Plano de Continuidade de Negócio

Complemento a Política de Segurança da Informação

Área de Gestão de Compliance

Versão 2.0

I – Controle de Versão

Versão	Data	Nome	Ação (Elaboração, Revisão, Alteração, Aprovação)	Conteúdo
1.0	06/2016	Marcelo Couto	Elaboração	Primeira versão do documento.
2.0	09/11/2017	Claudio Fernandes	Revisão	Revisão anual do documento
	13/11/2017	Diretoria Tercon	Aprovação	

II – Sumário Executivo

Objetivos do Plano:

- Definir as regras aplicáveis com base na estrutura da **Tercon** e
- Assegurar que todos conheçam o Plano de Continuidade de Negócio (PCN).

Processos Vitais:

- Execução de ordens;
- Liquidação de operações;
- Gerenciamento de riscos, limites e concentração;
- PLD; e
- Comunicação ao COAF.

Site de Contingência:

Localização	Rua Princesa Isabel, 232 Sala 15 – Brooklin Paulista Escritório da BRIANEZI INFORMATICA LTDA
CONTATO	Andre Brianezi - Diretor Comercial / Técnico
Telefones	Tel.: 55 (11) 3522-6609 Cel.: 55 (11) 99902-9657
e-mail	andre@brianezi.com.br

Responsáveis pelo Continuidade do Negócio:

Staff	Nome	Telefones
Diretor de Contingência	Marcelo Couto	Residencial: 11 3772-6693 Celular: 11 98252-4723
1º Líder de Contingência	Ângela Vasconcellos	Celular: 11 99194-9257

III. Premissas e Objetivos do Projeto

O Plano de Continuidade de Negócios (PCN) assegurará à **TERCON** a continuidade de seus negócios em caso de paralisação, decorrente de sinistro, de um ou mais processos considerados críticos. O sinistro torna-se realidade quando ameaças internas ou externas exploram as vulnerabilidades dos processos.

Os processos críticos ao negócio da **TERCON** foram mapeados por meio de levantamento de informações com os Gestores das principais áreas de negócio.

Para tanto, o PCN é definido como (PCN = PAC + PCO + PRD), a saber:

- PAC = Programa de Administração da Crise – É acionado após decretada a Crise, e é voltado para todo o processo. Tem seu término quando se volta à normalidade;

- PCO = Plano de Continuidade Operacional – São acionados os primeiros procedimentos do PAC, e é voltado aos processos de negócio;

- PRD = Plano de Recuperação de desastres – É acionado junto com o PCO, e é focado na recuperação/restauração de componentes que suportam o PCN.

O desenvolvimento do Plano de Continuidade de Negócios é baseado na avaliação dos processos críticos estabelecidos pela Administração compreendendo às suas principais etapas:

- Análise de riscos de TI;

- Análise de Impacto nos Negócios (BIA);

- Estratégia de recuperação.

Desta forma será necessário simular situações de emergências, definir responsabilidades e escopo de atuação para cada colaborador na execução do PCN. A manutenção do PCN atualizado e o treinamento dos colaboradores são fatores crítico de sucesso.

IV. Site Principal e Site Redundância

A **TERCON** conta com duas unidades: a principal e a de redundância.

A unidade principal (Site Principal) situa-se à Rua Américo Brasiliense, 1765 – 5º Andar conjunto 52, onde a administração de carteiras de valores mobiliários é executada em condições normais.

A unidade de redundância (Site Redundância) contém exatamente todos os mesmos recursos tecnológicos da Unidade Principal, podendo cada estação de trabalho utilizar tanto a Unidade Principal como o Site de Redundância. Portanto, em situações de contingência, os funcionários designados devem se dirigir para esse endereço de forma que haja o mínimo impacto possível dentro das atividades da

TERCON. Para reduzir esse impacto, o site de redundância contém servidor espelho em tempo real do servidor do Site Principal da **TERCON**.

IV.1. Site de Redundância

LOCALIZAÇÃO	Rua Princesa Isabel, 232 Sala 15 – Brooklin Paulista Escritório da BRIANEZI INFORMATICA LTDA
CONTATO	Andre Brianezi - Diretor Comercial / Técnico
TELEFONES	Tel.: 55 (11) 3522-6609 Cel.: 55 (11) 99902-9657
e-mail	andre@brianezi.com.br

Em função do site de redundância atender os processos críticos em caso de contingência, segue abaixo a designação do local que os colaboradores das áreas devem se dirigir nessas situações:

Área	Local de Contingência
Gestão	Site Redundância
Risco e Compliance	Site Redundância
Distribuição	Home Office
Administrativo/Financeiro	Home Office
TI	Depende da situação

V. Plano de Monitoração e Declaração de Desastre

V.1. Definição de Desastre

Será considerado desastre quando o tempo total de recuperação dos processos for superior ao tempo máximo apontado no item VI – Processos e Sistemas Críticos.

V.2. Monitoração de Comunicação de Eventos

Qualquer colaborador da **TERCON**, ao constatar alguma anormalidade que paralise quaisquer processos apontados no item VI deste Plano deverá comunicar o fato ao seu superior imediato, este por sua vez comunicará o fato a um dos Líderes de Contingência, a saber:

Staff	Nome	Telefones	E-mail
Diretor de Contingência	Marcelo Couto	Residencial: 11 3772-6693 Celular: 11 98252-4723	marcelo.couto@terconbr.com.br marceloalbertocouto@gmail.com
1º Líder de Contingência	Ângela Vasconcellos	Celular: 11 99194-9257	angela@terconbr.com.br aavascon3@gmail.com
2º Líderes de Contingência	Danilo Castro Ferreira	Residencial: 11 5011-5468 Celular: 11 95482-7441	danilocastroferreira@outlook.com.br
	Claudio Blanco Moreno	Residencial: 11 4238-5891 Celular: 11 97092-4807	claudio@terconasset.com.br
	João Douglas Oliveira	Celular: 11 96677-5893	Joao.douglas@terconasset.com.br

Este é o meio de comunicação a ser utilizado pelos colaboradores da **TERCON** como ponto central de contato para solicitar ajuda ou relatar alguma situação que demande o acionamento do PCN.

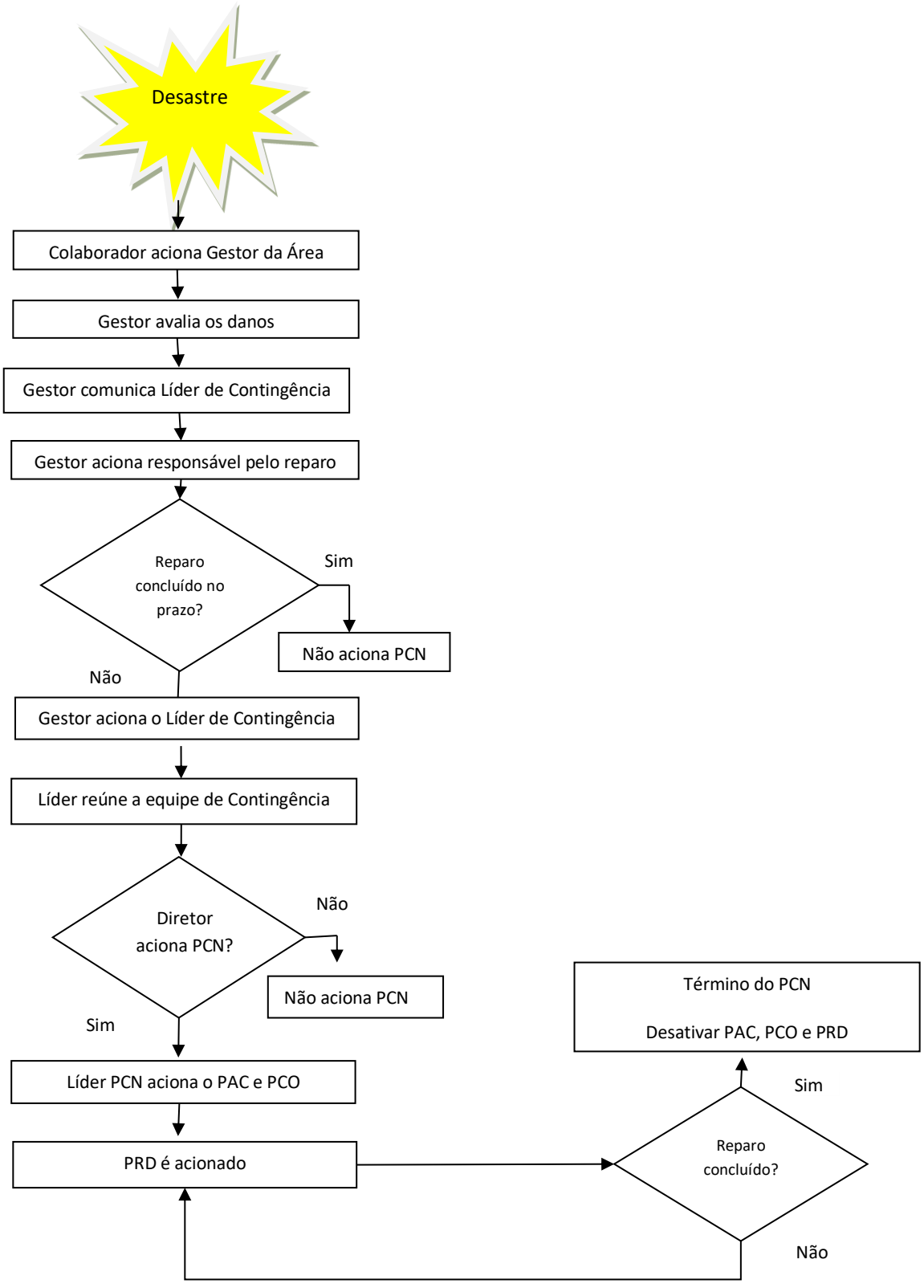
V.3. Declaração de Desastre/Contingência

Ao ocorrer quaisquer eventos que paralise algum processo essencial ao negócio, o líder de Contingência avaliará a ocorrência e comunicará ao Diretor responsável pelo PCN.

Com base nas informações recebidas e avaliação do grau de impacto versus horário crítico, compete ao Diretor declarar ou não a contingência.

Em caso da ausência do Diretor responsável pelo PCN assumirá interinamente o 1º líder de Contingência.

Na figura abaixo está descrito Fluxo de Acionamento do PCN que resultará ou não na declaração da contingência.


Desastre
Colaborador aciona Gestor da Área
Gestor avalia os danos
Gestor comunica Líder de Contingência
Gestor aciona responsável pelo reparo
Reparo concluído no prazo?
Sim
Não aciona PCN
Não
Gestor aciona o Líder de Contingência
Líder reúne a equipe de Contingência
Diretor aciona PCN?
Não
Não aciona PCN
Sim
Líder PCN aciona o PAC e PCO
PRD é acionado
Reparo concluído?
Sim
Término do PCN
Desativar PAC, PCO e PRD
Não

VI. Processos e Sistemas Críticos

Processo crítico pode ser definido como um processo de trabalho que uma vez paralisado por tempo superior ao definido pela unidade gestora do negócio irá afetar sensivelmente as operações e serviços da organização gerando maior impacto nos clientes internos e externos, definido pela fórmula (MTD = RTO + WRT).

Definição:

- MTD (Maximum Tolerable Downtime) = Trata-se do tempo máximo que um negócio pode tolerar a ausência ou indisponibilidade de uma função de negócio em particular. Diferentes funções de negócio terão diferentes MTD's.

- RTO (Recovery Time Objective) = Tempo disponível para recuperar sistemas e recursos de uma ruptura.

- WRT (Work Recovery Time) = Tempo que leva para copiar e rodar uma vez os sistemas (hardware, software e configuração) a serem restaurados para as funções de negócios críticas.

VI.1. Processos com MTD de até 30 minutos até às 14:00h e MTD IMEDIATO APÓS às 14:00h

Área	**Processo**	**Sistemas**
Gestão/Distribuição	Executar ordens	Todos
Back Office/Financeiro	• Liquidar operações • Internet banking	Todos
Compliance e Risco	• PLD • Comunicação COAF • Gerenciamento de riscos, limites e concentração	Todos

VII. Abrangências

VII.1. Ameaças Relacionadas

No entendimento dos gestores das áreas avaliadas as ameaças com grau de vulnerabilidade significante estão divididas em:

a. Humanas

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

b. Tecnológicas

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.

c. Infraestrutura

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

d. Naturais

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

e. Físicas

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

Cabe ressaltar que paradas não programadas podem resultar em perdas tangíveis e intangíveis aos negócios da **TERCON**, acarretando perda de confiança de colaboradores e clientes nos processos de negócios. Desta forma, os potenciais impactos apontados pelos gestores numa eventual interrupção no negócio são:

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

VIII. Ações e Procedimentos

Qualquer colaborador deverá estar apto a identificar as ameaças que possam levar a paralisação dos negócios e comunicar imediatamente ao líder do Plano de Continuidade de Negócios.

VIII.1. Impossibilidade de Acesso ao Prédio

Dentre as ameaças que impossibilitam o acesso ao prédio destacamos:

- Princípio de Incêndio;
- Ameaça de Bomba;
- Bloqueios;
- Manifestações.

VIII.1.1. Ações de 05 a 10 minutos após a evidência

Responsável: Líder do PCN

Procedimentos:

A Área Administrativa entrará em contato com a Administração do Condomínio para esclarecimentos e caso necessário, também fazer contato com os seguintes órgãos públicos:

- Administração do prédio: MARIO DAL MASO IMÓVEIS

  Rua dos Chanés, 95 - Moema 04087-030 - São Paulo/SP

  Tel. (11) 5095-1335

  Marlene – Marlene@mariodalmaso.com.br

- Zelador: Guto (11) 5181-4130;

- Síndico: Edmundo Mussi – 11 5184-0511 / 5184-0401 / 11 98318-1068

  www.mussi.com.br;

- Bombeiros: 193 (Incêndio e Ameaça de Bomba);

- Defesa Civil: 199 (Ameaça de Bomba, Greves, Bloqueios e Inundações);

- Polícia Civil: 147 (Ameaça de Bomba, Roubo e Furto de Informações e ativos).

VIII.1.2. Ações em até 20 minutos após a conclusão da etapa anterior

- Entrar em contato com o responsável pelo site backup, conforme indicação no item 2, para avisá-lo sobre a ocupação dos integrantes das áreas contingenciadas e disponibilizar local, notebook e impressora, assim como acesso à Internet, bem como avisar os componentes que atuarão em regime Home Office.

- Avisar aos integrantes das áreas contingenciadas para que se dirijam ao endereço do site redundância, ou as residências para atuação no regime Home Office, conforme relação indicada abaixo:

ÁREA CONTINGENCIADA	NOME	CONTATO	E-MAIL
Distribuição	Luiz Fernando Vasconcellos	11 – 99325-7919	lfernando@terconbr.com.br lfernandov@terra.com.br
BackOffice	Marcelo Couto	11 – 98252-4723	Marcelo.couto@terconbr.com.br marceloalbertocouto@gmail.com
Administrativo/Financeiro	Ângela Vasconcellos	11 –99194-9257	angela@terconbr.com.br angelaav@terra.com.br
Compliance e Risco	Marcelo Couto	11 – 98252-4723	Marcelo.couto@terconbr.com.br marceloalbertocouto@gmail.com
Tecnologia da Informação	Andre Brianezi Brianezi Informática	11 – 99902-9657 11-3522-6609	andre@brianezi.com.br

- Disponibilizar alertas no site da TERCON indicando o status de contingência, telefones dos colaboradores e telefone fixo do site backup para atendimento.

VIII.2 Falha na Infraestrutura e Tecnologia

Para não haver interrupções nas atividades o ambiente de TI no site principal da sede a Unidade de Redundância será o site de contingência da sede.

A comunicação entre as unidades de negócio é feita por links redundantes. A seguir destacamos a infraestrutura de TI de cada unidade de negócio.

- Servidores
- Telecom
- Energia Elétrica

Na falta de energia elétrica, além das baterias próprias dos Notebooks, são ativados automaticamente os nobreaks localizados no site principal no CPD com autonomia de 3 horas.

As áreas abastecidas pelos Nobreaks são as mesmas mapeadas com processos críticos pelo BIA.

- Distribuição
- Tecnologia da Informação
- BackOffice
- Administrativo/Financeiro
- Gestão de Riscos e Compliance

VIII.3 Acionamento da Contingência externa

Manter contato com o gestor da empresa contratada para prestação de serviços de redundância / backup e contingência e avisar do início do processo de contingência.

As equipes irão para o lugar destinado a cada uma delas.

Manter contato com a empresa TKS Telecomunicações Ltda. - José Rodrigues Junior – Tel. (11) 3488-0600 (Manutenção do PABX) e solicitar o encaminhamento de todas as ligações para os ramais do escritório do Site de Contingência, se for o caso.

IX. Procedimentos de retorno à normalidade – Site Principal

Cabe ao Líder da Contingência encerrar o PCN e comunicar ao Diretor e aos Gestores envolvidos no processo.

Quando o acesso ao prédio estiver liberado e em condições de normalidade, comunicar a todos os colaboradores da TERCON por meio de seus gestores para que retornem aos seus postos de trabalho no dia seguinte.

Solicitar à área de TI que retire o comunicado publicado no site da TERCON sobre a situação de contingência.

X. Administração do Plano

A continuidade de negócios de uma organização, assim como a recuperação de desastres é o resultado da execução e da manutenção de um processo contínuo que envolve planejamento, formalização, monitoração e melhorias.

O processo de Continuidade de Negócios é de responsabilidade e gestão da área Compliance, que determina o ciclo e as etapas que deverão ser executadas para que tanto os cenários de risco e impacto sobre os negócios como as estruturas e estratégias que embasam o PCN possam ser atualizadas refletindo o ambiente de negócios da TERCON.

Para que a área de TI possa verificar o grau de atualização do PCN e decidir quanto ao momento em que o processo de continuidade de negócios será atualizado, os processos de planejamento de negócios e tecnológico, gerenciamento de mudanças, gerenciamento de riscos, tratamento de problemas e de incidentes devem prever a participação desta área nas decisões relevantes destes processos.

X.1 Divulgação e Treinamento

Um dos fatores de primordiais para o funcionamento deste plano são o conhecimento e a familiaridade das pessoas e demais envolvidos na execução das atividades de continuidade de negócios e recuperação de desastres com as estratégias e recursos definidos no planejamento.

Para que seja possível esta familiaridade e conhecimento do plano, conferindo-lhe credibilidade, a equipe da TERCON definiu que serão realizadas anualmente sessões de divulgação a todos os colaboradores e envolvidos no planejamento de continuidade de negócios.

Estas sessões serão organizadas pela área de TI em conjunto com a área de Administrativa/Financeira com o objetivo de manter os colaboradores atualizados sobre os conceitos de continuidade adotados, os objetivos pretendidos com o planejamento e sobre o funcionamento da estratégia de recuperação de desastres e continuidade de negócios.

Para que este conhecimento seja preservado, os colaboradores admitidos e os transferidos para funções de negócios críticas, principalmente aqueles que pertencem à equipe de contingência, deverão ser instruídos das suas respectivas responsabilidades no plano.

O programa de treinamento deverá contemplar os riscos, ameaças, controles, responsabilidades, premissas e as estratégias do PCN, incluindo as alterações recentes.

X.2 Realização de Testes

Os testes têm por objetivo assegurar a eficiência e a efetividade do PCN e deverão ser planejados e executados com periodicidade mínima anual a partir da data da sua implantação.

A responsabilidade pelo planejamento e organização dos testes, assim como pela definição dos cenários a serem contemplados é da área de Tecnologia da Informação.

Os cenários deverão ser definidos e registrados em um documento formal que deverá ser aprovado pela alta administração, que dever ser arquivado por um período mínimo de 5 (cinco) anos.

Os testes não deverão provocar quaisquer tipos de indisponibilidade ou parada nos ambientes de negócios da TERCON e deverão ser conduzidos pela equipe de contingência em total conformidade com o definido. As simulações deverão ser realizadas sobre cenários e ameaças contemplados no plano, devendo cobrir os riscos e ameaças com maior probabilidade de ocorrência.