HORIZONTES ASSET LTDA.

PLANO DE CONTINUIDADE DE NEGÓCIOS (BCP)

Versão	Data-base	Aprovação	Próxima revisão
1.1	Maio/2026	Diretoria Executiva	Anual (maio/2027)

1. Objeto e escopo

O presente Plano de Continuidade de Negócios ("BCP", do inglês *Business Continuity Plan*) tem por objeto estabelecer as diretrizes, os procedimentos e as responsabilidades aplicáveis à preservação das atividades essenciais da HORIZONTES ASSET LTDA. ("Horizontes" ou "Gestora"), inscrita no CNPJ sob o nº 58.805.121/0001-90, frente a eventos disruptivos de qualquer natureza que possam afetar sua capacidade de operação.

Este BCP é emitido em atendimento (i) ao art. 16 da Resolução CVM nº 21/2021, que exige que o gestor de recursos mantenha controles internos compatíveis com a sua atividade; (ii) às Diretrizes ANBIMA de Continuidade de Negócios, anexas ao Código ANBIMA de Administração e Gestão de Recursos de Terceiros; e (iii) à Resolução CVM nº 35/2021 e demais normas aplicáveis ao gestor de recursos de terceiros.

O escopo deste BCP abrange todas as atividades classificadas como essenciais à atuação da Gestora, em especial: (i) decisão e execução de operações de investimento; (ii) controles de risco, compliance e PLD; (iii) comunicação com investidores, administradores fiduciários, custodiantes, corretoras, reguladores e autorreguladores; (iv) guarda de informação confidencial e cumprimento de obrigações regulatórias periódicas.

2. Estrutura de governança do BCP

2.1. Comitê de Crise

O Comitê de Crise é o órgão colegiado responsável por declarar o acionamento do BCP, coordenar a resposta a evento disruptivo, autorizar comunicações externas e deliberar sobre o retorno à operação normal. É composto por:

- Diretor Executivo - coordenação geral, comunicação interna e externa, decisões estratégicas;
- Diretor de Gestão de Recursos - continuidade das atividades de investimento;
- Diretora de Compliance, Risco e PLD - avaliação de aderência regulatória, comunicação a reguladores e autorreguladores, atuação como Encarregada pelo Tratamento de Dados Pessoais (DPO);
- Representante do prestador de suporte técnico de TI - recuperação técnica e operação da infraestrutura.

O Comitê de Crise reúne-se em caráter extraordinário sempre que acionado, podendo deliberar presencialmente ou por meios eletrônicos (videoconferência, telefone, mensageria corporativa). As deliberações são registradas em ata simplificada, lavrada pela Diretora de Compliance, Risco e PLD.

2.2. Responsável pelo BCP

A Diretora de Compliance, Risco e PLD é a responsável pela manutenção, atualização, testes e divulgação interna deste BCP, observado o cronograma do item 7 abaixo.

3. Cenários cobertos

Este BCP cobre, no mínimo, os seguintes cenários de evento disruptivo:

Cenário	Descrição	Impacto principal
C1. Falha de tecnologia da informação	Indisponibilidade de sistemas, servidores, internet, energia elétrica, telefonia ou serviços em nuvem utilizados pela Gestora.	Perda de capacidade operacional, perda de dados, atraso em rotinas regulatórias.
C2. Indisponibilidade de pessoa-chave	Ausência prolongada ou definitiva de diretor estatutário ou de profissional com função técnica crítica (acidente, doença grave, falecimento, saída abrupta).	Risco de descontinuidade de função regulatória ou operacional crítica.
C3. Falha de prestador crítico	Falha, indisponibilidade ou descontinuidade de administrador fiduciário, custodiante, controladoria, corretora, escritório jurídico ou prestador de TI.	Comprometimento de liquidação, custódia, escrituração ou suporte técnico essencial.
C4. Evento externo grave	Pandemia, catástrofe natural, evento social ou político grave, atos de terceiros (incêndio, vandalismo), exigência de quarentena ou	Impossibilidade de uso do ambiente físico, restrição de mobilidade da equipe.

Cenário	Descrição	Impacto principal
	impedimento de acesso ao escritório.	
C5. Incidente cibernético	Ataque de ransomware, sequestro de dados, intrusão indevida em sistemas, vazamento de informação confidencial, comprometimento de credenciais.	Perda de dados, exposição de informação sensível, violação à LGPD, dano reputacional.
C6. Falha do ambiente físico	Indisponibilidade do escritório por sinistro (incêndio, alagamento), interdição administrativa ou bloqueio de acesso.	Necessidade de operação remota imediata e contínua.

4. Procedimentos de resposta

4.1. Métricas de referência (RTO e RPO)

Para fins de planejamento, a Gestora adota as seguintes métricas de referência para suas atividades essenciais:

- RTO (Recovery Time Objective) - tempo máximo aceitável para retomada da atividade essencial: até 4 (quatro) horas úteis para decisão de investimento e até 1 (um) dia útil para rotinas de controles internos não críticas. Esse RTO é compatível com o nível de serviço (SLA) contratado com o prestador de suporte técnico de TI para incidentes de gravidade grave;
- RPO (Recovery Point Objective) - perda máxima aceitável de dados em volume temporal: até 24 (vinte e quatro) horas, considerando-se a rotina diária de backup automatizado dos sistemas e arquivos da Gestora via AWS Backup.

As métricas acima são objetivos de planejamento e são reavaliadas, no mínimo, anualmente, com base em testes do BCP e em eventuais incidentes ocorridos no período.

4.2. Procedimento por cenário

A resposta a cada cenário previsto no item 3 segue o fluxo abaixo, sendo coordenada pelo Comitê de Crise:

Cenário	Resposta imediata (até 4 horas)	Recuperação e continuidade
C1. Falha de TI	Abertura imediata de chamado junto ao prestador de suporte técnico de TI contratado, observado o SLA aplicável (até 4 horas para	Recuperação a partir de backups automatizados via AWS Backup; teste de integridade dos dados;

Cenário	Resposta imediata (até 4 horas)	Recuperação e continuidade
	incidentes graves); migração para dispositivos de contingência (notebooks pessoais previamente autorizados); uso de canais alternativos de comunicação (celular corporativo, mensageria).	relatório técnico ao Comitê de Crise; lições aprendidas registradas em ata.
C2. Pessoa-chave	Acionamento do suplente estatutário previamente designado; comunicação interna aos demais diretores; preservação imediata de credenciais e arquivos sob custódia da pessoa ausente.	Avaliação pelo Comitê de Crise sobre eventual necessidade de comunicação à CVM e à ANBIMA; reorganização interna de atribuições; eventual contratação ou redistribuição formal.
C3. Prestador crítico	Contato imediato com o prestador para diagnóstico, observados os canais formais previstos no instrumento contratual; avaliação da extensão e da expectativa de retomada; comunicação aos demais prestadores que dependam da cadeia.	Em caso de prestador crítico de TI, ativação de prestador substituto previamente pré-qualificado, observados os critérios do item 5 da Política de Segurança Cibernética; comunicação aos administradores fiduciários e demais contrapartes; revisão do contrato e do plano de contingência do prestador.
C4. Evento externo	Acionamento do modo de operação remota (home office); confirmação de disponibilidade da equipe; checagem da continuidade dos prestadores críticos.	Operação remota continuada enquanto durar o evento, viabilizada pelo ambiente cloud AWS e pela VPN com MFA da Gestora; reavaliação periódica pelo Comitê de Crise; retorno gradual ao escritório quando seguro.
C5. Incidente cibernético	Isolamento dos sistemas afetados; preservação de evidências; troca imediata de credenciais; acionamento do prestador de TI e da DPO/Diretora de Compliance, Risco e PLD.	Avaliação do impacto sobre dados pessoais (LGPD); comunicação ao titular, à ANPD, à CVM e à ANBIMA quando exigida, conforme item 5; remediação técnica; recuperação a partir de backups íntegros.
C6. Ambiente físico	Comunicação imediata à equipe pelo canal de mensageria corporativa; ativação do modo de operação remota; preservação de acesso aos sistemas em nuvem.	Operação remota integral, viabilizada pelo ambiente cloud AWS, até a normalização do ambiente físico ou contratação de novo endereço; comunicação à JUCESP, CVM e ANBIMA caso o endereço mude formalmente.

5. Plano de comunicação

Acionado o BCP, a comunicação a stakeholders observa a seguinte ordem de prioridade e prazos máximos, salvo determinação diversa do Comitê de Crise diante de circunstância específica:

Destinatário	Prazo máximo	Responsável
Equipe interna	Imediato	Diretor Executivo
Administradores fiduciários dos fundos sob gestão	Até 4 horas úteis	Diretor de Gestão de Recursos
Custodiantes e corretoras parceiras	Até 4 horas úteis	Diretor de Gestão de Recursos
CVM (quando exigível)	No prazo regulatório aplicável	Diretora de Compliance, Risco e PLD
ANBIMA (quando exigível)	No prazo regulatório aplicável	Diretora de Compliance, Risco e PLD
ANPD (incidente com dados pessoais)	Em prazo razoável, conforme LGPD	Encarregada pelo Tratamento de Dados Pessoais (DPO)
Investidores (eventos materiais)	Em até 1 dia útil	Diretor Executivo

Os canais de comunicação preferenciais são o e-mail corporativo e, para o público interno, a ferramenta de mensageria corporativa. Em caso de indisponibilidade desses canais, são utilizados telefone, SMS ou aplicativos de mensagem alternativos.

6. Infraestrutura de contingência

A Gestora opera sobre infraestrutura corporativa hospedada em provedor de nuvem (Amazon Web Services - AWS), implantada e suportada por prestadores especializados formalmente contratados, com as seguintes características que sustentam a continuidade dos negócios:

- Arquitetura Virtual Private Cloud (VPC) dedicada, distribuída em múltiplas zonas de disponibilidade (Multi-AZ), garantindo redundância geográfica intra-região;
- Active Directory com dois controladores em zonas distintas, replicados, evitando ponto único de falha na autenticação corporativa;

- File server corporativo com volumes EBS otimizados, com permissões baseadas em grupos do Active Directory;
- Acesso remoto seguro por VPN site-to-client com autenticação multifator (TOTP), integrada ao Active Directory, permitindo operação integral em modo home office;
- Backup automatizado via AWS Backup, com política configurada para os volumes e recursos críticos, e teste de restauração realizado no mínimo semestralmente;
- Monitoramento contínuo via Amazon CloudWatch, com alarmes para eventos críticos e notificações automáticas por e-mail;
- Firewall dedicado (OPNsense) na borda do ambiente, com regras segmentadas por camada funcional;
- Suporte técnico contratado com SLAs por gravidade do incidente (até 4 horas úteis para incidentes graves, 12 horas para médios e 24 horas para leves), em horário 5x8;
- Plataforma operacional especializada para gestão de FIDC (Nullpointer - NPFlow + Sentinela + Gestora App, em fase de formalização contratual e implantação), com camadas de execução de fluxos (BPMN), vigilância cognitiva sobre corpus regulatório do segmento e rastreabilidade integral de operações;
- Lista de contatos atualizada de prestadores críticos, com canais primários e alternativos, mantida sob custódia da Diretora de Compliance, Risco e PLD;
- Diretrizes detalhadas de segurança cibernética conforme Política específica da Gestora, complementar a este BCP.

7. Testes, atualização e divulgação

Este BCP é submetido aos seguintes ciclos de manutenção:

- Teste anual obrigatório, conduzido pela Diretora de Compliance, Risco e PLD, com simulação de pelo menos um dos cenários previstos no item 3. O resultado é registrado em relatório interno e submetido ao Comitê de Crise para conhecimento;
- Revisão ordinária anual da redação deste documento, com atualização da matriz de cenários, das métricas RTO/RPO, da lista de prestadores críticos e dos canais de comunicação;
- Revisão extraordinária sempre que houver: (i) incidente real que tenha exigido acionamento do BCP, (ii) mudança relevante na estrutura societária ou operacional da Gestora, (iii) alteração regulatória relevante, (iv) substituição ou inclusão de prestador crítico, ou (v) determinação de regulador ou autorregulador.

Após a revisão, este documento será disponibilizado em sua versão atualizada na página eletrônica da Gestora (horizontesasset.com), em local de acesso público e gratuito, conforme exigências regulatórias aplicáveis.

8. Aprovação, vigência e publicação

O presente Plano de Continuidade de Negócios foi aprovado pela Diretoria Executiva da Horizontes Asset Ltda. e entra em vigor na data de sua publicação, permanecendo válido até a sua próxima revisão ordinária ou extraordinária, observado o disposto no item 7 acima.

9. Assinatura

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.