

Jive Investments Gestão de Recursos e Consultoria S.A.

Jive High Yield Gestão de Recursos Ltda.

Mauá Capital Investimentos Alternativos Ltda.

Mauá Capital Real Estate Ltda.

Política de Prevenção à Lavagem de Dinheiro, Combate ao Financiamento do Terrorismo e ao Financiamento da Proliferação de Armas de Destruição em Massa (“PLD/FTP”)

Este documento foi elaborado e é periodicamente atualizado pela Jive Investments Gestão de Recursos e Consultoria S.A., sendo aplicável a todas as empresas que compõem o grupo JiveMauá, incluindo as entidades legais listadas acima. As informações aqui apresentadas poderão ser alteradas a qualquer momento, sem necessidade de aviso prévio. É proibida a reprodução, alteração ou transmissão deste documento, total ou parcialmente, por qualquer meio ou forma, sem a autorização expressa da JiveMauá.

Última revisão: janeiro de 2026

Versão 6.0

Responsável pela elaboração: Departamento de Governança, Riscos e Compliance

Responsáveis pela aprovação: Comitê de Compliance e Riscos Corporativos e Comitê Executivo

Sumário

1.	Objetivo.....	3
2.	Introdução	3
3.	Papéis e Responsabilidades	4
4.	Avaliação Interna de Risco de LD/FTP (AIR)	5
4.1.	Avaliação de Risco de LD/FTP de Investimentos	5
4.2.	Avaliação de Prestadores de Serviços Essenciais de Demais Parceiros (KYP)	6
4.3.	Avaliação de Fornecedores (KYS)	7
4.4.	Avaliação de Colaboradores (KYE).....	7
4.5.	Avaliação de Clientes e Investidores (KYC).....	8
5.	Abordagem Baseada em Risco (ABR)	8
5.1.	Identificação de Beneficiário Final.....	9
5.2.	Pessoas Politicamente Expostas (PEP)	9
5.3.	Listas Restritivas e Sancionadoras	10
6.	Reporte de Transações Suspeitas.....	10
7.	Relatório Anual de Avaliação de Risco de LD/FTP	10
8.	Treinamentos.....	11
9.	Sanções	11
10.	Base Regulamentar	11
11.	Aprovações.....	12
12.	Glossário	12
13.	Atualização e Vigência.....	13
14.	Histórico de Versões	14

1. Objetivo

Esta Política tem como objetivo estabelecer diretrizes, regras e procedimentos que garantam a adoção das melhores práticas e a adequação das atividades da companhia às exigências legais e regulatórias referentes à prevenção e combate à lavagem de dinheiro, ao financiamento do terrorismo e à proliferação de armas de destruição em massa (ou simplesmente *Lavagem de Dinheiro* ou *LD/FTP*).

Com esse propósito, a presente Política se aplica a todos os administradores, colaboradores, terceiros, fornecedores, prestadores de serviços e parceiros de negócios da JiveMauá. Seu conhecimento é essencial para assegurar que todos os envolvidos estejam alinhados e cumpram integralmente as diretrizes e padrões definidos pela Instituição.

2. Introdução

O crime de lavagem de dinheiro (LD) consiste na atividade criminosa de disfarçar a origem de recursos financeiros ao ocultar ou dissimular a natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente, de atividade ilegal.

Já os crimes de financiamento ao terrorismo e à proliferação de armas de destruição em massa (FTP) consistem em atos voltados a prover, coletar, disponibilizar ou gerenciar recursos financeiros, bens ou valores com a finalidade de apoiar a prática de atividades terroristas ou o desenvolvimento, aquisição e transporte ilícitos de armas nucleares, químicas ou biológicas, podendo esses recursos serem de origem ilícita ou lícita.

As seguintes etapas compõem o processo de dissimulação da origem e/ou finalidade ilegal dos recursos movimentados que configuram os crimes de LD/FTP:

- i. **Colocação:** é a etapa inicial em que os recursos obtidos ilegalmente são colocados no sistema financeiro ou economia formal;
- ii. **Ocultação:** fase em que são realizadas transações econômicas e financeiras para dificultar o rastreamento dos recursos e ocultar seu vínculo com as atividades ilícitas que lhe deram origem;
- iii. **Integração:** etapa em que os recursos aparentemente lícitos passam a integrar os sistemas econômico e financeiro formais.

A fim de prevenir o envolvimento de suas empresas e fundos sob gestão em operações de Lavagem de Dinheiro, a JiveMauá estabeleceu governança formal e documentada através dessa política, definição de papéis e responsabilidades das estruturas organizacionais e processos de avaliação, mitigação, monitoramento e reporte para órgãos internos e externos.

3. Papéis e Responsabilidades

A estrutura organizacional da JiveMauá possui diferentes responsabilidades no combate aos crimes de LD/FTP, conforme detalhado a seguir:

Comitê Executivo:

- Estabelecer as diretrizes corporativas para prevenção aos crimes de LD/FTP;
- Nomear os membros do Comitê de Compliance e Riscos Corporativos;
- Receber o relatório anual de avaliação de risco LD/FTP e adotar as medidas necessárias, quando aplicável.

Comitê de Compliance e Riscos Corporativos:

- Zelar pelo cumprimento das diretrizes estabelecidas na presente Política;
- Monitorar os indicadores de processos, avaliar a qualidade do ambiente de controles e acompanhar os planos de ação necessários;
- Deliberar sobre contestações à classificação de risco definidas pelo DGRC;
- Receber o relatório anual de risco de LD/FTP e emitir recomendações à Diretoria de Compliance e PLD/FTP e ao Comitê Executivo, quando necessário.

Diretoria de Compliance e PLD/FTP:

- Implementar e zelar pelo cumprimento das diretrizes estabelecidas na presente Política;
- Atuar para garantir estrutura suficiente para execução das atividades de PLD/FTP;
- Monitorar os indicadores de processos e aprovar os planos de ação propostos para melhoria do ambiente de controles;
- Avaliar e aprovar a classificação de risco propostas para as operações;
- Decidir sobre a comunicação de situações suspeitas ao COAF;
- Enviar relatório anual de avaliação do risco LD/FTP aos órgãos de administração da companhia.

Departamento de Governança, Riscos e Compliance (DGRC):

- Garantir a atualização e adequação da presente Política;
- Implementar processo de avaliação e monitoramento de risco de operações e parceiros de negócios;

- Estabelecer e reportar indicadores de processos e definir planos de ação para melhoria do ambiente de controles de PLD/FT;
- Disponibilizar treinamentos que promovam a conscientização sobre a legislação de PLD/FTP;
- Investigar denúncias ou suspeitas de violação dos termos da presente Política e reportar suas conclusões ao Comitê de Compliance e Riscos Corporativos;
- Elaborar e apresentar relatório anual de avaliação do risco LD/FTP ao Diretor de Compliance e PLD/FTP.

Business Units (BUs):

- Providenciar os documentos e informações necessários para a avaliação de risco dos relacionamentos antes de sua apresentação aos Comitês de Investimentos e Desinvestimentos;
- Comunicar ao DGRC situações suspeitas de práticas dos crimes de LD/FTP.

Colaboradores:

- Ter conhecimento das diretrizes da presente Política;
- Realizar os treinamentos disponibilizados pela companhia;
- Comunicar ao DGRC situações suspeitas de práticas dos crimes de LD/FTP.

4. Avaliação Interna de Risco de LD/FTP (AIR)

Todos os novos relacionamentos, estabelecidos pela JiveMauá e fundos sob gestão, devem ser previamente avaliados sob a perspectiva de LD/FTP, incluindo a identificação dos beneficiários finais. Para isso, foram definidos processos específicos para a análise de investimentos, prestadores de serviços essenciais, fornecedores, colaboradores e clientes, em um fluxo sistemático e contínuo de avaliação, mitigação, monitoramento e reporte.

Cada avaliação resulta em uma classificação de risco, que determina a alçada de aprovação do relacionamento e a periodicidade de sua revisão. Essa revisão será realizada, no máximo, a cada dois anos, ou sempre que houver alterações significativas nos perfis de risco que a fundamentam.

O detalhamento técnico e operacional dos processos de avaliação de risco de LD/FTP devem ser formalmente documentados em manuais de procedimentos complementares a esta Política.

4.1. Avaliação de Risco de LD/FTP de Investimentos

Todos os investimentos realizados pelos fundos sob gestão são avaliados e aprovados pelos Comitês de Investimentos das respectivas *Business Units*.

Para aprovação do Comitê de Investimentos, todas as oportunidades deverão ser previamente submetidas a análise do DGRC para fins de identificação de aspectos relacionados aos crimes de LD/FTP. Essa análise considera:

- Setor econômico de atuação;
- Jurisdição e região geográfica;
- Citação em processos Judiciais e/ou Administrativos;
- Presença em listas restritivas;
- Exposição política e eleitoral;
- Existência de notícias desabonadoras.

Caso sejam identificadas situações atípicas, o DGRC entrará em contato com o proponente da operação para solicitar informações e documentos adicionais que subsidiem a classificação de risco.

Os resultados dessas análises, conforme a Régua de Classificação de Risco de LD/FTP, são disponibilizados aos membros do Comitê de Investimentos, com o objetivo de subsidiar o processo de tomada de decisão.

Investimentos classificados como de risco alto ou crítico devem ser previamente submetidos ao Diretor de Compliance e PLD/FTP e, após aprovação pelo Comitê de Investimentos, apresentados ao Comitê de Compliance e Riscos Corporativos, que poderá determinar condicionantes para a efetivação da operação ou solicitar que sua aprovação seja submetida também ao Comitê Executivo.

Para investimentos em que não seja possível realizar avaliação individualizada dos emissores - como Certificados de Recebíveis Imobiliários (CRI) pulverizados - a classificação de risco será atribuída conforme avaliação da robustez das políticas e procedimentos de PLD/FTP dos prestadores de serviço associados à sua emissão (por exemplo, empresa securitizadora ou banco coordenador).

A solicitação de avaliação prévia do risco de LD/FTP é de responsabilidade da *Business Unit* proponente do investimento, que deve disponibilizar as informações necessárias para identificação e análise das partes relacionadas envolvidas na operação.

4.2. Avaliação de Prestadores de Serviços Essenciais de Demais Parceiros (KYP)

A JiveMauá reconhece a importância da adoção de medidas preventivas também em seus relacionamentos institucionais, especialmente prestadores de serviços essenciais, distribuidores, empresas securitizadoras ou quaisquer outras partes externas com as quais mantém relação

contratual ou estratégica. Nesse sentido, adota práticas estruturadas de “Know Your Partner” (KYP) como parte integrante do seu programa de PLD/FT.

O Procedimento de KYP visa garantir que todos os parceiros de negócio da JiveMauá sejam previamente avaliados quanto à sua integridade, reputação, estrutura de governança, origem de recursos, atividades desempenhadas e histórico de conformidade legal e regulatória, reduzindo a exposição a riscos legais, reputacionais e operacionais relacionados à PLD/FT.

Assim, conforme estabelecido na “Política de Seleção, Contratação e Monitoramento de Terceiros”, a avaliação desses parceiros é realizada por meio do envio de um questionário de *due diligence* e da análise de suas políticas e documentos institucionais. Quando necessário, também são realizadas reuniões para detalhamento dos pontos avaliados.

4.3. Avaliação de Fornecedores (KYS)

A JiveMauá adota medidas preventivas na seleção, contratação e manutenção de fornecedores, com o objetivo de garantir a integridade das relações comerciais, prevenir riscos de envolvimento com atividades ilícitas e assegurar o cumprimento das normas legais e regulatórias aplicáveis, especialmente no que se refere à PLD/FTP.

Aplica-se a todos os fornecedores de bens e serviços contratados diretamente pela JiveMauá ou pelos fundos sob sua gestão, incluindo, mas não se limitando a:

- Pessoas jurídicas e físicas;
- Prestadores de serviços especializados;
- Fornecedores estratégicos ou recorrentes;
- Fornecedores locais e internacionais.

A avaliação deve ser solicitada, pela área responsável pela contratação, antes da efetiva aquisição dos bens e/ou serviços, mediante o registro das informações necessárias no sistema de cadastro de fornecedores. A ausência dessa solicitação impedirá a liquidação dos pagamentos devidos até a regularização da situação.

4.4. Avaliação de Colaboradores (KYE)

No contexto de seu programa de PLD/FTP, a JiveMauá adota práticas rigorosas de identificação, verificação e monitoramento de seus colaboradores (“Know Your Employee”), com o objetivo de assegurar a integridade, a idoneidade e a conformidade ética de seu quadro funcional.

O Procedimento de KYE visa assegurar que todos os profissionais vinculados à JiveMauá possuam reputação ilibada, estejam alinhados com os valores éticos e legais da instituição e não representem risco de envolvimento com atividades ilícitas, inclusive relacionadas à PLD/FTP.

São considerados colaboradores, da JiveMauá:

- Sócios e diretores da companhia;
- Membros do conselho de administração;
- Empregados formais;
- Estagiários;
- Prestadores de serviço que atuem em nome da Instituição.

Todos os profissionais são avaliados previamente à sua contratação, a qual é revisada, no mínimo, anualmente.

4.5. Avaliação de Clientes e Investidores (KYC)

São considerados clientes da JiveMauá as contrapartes, pessoas naturais ou jurídicas, que adquiram ativos pertencentes aos fundos sob gestão - por exemplo, aquisição ou locação de imóveis, precatórios ou outros títulos de dívida não negociados em mercado organizado.

Também são enquadrados como clientes os investidores, pessoas naturais ou jurídicas, com os quais exista relacionamento comercial direto, incluindo, quando aplicável, cotistas de fundos ou veículos de investimento exclusivos e/ou restritos.

Nesses casos, cabe às áreas comerciais das *Business Units* realizar a identificação e avaliação destas contrapartes, bem como a formalizar contratualmente a negociação, podendo, a seu critério, comunicar o DGRC para análise complementar, quando julgarem necessário.

Nos demais casos, que não se enquadrem nas hipóteses acima, a responsabilidade pela fiscalização do passivo é atribuída aos administradores e distribuidores, os quais devem dispor de políticas e procedimentos próprios de identificação de clientes e prevenção ao risco de LD/FTP.

5. Abordagem Baseada em Risco (ABR)

A JiveMauá adota metodologia de abordagem baseada em risco (ABR) para implementação de medidas preventivas e controles proporcionais à classificação de risco de suas contrapartes.

Assim, conforme classificação de risco, as diferentes instâncias de governança de PLD/FTP da companhia podem determinar condições precedentes ao estabelecimento do relacionamento ou efetivação do investimento.

Também conforme critérios de ABR são estabelecidos os prazos máximos de revisão da classificação de risco destes relacionamentos, conforme abaixo:

- Risco Crítico: a cada 06 meses;
- Risco Alto: a cada 06 meses;
- Risco Médio: a cada 12 meses;
- Risco baixo: a cada 24 meses.

5.1. Identificação de Beneficiário Final

Os procedimentos de qualificação das partes relacionadas que sejam pessoas jurídicas contemplam a análise completa da cadeia societária, até a identificação da pessoa natural que se enquadre como Beneficiário Final.

Cada beneficiário final é submetido a análise de risco considerando jurisdição, setor de atuação, participações societárias, histórico de exposição política, consulta a listas restritivas nacionais e internacionais, informações públicas e registros corporativos, bem como informações de distribuição de processos judiciais e administrativos.

Todas as informações relativas aos beneficiários finais são revisadas periodicamente e sempre que houver alterações relevantes na estrutura de propriedade ou operação. Situações de maior risco podem resultar em solicitações de informações adicionais, restrições a operações ou comunicação às autoridades competentes.

5.2. Pessoas Politicamente Expostas (PEP)

Para fins de PLD/FTP, a JiveMauá adota cuidados específicos ao analisar operações envolvendo pessoas politicamente expostas (“PEP”), conforme definido na regulamentação aplicável.

Todas as contrapartes, colaboradores, parceiros de negócios e fornecedores são avaliados quanto ao status de PEP. As informações coletadas incluem dados pessoais, informações de familiares e colaboradores próximos, bem como dados de empresas e veículos de investimento nos quais a PEP exerça influência relevante.

As PEPs e suas operações são acompanhadas de forma contínua, com revisões periódicas ou sempre que ocorrerem fatos relevantes que possam alterar o risco. Em situações de maior risco, a JiveMauá pode solicitar informações adicionais, restringir operações e comunicar autoridades competentes.

Ressalta-se que todos os dados, análises e decisões, envolvendo Pessoas Politicamente Expostas, são registrados para assegurar rastreabilidade e conformidade com a regulamentação vigente.

5.3. Listas Restritivas e Sancionadoras

A JiveMauá verifica todas as listas restritivas e sancionadoras, nacionais e internacionais, para todas as contrapartes, colaboradores, parceiros de negócios e fornecedores com as quais mantém relacionamento.

Caso seja identificado qualquer apontamento em listas restritiva ou sancionadora, a JiveMauá realiza análise detalhada para determinar o impacto sobre a operação, considerando os riscos legais, regulatórios e reputacionais. Conforme resultado da análise, podem ser adotadas medidas como recusa, bloqueio ou suspensão de operações ou relacionamentos.

6. Reporte de Transações Suspeitas

Quaisquer operações, situações ou propostas de negócios que possam configurar suspeita de cometimento de crimes relacionados a LD/FTP, envolvendo a Companhia ou os fundos sob gestão, devem ser imediatamente comunicadas ao DGRC para registro e análise dos indícios.

A análise conduzida pelo DGRC deve ser fundamentada e conter, no mínimo:

- (i) data de início do relacionamento com as partes envolvidas;
- (ii) a descrição dos sinais de alerta identificados;
- (iii) a caracterização detalhada da operação; e
- (iv) as qualificações e informações obtidas nos processos de diligência realizados.

As conclusões do DGRC devem ser apresentadas ao Diretor de Compliance e PLD/FTP, responsável pela decisão e aprovação de comunicação ao Conselho de Controle de Atividades Financeiras (COAF), a qual deverá ocorrer no prazo de até 24 horas.

Após a efetivação da comunicação, esta deve ser reportada aos membros do Comitê Executivo e do Comitê de Compliance e Riscos Corporativos.

Todas as pessoas envolvidas no processo de análise, decisão ou comunicação, ou que tenham tomado conhecimento da ocorrência, devem manter absoluto sigilo, abstendo-se de dar ciência do fato a terceiros, inclusive àqueles a quem a informação se refira.

7. Relatório Anual de Avaliação de Risco de LD/FTP

O Diretor de Compliance e PLD/FTP deve elaborar relatório anual de avaliação interna de risco de LD/FTP e disponibilizá-lo aos membros do Comitê Executivo e do Comitê de Compliance e Riscos Corporativos, nos termos do Art. 6º da Resolução CVM 50/2021, com destaque para:

- (i) A identificação e análise das situações de risco de LD/FTP, considerando as respectivas ameaças, vulnerabilidades e consequências;
- (ii) Efetividade das recomendações e correções adotadas em relação às fragilidades apontadas nos anos anteriores;
- (iii) Volumetria de operações, análises, situações atípicas detectadas e comunicações ao COAF;
- (iv) A avaliação dos procedimentos de KYC, KYP, KYS e KYE;
- (v) Medidas de desenvolvimento da cultura organizacional e programas de capacitação.

O Relatório de PLD/FTP ficará à disposição da CVM e, quando aplicável, de entidades autorreguladoras, podendo ser elaborado em documento único ou integrar o relatório previsto no art. 25 da Resolução CVM 21/21, conforme regulamentação aplicável.

8. Treinamentos

O DGRC deverá manter um programa contínuo de treinamento, obrigatório para todos os colaboradores, com objetivo de divulgar essa Política, bem como suas regras, procedimentos e controles internos.

9. Sanções

Qualquer ato ou indício de conduta em desacordo com esta Política será devidamente apurado e poderá resultar na aplicação de sanções, conforme previsto na legislação vigente e nas disposições aqui estabelecidas. As penalidades podem incluir o desligamento por justa causa, no caso de colaboradores empregados da JiveMauá, e, no caso de sócios, a exclusão do quadro societário por justa causa, sem prejuízo das demais consequências legais cabíveis, inclusive de natureza criminal, conforme a gravidade da infração.

10. Base Regulamentar

- Lei nº 9.613, de 03 de março de 1998;
- Resolução CVM nº 21, de 25 de fevereiro de 2021;
- Resolução CVM nº 50, de 31 de agosto de 2021, com as alterações introduzidas pela Resolução CVM Nº 179/23;
- Guia de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo no Mercado de Capitais Brasileiro divulgado pela ANBIMA.

11. Aprovações

Esta Política deverá ser aprovada pela maioria simples dos membros do Comitê de Compliance e Riscos Corporativos e do Comitê Executivo, por meio de ferramenta eletrônica. As aprovações ficarão armazenadas e poderão ser consultadas na própria ferramenta.

12. Glossário

Abordagem Baseada em Risco (ABR): metodologia que permite que as medidas de prevenção à lavagem de dinheiro e financiamento ao terrorismo (PLD/FTP) sejam aplicadas de forma proporcional à natureza dos riscos, tornando mais eficientes os procedimentos implementados;

Avaliação Interna de Risco (AIR): processo contínuo e documentado de identificação, mensuração e gestão dos riscos de exposição a LD/FTP, considerando as características, produtos, serviços, clientes e operações da instituição;

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

Ambiente de Negociação de Ativos: entende-se como ambientes de negociação na Bolsa de Valores;

Administradores: são os sócios, comitê executivo e conselho de administração da JiveMauá;

Background Check: processo de avaliação sistemática para verificação de antecedentes e idoneidade de parceiros comerciais.

Beneficiário Final: a pessoa física que, em última instância, possui ou controla uma empresa, organização ou ativo, mesmo que essa pessoa não apareça diretamente como dona nos documentos oficiais;

CVM: Comissão de Valores Mobiliários;

Colaboradores: todos os sócios, diretores, empregados e estagiários da JiveMauá;

DGRC: Departamento de Governança, Riscos e Compliance;

FTP: Financiamento ao Terrorismo e Proliferação de Armas de Destruição em Massa - consiste no ato de prover, arrecadar ou disponibilizar recursos financeiros ou bens com a intenção de apoiar, direta ou indiretamente, a prática de atos terroristas ou financiamento da proliferação de armas de destruição em massa. Esses recursos podem ser usados para planejar, preparar ou executar ações terroristas, bem como para manter grupos ou indivíduos ligados ao terrorismo, e podem ser de origem ilícita ou lícita;

Fundo Exclusivo: fundo, classe ou subclasse de cotas constituído para receber aplicações exclusivamente de um único investidor profissional, de cotistas que possuam vínculo societário familiar ou de cotistas vinculados por interesse único indissociável;

Fundo Restrito: fundo, classe ou subclasse de cotas constituído para admitir um número limitado de cotistas e distribui cotas exclusivamente para investidores previamente determinados.

Indie Asset Pro (Indie): plataforma de gestão de investimentos e onde são registradas as características das operações, suas partes relacionadas e onde as avaliações de *Background Check* são registradas;

LD: Lavagem de Dinheiro - consiste na atividade criminosa de disfarçar a origem ilícita de recursos financeiros de forma a parecerem de origem legal;

Pessoa Exposta Politicamente (“PEP”): toda pessoa natural que desempenha ou tenha desempenhado nos últimos 5 (cinco) anos funções públicas relevantes, no Brasil ou no exterior, assim como seus representantes, familiares e pessoas de seu relacionamento próximo;

Red Flags: apontamentos verificados sobre determinado Contato. Tais apontamentos podem ser processos, mídias desabonadoras, presença em listas restritivas (OFAC; IBAMA; etc.) ou mesmo o fato de o Contato ser PEP ou relacionado a uma PEP (grau de parentesco ou possuir sociedade empresarial).

13. Atualização e Vigência

Esta Política será revisada, no mínimo, a cada 2 (dois) anos ou sempre que necessário, em razão de alterações regulatórias, mudanças relevantes nas atividades da Companhia ou por deliberação dos órgãos de governança competentes.

14. Histórico de Versões

Versão	Data de Aprovação	Autor/Modificador	Motivo da Alteração
v.01	2020	DGRC	<ul style="list-style-type: none"> • Versão inicial
v.02	11/2021	DGRC	<ul style="list-style-type: none"> • Reestruturação da Política. • Alteração para atendimento à Resolução CVM nº 50, inclusive do nome da Política para inclusão do termo “FTP”. • Inclusão dos itens 1; 3; 4; 5; 9; 10;11; 13; 14. • Especial atenção às inclusões dos capítulos 9 (Abordagem Baseado a Risco) e 10 (Treinamento), a fim de refletir recomendações da consultoria RRZ. • Para o capítulo 6 foi adicionada a necessidade de inclusão de cláusula anticorrupção em contratos de prestadores de serviço. • O capítulo 11 foi incluído visto a experiências de boas práticas de mercado.
v.03	10/2022	DGRC e Cascione Advogados	<ul style="list-style-type: none"> • Revisão anual.
v.04	03/2024	DGRC	<ul style="list-style-type: none"> • Revisão anual.
v.05	05/2025	DGRC	<ul style="list-style-type: none"> • Revisão anual. • Inclusão dos termos das Legislações Anticorrupção; e • Revisão de responsabilidades
v.06	01/2026	DGRC	<ul style="list-style-type: none"> • Exclusão dos temas relacionados a Anticorrupção. • Revisão Capítulo 3 (papéis e Responsabilidades); 4 (avaliação interna de risco); 5 (abordagem baseada em risco); 6 (relatório de transações suspeitas) e 7 (relatório anual).