PLANO DE CONTINUIDADE DE NEGÓCIO

JTR GESTÃO DE RECURSOS LTDA.

("Gestora")

Junho/2026

Sumário

1. OBJETIVO

Este Plano de Continuidade de Negócio ("Plano") tem por objetivo estabelecer medidas a serem tomadas para identificar e prevenir contingências que possam causar prejuízos para as atividades da Gestora

Para minimizar perdas e evitar danos às atividades essenciais da empresa, a Gestora mapeou as contingências mais relevantes do negócio, e desenvolveu o presente Plano de Continuidade de Negócio visando permitir que, após a ocorrência de uma eventualidade ou desastre, a Gestora reassuma o processamento das operações críticas dentro de um intervalo de tempo adequado às necessidades de negócio.

Com base no Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros ("Código ANBIMA") e demais normas aplicáveis, observaram-se os eventos com maior possibilidade de ocorrência, buscando mitigar os riscos nos pontos de vulnerabilidade da sua estrutura de tecnologia.

Todos os Colaboradores da Gestora devem conhecer o presente Plano e suas alterações para, em caso de eventualidades, estarem preparados.

2. DIRETRIZES DO PLANO DE CONTINUIDADE DE NEGÓCIO

Para a eficaz implementação deste Plano de Continuidade de Negócios, a Gestora busca conhecer e reparar os principais pontos de vulnerabilidade de suas instalações e equipamentos. Para tal finalidade, são tomadas medidas que permitem a Gestora:

a) Conhecer e minimizar os danos no período pós-contingência;

b) Minimizar as perdas para si, seus clientes, seus sócios e colaboradores advindos da interrupção de suas atividades; e

c) Normalizar o mais rápido possível as atividades de gestão.

Para redução e controle de eventuais perdas com contingências, todos os sócios e Colaboradores da Gestora deverão conhecer os procedimentos de *backup* e salvaguarda de informações (confidenciais ou não), planos de evacuação das instalações físicas e melhores práticas de saúde e segurança no ambiente de trabalho.

Os horários críticos para acionamento do plano de continuidade de negócio são das 9h às 17h.

A Gestora possui como sede a unidade localizada na cidade de São Paulo, Estado de São Paulo, na Av. Presidente Juscelino Kubitscheck, 1600, 5º Andar, onde estão alocados seus recursos e operações, além da infraestrutura tecnológica necessária para as atividades de administração e gestão das carteiras de valores mobiliários.

Não obstante, para eventual necessidade extraordinária, conforme termos deste Plano, a Gestora pode contar com o escritório de contingência ("Site de Contingência"), localizado na cidade de São Paulo, Estado de São Paulo, na Rua Teodoro Sampaio, 1765, 4º Andar, sendo que o local dispõe de 4 (quatro)

posições fixas de trabalho, mais sala de reunião para utilização de notebook, com internet cabeada e sem fio para conexão dos equipamentos e 4 (quatro) linhas telefônicas para contato com os clientes.

Outrossim, a Gestora tem plena capacidade de operar em sistema de trabalho remoto *home office* e/ou sistema híbrido, adaptando-se às circunstâncias específicas de cada área, sendo avaliado e aprovado ou não pelos Gerentes, com respaldo da Alta Direção. O modelo busca, de maneira eficiente, que o nível de produtividade e segurança se mantenham, em conformidade com este plano de continuidade de negócios, não interrompendo as operações em andamento, tornando-a mais célere, flexível e dinâmica.

2.1 MONITORAMENTO

Todos os sistemas que são cruciais para as operações de negócios da Gestora, incluindo, mas não limitados a sistemas que garantam processamento imediato das transações de valores mobiliários, manutenção de contas de clientes e acesso a contas de clientes, são considerados sistemas críticos de missão. Alguns colaboradores selecionados têm acesso a sistemas críticos de suas casas.

Os principais pontos de atenção monitorados pela Gestora são:

- Internet
- Telefonia
- Rede Elétrica
- Manutenção preventiva aos equipamentos

Tais serviços possuem monitoramento ativo, tanto por parte dos fornecedores como por parte de nossa equipe interna, visando antecipar o conhecimento da possível falha, uma vez identificada a inatividade total ou parcial de algum destes serviços, o departamento de TI deve mensurar o tempo para restabelecimento do pleno funcionamento, dados estes que serão utilizados pelo Gestor para tomada de decisão.

2.1.1 AMEAÇAS MENSURADAS

A) Back-up e Recuperação de Dados

A Gestora mantém cópias eletrônicas de todas as informações fundamentais relacionadas aos fundos de investimento e seus investidores no seu servidor e em um ambiente seguro na "nuvem".

Os arquivos do *data center* são copiados diariamente para uma cópia local, e duas cópias em nuvem, caso ocorra alguma falha que comprometa o acesso local a essas informações, os usuários receberam um *link* de acesso ao seu perfil na nuvem onde poderão utilizar os arquivos em caráter de contingência.

B) Impossibilidade de Acesso ao Escritório

Se, por qualquer circunstância, os colaboradores não conseguirem chegar ao escritório, os colaboradores poderão ser direcionados ao Site de Contingência ou poderão trabalhar de casa, conforme decisão do Diretor de Compliance, Risco e PLD, com o acesso de segurança usando o acesso remoto (VPN).

C) Testes Operacionais

A Gestora irá testar anualmente sua prontidão em caso de desastres para garantir que os sistemas fundamentais da Gestora estão aptos a operar de uma localidade remota. A Gestora também irá verificar se as cópias eletrônicas das informações dos fundos de investimento e Investidores que são mantidas no escritório da Gestora e na "nuvem" não foram corrompidas e estão disponíveis para uso pela Gestora.

D) Métodos Alternativos de Comunicação

A Gestora possui meios disponíveis pelos quais Administrador e Investidores podem contatar colaboradores e pelos quais os colaboradores podem contatar uns aos outros, incluindo endereços de e-mails de trabalho, números de telefones de trabalho, números de telefones domésticos e números de telefones celulares.

E) Providências complementares e informações a clientes

Na ocasião de uma emergência ou outra interrupção de negócios significativa, a Gestora irá contatar o Administrador, Investidores e todos os órgãos reguladores que supervisionam a Gestora a fim de informar da condição da Gestora e de oferecer informações de contato através dos quais a Gestora pode ser contatada, o quanto antes possível.

E) Infraestrutura

Em caso de falha no fornecimento elétrico os nobreaks são ativados para estações de trabalho e servidores, com autonomia de 30 minutos, tempo para o gerador do condomínio entrar em atividade o qual possuí autonomia de algumas horas de funcionamento.

O site principal, possuí 3 (três) links de internet para redundância, em caso de falha do link principal, o primeiro link redundante é acionado, em caso de falha destes dois links, o modem 4G com Wi-Fi é ativado para suprimir as necessidades críticas.

Para telefonia caso o link E1 não possa ser utilizado 3 (três) linhas móveis são disponibilizadas para uso da equipe.

F) Invasão da intranet por hackers

Anualmente a Gestora realiza teste de invasão externa, contratado junto a provedor terceirizado de serviços. Duas portas são testadas por vez, e o ataque simulado é anônimo, sendo que a Gestora recebe o reporte do teste ao final do processo.

São também ameaças que podem ensejar na aplicação deste Plano:

- Humana: Greves, Distúrbio Civil, Falha de Prestador de Serviços/Parceiro, Acesso Indevido às Instalações e Erro Humano não intencional.

- Tecnológica: Falha em Aplicativo (SW), Falha em Hardware (HW), Falha em sistemas Operacionais, Vírus de Computador, Falha em Rede Interna (LAN), Falha na Entrada de Dados, Falha em Rede Externa (WAN), Falha de Telecom – Dados e Falha em Sistema de Acesso.

- Infraestrutura: Falha em Telecom - Voz, Falha em Sistema de Refrigeração, Interrupção de Energia Elétrica, Falha em Instalações Elétricas.

- Natural Alagamento Interno do Ambiente, Queda de Raios, Vendaval e Incêndio.

- Física: Problema Estrutural ou de Instalações e Rompimento de Tubulação Interna (água, esgoto e gás).

2.1.2 MEDIDAS PARA RETOMADA RÁPIDA

Ainda, para a retomada célere e eficaz das operações após uma contingência, a Gestora mantém procedimentos que a permitem:

a) Utilizar alternativas de dentro ou fora da Gestora para substituição de equipamentos danificados;
b) Manter saldo financeiro e/ou acesso a crédito para qualquer despesa de contingência ou compra de equipamentos ou serviços que se fizerem necessários;
c) Manter suas atividades mesmo durante os efeitos da contingência, através de acesso remoto por parte de seus Colaboradores;
d) Disponibilizar notebooks para os colaboradores seguirem desempenhando suas atividades remotamente em casos de contingência;
e) Retornar definitivamente a utilização das instalações de sua sede após a ocorrência da contingência; e
f) Avaliar as perdas da interrupção dos negócios.

3. DIVULGAÇÃO E TREINAMENTO

A divulgação deste plano deve ser realizada em ocasião de contratação de novos funcionários, este material deve estar à disposição dos colaboradores através da rede interna, bem como divulgação na intranet (*Sharepoint*). Este Plano é de uso restrito dos Colaboradores da Gestora e não pode ser divulgado para terceiros, exceto se autorizado pelo Diretor de Compliance, Risco e PLD.

Deverão ser realizados treinamentos com a execução prática de acionamento e deslocamento da contingência com periodicidade bienal.

4. REALIZAÇÃO DE TESTES

Os testes de funcionamento de todos os serviços da contingência devem ser realizados pelo menos uma vez ao ano pelo departamento de TI.

Os testes e simulações devem ser formalmente documentados, para fornecer material útil a futuras tomada de decisão relacionadas a melhorias do plano de continuidade de negócio. Este plano deve ser revisado anualmente dispensando sua alteração caso não haja melhorias pertinentes a escopo de plano de ação.

5. ÁREA RESPONSÁVEL

O processo de continuidade de negócio é de responsabilidade e gestão do Diretor de Compliance, Risco e PLD, que determina as etapas que deverão ser executadas e os cenários de risco e impacto sobre o negócio e quais as ações que deverão ser executadas para a manutenção de um ambiente sempre protegido. Abaixo apresentamos informações do referido Diretor:

Informações do Diretor de Compliance, Risco e PLD
Nome: Sr. João Baptista Peixoto Neto
Cargo: Diretor de Compliance, Risco e PLD
Telefone para contato: (11) 3080-8170
E-mail para contato: compliance@jtrinvestimentos.com.br

6. Versões

Histórico das atualizações		
Data	**Versão**	**Responsável**
Junho de 2026	1ª e atual	Diretor de Compliance, Risco e PLD