NOCTUA ASSET MANAGEMENT LTDA.

PLANO DE CONTINGÊNCIA E CONTINUIDADE DE NEGÓCIOS

("**Política**")

[•]/2026

Válido a partir de	Janeiro/2026
Área responsável	Compliance
Autor	Diretora de Compliance
Contato	compliance@noctuaasset.com.br
Escopo/Destinatários	Todos os Colaboradores e Terceiros Relacionados da Noctua Asset, conforme aplicável

Comentado [LF1]: Confirmar e-mail

Capítulo 1 — Introdução

1.1 Objetivo e Finalidade

O presente Plano de Contingência e Continuidade de Negócios estabelece diretrizes e protocolos para assegurar a continuidade operacional da Noctua Asset Management Ltda., CNPJ nº 42.329.349/0001-11 ("**Noctua**" ou "**Gestora**"), frente a eventos adversos que possam comprometer suas atividades.

Este documento dirige-se a todos os sócios, diretores, colaboradores, prestadores de serviços e demais profissionais vinculados às operações da Gestora (denominados coletivamente "**Colaboradores**"), estabelecendo responsabilidades e procedimentos para mitigação de riscos e recuperação de atividades críticas.

O objetivo central é mapear vulnerabilidades, identificar processos essenciais e implementar medidas preventivas e reativas que garantam a prestação ininterrupta dos serviços de gestão de fundos de investimento, preservando os interesses dos cotistas e a integridade das operações.

Este Plano integra o arcabouço de controles internos da Gestora, conforme disposto no Manual de Controles Internos, e observa a metodologia de identificação de riscos estabelecida na Política de Gestão de Riscos.

1.2 Base Legal

(i) Resolução da Comissão de Valores Mobiliários ("**CVM**") nº 21, de 25 de fevereiro de 2021, conforme alterada ("**Resolução CVM nº 21**");

(ii) Resolução CVM nº 175, de 23 de dezembro de 2022, conforme alterada ("**Resolução CVM nº 175**") e seus anexos normativos;

(iii) Código da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais ("**ANBIMA**") de Administração e Gestão de Recursos de Terceiros ("**Código AGRT**");

(iv) Regras e Procedimentos de Administração e Gestão de Recursos de Terceiros, especialmente seu Anexo Complementar III ("**Regras e Procedimentos do Código AGRT**"); e

(v) Demais manifestações e ofícios orientadores dos órgãos reguladores e autorreguladores aplicáveis às atividades da Gestora.

1.3 Interpretação e Aplicabilidade

A interpretação deste Plano observará os seguintes critérios:

(i) Os termos técnicos adotam as definições previstas na Resolução CVM nº 175, salvo disposição expressa em contrário;

(ii) As referências genéricas a "fundos" englobam todas as classes, subclasses e séries, quando aplicável;

(iii) Menções a "regulamento" incluem anexos, apêndices e demais documentos constitutivos dos fundos;

(iv) As disposições aplicam-se tanto aos fundos constituídos após 02/10/2023 quanto àqueles adaptados à Resolução CVM nº 175.

Para fundos ainda não adaptados à Resolução CVM nº 175, mantêm-se aplicáveis as regras da Instrução CVM 555/14 e demais normativos específicos de cada categoria de fundo, observadas as responsabilidades e atribuições da Gestora.

Capítulo 2 — Estrutura de Gestão de Contingência

2.1 Equipe Responsável

A gestão e execução deste Plano são de responsabilidade da Equipe de Contingência, composta pelos seguintes membros:

(i) Diretor responsável pela contingência: Diretor de Compliance, Risco e PLD;

(ii) Membro Executivo: Diretor de Gestão;

(iii) Suplente do Diretor responsável: Analista da Equipe de Compliance, Risco e PLD (assume as funções do Diretor responsável em sua ausência, em conjunto com o Diretor de Gestão).

Compete à Equipe de Contingência avaliar cenários de risco, determinar o acionamento do Plano, coordenar ações de resposta e comunicação, e monitorar o restabelecimento das operações normais. As decisões estratégicas devem ser tomadas de forma colegiada ou, em caso de urgência, pelos administradores da Gestora.

2.2 Processo de Acionamento

O acionamento do Plano de Contingência segue o protocolo abaixo:

a) Identificação do Evento: Qualquer Colaborador que identifique situação que possa comprometer a continuidade das operações deve comunicar imediatamente o Diretor responsável pela contingência.

b) Avaliação Preliminar: O Diretor responsável avalia a natureza, gravidade e impacto potencial do evento, consultando o Diretor de Gestão e demais membros relevantes.

c) Declaração de Contingência: Confirmada a necessidade, o Diretor responsável declara formalmente o estado de contingência e determina as medidas aplicáveis.

d) Comunicação Interna: Todos os Colaboradores são notificados sobre a situação, as medidas em vigor e as responsabilidades individuais durante o período de contingência.

e) Implementação de Medidas: As ações previstas neste Plano são executadas de acordo com a natureza do evento (seção 3).

f) Monitoramento e Ajustes: O Diretor responsável acompanha continuamente a situação, reporta atualizações e promove ajustes conforme necessário até o retorno à normalidade.

g) Encerramento e Avaliação: Após a normalização, documenta-se o evento, avalia-se a efetividade das respostas e implementam-se melhorias ao Plano.

2.3 Comunicação Externa

Em situações de contingência que possam afetar a prestação de serviços aos Fundos ou o cumprimento de obrigações regulatórias, o Diretor responsável pela contingência avaliará a necessidade de comunicação às seguintes partes:

(i) Administrador Fiduciário dos Fundos afetados;

(ii) CVM, quando exigível pela regulamentação; e

(iii) ANBIMA, conforme aplicável.

A comunicação será realizada pelo Diretor responsável pela contingência ou, em sua ausência, pelo Diretor de Gestão, observados os prazos regulamentares aplicáveis.

2.4 Metas de Tempo de Recuperação

A Gestora estabelece as seguintes metas indicativas, não se configurando SLA contratual, para recuperação de atividades críticas:

(i) Ativação de operação remota: até 4 (quatro) horas;

(ii) Restabelecimento de comunicação com prestadores de serviços essenciais: até 4 (quatro) horas; e

(iii) Recuperação de acesso a sistemas críticos e backups: até 24 (vinte e quatro) horas.

Tais metas são indicativas e poderão ser ajustadas conforme a natureza e gravidade do evento, sendo seu cumprimento monitorado nos testes periódicos de efetividade.

Capítulo 3 — Análise de Riscos e Procedimentos

3.1 Infraestrutura Física

A Gestora identificou três dimensões críticas para a continuidade de suas operações: infraestrutura física, recursos tecnológicos e recursos humanos. Para cada dimensão, foram mapeados os principais riscos e estabelecidos protocolos de resposta.

A estratégia de contingência baseia-se na capacidade comprovada da Gestora de operar em regime remoto, com acesso cloud aos sistemas essenciais, redundância de comunicação e estrutura de backup entre colaboradores.

A sede operacional da Gestora concentra os recursos necessários para execução das atividades diárias. Eventuais impossibilidades de acesso ou utilização do espaço físico exigem rápida transição para operação remota.

SITUAÇÕES DE RISCO	MEDIDAS DE RESPOSTA
Falhas Utilitárias e Ambientais Interrupção de energia elétrica, desabastecimento de água, falhas no sistema de climatização, danos estruturais ao imóvel, falhas de conectividade (internet/telefonia).	Ativação imediata de operação remota. Colaboradores acessam sistemas via cloud computing, utilizam dispositivos pessoais para comunicação (celulares corporativos, aplicativos de mensageria) e mantêm fluxo operacional sem dependência da infraestrutura física. Diretorias avaliam necessidade de espaço alternativo caso a indisponibilidade seja prolongada.
Impedimentos de Acesso Bloqueios causados por manifestações, greves de transporte, interdições de autoridades públicas, condições climáticas adversas, emergências sanitárias ou quaisquer eventos que dificultem ou impeçam o deslocamento até a sede.	Regime de trabalho remoto com manutenção integral das atividades críticas. Diretor responsável monitora a evolução da situação e mantém comunicação constante com a equipe. Decisões operacionais e investimentos continuam sendo executados normalmente via ferramentas digitais.

3.2 Recursos Tecnológicos

A infraestrutura tecnológica constitui elemento fundamental para gestão de fundos, abrangendo sistemas de análise, comunicação com prestadores de serviços (administradores, custodiantes, auditores), relacionamento com investidores e armazenamento seguro de informações. A arquitetura cloud-native da Gestora mitiga significativamente riscos de indisponibilidade.

SITUAÇÕES DE RISCO	MEDIDAS DE RESPOSTA
Falhas Tecnológicas Sistêmicas Indisponibilidade de plataformas de administradores, queda de sistemas de informação financeira, comprometimento de equipamentos (hardware), ataques cibernéticos, perda de acesso a repositórios de dados, falhas em provedores de serviços tecnológicos.	Sistemas críticos são acessíveis via navegadores web de qualquer localidade com conexão à internet, eliminando dependência de equipamentos específicos. Comunicação migra para canais alternativos (telefonia móvel, WhatsApp corporativo, e-mail pessoal temporário). Dados armazenados em cloud possuem backup automático e redundância geográfica. Em caso de comprometimento de equipamentos individuais, colaboradores utilizam dispositivos alternativos. Para indisponibilidade de fornecedores externos, ativa-se contato direto com suporte técnico e, se necessário, canais alternativos de acesso às informações.

3.3 Recursos Humanos

A estrutura enxuta e qualificada da Gestora concentra expertise crítica em profissionais-chave. A indisponibilidade súbita desses profissionais representa risco significativo, mitigado por sistema de sucessão e capacitação cruzada.

A Gestora mantém matriz de sucessão interna, atualizada pelo Diretor responsável pela contingência, contendo a relação de funções críticas e respectivos substitutos designados. A matriz é revisada sempre que houver alteração na estrutura de pessoal.

SITUAÇÕES DE RISCO	MEDIDAS DE RESPOSTA
Ausências Críticas de Colaboradores Desligamento inesperado de diretores ou profissionais essenciais, afastamentos por motivos de saúde, ausências coletivas (surtos de doenças, emergências pessoais simultâneas), impedimentos legais ou regulatórios.	A Gestora mantém matriz de sucessão com profissionais capacitados para assumir temporariamente funções críticas. Durante ausências programadas (férias, licenças), colaboradores substitutos já assumem responsabilidades. Para eventos súbitos, ativa-se imediatamente o plano de sucessão, com o substituto designado assumindo atribuições essenciais sob supervisão da Diretoria. Em situações extremas, avalia-se contratação emergencial ou redistribuição temporária de responsabilidades.

Capítulo 4 — Governança e Testes de Efetividade

4.1 Confidencialidade

Este Plano contém informações estratégicas e operacionais sensíveis, sendo sua circulação restrita aos Colaboradores da Gestora. Qualquer compartilhamento externo requer autorização expressa da Equipe de Contingência.

4.2 Atualização e Revisão

O Diretor responsável pela contingência é responsável por manter este documento atualizado e aderente à realidade operacional da Gestora. Revisões obrigatórias ocorrem anualmente, sem prejuízo de atualizações extraordinárias motivadas por:

(i) Alterações significativas na estrutura operacional ou tecnológica;

(ii) Mudanças na composição da Equipe de Contingência;

(iii) Identificação de vulnerabilidades não mapeadas;

(iv) Publicação de novas normas regulatórias aplicáveis;

(v) Lições aprendidas em eventos de contingência reais ou simulados.

4.3 Testes Periódicos

A Gestora realizará, no mínimo anualmente, simulações de contingência para validar a efetividade deste Plano. Os testes abrangerão:

(i) Verificação de acesso remoto aos sistemas críticos;

(ii) Teste de comunicação via canais alternativos;

(iii) Validação de recuperação de backups;

(iv) Simulação de acionamento da cadeia de sucessão;

(v) Avaliação do tempo de resposta da Equipe de Contingência.

Os resultados dos testes serão documentados em relatório específico, identificando não conformidades e estabelecendo planos de ação corretivos. O relatório subsidiará a revisão periódica do Plano.

Histórico das atualizações desta Política

Data	Versão	Responsáveis
Janeiro de 2026	1.0	Diretor de Compliance, Risco e PLD