PLANO DE CONTINUIDADE DE NEGÓCIO

TUERI GESTORA DE RECURSOS LTDA.

Abril/2026 – Versão 2.0

ÍNDICE

Controle do Documento

Campo	Descrição
Título	Plano de Continuidade de Negócio
Área Responsável	Compliance
Versão	2024.1
Classificação	Confidencial
Próxima Revisão	Anual
Diretor Responsável	André Tavares Castanheira — Diretor de Risco e Compliance
Telefone	(11) 3884-9356
E-mail	atc@tueriinvest.com
Site	https://www.tueriinvest.com
1º Líder de Contingência	Pedro Emerique
Telefone (Líder)	(11) 94424-0584
E-mail (Líder)	pe@tueriinvest.com.br

Documentos Vinculados

Documento	Finalidade
Política de Segurança da Informação	Reduzir riscos de fraudes, espionagem, sabotagem, vandalismo, vírus, uso indevido e roubo de informações que comprometam os princípios básicos da segurança da informação.
Matriz de Segurança das Informações	Descreve os procedimentos a serem adotados em casos de falhas na infraestrutura e em processos vitais.

1. Sumário Executivo

O Plano de Continuidade de Negócio (PCN) da **TUERI** tem como propósito garantir que as operações críticas da organização sejam mantidas ou rapidamente retomadas em situações de interrupção causadas por eventos internos ou externos.

1.1 Objetivos

- Definir as regras e responsabilidades aplicáveis à gestão de crises e continuidade operacional;
- Assegurar que todos os colaboradores conheçam e estejam capacitados para executar o PCN;
- Minimizar o impacto de interrupções sobre clientes, operações e imagem institucional;
- Garantir conformidade com requisitos regulatórios vigentes.

1.2 Processos Vitais

#	Processo Vital
1	Execução de ordens
2	Liquidação de operações
3	Gerenciamento de riscos, limites e concentração
4	PLD/FTP
5	Comunicação ao COAF

2. Premissas e Estrutura do PCN

O PCN assegura à **TUERI** a continuidade dos negócios em caso de paralisação de um ou mais processos críticos. Um sinistro se concretiza quando ameaças internas ou externas exploram vulnerabilidades nos processos.

Os processos críticos foram mapeados por meio de levantamentos junto aos gestores das principais áreas de negócio.

2.1 Composição do PCN

PCN = PAC + PCO + PRD

Componente	Sigla	Descrição
Programa de Administração da Crise	**PAC**	Acionado após a declaração de crise. Abrange todo o processo até o retorno à normalidade.
Plano de Continuidade Operacional	**PCO**	Primeiros procedimentos do PAC, voltados aos processos de negócio.
Plano de Recuperação de Desastres	**PRD**	Acionado junto ao PCO; focado na recuperação e restauração dos componentes que suportam o PCN.

2.2 Etapas de Desenvolvimento

1. Análise de riscos de TI;
2. Análise de Impacto nos Negócios (BIA — *Business Impact Analysis*);
3. Definição da estratégia de recuperação.

---

3. Infraestrutura — Site Principal e Site de Redundância

3.1 Site Principal

Localizado na **Alameda Lorena, nº 427, Sala 60 – Jardim Paulista, CEP 01424-003, São Paulo/SP**, onde a administração de carteiras de valores mobiliários é executada em condições normais.

3.2 Ambiente de Redundância — Nuvem

A **TUERI adota uma estratégia de redundância totalmente baseada em nuvem**, eliminando a dependência de um site físico de backup. O acesso a todos os sistemas é realizado via **navegador web**, permitindo que qualquer colaborador opere a partir de qualquer dispositivo com conexão à internet.

A infraestrutura de redundância é composta por duas camadas:

Camada 1 — Google Workspace (G Suite) Garante acesso contínuo a e-mails, documentos, arquivos e comunicação institucional:

Recurso	Finalidade em Contingência
Gmail	Comunicação interna e externa
Google Drive	Acesso a documentos, planilhas e arquivos institucionais
Google Meet	Reuniões e alinhamentos remotos
Google Docs / Sheets	Edição colaborativa de documentos em tempo real
Google Calendar	Gestão de agenda e coordenação de equipes

Camada 2 — Sistema Proprietário com Backup em Nuvem O sistema proprietário da TUERI possui **backup contínuo em servidor remoto na nuvem**, garantindo que as operações críticas — execução de ordens, liquidação, gestão de riscos e compliance — permaneçam acessíveis via web mesmo em caso de indisponibilidade do Site Principal.

Em situação de contingência, a estratégia adotada é a **operação remota via Home Office**, com todos os colaboradores acessando ambas as camadas por navegador, sem necessidade de software instalado ou site físico de backup.

3.3 Designação por Área em Contingência

Área	Local de Contingência
Gestão	Home Office
Risco e Compliance	Home Office
Distribuição	Home Office
Administrativo / Financeiro	Home Office
Tecnologia da Informação	A definir conforme a situação

4. Monitoração e Declaração de Desastre

4.1 Definição de Desastre

Será considerado **desastre** quando o tempo total de recuperação dos processos for superior ao **MTD (Maximum Tolerable Downtime)** definido para cada processo crítico (ver Seção 5).

4.2 Comunicação de Eventos

Qualquer colaborador que identificar uma anormalidade capaz de paralisar processos críticos deverá:

1. Comunicar imediatamente ao seu **superior imediato**;
2. O superior comunicará ao **Líder de Contingência**;
3. O Líder de Contingência avaliará o ocorrido e comunicará ao **Diretor responsável pelo PCN**.

O canal de comunicação centralizado é o ponto de contato oficial para acionamento do PCN.

4.3 Declaração de Contingência

Com base no impacto avaliado e no horário crítico do evento, compete ao **Diretor responsável pelo PCN** declarar ou não a contingência.

Diretor responsável: André Tavares Castanheira — (11) 3884-9356 | atc@tueriinvest.com

1º Líder de Contingência: Pedro Emerique — (11) 94424-0584 | pe@tueriinvest.com.br Na ausência do Diretor, Pedro Emerique assumirá interinamente.

---

5. Processos e Sistemas Críticos

5.1 Conceitos e Definições

Sigla	Termo	Definição
MTD	*Maximum Tolerable Downtime*	Tempo máximo que a organização pode tolerar a ausência de uma função crítica.
RTO	*Recovery Time Objective*	Tempo disponível para recuperar sistemas e recursos após uma interrupção.
WRT	*Work Recovery Time*	Tempo necessário para restaurar e validar os sistemas em pleno funcionamento.

Fórmula: MTD = RTO + WRT

5.2 Processos Críticos e MTD

Área	Processo	Sistemas	MTD
Gestão / Distribuição	Execução de ordens	Todos	Até 30 min (antes das 14h) / Imediato (após 14h)
Back Office / Financeiro	Liquidação de operações; Internet banking	Todos	Até 30 min (antes das 14h) / Imediato (após 14h)
Compliance e Risco	PLD; Comunicação ao COAF; Gerenciamento de riscos e limites	Todos	Até 30 min (antes das 14h) / Imediato (após 14h)

6. Ameaças e Abrangência

6.1 Classificação das Ameaças

Categoria	Ameaças
Humanas	Greves, distúrbio civil, falha de prestador de serviços, acesso indevido às instalações, erro humano não intencional.
Tecnológicas	Falha em aplicativo (SW), falha em hardware (HW), falha em sistema operacional, vírus de computador, falha em rede interna (LAN) ou externa (WAN), falha na entrada de dados, falha em telecom e em sistema de acesso.
Infraestrutura	Falha em telecom (voz), falha no sistema de refrigeração, interrupção de energia elétrica, falha em instalações elétricas.
Naturais	Alagamento interno, queda de raios, vendaval, incêndio.

Categoria	Ameaças
Físicas	Problema estrutural ou de instalações, rompimento de tubulação interna (água, esgoto ou gás).

6.2 Potenciais Impactos

- Interrupção da prestação de serviços a clientes;
- Multas e sanções regulatórias;
- Perda da capacidade de gestão e controle;
- Comprometimento da imagem institucional;
- Exposição negativa na mídia e perda de vantagem competitiva.

---

7. Ações e Procedimentos

7.1 Impossibilidade de Acesso ao Prédio

Ameaças enquadradas: princípio de incêndio, ameaça de bomba, bloqueios, manifestações.

Em até 20 minutos após o evento:

1. Contatar o responsável pelo Site de Redundância para comunicar a ocupação e solicitar disponibilização de local, notebooks, impressoras e acesso à internet;
2. Comunicar os colaboradores que atuarão em regime de Home Office;
3. Orientar cada área a se dirigir ao destino de contingência conforme a tabela da Seção 3.3;
4. Publicar alerta no site da TUERI informando o status de contingência, telefones dos colaboradores e número de contato fixo do site backup.

7.2 Falha na Infraestrutura e Tecnologia

A Unidade de Redundância atuará como site de contingência em caso de falha no ambiente de TI do Site Principal. A comunicação entre as unidades é realizada por **links redundantes**.

Recursos de TI contemplados:

- **Servidores:** espelhamento em tempo real entre Site Principal e Site de Redundância.
- **Telecom:** links redundantes de dados e voz.
- **Energia elétrica:** na falta de energia, os nobreaks do CPD são ativados automaticamente com **autonomia de 3 horas**. As áreas abastecidas são as mapeadas como críticas pelo BIA:

Área
Distribuição
Tecnologia da Informação
Back Office
Administrativo / Financeiro
Gestão de Riscos e Compliance

7.3 Acionamento da Contingência Externa

1. Contatar o gestor da empresa contratada para prestação de serviços de redundância/backup e informar o início da contingência;
2. Contatar a empresa **XXXX** — para encaminhar todas as ligações para os ramais do Site de Contingência, se necessário;
3. Direcionar cada equipe ao local designado conforme Seção 3.3.

---

8. Retorno à Normalidade

1. O **Líder da Contingência** encerra formalmente o PCN e comunica o Diretor e os Gestores envolvidos;
2. Quando o acesso ao prédio estiver liberado e em condições normais, todos os colaboradores serão comunicados por seus gestores para **retornar no dia seguinte**;
3. Solicitar à área de TI a remoção do comunicado de contingência no site da TUERI.

---

9. Administração do Plano

A gestão do PCN é de responsabilidade da **área de Compliance**, que determina o ciclo e as etapas de atualização do plano, garantindo que os cenários de risco, impactos e estratégias reflitam o ambiente de negócios atual da TUERI.

A área de TI deve participar ativamente das decisões relacionadas a:

- Planejamento tecnológico;
- Gerenciamento de mudanças;
- Gerenciamento de riscos;
- Tratamento de problemas e incidentes.

9.1 Divulgação e Treinamento

- Sessões de divulgação realizadas **anualmente** para todos os colaboradores;
- Organização conjunta entre as áreas de **TI** e **Administrativo/Financeiro**;
- Novos colaboradores admitidos em funções críticas devem ser treinados **imediatamente** após admissão;
- O programa de treinamento deve contemplar: riscos, ameaças, controles, responsabilidades, premissas, estratégias e alterações recentes do PCN.

9.2 Realização de Testes

Item	Descrição
Periodicidade	Mínimo anual
Responsável	Área de Tecnologia da Informação
Aprovação	Alta Administração
Arquivo	Mínimo de 5 anos
Restrição	Os testes **não devem causar indisponibilidade** nos ambientes de negócio
Escopo	Cenários e ameaças com maior probabilidade de ocorrência, conforme o

Item	Descrição
	plano

Anexo I — Controle de Versão

Versão	Data	Responsável	Descrição das Alterações
2026.1	2026	Compliance	Versão inicial do documento
0	Abril/ 2026	Tueri Invest	Atualização regulatória 2026

São Paulo, 15 de abril de 2026.

_____

André Castanheira