HORIZONTES ASSET LTDA.

POLÍTICA DE GESTÃO DE RISCOS

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	Definir a estrutura de risco da gestora e a forma de monitoramento das carteiras e da própria instituição.
Abrangência	Aplicável à gestora, aos veículos sob gestão, às classes e aos terceiros relevantes no processo de investimento e operação.
Responsável	Diretoria de Compliance, Risco e PLD/FTP
Aprovador	Diretoria Executiva
Base normativa principal	Resolução CVM 21; Resolução CVM 175; Código ANBIMA de Administração e Gestão de Recursos de Terceiros; Regras e Procedimentos de AGRT.

1. Finalidade, escopo e premissa de aplicação

Esta Política de Gestão de Riscos define a estrutura, a governança, as metodologias e os fluxos de monitoramento que a HORIZONTES ASSET LTDA. adotará para identificar, mensurar, acompanhar, limitar, escalar e reportar os riscos inerentes às atividades de gestão de recursos e às estratégias inicialmente previstas para a casa. A política é aplicável tanto à fase de preparação operacional quanto à fase de operação efetiva dos veículos.

A política foi construída para ser operacional no momento em que a gestora iniciar a administração de classes e fundos. Por essa razão, contém parâmetros e responsabilidades para FIDC consignado público e privado, fundos imobiliários e fundo multimercado, além dos riscos institucionais e operacionais da própria sociedade. Quando

uma estratégia não estiver ativa, a seção correspondente funcionará como regra de readiness, devendo orientar a seleção de prestadores, a configuração sistêmica e a montagem de dossiês.

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, segurança cibernética, continuidade de negócios ou deliberação em comitê, aplica-se interpretação conjunta das políticas.

2. Governança de risco, independência e reporte

A função de risco é exercida pela Diretora de Compliance, Risco e PLD/FTP, com independência em relação à tomada de decisão de investimento e acesso irrestrito às informações necessárias ao desempenho de sua função. A Diretoria de Gestão detém a responsabilidade primária pela conformidade das decisões de alocação aos documentos dos veículos e aos limites aprovados; a área de risco monitora, questiona, valida metodologias, reporta desvios e recomenda medidas de reenquadramento ou bloqueio.

A governança formal de risco será apoiada pelo Comitê de Risco, Compliance e PLD/FTP, que receberá relatórios periódicos, incidentes, testes e escaladas de exceção. A gestão poderá defender teses, propor limites específicos e justificar exceções; contudo, a avaliação independente da área de risco deverá sempre ficar registrada, sobretudo quando houver concentração relevante, liquidez reduzida, ativo estruturado, conflito ou dependência material de premissa sensível.

Os relatórios de risco serão emitidos em frequência mínima mensal para as carteiras sob gestão, sem prejuízo de relatórios extraordinários quando a materialidade do evento assim exigir. Na fase pré-operacional, a área de risco produzirá relatórios de readiness sobre limites, matrizes de risco, parametrização sistêmica, prestadores e documentação crítica.

3. Taxonomia de riscos

A Horizontes reconhece, sem caráter exaustivo, os seguintes grupos de risco: risco de mercado, risco de crédito e contraparte, risco de liquidez, risco de concentração, risco operacional, risco legal e documental, risco de modelo, risco de valuation e apreçamento, risco de terceiros, risco reputacional, risco de conflito de interesses, risco socioambiental e risco de descasamento entre a complexidade do produto e a capacidade operacional da gestora.

A materialidade de cada grupo de risco será aferida segundo o tipo de produto, a liquidez do ativo, a existência de garantias, a qualidade do devedor ou emissor, a dispersão do passivo, a dependência de prestador crítico, a complexidade documental, a exposição a derivativos, a concentração em convenentes, a estabilidade de fluxo, a relevância de premissas de valuation e a possibilidade de conflito estrutural.

3.1 Risco operacional e tecnológico - detalhamento

No grupo de risco operacional, a Gestora reconhece, em especial, o risco tecnológico, compreendendo eventos como indisponibilidade de sistemas, falha de infraestrutura de nuvem, incidentes cibernéticos, vazamento de dados pessoais (com reflexos em LGPD), descontinuidade de prestador crítico de tecnologia e falha de processo automatizado. A gestão desses riscos é realizada de forma integrada à Política de Segurança Cibernética e ao Plano de Continuidade de Negócios da Gestora, que estabelecem os controles técnicos, organizacionais e contingenciais aplicáveis, bem como a matriz de prestadores críticos formalmente contratados (BAlves, Manucom e Nullpointer).

4. Metodologia transversal de gestão de riscos

4.1 Identificação prévia e aprovação de limites

Nenhuma tese de investimento ou produto poderá entrar em operação sem identificação prévia dos riscos relevantes, definição de limites, indicação de métricas de acompanhamento e validação de que a estrutura da gestora e dos prestadores consegue produzir monitoramento tempestivo. A proposta de limite pode ser formulada pela gestão, mas deverá ser documentada e submetida à área de risco e, quando cabível, ao comitê competente.

A configuração de limites deverá considerar, de forma proporcional ao veículo e quando cabível, concentração por ativo, emissor, devedor, originador, cedente, grupo econômico, convenente, segmento, indexador, prazo, contraparte, garantia, setor, região, estágio de obra, liquidez, derivativos, rating e demais fatores relevantes aplicáveis. Em ativos ou

estruturas de baixa liquidez, a casa dará primazia à governança de pré-aprovação e à robustez da diligência, em vez de depender exclusivamente de métricas quantitativas ex post.

Na avaliação de risco operacional e tecnológico de novo produto ou estratégia, a área de risco verifica também a aderência da infraestrutura tecnológica da Gestora (hospedada em ambiente AWS Multi-AZ, com Active Directory redundante, VPN com MFA, backup automatizado e monitoramento contínuo) à complexidade da operação proposta, bem como a suficiência dos prestadores críticos de TI para sustentar a operação no estágio pretendido.

4.2 Monitoramento, exceção e reenquadramento

O monitoramento deverá combinar indicadores quantitativos e verificações qualitativas. Desenquadramentos regulatórios, mandatórios ou prudenciais deverão ser imediatamente reportados à gestão e à Diretoria Executiva, com indicação de causa, materialidade, risco de permanência e caminho proposto de reenquadramento. Exceções autorizadas em comitê não equivalem a dispensa permanente; deverão ter prazo, fundamento, responsável e reavaliação.

Em situação de risco elevado ou documentação insuficiente, a área de risco poderá recomendar bloqueio temporário da nova alocação, reforço documental, redução de posição, substituição de prestador, convocação extraordinária de comitê ou comunicação ao administrador fiduciário. Persistindo divergência entre gestão e risco em matéria sensível, o tema será escalado ao Diretor Executivo e registrado em ata.

4.3 Documentação e trilha de evidências

Cada decisão material de risco deve ser documentada de forma apta a demonstrar, em revisão posterior, o que se sabia à época, quais foram as premissas adotadas, quem decidiu, quem discordou, quais limites estavam em vigor, quais testes foram realizados e como o tema foi monitorado depois da decisão. O objetivo não é produzir burocracia, mas preservar memória institucional e defensabilidade regulatória.

5. Regras específicas por linha de produto

5.1 FIDC consignado público e privado

Nos FIDC consignado, a gestão de riscos terá como eixo principal o risco de crédito do fluxo cedido, a rastreabilidade do lastro, a segurança jurídica da cessão, a consistência da averbação ou mecanismo funcional equivalente, a concentração em originadores, convenentes e empregadores, a qualidade da cobrança, a efetividade das garantias, a

existência de recompras, coobrigação ou suporte econômico de terceiros e a confiabilidade dos dados operacionais utilizados na formação da carteira.

O monitoramento deverá contemplar, no mínimo, elegibilidade formal, concentração por cedente/originador, concentração por convenente, vintage, inadimplência, pré-pagamento, repactuação, fraude, backtesting de premissas e eventos de deterioração. Em consignado público, a política exigirá especial atenção a riscos reputacionais, interação com entes públicos, convênios e eventuais pessoas expostas politicamente. Em consignado privado, o foco reforçado recairá sobre estabilidade da fonte pagadora, qualidade dos empregadores e robustez dos mecanismos operacionais de desconto em folha.

Quando a operação depender de originador ou estruturador vinculado, a análise de risco deverá ser complementada pela política de conflitos e pela política de crédito, com manifestação específica sobre independência da decisão e comutatividade econômica.

5.2 Fundos imobiliários e ativos reais

Nos FII e ativos reais, a gestão de riscos abrangerá risco jurídico e registral, risco de obra, risco de vacância, risco de locatário, risco de concentração geográfica, risco de valuation, risco ambiental, risco de caixa da estrutura, risco de garantias, risco de liquidez do ativo e risco de conflito quando houver relação com estruturadores, incorporadoras, consultores, originação própria ou ativações ligadas à vertical imobiliária da casa.

A aprovação de ativo imobiliário ou crédito imobiliário deverá considerar diligência documental, laudos e pareceres adequados, cenário base e cenário conservador, premissas de saída, dependência de alavancagem, governança da SPE quando existente e sensibilidade a eventos de mercado. Ativos em desenvolvimento, operações com fluxo futuro e estruturas dependentes de performance operacional deverão receber tratamento mais conservador em limites, gatilhos e monitoramento.

5.3 Fundo multimercado

No fundo multimercado, a gestão de riscos contemplará risco de mercado, risco de liquidez, risco de contraparte, risco de derivativos, risco de concentração, risco de estresse e risco operacional associado à execução. O enquadramento deverá observar limites formais por classe de ativo, contraparte, alavancagem econômica, margem, exposição líquida e bruta, sensibilidade e demais métricas coerentes com o regulamento do veículo.

Operações com derivativos somente serão permitidas quando a documentação do veículo, a infraestrutura de middle office, as rotinas de margem e o monitoramento de

risco estiverem implementados e testados. A área de risco deverá ter acesso às posições, garantias e cenários de estresse em tempo compatível com a materialidade do veículo.

6. Conflitos entre risco e investimento

A política reconhece que risco e investimento não atuam no mesmo plano decisório. A gestão é responsável por formular e executar a tese; a área de risco é responsável por testar sua aderência, monitorar seus efeitos e apontar fragilidades. Conflito entre as duas funções é esperado em uma casa séria e não deve ser suprimido artificialmente. O que se exige é que o conflito seja produtivo, documentado e resolvido por mecanismo institucional, nunca por informalidade.

A Diretoria de Compliance, na função independente de risco, participará dos comitês de investimento, crédito e imobiliário como observadora com direito de requerer esclarecimentos, condicionantes e escalada. O Diretor Executivo atuará como instância de governança para assegurar que divergências sejam endereçadas com base em documentação e não em hierarquia informal.

7. Revisão e guarda

Esta Política será revista, no mínimo, anualmente e sempre que houver ingresso em nova estratégia, alteração regulatória, contratação ou substituição de prestador crítico, incidente relevante ou recomendação de auditoria, administrador fiduciário ou autorregulador. A revisão ordinária considerará também os relatórios de testes de continuidade (BCP), os relatórios de testes de controles de segurança cibernética, eventuais incidentes de TI ou cibernéticos e os resultados da reavaliação periódica dos prestadores críticos de TI, conforme item 5 da Política de Segurança Cibernética. Os relatórios, matrizes, atas, logs e demais evidências produzidos em sua execução serão mantidos em arquivo organizado, físico ou eletrônico, pelo prazo legal aplicável, observada a política de retenção documental.

Anexos operacionais

Anexo I – matriz exemplificativa de indicadores por produto

Produto	Indicadores mínimos
FIDC consignado	concentração por cedente/convenente, inadimplência, pré-pagamento, vintage, eventos de fraude, recompras e cobertura documental

Produto	Indicadores mínimos
FII / ativos reais	vacância, cronograma de obra, cobertura de garantias, fluxo projetado, concentração, laudos e sensibilidade de valuation
Multimercado	exposição líquida e bruta, concentração, margem, estresse, liquidez da carteira e contraparte
Risco institucional	cadastros, prestadores críticos, incidentes, treinamento, continuidade, conflitos e aderência documental
Risco operacional e tecnológico	indisponibilidade de sistemas, falha de nuvem, incidentes cibernéticos, vazamento de dados pessoais, descontinuidade de prestador crítico de TI, falha de processo automatizado e aderência a controles do BCP e da Política de Cyber

Anexo II – escalada mínima de desenquadramentos

Nível	Tratamento
Baixo	registro e saneamento pela área responsável, com ciência de risco no relatório periódico
Médio	plano de ação formal, prazo definido e acompanhamento pelo Comitê de Risco, Compliance e PLD/FTP
Alto	comunicação imediata ao Diretor Executivo e ao Diretor de Gestão, avaliação de bloqueio, reenquadramento e eventual comunicação a prestadores
Crítico	convocação extraordinária de comitê, preservação de evidências, decisão executiva e tratamento prioritário

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 do subitem 3.1 detalhando o risco operacional e tecnológico, com referência à Política de Segurança Cibernética, ao BCP e aos prestadores críticos de TI (BAlves, Manucom, Nullpointer). Inclusão, no item 4.1, de parágrafo sobre verificação da aderência da infraestrutura tecnológica (AWS Multi-AZ, AD redundante, VPN/MFA, AWS Backup, CloudWatch) à**

Versão	Data-base	Aprovação	Principais alterações
			complexidade da operação. Inclusão, na matriz do Anexo I, de linha sobre risco operacional e tecnológico. Atualização do item 7 para considerar relatórios de BCP, Cyber e reavaliação de prestadores de TI na revisão ordinária. Atualização do item 1 para inclusão de cibersegurança e continuidade no rol de matérias de interpretação conjunta das políticas.

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.