HORIZONTES ASSET LTDA.

MANUAL DE COMPLIANCE E CONTROLES INTERNOS

Versão	2.0
Data-base	Maio/2026
Elaboração	Projeto de estruturação jurídico-regulatória e de governança
Classificação	Documento interno / base institucional para uso regulatório, autorregulatório e de diligência.
Objetivo	Estabelecer a estrutura e os ritos de compliance e controles internos da gestora.
Abrangência	Aplicável a toda a gestora e, por reflexo, aos terceiros e fóruns submetidos aos seus controles.
Responsável	Diretoria de Compliance, Risco e PLD/FTP
Aprovador	Diretoria Executiva
Base normativa principal	Resolução CVM 21; Código ANBIMA de Administração e Gestão de Recursos de Terceiros; Regras e Procedimentos de Deveres Básicos; Lei nº 13.709/2018 (LGPD).

1. Objeto e premissas de governança

Este Manual de Compliance e Controles Internos disciplina a forma pela qual a HORIZONTES ASSET LTDA. implementa, executa, monitora e prova a observância das normas externas e internas aplicáveis à atividade de gestão de recursos. O manual foi redigido para uma gestora que se encontra em fase final de implantação operacional, e necessita demonstrar, perante ANBIMA, CVM, prestadores essenciais e investidores, como pretende atuar desde o primeiro fundo sob gestão.

O documento fixa responsabilidades, ritos de aprovação, fluxos de revisão, periodicidades mínimas, escaladas, evidências e interfaces com as demais políticas da casa. Por essa razão, a sua leitura deve ser feita em conjunto com o Código de Ética, a Política de Riscos, a Política de Crédito, o Manual de Liquidez, a Política de PLD/FTP, a Política de Conflitos,

a Política de Terceiros, o Regimento dos Comitês, a Política de Segurança Cibernética e o Plano de Continuidade de Negócios.

Os documentos do presente pacote foram redigidos para funcionar como um sistema único. O Diretor de Gestão conduz a formulação da tese, o apoio de gestão e os analistas estruturam memorandos e diligências, o middle office formaliza a trilha operacional e de arquivo, a Diretora de Compliance, Risco e PLD/FTP atua de forma independente na verificação de aderência normativa, de risco e de conflitos, e o Diretor Executivo responde pela coordenação institucional, pela aprovação das contratações críticas e pelo endereçamento das matérias estratégicas ou sensíveis. Nenhum documento deve ser lido isoladamente; sempre que uma matéria envolver crédito, liquidez, conflito, barreiras de informação, contratação de terceiros, PLD/FTP ou deliberação em comitê, aplica-se interpretação conjunta das políticas.

2. Estrutura de compliance, independência e reporte

A função de compliance é exercida pela Diretora de Compliance, Risco e PLD/FTP, com independência em relação à gestão, à captação e à eventual distribuição própria. Essa independência não significa isolamento operacional; significa liberdade técnica para requisitar informações, revisar documentos, escalar divergências, recomendar suspensão de operação, exigir reforço de controles e reportar diretamente à administração sem necessidade de anuência prévia da gestão.

No desenho atual da Horizontes, a Diretora de Compliance, Risco e PLD/FTP conta com apoio funcional do middle office para organização de evidências e controle de agendas, sem prejuízo da sua autonomia decisória. O Diretor Executivo responde pelo suporte institucional à função de compliance, garantindo recursos, prioridade de pauta e implementação dos planos de ação aprovados. O Diretor de Gestão, por sua vez, tem dever positivo de cooperação e de resposta tempestiva às recomendações, sem poder limitar a independência do controle.

O reporte ordinário de compliance ocorrerá por meio de relatórios periódicos, registros de exceção, atas do Comitê de Risco, Compliance e PLD/FTP, logs de treinamentos e monitoramentos temáticos. O reporte extraordinário ocorrerá sempre que houver indício de infração regulatória, conflito material, falha relevante de processo, incidente com impacto reputacional ou qualquer evento que possa comprometer a regularidade da atividade.

3. Eixos permanentes de controle

3.1 Monitoramento regulatório e autorregulatório

A área de compliance manterá acompanhamento contínuo de alterações legislativas, regulamentares e autorregulatórias relevantes para a atividade da gestora, com especial atenção à Resolução CVM 21, à Resolução CVM 50, à Resolução CVM 175 e seus anexos, ao Código ANBIMA de Administração e Gestão de Recursos de Terceiros, às Regras e Procedimentos de AGRT e aos Deveres Básicos. Alterações materiais deverão ser consolidadas em memorando de impacto, acompanhadas de plano de atualização documental e, quando necessário, submetidas ao Comitê de Risco, Compliance e PLD/FTP e à Diretoria Executiva.

Esse monitoramento não se limitará a normas abstratas. Também deverão ser observados os documentos dos fundos, contratos de prestadores, acordos operacionais, obrigações cadastrais, prazos de envio de informações, exigências recebidas de administradores fiduciários e orientações emitidas em diligências, auditorias ou processos de onboarding.

3.2 Controle de políticas, procedimentos e versionamento

Todas as políticas da gestora deverão ter versão vigente, data de aprovação, histórico de revisões, responsável funcional e evidência de ciência dos destinatários relevantes. Alterações materiais não podem ser feitas por circulação informal de arquivo, edição sem controle ou uso simultâneo de versões conflitantes. Nicole responderá pelo controle administrativo de versões e Giulia pelo arquivo operacional, cabendo à Diretora de Compliance, Risco e PLD/FTP validar qual é a versão vigente para fins de uso regulatório e diligência.

Sempre que uma política depender de outra para produzir efeito, a revisão deverá ser coordenada. Assim, revisão da política de crédito exige verificação de reflexos em riscos, conflitos, terceiros, comitês e PLD/FTP; revisão do manual de liquidez exige checagem de interface com gestão, middle office e administrador fiduciário; e revisão da política de voto exige aderência à estrutura de comitês e ao disclosure público.

3.3 Aprovação de materiais públicos e institucionais

Nenhum material institucional, comercial, de roadshow, website, FAQ, memorial de produto ou resposta formal a due diligence poderá ser divulgado sem revisão de compliance quando contiver informação regulatória, descrição de serviços, menção a performance, estrutura de governança, pessoas-chave, produtos, autorizações, adesões

a códigos, conflito de interesses ou qualquer informação capaz de criar expectativa legítima em investidor, parceiro ou regulador.

A revisão de compliance verificará coerência com contrato social, cadastros, website, formulário de referência, QDD, políticas internas e documentos dos veículos. Divergência material deverá ser tratada como não conformidade. O objetivo não é burocratizar a comunicação, mas evitar que o ambiente público conte uma história incompatível com a estrutura formal ou com a realidade operacional da gestora.

3.4 Onboarding, treinamento e offboarding

O ingresso de qualquer profissional ou terceiro com acesso a informação sensível dependerá, no mínimo, de cadastro interno, termo de confidencialidade, termo de adesão ao Código de Ética, termo de ciência das políticas aplicáveis à função, definição formal de acessos sistêmicos e participação em treinamento inicial. O treinamento mínimo deverá abranger ética, conflito de interesses, segurança de informação, PLD/FTP, reporte de incidentes, negociação pessoal e fluxos de comitês.

No desligamento, Giulia e Nicole deverão executar checklist de encerramento que contemple revogação de acessos, devolução de equipamentos e documentos, confirmação de arquivamento de materiais sob guarda do desligado, atualização da lista de pessoas cobertas pela política de negociação pessoal e manutenção do dever de sigilo após o término do vínculo.

3.5 Infraestrutura tecnológica e prestadores críticos de TI

A Gestora opera sobre infraestrutura tecnológica corporativa hospedada em provedor de nuvem (Amazon Web Services - AWS), implantada e suportada por prestadores formalmente contratados, observadas as diretrizes específicas estabelecidas na Política de Segurança Cibernética e no Plano de Continuidade de Negócios. Os prestadores críticos de tecnologia da informação atualmente contratados são: (i) BAlves Gestão em TI, responsável pela implantação e arquitetura da infraestrutura cloud; (ii) Manucom Tecnologia Ltda., responsável pelo suporte técnico (manutenção preventiva e corretiva), com SLAs por gravidade do incidente; e (iii) Nullpointer (em fase de formalização contratual e implantação), responsável pela plataforma operacional especializada NPFlow + Sentinela + Gestora App, voltada à execução, controle e monitoramento das atividades de gestão de FIDC. A Diretora de Compliance, Risco e PLD/FTP supervisiona a aderência desses prestadores às exigências regulatórias e contratuais, observada reavaliação periódica.

4. Programa de controles internos

O programa de controles internos será executado com base em matriz anual e testes temáticos. A intensidade dos testes deverá acompanhar a materialidade do risco e o estágio da operação. Na fase pré-operacional, o foco recairá sobre readiness documental, treinamento, segregação, cadastros, políticas, contratos de terceiros e website regulatório. Na fase operacional, o foco passará também a abranger enquadramento, atas, alocações, controles de ordens, dossiês de crédito, monitoramento de prestadores, incidentes, conflitos concretos e cumprimento de obrigações periódicas.

Os testes deverão registrar objetivo, universo, evidências analisadas, achados, criticidade, responsável pela remediação e prazo. Não conformidades críticas deverão ser imediatamente comunicadas ao Diretor Executivo e, quando impactarem atividade-fim ou decisão de investimento, também ao Diretor de Gestão. Não se admite arquivamento de achado crítico sem plano formal de tratamento.

Eixo de controle	Exemplos de verificação
Governança documental	versão vigente de políticas, assinaturas, ciência, histórico de revisão e compatibilidade entre documentos
Fluxos de comitês	convocação, quórum, atas, materiais de suporte, recusas por conflito e implementação das deliberações
Operação e middle office	captura de ordens, reconciliação, arquivo, interface com prestadores e trilha de execução
Crédito e ativos reais	dossiês de elegibilidade, pareceres, laudos, memórias de comitê e monitoramento de ativos
Website e divulgação	coerência entre documentos públicos, cadastros, FR, QDD e materiais institucionais
Pessoas e acessos	treinamento, termos, acessos sistêmicos, listas restritas e offboarding
Infraestrutura tecnológica e segurança cibernética	aderência aos controles previstos na Política de Cyber, testes de restauração de backup, revisão de privilégios de acesso, reavaliação de prestadores críticos de TI

5. Integração com risco, crédito, PLD/FTP e comitês

O manual de compliance parte da premissa de que os controles internos da gestora não se esgotam em uma área única. O controle efetivo resulta da interação entre gestão, risco, middle office, jurídico e PLD/FTP. Por isso, a Diretora de Compliance, Risco e PLD/FTP

participa, como observadora ou presidente conforme o caso, dos fóruns em que podem surgir conflitos, descumprimentos ou concentração excessiva de poder decisório.

No Comitê de Investimentos, a presença de compliance tem função de resguardo do processo, não de co-gestão. No Comitê de Crédito e Elegibilidade, o papel é verificar integridade do rito, conflito, documentação e aderência à política. No Comitê Imobiliário, o papel é controlar especialmente conflitos estruturais, independência de laudos e trilha de diligência. No Comitê de Risco, Compliance e PLD/FTP, a função é deliberar sobre achados, planos de ação, incidentes e exceções. A gestão conserva a competência decisória de investimento; compliance conserva a competência de controle e escalada.

A função de compliance acumula, também, o papel de Encarregada pelo Tratamento de Dados Pessoais (DPO), na forma do art. 41 da Lei nº 13.709/2018 (LGPD), competindo à Diretora de Compliance, Risco e PLD/FTP (Natália Uchôa Brandão) a recepção de comunicações de titulares de dados, a interlocução com a ANPD e a supervisão do cumprimento da LGPD pela Gestora. Os detalhes operacionais dessa função estão previstos na Política de Segurança Cibernética da Gestora.

6. Relatórios, registros e agenda regulatória

A área de compliance manterá agenda regulatória anual com prazos de CVM, ANBIMA e COAF/Siscoaf aplicáveis à gestora e, futuramente, aos veículos. As entregas anuais mínimas incluem, entre outras, formulário de referência, declaração eletrônica de conformidade, relatório anual de compliance e controles internos, relatório anual da AIR de PLD/FTP e comunicação de não ocorrência ou comunicações suspeitas quando exigíveis.

Integram, ainda, o acervo regulatório de compliance: relatórios anuais de testes de segurança cibernética, relatórios de testes de continuidade (BCP), registros de incidentes de TI ou de dados pessoais, e evidências de reavaliação periódica dos prestadores críticos de tecnologia da informação.

Todos os relatórios anuais deverão conter síntese executiva, escopo de testes, conclusões, recomendações, cronograma de saneamento e manifestação dos responsáveis impactados. A forma do relatório deve permitir leitura por auditor, administrador fiduciário, regulador e sócio, sem perda de rigor técnico. Atas, logs de treinamento, registros de exceção, dossiês de revisão de materiais e memorandos regulatórios integram o acervo probatório e deverão ser mantidos pelo prazo legal ou superior quando aplicável.

7. Tratamento de incidentes, irregularidades e remediação

Incidente, para fins deste Manual, é qualquer evento que revele ou possa revelar falha de processo, descumprimento normativo, quebra de sigilo, falha de diligência, atraso regulatório, incongruência pública, indício de fraude, indisciplina operacional, não observância de quórum de comitê, violação de política de negociação pessoal, defasagem de cadastro, falha de terceiros críticos ou insuficiência material de documentação.

Detectado o incidente, a área responsável deverá acionar imediatamente a Diretora de Compliance, Risco e PLD/FTP e preservar evidências. Será aberta ficha de ocorrência com classificação de severidade, descrição dos fatos, providências imediatas, causas prováveis e plano de remediação. Incidentes severos serão levados ao Comitê de Risco, Compliance e PLD/FTP e, se necessário, à Diretoria Executiva no mesmo dia útil ou no primeiro dia útil subsequente.

8. Vigência, revisão e aprovação

Este Manual entra em vigor na data de sua aprovação pela administração e deverá ser observado desde já, inclusive na fase preparatória. A revisão ordinária será anual, sem prejuízo de revisão extraordinária sempre que houver alteração relevante de norma, de escopo, de estrutura societária, de equipe, de produto, de prestador crítico ou de entendimento regulatório.

A aprovação e a revisão deste Manual não eximem qualquer profissional do dever de cumprir diretamente a regulação e a autorregulação vigentes. A ausência de previsão expressa para um fato concreto não autoriza comportamento incompatível com a função fiduciária da gestora.

Anexos operacionais

Anexo I – matriz anual mínima de testes

Trimestre	Tema mínimo	Evidência esperada
1º	website, FR, cadastros e agenda regulatória	prints, protocolos, checklist e validação de consistência
2º	controles de comitês, conflitos e arquivos	atas, dossiês, registros de recusa e trilha de arquivo
3º	terceiros críticos, ordens, middle office e reconciliações	QDDs, contratos, amostras operacionais e evidência de monitoramento

Trimestre	Tema mínimo	Evidência esperada
4º	treinamento, negociação pessoal, listas restritas e revisão documental	planilhas, termos, logs, evidências de atualização e plano de ação

Anexo II – documentos sujeitos a revisão prévia de compliance

Categoria	Exemplos
Públicos	website, formulários, apresentações, FAQs, materiais de captação e press releases
De diligência	QDDs, DDQs, respostas a RFIs, memoriais institucionais, data room e formulários de onboarding
De produto	regulamentos, anexos-classe, prospectos, memorandos de oferta, atas e minutas com investidores
De governança	políticas, regimentos, termos, atas de comitê e comunicações de incidentes relevantes

Histórico de revisões

Versão	Data-base	Aprovação	Principais alterações
1.1	14/04/2026	Diretoria Executiva	Versão anterior em vigor.
2.0	**Maio/2026**	**Diretoria Executiva**	**Inclusão da subseção 3.5 sobre infraestrutura tecnológica e prestadores críticos de TI (AWS, BAlves, Manucom, Nullpointer). Inclusão de linha sobre infraestrutura tecnológica e segurança cibernética na matriz do item 4. Inclusão, no item 5, de previsão sobre acumulação da função de Encarregada pelo Tratamento de Dados Pessoais (DPO/LGPD) pela Diretora de Compliance, Risco e PLD/FTP. Inclusão, no item 6, de referência ao acervo de relatórios de testes de cibersegurança, BCP e LGPD. Atualização da base normativa principal (inclusão da LGPD).**

Aprovação

São Paulo, 19 de maio de 2026.

IRAPUA DE CARVALHO DANTAS:00800251458

Assinado de forma digital por IRAPUA DE CARVALHO DANTAS:00800251458

Irapuã de Carvalho Dantas
Diretor Executivo
Horizontes Asset Ltda.