HORIZONTES ASSET LTDA.

POLÍTICA DE SELEÇÃO, CONTRATAÇÃO E MONITORAMENTO DE TERCEIROS

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	Disciplinar a forma pela qual a gestora selecionará, contratará, monitorará e substituirá terceiros e prestadores relevantes.
Abrangência	Prestadores críticos, relevantes e ordinários ligados à implantação e à operação dos veículos sob gestão.
Responsável	Diretoria Executiva e Diretoria de Compliance, Risco e PLD/FTP, com apoio do middle office e da área de gestão.
Aprovador	Diretoria estatutária e Comitê Executivo e de Governança.
Base normativa principal	Resolução CVM 50; Resolução CVM 175; Código ANBIMA de Administração e Gestão de Recursos de Terceiros; Regras e Procedimentos ANBIMA de Deveres Básicos; Lei nº 13.709/2018 (LGPD).

1. Objetivo e abrangência

Esta política disciplina a seleção, contratação, avaliação, monitoramento e substituição de prestadores e terceiros relevantes da HORIZONTES ASSET LTDA., inclusive prestadores essenciais e complementares relacionados à atividade de gestão de recursos, à implantação de veículos, à administração fiduciária, custódia, controladoria, escrituração, distribuição, auditoria, consultoria, cobrança, rating, tecnologia, nuvem, segurança da informação e suporte documental, conforme detalhado na Política de Segurança Cibernética e no Plano de Continuidade de Negócios.

Como a gestora se encontra em fase final de implantação e pretende iniciar atividade com FIDC consignado público e privado, fundo imobiliário e fundo multimercado em até 60

dias, esta política é prospectiva e operacional ao mesmo tempo. Ela orienta a diligência pré-contratação dos prestadores que viabilizarão os primeiros produtos e também estabelece o padrão de monitoramento contínuo a ser adotado após a entrada em operação.

2. Classificação de criticidade e critérios de escolha

Os terceiros serão classificados em, no mínimo, três níveis: críticos, relevantes e ordinários. Serão considerados críticos os terceiros cuja falha possa comprometer o cumprimento regulatório, a integridade do portfólio, a guarda de ativos, a segurança da informação, a continuidade da operação ou a relação com investidores, como administrador fiduciário, custodiante, controladoria, escrituração, registradora, servicer, plataforma de nuvem, provedor de sistemas centrais, auditor independente e distribuidor. Serão relevantes os terceiros que influenciam materialmente o processo, ainda que não sejam prestadores essenciais formais, como correspondentes, consultores especializados, escritórios jurídicos, avaliadores, agentes de cobrança e provedores de diligência.

A matriz nominal de prestadores críticos de tecnologia da informação atualmente contratados está consolidada no item 5.2 da Política de Segurança Cibernética, sem prejuízo da remissão específica feita no item 5.1 desta Política.

A seleção observará capacidade técnica, aderência regulatória, experiência específica na estratégia do produto, estrutura operacional, governança, independência, reputação, segurança da informação, contingência, estabilidade financeira, histórico de incidentes, capacidade de integração tecnológica, qualidade contratual e aderência do custo à necessidade da gestora. Em FIDC consignado, a experiência com carteira pública e privada, convênios, registros, cobrança e conciliação é elemento central. Em FII e real estate, a qualidade da diligência jurídica, técnica e de monitoramento de ativos é fator crítico. Em multimercado, a robustez de execução, middle, controladoria e sistemas assume maior relevância.

3. Due diligence inicial, contratação e cláusulas mínimas

Nenhum terceiro crítico ou relevante será contratado sem documentação mínima de due diligence. A diligência poderá incluir questionário, análise documental, checagem de registros, validação de estrutura, referências, reunião técnica, avaliação de segurança, exame contratual e, quando proporcional, visita ou diligência ampliada. A profundidade da análise deverá refletir a criticidade do serviço; simplicidade operacional não justifica superficialidade quando o terceiro é estrutural para o produto.

Os contratos deverão conter, conforme o caso, definição clara de escopo, níveis de serviço, confidencialidade, proteção de dados, segurança da informação, subcontratação, plano de continuidade, cooperação regulatória, dever de informação, tratamento de incidentes, direito de auditoria ou solicitação de evidências, responsabilidades por falhas, guarda de registros, prazo de retenção, regras de rescisão e transição assistida. Em prestadores críticos, a ausência de cláusula adequada equivale a fragilidade de governança.

Em prestadores de tecnologia da informação ou prestadores que tratem dados pessoais por conta da Gestora, a diligência inicial inclui, adicionalmente, verificação dos controles previstos na Política de Segurança Cibernética da Gestora e dos compromissos do prestador quanto ao tratamento de dados pessoais (LGPD), com inclusão de cláusulas contratuais específicas de operador e de comunicação de incidentes à Encarregada pelo Tratamento de Dados Pessoais (DPO), na forma do art. 41 da Lei nº 13.709/2018.

4. Monitoramento contínuo, planos de ação e substituição

Após a contratação, a gestora manterá rotina de monitoramento compatível com a criticidade do prestador. Prestadores críticos serão monitorados de forma periódica e documentada, com análise de indicadores operacionais, incidentes, reclamações, mudanças societárias, alterações de equipe-chave, certificações, relatórios, evidências de testes e qualidade do atendimento. Prestadores relevantes serão monitorados por evento e por revisão periódica. A área de Middle office concentrará a trilha operacional dos contratos e níveis de serviço; A área administrativa apoiará a organização documental; A Diretoria de Compliance supervisionará o cumprimento da política; A Diretoria Executiva aprovará substituições críticas; A Diretoria de Gestão participará quando a qualidade do prestador afetar diretamente a estratégia de investimento.

Os prestadores críticos de tecnologia da informação são reavaliados, no mínimo, anualmente, conforme o item 5.2 da Política de Segurança Cibernética. Eventuais incidentes de TI ou cibernéticos detectados em prestador crítico acionam, adicionalmente, o fluxo previsto no Plano de Continuidade de Negócios (Cenário C3 - Falha de prestador crítico, e, quando aplicável, Cenário C5 - Incidente cibernético).

Ressalvas identificadas em diligência ou monitoramento deverão ser classificadas por gravidade, receber plano de ação e prazo de correção. O fato de um prestador ser conhecido no mercado não dispensa acompanhamento. Reputação setorial é elemento útil, mas não substitui evidência contemporânea de que o terceiro continua apto, seguro e aderente à necessidade concreta da gestora.

5. Prestadores-alvo da fase inicial

Considerando o plano de entrada em operação, a gestora deverá priorizar, na fase inicial, a seleção e contratação dos seguintes blocos: administrador fiduciário com experiência em FIDC, FII e fundos sob a Parte Geral da Resolução CVM 175; custodiante e controladoria compatíveis com crédito estruturado e ativos líquidos; escriturador/registradora e infraestrutura de conciliação; auditor independente; assessor jurídico regulatório e transacional; prestadores de cobrança e monitoramento de carteira para FIDC; provedor de dados, storage e controle de documentos; sistema de middle/controle; provedores de assinatura e data room; e, quando necessário, agência de rating, avaliadores e consultorias técnicas.

5.1 Prestadores críticos de tecnologia da informação já contratados

Na data-base desta Política, a Gestora mantém os seguintes prestadores críticos de tecnologia da informação: (i) BAlves Gestão em Tecnologia da Informação — implantação e arquitetura da infraestrutura cloud corporativa em AWS (Proposta Comercial PROP-2026-001, aceite formal pela Diretoria Executiva em 24/04/2026); (ii) Manucom Tecnologia Ltda. - suporte técnico em tecnologia da informação com SLAs por gravidade do incidente (Contrato de Suporte Técnico nº 357-2026, assinado eletronicamente em 30/04/2026, vigência iniciada em 01/03/2026, prazo indeterminado); (iii) Nullpointer - plataforma operacional especializada NPFlow + Sentinela + Gestora App, voltada à execução, controle e monitoramento das atividades de gestão de FIDC (em fase de formalização contratual e implantação técnica). Cada prestador acima foi submetido à diligência prevista no item 3 desta Política, observa as cláusulas mínimas contratuais aplicáveis e está sujeito ao regime de monitoramento contínuo do item 4.

Anexos operacionais

Anexo I – Matriz mínima de due diligence de terceiros

Bloco	Conteúdo mínimo de análise
Regulatório	Registro, autorregulação, histórico sancionador, licenças e situação cadastral
Operacional	Equipe, contingência, volumes suportados, integrações, rotinas e SLA
Jurídico-contratual	Escopo, responsabilidade, incidentes, confidencialidade, dados, rescisão e transição
Tecnologia e segurança	Ambiente, controles de acesso, backup, logs, resposta a incidentes e subcontratação

Bloco	Conteúdo mínimo de análise
Financeiro/reputacional	Estabilidade, referências, litígios relevantes e histórico de falhas
LGPD e proteção de dados pessoais	papel (controlador/operador), bases legais de tratamento, cláusulas de DPA, comunicação de incidentes à ANPD e ao Encarregado da Gestora, prazo de retenção e procedimento de devolução ou destruição

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 LGPD na base normativa principal. Inclusão, no item 1, de referência à Política de Cyber e ao BCP. Inclusão, no item 2, de remissão à matriz nominal de prestadores críticos de TI consolidada na Política de Cyber. Inclusão, no item 3, de parágrafo sobre diligência específica de prestadores de TI e cláusulas LGPD (operador). Inclusão, no item 4, de parágrafo sobre reavaliação anual de prestadores de TI e acionamento do BCP em caso de incidente. Inclusão da nova subseção 5.1 nominando os prestadores críticos de TI já contratados (BAlves, Manucom, Nullpointer). Inclusão, no Anexo I, de linha sobre LGPD e proteção de dados pessoais.**

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.