de condutas ilícitas, deverá reportar-se imediatamente à Diretoria de Risco, *Compliance* e PLDFT.

O rol não taxativo a seguir apresenta mais algumas situações de alerta:

i. Constantes movimentações financeiras para terceiros identificados como PPE.
ii. Situações de resistência em facilitar as informações necessárias, fornecimento de informação falsa ou prestação de informação de difícil ou onerosa verificação (beneficiário final ou informações patrimoniais).
iii. Atuação, de forma contumaz, em nome de terceiros ou sem a revelação da verdadeira identidade do beneficiário.
iv. Abertura e/ou manutenção de numerosas contas com vistas ao acolhimento de depósitos em nome de um mesmo cliente.
v. Abertura e/ou movimentação de conta de Pessoa Física por detentor de procuração ou qualquer outro tipo de mandato.
vi. Saques ou depósitos irregulares e de valores relevantes, não compatíveis com o tipo de conta ou com o patrimônio legítimo já documentado.
vii. Solicitação de sigilo de determinada movimentação.
viii. Solicitação de registro de determinada movimentação em nome de terceiros (Pessoa Física ou Pessoa Jurídica).
ix. Operação de valor muito superior ao que o cliente costuma operar, ocasionando em descasamento da capacidade financeira com a movimentação.
x. Proposta de operação que, por sua natureza, frequência, valores, partes envolvidas, possa caracterizá-la como atípica.

Quaisquer destas situações deverão ser reportadas ao Diretor de Risco, *Compliance* e PLDFT que, conforme o caso, levará à mesa de discussão do Comitê de *Compliance*. A conclusão desses procedimentos poderá ensejar comunicação aos órgãos fiscalizadores.

A Política de KYC, e outros documentos internos da SIGA detalharão mais minuciosamente os procedimentos adotados.

14.8.1. Formulários Adicionais

Os clientes classificados como Alto ou Médio Risco e/ou que sejam "Aprovados com Ressalvas" ou, ainda, de acordo com a discricionariedade do Diretor de Risco, *Compliance* e PLDFT, deverão ter formulário adicional preenchido, de acordo com as melhores práticas de mercado, e deverá incluir:

i. Motivos pelos quais o cliente deseja manter relacionamento com a SIGA.
ii. Situação financeira e escopo de negócio, com o objetivo de se identificar os recursos dos fundos a serem transacionados.
iii. Checagem da consistência entre as negociações pretendidas, os ativos e a posição financeira.
iv. Declaração jurídica atestando a legalidade da origem dos Fundos.

Os formulários deverão ser preenchidos e remetidos ao Diretor de Risco, *Compliance* e PLDFT.

14.9. Cadastro de Clientes Provenientes de Coordenadores de Ofertas e Demais Membros Participantes do Mercado de Valores Mobiliários

Em decorrência da qualidade da SIGA, tão somente como Gestora de Recursos e distribuidora dos próprios Fundos, ela está sujeita à Resolução CVM 50/2021.

A Gestora deverá cumprir com diferentes obrigações, a depender do relacionamento com cada tipo de cotista, conforme explicado abaixo.

14.9.1. Fundos de Investimentos com Múltiplos Cotistas

Em se tratando de fundo de investimento com múltiplos cotistas, considera-se como cliente do gestor o próprio fundo. Nessa hipótese, estabelece-se uma presunção, pela própria

natureza do veículo de investimento, de que o gestor de recursos não mantém relacionamento comercial direto com o cliente cotista

14.9.2. SIGA como distribuidora dos próprios Fundos e Carteiras Administradas

Trata-se aqui da hipótese em que o gestor desempenha simultaneamente duas atividades distintas, quais sejam, gestão de recursos e distribuição de seus próprios fundos.

Dado o acúmulo dessas duas atividades, mesmo que se trate de fundo de investimento com múltiplos cotistas, será a Gestora responsável pelo cliente cotista, com o qual manterá relacionamento comercial direto. Assim, observará, cumulativamente, as normas aplicáveis às atividades de Gestão e de Distribuição, conforme já explicitado neste documento, em conjunto com o Guia Anbima de PLDFT.

14.10. SIGA como Adquirente de Ativos para Fundos ou Carteiras Administradas

A SIGA adota todos os procedimentos previstos neste documento, em sua Política de KYC e PLDFT, e demais normas (auto)reguladoras, na hipótese de adquirir ativos para integrar as carteiras de seus Fundos ou Carteiras Administradas.

A análise dos Ativos também está sujeita à ABR prevista neste capítulo. Além disso, procedem-se às seguintes considerações na tomada de decisão sobre a aquisição de ativos:

i. tipo de emissão: o tipo de emissão ou a forma de negociação do ativo influenciam diretamente a classificação de risco de LD/FTP e seu monitoramento. A título de exemplo, as situações elencadas a seguir, por se referirem a ativos sujeitos à observância de uma série de obrigações regulatórias, dispensam o gestor de recursos de diligências de PLD/FTP suplementares no que se refere a PLD/FTP:
    a. ativos que tenham sido objeto de ofertas públicas iniciais e secundárias registradas de acordo com as normas emitidas pela CVM.
    b. ativos que tenham sido objeto de ofertas públicas com esforços restritos, dispensadas de registro de acordo com as normas emitidas pela CVM.
    c. ativos emitidos ou negociados por instituição financeira ou equiparada.

d. ativos emitidos por emissores de valores mobiliários registrados na CVM.
e. ativos de mesma natureza econômica dos listados acima, quando negociados no exterior, desde que (a) sejam admitidos à negociação em bolsas de valores, de mercadorias e futuros, ou registrados em sistema de registro, custódia ou de liquidação financeira, devidamente autorizados em seus países de origem e supervisionados por autoridade local reconhecida pela CVM, ou (b) cuja existência tenha sido assegurada por terceiros devidamente autorizados para o exercício da atividade de custódia em países signatários do Tratado de Assunção ou em outras jurisdições, ou supervisionados por autoridade local reconhecida pela CVM.

ii. agentes envolvidos: ressalvadas as hipóteses relacionadas acima, visto que, a depender do tipo de emissão não cabem diligências suplementares, a SIGA, a partir do relacionamento mantido com os agentes envolvidos na emissão, distribuição, intermediação, entre outros, adota tais procedimentos:
   a. solicitar a política de PLD/FTP do agente, a fim de verificar quais são seus processos e controles.
   b. realizar *due diligence* para fins de PLD/FTP (procedimento conheça seu prestador de serviço).
   c. solicitar informações a fim de buscar conhecer o beneficiário final, quando aplicável.

iii. tipo de ativo: o tipo de ativo a ser adquirido pela SIGA para o fundo ou carteira administrada pode demandar graus diversos de diligência em função de sua maior ou menor complexidade, estrutura do ativo e da própria ABR do gestor. Recomendamos que os gestores prevejam em documento mencionado na política, escrito e passível de verificação, quais diligências, para fins de PLD/FTP, serão empreendidas previamente à sua aquisição ativos. Por exemplo:
   a. ativos virtuais: para aquisição de ativos virtuais, nos termos permitidos pela regulamentação vigente, recomendamos que os gestores observem no mínimo, no que couber, o ofício circular da CVM nº 11/2018/CVM/SIN68, assim como o Manual de Boas Práticas em PLD/FTP para "*Exchanges*" Brasileiras69 e o Código de Conduta e Autorregulação70 publicados pela ABcripto (Associação Brasileira de Criptoeconomia) em seu site na internet,

sem prejuízo de novos guias ou recomendações de melhores práticas a serem publicados pela indústria ou reguladores.

b. FIDC: é recomendável que o gestor, de acordo com a sua ABR, busque identificar na estrutura de cada operação eventuais riscos específicos de LD/FTP e construa mecanismos adequados de *due diligence* e monitoramento. Nesse contexto, é recomendável que mantenha procedimentos de verificação de riscos no processo de originação do crédito e nos participantes da estrutura, incluindo, quando aplicável, cedentes, originadores e sacados, sendo aconselhável que adote critérios proporcionais em sua análise, de que são exemplos a representatividade financeira ou concentração mais ou menos expressiva em um ou mais cedentes, originadores e/ou sacados. Deve-se dedicar atenção especial às situações em que um mesmo agente, ou grupo de agentes relacionados ou ligados entre si, esteja presente em várias pontas da operação (por exemplo, um cotista exclusivo que seja também o originador do crédito), ou desempenhem funções que dependam ou sofram ingerência umas das outras. Da mesma forma, é recomendável a realização de *due diligence* com especial ênfase em pessoas sujeitas à adoção de mecanismos de controles nos termos do art. 9º da Lei 9.613/98 (ex. empresas de *factoring*, consultores de investimento e instituições financeiras que atuam como "bancarizadores" de operações originadas por não financeiras).

c. FIP: é recomendável que o gestor realize diligência previamente ao investimento na empresa objeto, de forma a identificar eventuais indícios de LD/FTP. Tal diligência pode ser realizada diretamente pelo gestor, ou mediante contratação de empresa ou escritório especializado, podendo abranger, por exemplo, a análise da estrutura societária da empresa objeto, detecção de apontamentos em listas restritivas ou mídias negativas – seja em relação à própria empresa, como também aos seus principais sócios e administradores – ou ainda por outros meios que se mostrem adequados às peculiaridades do caso concreto. A análise da contraparte da operação é também fator importante nesta abordagem. Recomenda-se, ainda, especial atenção a estruturas em que uma mesma parte, ou grupo de partes

relacionadas ou ligadas entre si, ocupem diferentes pontas da operação, ou desempenhem funções que dependam ou sofram ingerência umas das outras.

14.10.1. Monitoramento dos Ativos Adquiridos

A SIGA busca monitorar, quando cabível, as operações realizadas pelos seus fundos de investimento e carteiras administradas, de modo a identificar eventuais atipicidades que possam configurar indícios de LD/FTP. Em especial, dispensa especial atenção ao monitoramento de atipicidades envolvendo operações dos fundos, com destaque para:

a. recorrência ou concentração de ganhos ou perdas.
b. mudança de padrão em termos de volume de negócios e de modalidade operacional.
c. variação dos preços dos ativos negociados pelos fundos em comparação aos preços praticados no mercado.

14.10.2. Compartilhamento de Dados com Distribuidores e Administradores Fiduciários

De acordo com a CVM, os prestadores de serviço dos fundos de investimento devem, para fins de cumprimento das regras de PLD/FTP, sobretudo nas operações e situações de maior risco, utilizar-se do compartilhamento de informações – inclusive sobre cotistas diretos e indiretos quando necessário – entre os prestadores de serviços de fundos de investimento, notadamente administradores fiduciários, gestores de recursos, custodiantes e distribuidores.

Na esteira das melhores práticas e buscando prevenir e combater os ilícitos de LD/FTP, a CVM, por meio do Ofício-Circular 01/2022, esclareceu que, no entendimento da Autarquia, a troca de informações protegidas por sigilo segundo a Lei Complementar 105/01 entre os prestadores de serviços de fundos de investimento, inclusive com o gestor de recursos e o administrador fiduciário que não sejam classificados como uma instituição financeira, é permitida e está em consonância com o espírito e a finalidade da mencionada lei e das demais normas aplicáveis, em especial a regulamentação editada pela CVM, devendo,

naturalmente, ser observadas as obrigações de confidencialidade previstas na Resolução CVM 21/21.

A CVM relembra, ainda, que no âmbito do Decreto 10.270/20, e considerando a proximidade da nova avaliação mútua do Brasil pelo Gafi, foram disponibilizados para todas as pessoas obrigadas no Siscoaf, em 21 de maio de 2021, (i) a primeira Avaliação Nacional de Riscos de LD/FTP (ANR), (ii) seu respectivo sumário executivo, (iii) a avaliação nacional de riscos – metodologia e (iv) casos e casos – coletânea de tipologias de LD/FTP.

Nesse sentido, a CVM reforça que a alta administração e os diretores responsáveis pela Resolução CVM 50/21 das instituições devem acessar e analisar esses documentos, especialmente a Avaliação Nacional de Riscos, para efeitos da elaboração de suas avaliações internas de risco e da parametrização de suas matrizes de risco e sistemas de monitoramento.

14.11 Know Your Employee (Kye)

A SIGA confia em sua equipe e no fato de que os negócios serão conduzidos com um forte compromisso ético, honestidade, transparência, probidade e experiência profissional qualificada.

14.11.1 Recrutamento e Contratação

A solicitação de uma nova contratação ou reposição de colaborador deverá ser realizada por meio do gestor responsável, com requerimento escrito à Diretoria.

O processo de recrutamento e seleção será realizado pela Diretoria para contratação de auxiliares até a função de analistas.

Para os casos de contratação de profissionais para os cargos de gestão, a Diretoria poderá contratar uma empresa de consultoria especializada em Recolocação Profissional.

As etapas da seleção englobarão:

i. Dinâmicas em grupo;
ii. Testes de avaliação comportamental;
iii. Provas escritas de conhecimento para exercer a função;
iv. Entrevistas com a Diretoria.

Quando da aprovação, antes de informar o resultado ao candidato, a Diretoria irá consultar o perfil do profissional na internet, a existência de processos judiciais e/ou administrativos em andamento ou arquivados e em órgãos de proteção ao crédito.

Para fins de recrutamento e seleção, a SIGA irá solicitar a seguinte documentação:

(i) *Curriculum Vitae*;

(ii) Antecedentes Pessoais e Profissionais

Quando aprovado para contratação, o profissional, antes de realizar o teste admissional, deverá apresentar a seguinte documentação:

i. Carteira de Trabalho e Previdência Social (CTPS);
ii. PIS;
iii. RG e CPF;
iv. Título de Eleitor;
v. Certificado de Reservista;
vi. Certidão de Nascimento/Casamento/Divórcio;
vii. Certidão de Nascimento de seus dependentes, se houver;
viii. Antecedentes criminais;
ix. Todos os formulários exigidos pela SIGA devidamente preenchidos.

Os supervisores dos departamentos deverão conhecer os colaboradores, que atuem diretamente com eles, e relatar quaisquer mudanças na situação financeira ou hábitos de gastos destes.

Ao mesmo tempo, a Diretoria de Risco, *Compliance* e PLDFT deve controlar e diligenciar se o nome do colaborador não se inclui em nenhuma daquelas citadas no tópico 13 deste Manual. Os colaboradores, inclusive, serão listados como Alto, Médio ou Baixo Risco.

Enfim, todas as políticas do KYC poderão ser aplicadas no recrutamento e seleção dos colaboradores.

14.11.2 Monitoramento do Comportamento dos Colaboradores

Buscando assegurar a integridade da SIGA, os supervisores deverão monitorar o comportamento de seus subordinados, com o escopo de identificar e reportar quaisquer situações que possam ser consideras suspeitas.

A seguinte lista, meramente exemplificativa, demonstram situações que devem ser observadas:

i. Súbita ou significante alteração nos padrões de vida.
ii. Estilo de vida e hábitos de gastos que não sejam condizentes com os salários, condição financeira ou endividamento.
iii. Se o colaborador se recusar a ter folga sem motivo aparente.
iv. Colaboradores que não autorizam outros colegas a assistirem a certos clientes.
v. Se o colaborador receber presentes ou amenidades regularmente.
vi. Colaboradores que se demonstram relutantes em receber promoções ou mudanças em suas atividades.
vii. Colaboradores que ficam no escritório após cumprida a carga horária diária ou que compareçam a ele em horários estranhos sem explicação razoável.

Os supervisores serão responsáveis por detectar estes comportamentos e mudanças na conduta dos colaboradores e relatá-los ao Diretor de Risco, *Compliance* e PLDFT.

Além disso, atividades incomuns em operações em nome e por ordem dos colaboradores serão identificadas por meio de processo de monitoramento da SIGA e será avaliado com base nos seus perfis e na remuneração.

14.11.3. Avaliação de Desempenho, Recompensas e Medidas Disciplinares

A devida diligência no cumprimento das normas para a prevenção de lavagem de dinheiro será considerada mais um elemento a ser verificado na avaliação do desempenho dos colaboradores.

O não cumprimento das Políticas de PLDFT é prejudicial para a SIGA, executivos e colaboradores. Como a reputação de sua equipe, vincula-se diretamente à reputação da empresa, qualquer infração terá um duplo impacto. Além do mais, qualquer violação destas políticas significará que o colaborador pode estar sujeito a medidas disciplinares internas e que a SIGA e seus Diretores e colaboradores podem estar sujeitos a sanções, nos termos explanados no Código de Ética e Conduta.

14.11.4. Política de Treinamento de Colaboradores

A SIGA acredita que criar uma cultura de conformidade e controle entre seus colaboradores é a melhor ferramenta para combater a lavagem de dinheiro e o financiamento ao terrorismo e preservar a confidencialidade das informações.

Portanto, há um esforço contínuo para promover programas de treinamento, desenvolvimento e conscientização da equipe em torno dos muitos aspectos que envolvem PLDFT.

Esta política de treinamento abrange administradores, empregados e colaboradores que possuam acesso a informações confidenciais, participem do processo de decisão de investimento ou participem do processo de distribuição de cotas de fundos de investimento. O treinamento abrange as políticas e procedimentos adotados pela empresa e tem perfil compatível com a atividade desempenhada pelo administrador, sócio ou funcionário.

14.11.4.1 Integração Inicial

O processo de contratação de um novo colaborador é constituído por rotinas de integração, incluindo a leitura e aceitação prévia de todos os códigos, manuais, políticas e procedimentos internos. Pretende-se, com isto, que o Colaborador tome ciência dos princípios gerais, normas internas e da filosofia que norteia as atividades da Gestora. Através deste treinamento o colaborador toma conhecimento das principais leis, regras e normas incidentes direta ou indiretamente sobre estas atividades. Os seguintes documentos internos da Gestora são apresentados ao Colaborador por ocasião da Integração Inicial:

a) Código de Ética e Conduta

b) Manual de *Compliance*, Regras, Procedimentos e Controles Internos;

c) Políticas de KYC, KYE, KYP e KYS;

d) Política de Compra e Venda de Valores Mobiliários por Administradores e Colaboradores;

e) Política de *Suitability*;

f) Política de Segregação de Atividades e Confidencialidade;

g) Política de Prevenção à Lavagem de Dinheiro e ao Financiamento ao Terrorismo;

h) Política de Rateio e Divisão de Ordens;

O Colaborador, na ocasião desta Integração Inicial, atestará que passou a ter ciência dos documentos e do conteúdo destes, estando plenamente de acordo e se comprometendo a cumprir as regras previstas.

14.11.4.2. Curso Inicial

Este curso visa informar os novos colaboradores sobre as políticas e procedimentos acerca da PLDFT, bem como para conscientizá-los sobre os riscos para si e para a entidade em se tratando desta matéria.

Este curso deverá ser conduzido por, no mínimo, 45 dias a partir da data de contratação.

Ao final do curso, o colaborador deverá fazer uma prova, a ser elaborada pela Diretoria de Risco, *Compliance* e PLDFT para fins de verificação de adesão aos procedimentos.

14.11.4.3 Treinamento Contínuo

Não obstante a obrigatoriedade insculpida no art. 24, III da Resolução CVM 21/2021, a SIGA entende imprescindível que todos os colaboradores, principalmente aqueles que atuam nas áreas que tenham acesso a informações confidenciais, participem de processo de decisão de investimento ou participem de processo de distribuição de cotas de fundos de investimento, possuam conhecimento de todas e atuais melhores práticas de mercado. Para tanto, no mínimo, existe a obrigatoriedade de conclusão de todos os cursos online oferecidos gratuitamente no website da ANBIMA.

Para os cursos pagos da ANBIMA ou outras entidades cujo trabalho seja relevante à atividade exercida pela Gestora, cabe ao diretor de Risco, *Compliance* e PLDFT indicar quais cursos são mais adequados para cada funcionário, ocasião na qual SIGA custeará as despesas. Ademais, este programa consiste, também, em disponibilidade semanal de reunião geral da equipe com a diretoria de *Compliance* para que todas as dúvidas sejam sanadas, sem prejuízos das consultas individuais quando necessárias.

14.11.4.4. Cursos de Atualizações Regulamentares

Os colaboradores devem sempre estar atualizados sobre os regulamentos existentes. Para tanto, serão realizados cursos sempre que o Diretor de Risco, *Compliance* e PLDFT julgar necessário. Em regra, os cursos abrangerão as seguintes matérias:

i. Tendências na prevenção da lavagem de dinheiro.
ii. Estrutura legal e regulamentos internos.
iii. Programa de Identificação de Clientes.
iv. Programa KYC.
v. Perfil de risco do cliente.
vi. Monitoramento de transações.
vii. Relatório de transações suspeitas.
viii. Metodologias de lavagem de dinheiro e financiamento ao terrorismo.

Os mencionados são cursos obrigatórios para os colaboradores. Sempre que possível, a equipe realizará testes nestas áreas para avaliar a compreensão e a aquisição de conhecimento. O certificado de participação e os resultados dos testes serão arquivados no dossiê do colaborador. A Diretoria de Risco, *Compliance* e PLDFT manterá um registro de todos os cursos de treinamento realizados, bem como da equipe que compareceu e obteve notas de aprovação.

Os membros da Diretoria de Risco, *Compliance* e PLDFT, bem como os integrantes do Comitê de *Compliance* realizarão, ao menos, um curso por ano, conduzido por um terceiro independente da SIGA, preferencialmente proferidos pela Associação Brasileira das Entidades dos Mercados Financeiros e de Capitais (ANBIMA) ou instituição reconhecida no mercado.

14.11.4.5. Tipos de Treinamento

Os treinamentos a serem oferecidos pela SIGA englobam, Reciclagem e Atualização – Sempre que houver defasagem entre as competências dos colaboradores e as melhores práticas de mercado, seja por alteração de sistema de segurança de informação, atualização das normas de PLDFT etc. – capacitação profissional, técnicas de mitigação de conflitos de interesses e segurança e confidencialidade de informação, entre outros que buscam aprimorar os procedimentos e controles internos impostos pela SIGA. Os cursos serão ministrados das seguintes formas: (i) Treinamento *in company*; (ii) *E-learning*; (iii) *Microlearning*; (iv) Sala de aula

invertida; (v) aprendizagem social. Ademais, todos os colaboradores, antes de iniciarem as suas funções, são obrigados a concluir os cursos online oferecidos gratuitamente pela ANBIMA em seu site até a data do início da função."

14.11.4.5. Adesão

Todos os colaboradores deverão assinar um termo comprovando o recebimento deste documento, bem como ciência de todo o seu conteúdo, obrigando-se a respeitá-lo integralmente.

Todos os colaboradores, ainda, deverão aderir aos treinamentos dispostos no tópico 14 deste documento.

15. POLÍTICA DE *KNOW YOUR PARTNER* (KYP) E *KNOW YOUR SUPPLIER* (KYS)

A seleção, contratação e supervisão de prestadores de serviços seguem os procedimentos de *Know Your Partner* (KYP) e *Know Your Supplier* (KYS). Tendo como objetivo identificar e aprovar parceiros de negócios e fornecedores, visando prevenir que a SIGA realize negócios com contrapartes inidôneas ou suspeitas de envolvimento em atividades ilícitas, bem como assegurar que eles possuam procedimentos adequados de PLDFT, quando aplicável.

Os processos de KYP e KYS têm o objetivo de adquirir melhor conhecimento da empresa, da instituição financeira ou equiparada pelo Banco Central do Brasil a ser contratada, buscando observar suas práticas de governança, incluindo visitas físicas com equipe específica para realização de *due diligence*.

i. São requisitos de pesquisa mínimos para a possibilidade de firmar negócios:
ii. Identificação de regularidade fiscal junto à Receita Federal do Brasil.
iii. Identificação da situação de crédito junto aos órgãos de proteção ao crédito.
iv. Identificação da estrutura organizacional da empresa.
v. Identificação do beneficiário final.
vi. Pessoa Natural que em última instância, de forma direta ou indireta, possui, controla ou influencia significativamente a contratada.
vii. A Pessoa Natural em nome da qual a transação é conduzida.
viii. Avaliação do questionário *due diligence*.

ix. Avaliação da documentação referente à estrutura de Controles Internos e de *Compliance*.

Não exaustivo, serão solicitadas as principais políticas e manuais internos, de forma que a SIGA possa obter razoável conforto sobre os procedimentos e controles existentes na instituição contratada para prestação de serviços.

O conteúdo das informações e análises possui validade de 12 meses, sendo obrigatória a renovação e atualização dos dados cadastrais e de *Compliance*.

Uma vez aprovada a contratação de qualquer fornecedor, providenciar a assinatura de contrato e do Termo de Compromisso e ciência do Código de Ética e Conduta e demais procedimentos, códigos, manuais e políticas internas da SIGA. A critério do Diretor de Risco, *Compliance* e PLDFT, prestadores renomados no mercado pelo serviço a ser contratado podem ser dispensados destes procedimentos.

Detalhes sobre os procedimentos poderão ser visualizados na Política de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo (PLDFT) e na Política de *Know Your Customer* (NYC)*, Know Your Employee* (NYE)*, Know Your Partner* (NYP) *e Know Your Supplier* (NYS).

16. POLÍTICA DE *SUITABILITY*

A Política de *Suitability* tem como objetivo estabelecer metodologia da SIGA para a verificação da adequação dos produtos, serviços e operações ao Perfil *Suitability* do Investidor, considerando seus objetivos de investimento, sua situação financeira, seu grau de conhecimento e experiência necessários para compreender os riscos relacionados aos negócios.

Esta Política está de acordo com as Resoluções CVM nº 19/2021, 30/2021 e 50/2021, suas alterações posteriores e com o Roteiro Básico do Programa de Qualificação Operacional (PQO) da B3.

A adequação do perfil de risco do cliente ao produto por ele adquirido é importante na medida em que informa ao cliente quais produtos são mais adequados ao seu perfil de investimentos e impede que enfrente riscos acima do suportado.

Os colaboradores devem se atentar ao estrito sigilo de informações de clientes. A Diretoria de Risco, *Compliance* e PLDFT fiscalizará o sigilo, nos termos previstos neste Manual e, também, na Política de Segregação de Atividades e Confidencialidade, disponível no site da SIGA (www.sigafinance.com.br).

A Política e Manual de *Suitability*, que demonstra de forma completa as diretrizes e monitoramentos aplicáveis, pode ser acessada pelo website da gestora (www.sigafinance.com.br).

17. POLÍTICA DE RATEIO E DIVISÃO DE ORDENS

O princípio da Política de Rateio e Divisão de Ordens é *Best Execution,* que está relacionado com o tratamento justo e equitativo de todos os clientes com relação às transações executadas. A SIGA e seus colaboradores deverão tomar todas as providências cabíveis para obter a melhor execução possível nas transações realizadas para todos os seus clientes.

A política adotada pela entidade deverá obedecer a critérios que determinem a importância relativa dos fatores de execução, tais como as características:

i. a ordem;
ii. dos instrumentos financeiros;
iii. mercados para os quais elas podem ser direcionadas;
iv. dos clientes.

Visando o melhor resultado possível, os seguintes critérios também serão levados em consideração:

i. velocidade da execução;
ii. probabilidade da liquidação;
iii. tamanho e natureza da ordem;
iv. impacto no mercado;
v. custos de transação.

A política completa de Rateio e Divisão de ordens também poderá ser acessada junto ao website da gestora (www.sigafinance.com.br)

18. POLÍTICA DE CERTIFICAÇÃO CONTINUADA

Esta normativa objetiva incluir a totalidade dos Colaboradores da gestora em Conformidade ao Código ANBIMA de Regulação e Melhores Práticas para o Programa de Certificação Continuada ("Código"), estabelecendo diretrizes e princípios que irão disciplinar o Controle das Certificações, visando a garantia de que os Colaboradores estejam enquadrados nos termos exigidos pela entidade de Autorregulação.

Ainda, objetiva atualizar a atenção da SIGA nos termos da atualização do Código ANBIMA de Regulação e Melhores Práticas para o Programa de Certificação Continuada, cuja vigência iniciou em 01º de julho de 2021.

18.1 Atividades Elegíveis

Conforme disposto no Código, as seguintes certificações são critérios aos Profissionais para o exercício das atividades dispostas:

CFG: Profissionais que desempenham o exercício profissional de Gestão de Recursos de Terceiros, não possuindo caráter obrigatório e não é condição para atuar em nenhuma atividade específica.

CGA: Destinada aos profissionais que desempenham o exercício profissional de Gestão de Recursos de Terceiros de Fundos 555 classificados como renda fixa, ações, multimercados, cambiais e Carteiras Administradas.

CGE: A CGE é destinada aos profissionais que desempenham o exercício profissional de Gestão de Recursos de Terceiros de Fundos estruturados.

Ainda, não se pode olvidar que os Profissionais Certificados e Aprovados pela CGA com dois módulos válidos terão sua certificação convertida automaticamente para CFG, CGA e CGE, não sendo necessário realizar novo exame.

Conforme permitido pela Resolução CVM 21/2021, a SIGA utiliza a estrutura responsável pela gestão de seu portfólio para efetuar a distribuição somente dos produtos geridos por si.

Dentre as áreas de trabalho exercidas pela SIGA, a área de Gestão e Distribuição são as únicas elegíveis à Certificação.

As Certificações Mínimas para estes Gestores são o CGA e o CGE, conforme o Código ANBIMA, uma vez que os profissionais deste setor da SIGA exercem as atividades de Gestão de Recursos de Terceiros de Fundos 555 classificados como renda fixa, ações, multimercados, cambiais e Carteiras Administradas e Gestão de Recursos de Terceiros de Fundos estruturados

Os analistas que exercem atividades de apoio, *Back Office* ou *Back Middle Office*, por sua vez, não são elegíveis às certificações, uma vez que não desempenham as atividades acima informadas.

Considerando a estrutura enxuta da SIGA, 100% dos profissionais que exercem as atividades mencionadas possuem as certificações CGA, CGE e CFG..

As demais áreas da SIGA, apesar de não serem elegíveis à Certificação, estão devidamente identificadas na planilha de Controla das Áreas Elegíveis e Profissionais Certificados.

Não obstante, apesar da não elegibilidade, a SIGA solicita, veementemente, a todos os seus colaboradores não elegíveis, que obtenham, no mínimo, a certificação CPA-20, independentemente de sua atribuição, no prazo máximo de 24 (vinte e quatro) meses a partir de sua contratação.

18.2 Regras e Procedimentos

Para assegurar o cumprimento do Código, a SIGA implementou, neste Documento, as regras, procedimentos e controles internos, nos termos das cláusulas a seguir alinhavadas.

18.2.1. Identificação dos Profissionais na Admissão e Desligamento

O profissional contratado (não certificado) receberá, no momento da contratação, as instruções sobre a necessidade de certificação, a depender da atividade que exercerá dentro da SIGA. A Diretoria de *Compliance* efetuará os devidos registros junto às entidades pertinentes.

O profissional que não apresentar a certificação necessária, deve ser impedido de iniciar as suas atividades. Se completado o prazo estabelecido pela Diretoria de Risco, *Compliance* e PLDFT, para a retirada da certificação, e o profissional não tiver apresentado, cabe a esta a responsabilidade da comunicação ao responsável pela área para a qual o respectivo colaborador foi contratado e ao RH de que o profissional ainda não está habilitado a exercer as atividades pelas quais foi contratado.

Cabe ao RH, em conjunto com o responsável pela área que fez a contratação do novo colaborador, a definição sobre o eventual remanejamento para uma outra área, a sua manutenção em atividades não elegíveis, devidamente supervisionado por funcionários que possuem a certificação, ou a sua demissão.

A Diretoria de Risco, *Compliance* e PLDFT fica responsável pela identificação de profissionais elegíveis à certificação no momento da admissão, bem como em casos de transferência interna que ocorram nas áreas da Instituição, além da atualização do banco de dados da ANBIMA.

Em relação ao profissional que já possui a certificação, será feito o registro no Banco de Dados do sistema interno da ANBIMA no momento de sua admissão. O registro de vinculação daqueles que precisam realizar a prova de certificação serão realizados assim que for apresentado o certificado.

Os profissionais desligados, admitidos e transferidos deverão ser atualizados no Banco de Dados da ANBIMA até o último dia do mês subsequente, considerando a data do evento. Tal regra também é aplicável a atualização da área de atuação do profissional.

18.2.2 Critérios Adotados para Determinar as Atividades Elegíveis para Cada uma Das Certificações

Os Critérios adotados pela SIGA para determinar as Atividades Elegíveis para cada uma das certificações são exatamente as mesmas dispostas no Código ANBIMA de Certificação, quais sejam:

CFG: Profissionais que desempenham o exercício profissional de Gestão de Recursos de Terceiros, não possuindo caráter obrigatório e não condicionado para nenhuma atuação em nenhuma atividade específica.

CGA: Destinada aos profissionais que desempenham o exercício profissional de Gestão de Recursos de Terceiros de Fundos 555 classificados como renda fixa, ações, multimercados, cambiais e Carteiras Administradas.

CGE: A CGE é destinada aos profissionais que desempenham o exercício profissional de Gestão de Recursos de Terceiros de Fundos estruturados.

O responsável pela área elegível deverá manter, ao menos, um substituto devidamente certificado apto para assumir as funções do cargo em vacância.

18.2.3 Critérios de Identificação de Elegibilidade de Profissionais Transferidos ou Contratados

Ao deliberar sobre a necessidade de um novo integrante ou substituição, o responsável pela área contratante deverá informar à área de *Compliance* se existe a necessidade de que seja contratado um profissional certificado.

Em caso positivo, este aspecto deve ser levado em consideração na triagem dos candidatos. Em caso negativo, quando da admissão de qualquer Colaborador deverá ser questionado se detém alguma certificação ou dispensa/isenção perante a ANBIMA.

Em sendo certificado ou possua dispensa/isenção, mesmo que para cargo não elegível, o novo Colaborador deverá ter o seu cadastramento atualizado, junto ao Banco de Dados da ANBIMA, até o último dia do mês subsequente à data dos respectivos eventos.

Na eventualidade de mudança de área de um profissional certificado para uma área não elegível à certificação, o gestor responsável pela área elegível deverá manter um substituto devidamente certificado para as atividades.

No caso de um profissional não certificado se candidatar a um cargo elegível, este deverá buscar a certificação elegível antes de assumir o referido cargo. O monitoramento destes procedimentos cabe, também, à Diretoria de Risco, *Compliance* e PLDFT.

18.2.4 Procedimento Adotado para a Atualização da Certificação dos Profissionais que Atuam em Atividades Elegíveis

A Diretoria de Risco, *Compliance* e PLDFT verifica, periodicamente, se todos os Colaboradores elegíveis estejam certificados e que as respectivas certificações sejam válidas.

A CGA e CGE são válidas por prazo indeterminado, desde que o profissional esteja exercendo atividades que dela sejam objeto.

Compete à Diretoria de Risco, *Compliance* e PLDFT garantir que um Colaborador não certificado não exerça função que pressuponha certificação ou que a obtenha nos termos ditados pela ANBIMA.

Caso o Colaborador não disponha da certificação aplicável, o *Compliance* é responsável por manter a documentação formal que evidencie o afastamento do Colaborador das atividades elegíveis a certificação.

Cabe à Diretoria de Risco, *Compliance* e PLDFT monitorar o cumprimento as demais diretrizes estabelecidas no "Código ANBIMA de Regulação e Melhores Práticas – Programa de Certificação Continuada".

18.2.5 Procedimentos para Afastamento dos Profissionais que Desempenhem Atividades Elegíveis

Todos os profissionais que desempenham atividades elegíveis sem a devida certificação, ou com a certificação vencida, serão afastados imediatamente, a exemplo dos profissionais de gestão de recursos de terceiros, que somente poderão atuar na função com a certificação CGA ou CGE válidas.

Os profissionais em processo de certificação que forem afastados receberão uma requisição de afastamento com as devidas justificativas e deverão assinar o documento, o qual deverá ser mantido como registro de comprovação.

18.2.6 Procedimento para Atualização do Banco de Dados junto à ANBIMA

A Diretoria de Risco, *Compliance* e PLDFT será responsável pela veracidade e manutenção do banco da dados da ANBIMA. As seguintes informações deverão ser inseridas no sistema: (i) Data de admissão; (ii) Data de Desligamento; (iii) Atividade Exercida; (iv) Área de Atuação; (v) Cargo; (vi) Tipo de Gestor; (vii) Endereço Eletrônico.

19. *SOFT DOLLAR*

O *Soft Dollar* é definido como o benefício econômico, não pecuniário, eventualmente concedido à SIGA, por corretoras e outros fornecedores, em contraprestação ao direcionamento de transações dos fundos de investimentos geridos por si, para fins de auxílio no processo de tomada de decisões de investimento em relação aos respectivos Fundos.

Estes benefícios não poderão ter caráter pecuniário e não deverão servir exclusivamente como base para tomada de decisões de investimentos e suporte à gestão dos Fundos geridos pela SIGA.

Os fornecedores não deverão ser selecionados considerando somente os benefícios recebidos por meio de acordos de *Soft Dollar*, mas deverá levar em consideração, primordialmente, a eficiência, produtividade e menores custos por eles oferecidos.

Sempre, ao firmar acordos de *Soft Dollar*, os colaboradores da SIGA deverão respeitar as seguintes regras de conduta:

i. Definir, com pauta na boa fé, se os valores pagos pelos clientes, e repassados aos fornecedores, são razoáveis em relação aos serviços ou benefícios que estejam sendo prestados.
ii. Inserir os interesses dos clientes acima dos seus ou da própria SIGA.
iii. Possuir convicção de que os benefícios recebidos auxiliarão diretamente no processo de tomada de decisões de investimento relativamente ao veículo que gerou referido benefício, devendo alocar os custos de acordo com a utilização correspondente.
iv. IV. Divulgar amplamente e com transparência, aos clientes, potenciais clientes e ao mercado, os critérios de políticas adotadas com relação às práticas de *Soft Dollar*, bem como os potenciais conflitos de interesses concebidos pela adoção destas práticas.

O *Soft Dollar* somente será permitido se contar com o conhecimento e consentimento do Diretor de Risco, *Compliance* e PLDFT e não interfiram de maneira alguma na relação de confiança que a SIGA mantém com seus clientes e com o mercado.

Ainda, em regra, é vedado aos colaboradores a aceitação de quaisquer tipos de gratificação, presentes ou benefícios de terceiro, que possam gerar conflitos de interesse, salvo com a autorização expressa da Diretoria de Risco, *Compliance* e PLDFT.

20. PRESENTES E BRINDES

Este tópico tem relação com a aceitação, solicitação ou oferta de brindes e presentes, hospitalidades e entretenimento, comissões ou vantagens de qualquer espécie e natureza, por parte de colaboradores da SIGA. Sejam estas aceitações, solicitações ou ofertas, vindas de colaboradores da SIGA ou de pessoas, Jurídicas ou Naturais, ou entidades com as quais tenham relacionamento comercial, ou algum tipo de interesse pessoal ou profissional.

Os colaboradores não poderão aceitar, solicitar ou oferecer qualquer gratificação, presente, entretenimento ou hospitalidade. Assim como vantagens indevidas, favores, dinheiro ou presentes de caráter pessoal, que possam influenciar decisões, não são permitidos.

Todos e quaisquer presentes oferecidos deverão ser recusados, informando à outra parte sobre a existência desta orientação.

São admitidos jantares e almoços pagos por fornecedores e qualquer outra parte que tenha relacionamento comercial com a entidade, desde que limitados a valores e frequências razoáveis.

Reciprocamente, jantares e almoços podem ser oferecidos a clientes nas mesmas condições.

São admitidos cursos, seminários, *workshops* e outros eventos semelhantes, bem como livros e publicações, até o limite de um salário mínimo. Ultrapassando estes valores, a proposta será submetida previamente à Diretoria de Risco, *Compliance* e PLDFT que providenciará os registros internos e deliberará sobre a aceitação ou não. Materiais de escritório (como agendas, canetas, calendários e assemelhados) não são considerados como brindes ou presentes e podem ser recebidos/oferecidos livremente.

21. PLANO DE CONTINGÊNCIAS E CONTINUIDADE DOS NEGÓCIOS

O Plano de Contingência e Continuidade dos Negócios demonstra, sumariamente, as medidas básicas a serem tomadas, em caso de qualquer interrupção dos negócios. Estas políticas devem garantir a capacidade da SIGA em operar constantemente e em bases contínuas.

A Política de Continuidade dos Negócios e Contingências tem como objetivo estabelecer diretrizes e procedimentos claros para identificar, avaliar e responder a eventos adversos que possam interromper as operações da SIGA, garantindo a rápida recuperação e a continuidade das atividades críticas.

O Plano de Contingência é mais bem detalhado na Política de Continuidade dos Negócios e Contingências, disponível no website da Gestora.

O Comitê de Gestão de Riscos ("Comitê") será responsável por avaliar a PNC e instaurar o Comitê de Contingências, quando necessário, para determinar as diretrizes quando da ocorrência de qualquer evento de contingência. Este Comitê é formado por profissionais da área de Gestão de Recursos de Terceiros, que apresentam os ativos pretendidos, e pela Diretoria de Risco, Compliance e PLDFT, que analisa o enquadramento da operação nas políticas internas, normas legais e (auto)reguladoras e regulamentos.

Em síntese, serão tratados os planos que envolvem quatro grupos de contingência:

a) Infraestruturas Físicas;
b) Pessoal;
c) Infraestruturas Tecnológicas;
d) Serviços Externos.

21.1. Contingência de Infraestruturas Físicas

Nestas são compreendidas as situações de caso fortuito ou força maior, que impeçam o acesso ou utilização das instalações da entidade.

Por força maior entendem-se desastres naturais, incêndios, desabamentos, entre outros.

Por caso fortuito entendem-se danos físicos relevantes às instalações ou equipamentos, intencionais ou não, e, ainda, falhas no fornecimento de energia elétrica.

As instalações da Gestora são em sua própria sede, localizada em prédio comercial, situado na Rua Dr. Brasílio Vicente de Castro, 111, Sala 303, Curitiba/PR. O edifício possui todos os alvarás de segurança necessários, plano de evacuação, brigadistas e todos os requisitos de segurança exigidos pela legislação.

O edifício, ainda, conta com monitoramento e portaria 24 horas. O acesso ao interior do prédio é restrito, somente sendo permitido com a identificação individual, cadastro junto ao sistema de segurança e autorização de colaborador da SIGA. O acesso se dá por catracas, que são liberadas por intermédio de reconhecimento facial

Dentro do escritório, o único acesso é por intermédio da sala de recepção e somente será permitido com acompanhamento contínuo de um dos colaboradores da SIGA. O acesso às áreas comuns é controlado por meio de sistema de controle de acesso eletrônico, por digital ou crachá. O acesso aos equipamentos críticos é permitido somente aos colaboradores específicos das áreas e equipe de TI.

As salas relativas às atividades que mantêm conflito de interesse com outras áreas são acessadas somente pelos colaboradores da área em questão, e para as atividades não conflitantes, como serviços de TI e limpeza.

21.1.1. Dos Casos de Impedimento ao Acesso na Entidade

Em caso de impedimento de acesso à sede da SIGA, os colaboradores, a depender de seu nível de acesso ao sistema, poderão:

(i) Ser direcionados ao trabalho *homeoffice*, aos que possuam e possam possuir acesso remoto às informações necessárias ao seu exercício laboral.

(ii) Ser dirigidos a um espaço de *coworking,* com supervisão da Diretoria, por meio de acesso remoto à rede.

Tão logo o acesso às estruturas físicas seja normalizado, os colaboradores serão imediatamente avisados sobre o retorno das atividades normais.

21.1.2. Dos Danos Físicos a Instalações ou Equipamentos Elétricos

Compreendem as situações de danos a instalações ou equipamentos da SIGA de tal forma que impeçam a utilização de suas dependências ou de algum equipamento relevante para suas atividades.

Em caso de danos a equipamentos críticos, que impossibilitem os trabalhos na sede da entidade, a contingência seguirá as premissas apontadas no tópico 21.1.1.

Nestes casos, ainda, os equipamentos receberão imediata atenção de técnicos contratados para consertá-los. Preferencialmente, autorizados das marcas.

21.1.3. Falha no Fornecimento de Energia Elétrica

A SIGA considera como serviço crítico às atividades o fornecimento de energia elétrica. A sede possui, para tanto, equipamentos de *nobreak* e *backup* que serão ativados automaticamente em caso de queda de energia elétrica.

A retomada será feita mediante eliminação dos efeitos motivadores da contingência. O Comitê de Contingência avisará aos colaboradores do retorno às instalações. Caso contrário nenhum movimento se faz necessário, pois a energia será estabelecida automaticamente.

Até a retomada dos trabalhos, o plano de contingência seguirá o disposto no tópico 21.1.1.

21.2. Contingências de Pessoal

Este tipo de contingência será acionada nos casos em que colaboradores-chave não estiverem presentes por motivos de greves, doença, licenças, entre outros.

O Diretor de Risco, *Compliance* e PLDFT terá a senha de acesso aos sistemas utilizados por colaboradores-chave. Em paralelo, haverá outro colaborador devidamente treinado para o exercício das funções. Em caso de necessidade de substituição, em reunião com o Diretor de Risco, *Compliance* e PLDFT, este poderá conceder o acesso para a continuidade dos trabalhos.

21.2.1. Greves de Transportes Públicos

Em caso de greves de sistemas de transportes públicos, os colaboradores que não se desloquem ao trabalho com veículo próprio, poderão se utilizar de meios alternativos, tais como táxis e aplicativos de transportes, e serão reembolsados pela SIGA, até a normalização da situação.

21.2.2. Licença Médica, Maternidade, Paternidade e Correlatas

As situações de ausência por licenças serão analisadas caso a caso. Os Diretores poderão optar pelas seguintes providências:

(i) Deslocamento de um colaborador para suprimento das funções exercidas pelo colaborador licenciado.
(ii) Contratação de um colaborador temporário em substituição.

Durante o período de licença é ativada uma mensagem de *"Out of Office"* do servidor de e-mail para que e-mails importantes não fiquem sem resposta.

Na mensagem constará o lapso temporal em que o colaborador ficará afastado e indicação de quem contatar durante o período de ausência.

Os acessos aos sistemas integrados à autenticação de rede serão bloqueados a partir da data de entrada em licença.

22. GESTÃO DE RISCOS

A Diretoria de Risco, *Compliance* e PLDFT da SIGA possui responsabilidade pela Gestão de Riscos, em conjunto com o Comitê de *Compliance*, quando convocado, e é encarregada do monitoramento e gerenciamento dos riscos envolvidos na atividade da entidade.

Esta estrutura foi idealizada para garantir que os controles sejam executados sem qualquer interferência dos responsáveis pela gestão das carteiras, de forma independente, evitando interferências no resultado da gestão de riscos, segregando as funções, física e operacionalmente.

Esta política está descrita no Manual de Gestão de Riscos e no Manual de Gestão de Riscos de Liquidez, disponíveis no site da SIGA (www.sigafinance.com.br). Tem como principal objetivo o gerenciamento dos riscos da entidade, contribuindo com atividades de identificação e avaliação de eventos, monitoramento contínuo para controle e mitigação, a fim de reduzir a probabilidade de que estes riscos se materializem ou de amenizar seu impacto.

Os instrumentos de gerenciamento de risco da SIGA incluem estrutura de controles internos revisada periodicamente com vistas à manutenção de um adequado acompanhamento dos riscos operacionais, de crédito, de liquidez, de mercado, de imagem e socioambiental.

Em que pese todo o aparato de controle disponível, e o empenho de sua equipe, os investimentos estão, por sua natureza, sujeitos a flutuações típicas do mercado, risco de crédito, condições adversas de liquidez e negociação atípica nos mercados de atuação e, mesmo que a SIGA mantenha rotinas e procedimentos de gerenciamento de riscos, não há garantia de completa eliminação da possibilidade de perdas.

As funções da Diretoria de Risco, *Compliance* e PLDFT englobam:

i. Garantir que os procedimentos e práticas adotados pelos profissionais estejam de acordo com os limites internos pré-estabelecidos e com aqueles recomendados pelos órgãos reguladores, pelos princípios éticos da SIGA e do mercado;
ii. Monitoramento de risco dos investimentos efetuados sob gestão da SIGA.

iii. Acompanhamento da gestão de valores mobiliários vis-à-vis os seus respectivos mandatos, regras e diretrizes.

A Política relativa aos riscos de Liquidez, Crédito, Mercado, Contraparte, Setor Elétrico e outros estão dispostas, mais bem explicadas, no Manual de Gestão de Riscos, disponibilizado no site da Gestora.

23. DISPOSIÇÕES GERAIS E FINAIS

O desrespeito a quaisquer das regras da SIGA resultarão em Processo Administrativo Interno, podendo imputar sanções internas, de acordo com deliberações da Diretoria, incluindo desligamento.

Eventuais medidas legais poderão ser tomadas pela entidade em face do infrator.

Em caso de dúvidas de interpretação ou eventuais antinomias entre as regras aqui dispostas e outras vigentes na entidade, deverá haver consulta imediata ao Diretor de Risco, *Compliance* e PLDFT.

Quaisquer alterações legais ou normativas expedidas pelos órgãos regulamentadores e competentes serão aplicadas imediatamente a esta política, e todos os colaboradores serão imediatamente alertados de eventuais mudanças.

Eventuais dúvidas deverão ser encaminhadas à Diretoria de Risco, *Compliance* e PLDFT, por intermédio do e-mail matheus.cardoso@sigafinance.com.br ou pelo telefone (41) 3044-7464.