ENTRY CAPITAL GESTÃO DE RECURSOS LTDA.

POLÍTICA DE EXERCÍCIO DE CONTINUIDADE DE NEGÓCIOS

Versão:	Motivo da alteração:	Data:	Aprovado por:	Data da aprovação:
02	Atualização	Janeiro/2026	Luis Massud	15/01/2026

1. OBJETIVO

1.1. **Esta Política de Continuidade de Negócios** ("Política" ou "PCN") estabelece as diretrizes, os procedimentos e as responsabilidades adotados pela Entry Capital Gestão de Recursos Ltda. ("Entry Capital", "Gestora" ou "Instituição") para assegurar a continuidade de suas atividades principais e críticas e a manutenção de seus compromissos perante investidores, clientes, prestadores de serviço, parceiros comerciais, órgãos reguladores e autorreguladores diante da ocorrência de eventos que possam interromper ou comprometer a operação normal da Instituição.

1.2. A Política tem por finalidade minimizar os impactos de eventos disruptivos sobre as atividades essenciais da Gestora, permitir a sua recuperação tempestiva e preservar a integridade, a confidencialidade e a disponibilidade das informações e dos recursos sob gestão.

2. ABRANGÊNCIA

2.1. Esta Política aplica-se a todos os sócios, administradores, associados, diretores, empregados, estagiários e demais colaboradores da Entry Capital, independentemente do vínculo ou da função exercida ("Colaboradores").

2.2. Aplica-se, ainda, no que couber, aos prestadores de serviço relevantes para a operação da Gestora, observados os termos dos respectivos contratos.

3. BASE NORMATIVA

3.1. Esta Política observa, entre outras normas e melhores práticas aplicáveis:

(a) Resolução CVM nº 21, de 25 de fevereiro de 2021, e suas alterações posteriores;

(b) Código ANBIMA de Administração de Recursos de Terceiros e respectivas Regras e Procedimentos;

(c) Lei nº 13.709/2018 (Lei Geral de Proteção de Dados — LGPD), no que se refere à proteção das informações; e

(d) demais normas aplicáveis à atividade de administração de carteiras de valores mobiliários, na modalidade gestão de recursos.

4. PRINCÍPIO DA PROPORCIONALIDADE

4.1. Em observância ao princípio da proporcionalidade, as diretrizes desta Política foram dimensionadas considerando o porte, a natureza, a complexidade e o perfil de risco das atividades da Entry Capital, que atua exclusivamente como gestora de recursos de terceiros, com estrutura

organizacional enxuta e terceirização de certas funções operacionais, como contabilidade, administração fiduciária, custódia e controladoria de ativos e passivos, a prestadores de serviço especializados e devidamente habilitados perante os órgãos regulamentares.

5. DEFINIÇÕES

5.1. Para os fins desta Política, consideram-se:

(a) **Continuidade de Negócios:** capacidade da Instituição de manter ou restabelecer suas atividades críticas em níveis aceitáveis após um Evento de Contingência;

(b) **Evento de Contingência:** qualquer ocorrência, interna ou externa, que interrompa ou ameace interromper a operação normal da Gestora;

(c) **Processos Críticos:** atividades cuja interrupção compromete de forma relevante a gestão das carteiras, o cumprimento de obrigações regulatórias ou o atendimento a investidores;

(d) **RTO** (**Recovery Time Objective**): tempo máximo aceitável para o restabelecimento de um Processo Crítico;

(e) **RPO** (**Recovery Point Objective**): volume máximo tolerável de perda de dados, expresso em unidade de tempo;

(f) **Sítio Alternativo:** local físico ou ambiente remoto a partir do qual as atividades críticas podem ser conduzidas; e

(g) **Análise de Impacto (BIA):** avaliação que identifica e prioriza os Processos Críticos e os respectivos tempos de recuperação.

6. GOVERNANÇA E RESPONSABILIDADES

6.1. **Diretor Responsável.** A responsabilidade pela elaboração, implementação, supervisão e atualização desta Política é do diretor responsável pela gestão de risco e pelo cumprimento de regras, procedimentos e controles internos da Entry Capital ("Diretor Responsável").

6.2. Compete ao Diretor Responsável: (i) acionar e coordenar a execução desta Política em situações de contingência; (ii) avaliar a severidade do evento e decidir sobre a ativação das estratégias de continuidade; (iii) conduzir a comunicação interna e externa; (iv) promover os testes e revisões periódicas; e (v) manter registro documental dos eventos e das medidas adotadas.

6.3. Compete aos Colaboradores conhecer e observar esta Política, comunicar imediatamente ao Diretor Responsável qualquer Evento de Contingência de que tomem conhecimento e cooperar com a execução das medidas de continuidade.

6.4. **Pessoa-chave e suplência.** Em razão da estrutura enxuta da Gestora, fica designada a compliance officer como contato suplente do Diretor

Responsável, apta a acionar esta Política e a representar a Instituição na sua ausência ou impedimento temporário.

7. ANÁLISE DE IMPACTO E PROCESSOS CRÍTICOS

7.1. A Gestora identifica como Processos Críticos as atividades cuja interrupção possa comprometer a gestão das carteiras, o cumprimento das obrigações regulatórias ou o atendimento aos investidores, conforme quadro abaixo, no qual os RTO indicados constituem referências a serem perseguidas e podem ser ajustados conforme a evolução da operação:

Processo crítico	RTO de referência	Responsável
Gestão e tomada de decisão de investimento das carteiras	Até 1 dia útil	Diretor de Gestão
Transmissão, registro e controle de ordens	Até 4 horas úteis	Diretor de Gestão
Monitoramento e gestão de risco das carteiras	Até 1 dia útil	Diretor de Risco
Cumprimento de obrigações regulatórias e envio de informações periódicas (CVM/ANBIMA)	Conforme prazo legal	Diretor de Compliance
Conciliação e troca de informações com administrador fiduciário e custodiante	Até 1 dia útil	Diretor de Gestão
Atendimento e comunicação a investidores e clientes	Até 1 dia útil	Diretor Responsável
Guarda, integridade e disponibilidade das informações	Conforme RPO de 24 horas	Diretor Responsável / TI

7.2. Os parâmetros de RTO e RPO devem ser revistos sempre que houver alteração relevante na estrutura, nos sistemas ou no volume de recursos sob gestão.

8. CENÁRIOS DE CONTINGÊNCIA

8.1. Esta Política contempla, de forma não exaustiva, os seguintes cenários de contingência:

(a) indisponibilidade das instalações físicas (incêndio, alagamento, falta prolongada de energia ou de telecomunicações, ou impossibilidade de acesso ao escritório);

(b) falha, indisponibilidade ou perda de dados de sistemas e infraestrutura de tecnologia da informação;

(c) indisponibilidade por prazo relevante de pessoa-chave (afastamento, doença, acidente ou falecimento);

(d) falha ou descontinuidade de prestador de serviço crítico (administrador fiduciário, custodiante, corretoras ou provedores de tecnologia);

(e) incidentes de segurança da informação e ataques cibernéticos; e

(f) eventos externos de grande escala, tais como pandemias, desastres naturais, guerras, ataques terroristas ou crises sistêmicas.

9. ESTRATÉGIAS DE CONTINUIDADE E RECUPERAÇÃO

9.1. **Trabalho remoto.** As atividades de gestão, controle de risco, compliance e atendimento podem ser conduzidas remotamente por meio de acesso seguro às ferramentas e aos sistemas da Gestora, viabilizando a manutenção da operação mesmo na indisponibilidade do escritório.

9.2. **Infraestrutura em nuvem.** Os principais sistemas e arquivos da Gestora são mantidos em ambiente de nuvem de provedor reputado, com redundância e acesso seguro a partir de qualquer localidade, reduzindo a dependência de equipamentos físicos específicos no escritorio.

9.3. **Indisponibilidade de pessoa-chave.** Na ausência ou no impedimento do Diretor Responsável, o contato suplente designado assume as funções essenciais. As senhas, os acessos e as informações críticas são documentados e mantidos de forma segura, de modo a permitir a transição ordenada das atribuições.

9.4. **Prestadores de serviço críticos.** Diante da descontinuidade de prestador crítico, a Gestora adota as providências para a substituição tempestiva, valendo-se da disponibilidade de outros prestadores habilitados no mercado. As funções de administração fiduciária, custódia e controladoria são, por sua natureza, substituíveis mediante contratação de instituição alternativa dentro de um prazo específico acordado contratualmente.

9.5. **Incidentes cibernéticos.** Identificado incidente de segurança, o Diretor Responsável determina o isolamento dos sistemas afetados, a restauração a partir de cópias de segurança íntegras e a comunicação às partes pertinentes, observada a LGPD.

9.6. **Sítio Alternativo.** Na impossibilidade de uso do escritório, as atividades podem ser retomadas a partir de Sítio Alternativo, assim entendido o ambiente remoto de trabalho dos Colaboradores ou outro local previamente identificado.

10. INFRAESTRUTURA, BACKUP E SEGURANÇA DA INFORMAÇÃO

10.1. A Gestora mantém rotina de cópias de segurança (backup) periódicas das informações críticas, armazenadas em ambiente segregado e seguro, na nuvem.

10.2. São adotadas medidas de controle de acesso, autenticação e, quando aplicável, criptografia, de modo a preservar a confidencialidade e a integridade das informações.

10.3. A integridade e a capacidade de restauração das cópias de segurança são verificadas no âmbito dos testes previstos no item 12.

11. ACIONAMENTO E PLANO DE COMUNICAÇÃO

11.1. Constatado um Evento de Contingência, o Colaborador que dele tomar conhecimento comunica imediatamente o Diretor Responsável e/ao Diretor de Compliance, a quem compete avaliar a severidade e decidir sobre a ativação das estratégias previstas nesta Política.

11.2. A comunicação observará a seguinte ordem de prioridade, conforme a natureza do evento: (i) Colaboradores; (ii) administrador fiduciário e custodiante; (iii) investidores e clientes afetados; (iv) corretoras e contrapartes; (v) órgãos reguladores e autorreguladores (CVM e ANBIMA), quando exigido; (vi) prestadores de serviço e parceiros comerciais.

11.3. Os contatos relevantes para acionamento em contingência constam do Anexo I, de preenchimento e atualização contínua pelo Diretor Responsável.

12. TESTES, MONITORAMENTO E REVISÃO

12.1. Esta Política é testada, no mínimo, anualmente, mediante simulação dos cenários considerados mais relevantes, com registro dos resultados e das eventuais oportunidades de melhoria identificadas.

12.2. A Política é revisada, no mínimo, anualmente ou sempre que ocorrer alteração relevante na estrutura, nos sistemas, nos prestadores de serviço, no quadro de Colaboradores ou no arcabouço regulatório aplicável.

12.3. As revisões e os testes são documentados e mantidos pelo prazo mínimo exigido pela regulamentação aplicável.

13. TREINAMENTO E DISSEMINAÇÃO

13.1. Esta Política é disponibilizada a todos os Colaboradores, que devem dela tomar ciência por ocasião de seu ingresso e a cada atualização relevante, sendo promovidas orientações periódicas sobre os procedimentos de continuidade.

14. DISPOSIÇÕES GERAIS

14.1. Os casos omissos e as situações não previstas nesta Política serão resolvidos pelo Diretor Responsável, à luz da regulamentação aplicável e das melhores práticas de mercado.

14.2. Esta Política entra em vigor na data de sua aprovação e permanece vigente por prazo indeterminado, até que seja revogada ou substituída por versão posterior.

ANEXO I — LISTA DE CONTATOS DE CONTINGÊNCIA

Quadro de contatos a ser preenchido e mantido atualizado pelo Diretor Responsável.

Função / Prestador	Contato responsável	Telefone / e-mail
Diretor Responsável pela PCN	Luis Chebl Massud Filho	11.98119-1200
Diretor de Gestão / substituto	Danilo Palinkas	11.98521-1535
Suporte de Tecnologia da Informação	Silva Souza	11.91160-1652
Administrador fiduciário	[__]	[__]
Custodiante / controladoria	[__]	[__]
Principais corretoras / contrapartes	[__]	[__]