# PLANO DE CONTINUIDADE DE NEGÓCIO

# 21.3 - PLANO DE MONITORAÇÃO E DECLARAÇÃO DE DESASTE

## 21.3.1 Definição de Desastre

Será considerado desastre quando o tempo total de recuperação dos processos for superior ao tempo máximo apontado no capítulo 21.4 – Processos e Sistemas Críticos.

## 21.3.2 Monitoração de Comunicação de Eventos

Qualquer colaborador da A7 Serviços, ao constatar alguma anormalidade que paralise quaisquer dos processos apontados no capítulo 4 deste documento deverá comunicar o fato ao seu superior imediato que comunicará ao Líder de Contingência da unidade de negócio a que pertence, a saber:

| Unidades | Líder | Telefones | E-mail |
|---|---|---|---|
| SEDE – São Paulo – Rua dos Trilhos | Controles Internos | (11)2601-9419 | operacional@a7servicos.com.br |
| SÃO PAULO Mooca 2 – Rua | Coordenadora de Atendimento | (11)2601-3623 | diretoria@a7servicos.com.br |

Este é o meio de comunicação a ser utilizado pelos colaboradores da A7 Serviços como ponto central de contato para solicitar ajuda ou relatar alguma situação que demande o acionamento do PCN.


# 21.3 - PLANO DE MONITORAÇÃO E DECLARAÇÃO DE DESASTRE

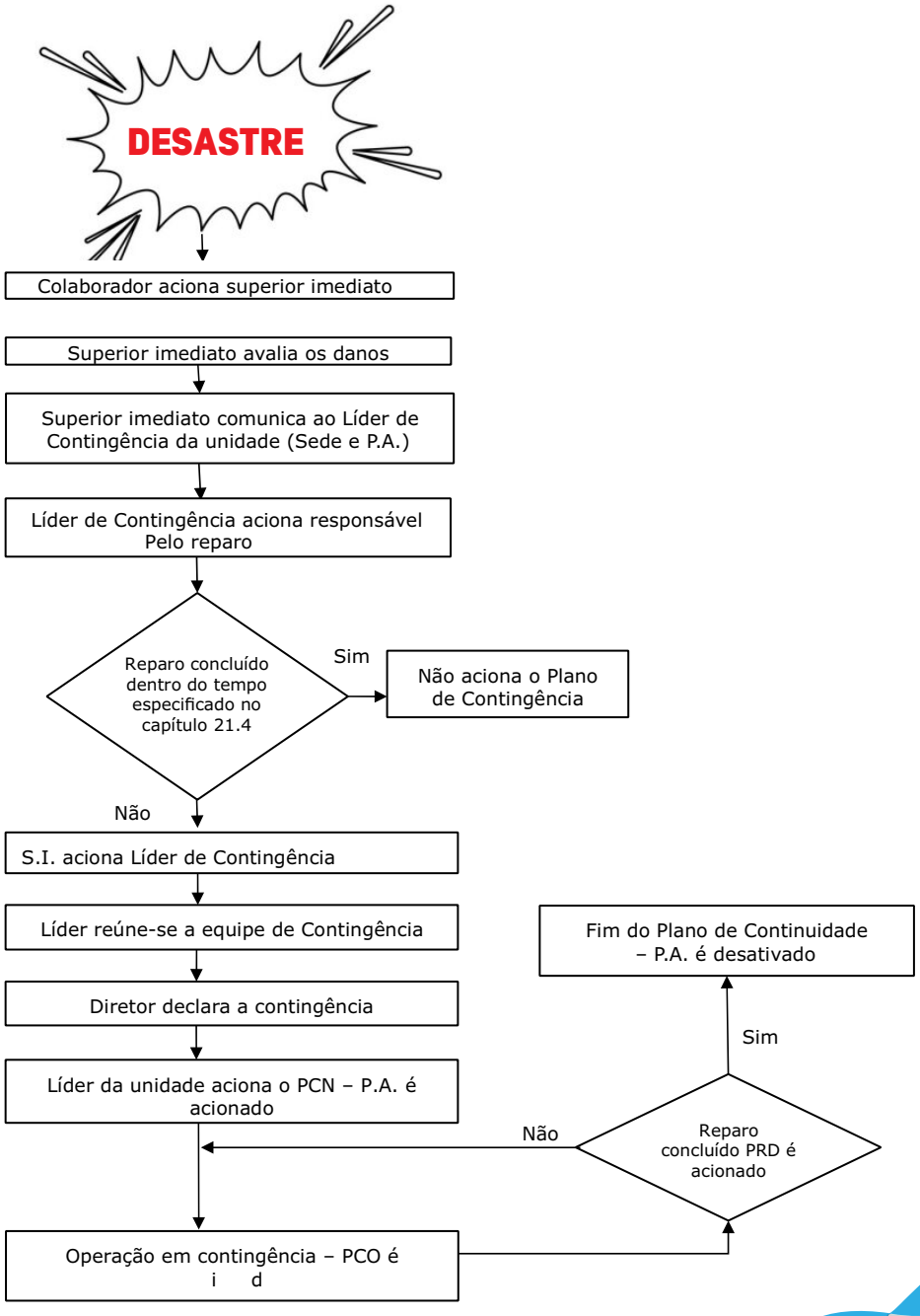
## 21.3.3 Declaração de Desastre/Contingência

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

Com base nas informações recebidas e avaliando o 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 líder da equipe de Contingência da unidade de São Paulo.

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

# 21.3 - PLANO DE MONITORAÇÃO E DECLARAÇÃO DE DESASTRE



# 21.3 - PLANO DE MONITORAÇÃO E DECLARAÇÃO DE DESASTRE

## 21.4 Processos e Sistemas Críticos

Processos e sistemas críticos podem ser definidos 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.

O resultado dessa etapa apresentou processos com MTD de 1 hora, 2 horas, 6 horas e 8 horas, que identificamos a seguir:


# 21.3 - PLANO DE MONITORAÇÃO E DECLARAÇÃO DE DESASTRE

### 21.4.1 Processos com MTD de até 1 Hora

**Tecnologia da Informação**

Procedimento:
Suporte à retomada das operações.
Preparar o ambiente de infraestrutura e sistemas para que todos possam dar continuidade na localidade backup.
Recursos:
Notebook e internet

### 21.4.2 Processos com MTD de até 2 Horas

**Financeiro**

Procedimento:
Entrar em contato com T.I.
Entrar em contato com os gerentes dos bancos para solicitar a liberação do acesso para outra máquina externa.

Recursos:
Acesso aos Bancos, Notebook e internet.

# 21.3 - PLANO DE MONITORAÇÃO E DECLARAÇÃO DE DESASTRE

### 21.4.3 Processos com MTD de até 6 horas

**Sistemas e internet**

Procedimento:
Entrar em contato com a empresa de sistemas para comunicar a interrupção e identificar prazo para restabelecimento do sistema.

Comunicar interrupção a operadora e identificar prazo de restabelecimento de internet.

Recursos:
Backup de internet.

### 21.4.4 Processos com MTD de até 8 horas

**Hardware e software**

Procedimento:
Entrar em contato com T.I.
Acompanhamento e Suporte à retomada das operações.
Recursos:
Notebook Backup.
Outros Equipamentos podem ser cedidos provisoriamente pela empresa de T.I.

# 21.3 - PLANO DE MONITORAÇÃO E DECLARAÇÃO DE DESASTRE

## 21.5 Cenários e Abrangências

Neste Plano de Continuidade de Negócios os cenários foram divididos em dois grandes eventos:

a)Impossibilidade de acesso ao prédio;

b)Falha na Infraestrutura e Tecnologia.

Esses eventos abrangem as seguintes áreas e unidades de negócio, todavia, todo processo de avaliação foi conduzido com os gestores das áreas de negócio da sede em São Paulo:

| Área | Unidade de Negócio |
|---|---|
| Financeiro | Sede |
| Relacionamento com associado | Posto de atendimento |
| Tecnologia da Informação | Empresa Terceirizada |

As principais preocupações da Diretoria em decorrência desses eventos e que deverão ser evitados são:

•Não atender clientes e fornecedores;
•Não realizar pagamentos e liberação de empréstimos.

# 21.3 - PLANO DE MONITORAÇÃO E DECLARAÇÃO DE DESASTRE

## 21.5.1 Ameaças Relacionadas

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

a)Humanas:

Greves internas, manipulação indevida de dados e sistemas, distúrbio civil, falha de prestador de serviços/parceiro, roubo e/ou furto de recursos, sequestro de dados e informações, 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.

# 21.3 - PLANO DE MONITORAÇÃO E DECLARAÇÃO DE DESASTRE

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 resultam em perdas tangíveis e intangíveis aos negócios da Organização, acarretando perda de confiança de colaboradores e associados. Desta forma, os potenciais impactos apontados pelos gestores numa eventual interrupção no negócio são:

•Operações de contas a pagar e receber;

•Não realizar pagamentos de salários, benefícios e tributos;

•Não atender clientes e colaboradores.

## 21.6 Ações e Procedimentos por Cenário para as Unidades em Contingência

Qualquer colaborador da área administrativa da A7 Serviços 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 de sua unidade, conforme Equipe de Contingência.

# 21.3 - PLANO DE MONITORAÇÃO E DECLARAÇÃO DE DESASTRE

## 21.6.1 Impossibilidade de Acesso ao Prédio

Dentre as ameaças que impossibilitam o acesso aos prédios destacamos: incêndio, ameaça de bomba e bloqueios.

### 21.6.1.1 Ações de 05 a 10 minutos após a evidência

**Responsável:** Líder do PCN da unidade sinistrada

**Procedimentos:** Relatar a ameaça à Administração do prédio/Segurança e aos seguintes serviços públicos, caso seja necessário:

- 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).

# 21.3 - PLANO DE MONITORAÇÃO E DECLARAÇÃO DE DESASTRE

### 21.6.1.2 Ações em até 20 minutos após a conclusão da etapa anterior

•**Sede** - São Paulo/SP

**Responsável:** Líder de Contingência

**Procedimentos:** Comunicar ao Líder de Contingência das unidades: Campinas e Mooca2 que a sede São Paulo se encontra em contingência.

Procedimentos: Comunicar ao Líder de Contingência dos Postos de atendimento na Sede da **A7 Serviços** em São Paulo, que a unidade se encontra em contingência.

Cada um dos analistas responsáveis pelos processos críticos das unidades em contingência deverá entrar em contato imediatamente com seus pares na unidade mais próxima de sua região e transferir todas as atribuições críticas ao negócio. Caso estas pessoas não possam ser localizadas, atribuir esta responsabilidade ao seu substituto imediato no PCN, e assim sucessivamente, conforme descrito na relação Equipe de Contingência deste documento.

# 21.3 - PLANO DE MONITORAÇÃO E DECLARAÇÃO DE DESASTRE

## 21.6.2 Falha na Infraestrutura e Tecnologia

### 21.6.2.1 São Bernardo do Campo - SEDE

**Infraestrutura**

O prédio possui 8 (oito) extintores (4 CO2 e 2 pó químico e 2 água), 6 (seis) equipamentos de ar condicionado Split e No-break de 15KVA.

Em caso de desastre na infraestrutura local, o serviço de brigada de incêndio entrará em ação, porém se a Infraestrutura for danificada, a estrutura de T.I. e Telecom poderá ser restaurada na unidade Mooca 2 em até um dia.

Essa restauração é realizada através do Ferramenta de Backup chamada Cloudberry que realiza uma imagem completa do servidor diariamente às 23:30 e pode ser restaurada em qualquer hardware independente da estrutura atual.

No caso de falha de energia, o Nobreak será acionado e todos os equipamentos continuarão funcionando normalmente por até 8 horas (tempo suficiente para o serviço de energia ser restaurado e o trabalho voltar à normalidade).

# 21.3 - PLANO DE MONITORAÇÃO E DECLARAÇÃO DE DESASTRE

**•Servidores Sede São Paulo**

Todos os servidores críticos têm fontes redundantes ligadas em circuitos distintos, e também discos com redundância (Raid 1 e Raid 5).

Se houver indisponibilidade de determinado serviço será acionada a contingência na unidade São Paulo Mooca 2.

Após constatação de falha no Servidor Local, o acionamento da empresa LBTEC será feito imediatamente. A LBTEC providenciará nova estrutura de equipamentos de servidores (em casos de perda de hardware) com uma nova instalação do ambiente Windows Server e realizará a restauração dos arquivos de rede através do backup que é realizado em HD externo (em poder do gestor) utilizando a ferramenta Cobian Backup 11 e reinstalação de softwares utilizados internamente. Retorno à normalidade:  até um dia após o incidente.

**•Servidor hospedagem de site**

Havendo a necessidade de restauração de Backup do Servidor de Site, a Infoexpress é informada e backup será disponibilizado conforme necessidade. Retorno à normalidade: até um dia.

# 21.3 - PLANO DE MONITORAÇÃO E DECLARAÇÃO DE DESASTRE

**•Servidor de E-mails**

A Infoexpress tem total acesso ao Servidor de e-mails no ambiente G-suite e o será disponibilizado conforme necessidade. Retorno à normalidade: até um dia.

Os serviços prestados na Sede da A7 Serviços serão restaurados em até 2 (duas) horas na unidade São Paulo Mooca2. Retorno à normalidade: até um dia.

**Servidores**

O servidor do sistema é alocado em nuvem e o acesso é feito por internet. O servidor da rede fica na sede da A7 Serviços, servidores críticos têm fontes redundantes ligadas em circuitos distintos, e também discos com redundância (Raid 1 e Raid 5).

Se houver indisponibilidade de determinado serviço será acionada a contingência da unidade do São Paulo Mooca 2.


# 21.3 - PLANO DE MONITORAÇÃO E DECLARAÇÃO DE DESASTRE

## 21.7 Procedimentos de retorno à normalidade - Site Principal

O Gestor da A7 Serviços será responsável por verificar se o acesso à sede de São Paulo está liberado e em condições confortáveis para o trabalho, o departamento de TI será responsável por revisar se os principais serviços estão funcionando a nível de desempenho aceitável.

## 21.8 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, definido para este plano como o Processo de Continuidade de Negócios.

O processo de Continuidade de Negócios é de responsabilidade e gestão da área de 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 atual da A7 Serviços.

Para que a área de Compliance possa verificar o grau de atualização do PCN e decidir quanto ao momento em que o processo de continuidade de negócios será iniciado, os processos de planejamento estratégico corporativo e tecnológico, gerenciamento de mudanças, gerenciamento de riscos, tratamento de problemas e de incidentes devem prever a participação.

# 21.3 - PLANO DE MONITORAÇÃO E DECLARAÇÃO DE DESASTRE

## 21.8.1 Divulgação e Treinamento

Um dos fatores de primordial importância 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 A7 Serviços definiu que serão realizadas semestralmente sessões de divulgação a todos os colaboradores e envolvidos no planejamento de continuidade de negócios.

Estas sessões serão organizadas pela área de Compliance em conjunto com a área de Recursos Humanos e deverão 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 vigente.

Para que este conhecimento seja preservado, os colaboradores admitidos e os transferidos para funções de negócios críticas, principalmente aqueles que pertencem a 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.



### 21.8.2 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 Compliance em conjunto com a área de Tecnologia da Informação, Administração e Recursos Humanos.

Os cenários deverão ser definidos e registrados em um documento formal que deverá ser aprovado pela alta Administração e mantido guardado como documento de validação das estratégias por um período mínimo de 2 (dois) anos.

Os testes não deverão provocar quaisquer tipos de indisponibilidade ou parada nos ambientes originais de negócios da A7 Serviços 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.