PROGRAMA DE GESTÃO CONTINUIDADE DE NEGOCIOS DE TI

DIRETRIZES PARA CONTINUAÇÃO, CONSERVAÇÃO E ININTERRUPÇÃO DOS SERVIÇOS ESSENCIAS

HISTÓRICO DE VERSÕES:

Versão 1.0

Criação: Thiago Bagnoli Moretti / Paulo Alberto Werhli Meier

Aprovação: Comitê de Segurança da Informação

Revisão 1.1: Thiago Bagnoli Moretti / Paulo Alberto Werhli Meier

SUMARIO

1 – CONCEITOS E DEFINIÇÕES

1.1 Ativos de informação: Entendem-se os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

1.2 Continuidade de Negócios: capacidade da empresa, tanto tática quanto estratégica, de se planejar e responder a incidentes e interrupções de negócios, de forma a manter suas operações em um nível aceitável, previamente definido, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas.

1.3 Desastre: Evento repentino e não planejado que causa perda para toda ou parte da organização e gera sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo de recuperação.

1.4 Incidente: evento que tenha causado algum dano, colocado em risco, algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação.

1.5 Data center: Todo espaço nos quais ficam os Ativos de Informação, bem como suas estruturas auxiliares como No-Break, Banco de Baterias e Gerador de Energia Elétrica.

2 – APRESENTAÇÃO

2.1 O Plano de Continuidade de Negócios (PCN) assegura à empresa a continuidade de seus negócios em caso de paralisação decorrente de sinistro de um ou mais processos considerados críticos, devendo estabelecer cenários de situações inesperadas ou incidentes, quer sejam operacionais, desastres ou crises. O plano de continuidade atuará como resposta aos resultados da Análise de Impacto nos Negócios e Análise de Riscos, tendo o dever de gerencia-los, dando a devida atenção para:

a. alternativas estratégicas, táticas e operacionais para responder à interrupção;
b. prevenção de novas perdas ou indisponibilidade de atividades prioritárias;
c. detalhes sobre como e em que circunstâncias a empresa irá se comunicar com as partes interessadas.

3 – OBJETIVO

3.1 Almeja-se com este Plano de Continuidade de Negócios (PCN), promover estratégias e medidas de proteção eficazes e rápidas para os processos críticos de TI, a fim de garantir sua preservação após a ocorrência de um desastre, até a retomada em tempo hábil. O PCN atuará como resposta aos resultados da Análise de Impacto nos Negócios e Análise de Riscos, provendo quais as ações serão realizadas em cada etapa do plano;

3.2 O processo de elaboração do PCN baseou-se em normas e pesquisas de outras instituições, dentro das melhores práticas para a construção de um Sistema de Gestão de Continuidade de Negócios. As atividades foram desenvolvidas pelos colaboradores e gestores, de forma colaborativa, com reuniões presenciais para alinhamento do plano com as políticas institucionais;

3.3 Este plano divide-se em outras 4 (quatro) etapas, as quais são:

3.3.1 **Plano de Administração de Crises (PAC)** - Define funções e responsabilidades das equipes envolvidas com o acionamento das ações de contingência, antes durante e após a ocorrência;

3.3.2 **Plano de Contingência (PC)** - Define as necessidades e ações mais imediatas. Deve ser utilizado somente quando todas as prevenções tiverem falhado;

3.3.3 **Plano de Recuperação de Desastres (PRD)** - Determina o planejamento para que, uma vez controlada a contingência e passada a crise, sejam retomados os níveis originais de operação e;

3.3.4 **Plano de Continuidade Operacional (PCO)** - Seu objetivo é restabelecer o funcionamento dos principais ativos que suportam as operações da instituição, reduzindo o tempo de queda e os impactos provocados por um eventual incidente.

3.4 Dentre os objetivos do Plano, destacam-se os seguintes procedimentos:

a) Identificar todos os processos de negócio de TI, definindo atividades críticas e classifica-las.
b) Identificar e documentar os riscos que possam comprometer a continuidade das atividades críticas;
c) Identificar ameaças, vulnerabilidades e estimar os riscos;
d) Identificar controles existentes;
e) Identificar, documentar e avaliar os possíveis impactos à continuidade das atividades críticas, caso tais riscos se concretizem;
f) Determinar e calcular o tempo e o custo de parada e da recuperação do negócio;
g) Definir, implementar e manter um processo formal e documentado para a Análise de Impacto nos Negócios;
h) Avaliação dos impactos de não realização das atividades críticas ao longo do tempo;
i) Fixação dos prazos de forma priorizada para a retomada das atividades, em um nível mínimo de execução tolerável, levando em consideração o tempo em que os impactos da interrupção tornem-se inaceitáveis;
j) Identificação de interdependências e recursos que suportam as atividades, incluindo fornecedores, terceiros e demais partes interessadas relevantes;
k) Determinar estratégias de continuidade de negócios adequada para proteger, estabilizar, continuar, retomar e recuperar as atividades prioritárias, bem como suas interdependências e recursos de apoio (Plano de Administração de Crises);
l) Estabelecer níveis adequados de autoridade e competência, no intuito de assegurar a comunicação efetiva às partes interessadas, bem como assegurar a continuidade das atividades críticas (Plano de Continuidade Operacional);
m) Viabilizar a continuidade e a recuperação das atividades críticas, em caso de interrupção (Plano de Recuperação de Desastres e Contingencia);
n) Realizar treinamentos e avaliações do PCN periodicamente para garantir a manutenção e o bom funcionamento dos planos de continuidade;
o) Realizar testes para garantir a eficiência da continuidade de negócios;
p) Promover a conscientização dos colaboradores;
q) Identificar oportunidades para melhorar a continuidade de negócios.

4 – MODELO DO PLANO (PDCA)

4.1 Os planos aqui definidos seguirão o Modelo **"PLAN-DO-CHECK-ACT" (PDCA)** para planejar, estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar continuamente a eficácia do Sistema.

4.2 **Modelo PDCA:** O modelo PDCA ajudará na melhoria contínua do Plano de Continuidade de Negócios:

a) **PLAN (estabelecer)** - Seguir uma política de continuidade de negócios, objetivos, metas, controles, processos e procedimento pertinentes para a melhoria da continuidade de negócios, de forma a ter resultados alinhados com os objetivos.

b) **Do (Implementar e operar)** - Implementar e operar a política de continuidade de negócios, controles, processos e procedimentos.

c) **CHECK (Monitorar e analisar criticamente)** - Monitorar e analisar criticamente o desempenho em relação aos objetivos e política de continuidade de negócios, reportar os resultados para a direção para análise crítica, definir e autorizar ações de melhorias e correções.

d) **ACT (Manter e Melhorar)** - Manter e melhorar o PCN, tomando ações corretivas e preventivas, baseadas nos resultados da análise crítica da direção e reavaliando o escopo, as políticas e objetivos de continuidade de negócios.

4.3 Para cada uma das etapas, deverá ser feito Planos de Ações, e estes deverão ser elaborados assim que dar-se os ocorridos, com base na sua temporalidade e impacto. Estes devem formar um log ou registro de ações, para que para cada acontecimento seja possível verificar o que foi feito em outros momentos similares.

5 – VIGÊNCIA DO PCN

5.1 Este Plano terá vigência de 4 (quatro) anos.

6 – REVISÕES

6.1 A revisão do Plano será realizada nas seguintes situações:

a) Em no máximo 2 (dois) anos;

b) Nos momentos em que a CSI julgar necessário;

c) Em função dos resultados dos testes realizados; ou

d) Após ocorrência de algum evento ou mudança significativa nos ativos de informação, nas atividades ou em algum de seus componentes.

7 – INVOCAÇÃO DO PLANO

1.1 O presente plano será acionado quando houver ocorrência de algum desastre, na ocorrência de um risco não conhecido ou caso uma vulnerabilidade tenha grande probabilidade de ser explorada. Também poderá ser acionado o plano quando ocorrer a necessidade de testes ou por determinação do CSI.

8 – PRICIPAIS RISCOS

8.1 O PCN foi elaborado para ser acionado quando houver alguma ocorrência de desastres que apresentem riscos à continuidade do negócio ou serviços essenciais. Abaixo segue o quadro que define estes riscos, bem como aponta quais os parâmetros para reportar as possíveis causas das ocorrências.

EVENTO DE DESASTRE	POSSÍVEIS CAUSAS
01- Interrupção de energia elétrica	Causada por fator externo a rede elétrica do prédio ou de sua localidade com duração da interrupção superior a 12 horas. Causada por fator interno que comprometa a rede elétrica do prédio com curto-circuitos, incêndio e infiltrações.
02 - Indisponibilidade de rede/circuitos	Rompimento de fibra ótica decorrente de execução de obras publicas, desastres ou acidentes.
03 - Falha humana	Qualquer ato causado por negligencia, imprudencia e/ou impericia.
04 - Ataques internos (funcionários insatisfeitos)	Ataque aos ativos do DataCenter ou aos Servidores internos
05 - Incêndio	
06 - Desastres Naturais	
07 - Falha de hardware	Falha que necessite reposição de peça ou cujo reparo ou aquisição Dependa de orçamento .
08 - Ataque cibernético	Ataque virtual que comprometa o desempenho, os dados ou configuração dos serviços essenciais.

9 – PAPÉIS E RESPONSABILIDADES

9.1 COMITÊ DE SEGURANÇA DA INFORMAÇÃO

INTEGRANTES:

ROBERTO CARLOS TEIXEIRA MENDES
PAULO ALBERTO WERHLI MEIER
TIAGO TAQUECHI KIRIHARA
MAURO De LEONARDIS
THIAGO BAGNOLI MORETTI

CONTATO (11) 2076-8664
EMAIL: seco@updi.net

ATRIBUIÇÕES

- Avaliar o plano periodicamente e decidir pelo seu acionamento quando da ocorrência de desastres, respondendo em nível institucional pela execução do plano e demais ocorrências relacionadas.

9.2 EQUIPE DE INSTALAÇÕES/AMBIENTE/SERVIDORES/APLICAÇÕES

LIDER: TIAGO TAQUECHI KIRIHARA
CONTATO (11) 2076-8664
EMAIL: pcop@updi.net

INTEGRANTES:

ROBERTO CARLOS TEIXEIRA MENDES
PAULO ALBERTO WERHLI MEIER

ATRIBUIÇÕES

- Responsável pelas instalações físicas que abrigam as estações de trabalho e servidores locais.
- Avaliar os danos e supervisionar os reparos para um local secundário, no caso de a localização primária sofrer destruição ou danos.
- O líder desta equipe administrará, manterá e reavaliará o Plano de Recuperação de Desastre.
- Avaliar os danos específicos de infraestrutura de rede interna, incluindo WAN, LAN e quaisquer outra infraestrutura externa junto aos prestadores de serviço.
- Fornecer a infraestrutura de servidores físicos e virtuais necessárias para que a equipe responsável execute suas operações e processos essenciais durante um desastre.
- Garantir que as aplicações essenciais funcionem como exigido para atender aos objetivos de negócios em caso de e durante um desastre. Eles serão os principais responsáveis por assegurar e validar o desempenho das aplicações essenciais e podem ajudar outras equipes de TI.

9.3 EQUIPE DE OPERAÇÕES

LIDER: MAURO De LEONARDIS
CONTATO (11) 2076-8664
EMAIL: oper@updi.net

INTEGRANTES:

ROBERTO CARLOS TEIXEIRA MENDES
PAULO ALBERTO WERHLI MEIER

ATRIBUIÇÕES

- Fornecer aos funcionários as ferramentas de que necessitam para desempenhar suas funções da forma mais rápida e eficiente possível.
- São responsáveis em provisionar ferramentas para que, no caso de um desastre, os colaboradores possam trabalhar remotamente com as ferramentas específicas à sua atuação.
- O líder desta equipe administrará e manterá o Plano de Continuidade Operacional.

9.4 EQUIPE DE COMUNICAÇÃO

LIDER: THIAGO BAGNOLI MORETTI
CONTATO (11) 2076-8664
EMAIL: comm@updi.net

INTEGRANTES:

TIAGO TAQUECHI KIRIHARA
MAURO De LEONARDIS

ATRIBUIÇÕES

- Responsável por todas as comunicações durante um desastre. Especificamente, eles se comunicarão com os funcionários, clientes e com quem mais se fizer necessário.
- O líder desta equipe administrará e manterá o Plano de Administração de Crise.

9.5 EQUIPE DE BACKUP

LIDER: ROBERTO CARLOS TEIXEIRA MENDES
CONTATO (11) 2076-8664
EMAIL: bkup@updi.net

INTEGRANTES:

PAULO ALBERTO WERHLI MEIER
TIAGO TAQUECHI KIRIHARA
MAURO De LEONARDIS

ATRIBUIÇÕES

- Analisar as perdas e mapear a quantidade de dados perdidos, tempo de recuperação desses dados e formular estratégias de recuperação de dados de acordo com as políticas pré-estabelecidas.

9.6 EQUIPE DE SEGURANÇA DA INFORMAÇÃO

LIDER: PAULO ALBERTO WERHLI MEIER
CONTATO (11) 2076-8664
EMAIL: sein@updi.net

INTEGRANTES:

ROBERTO CARLOS TEIXEIRA MENDES
THIAGO BAGNOLI MORETTI
TIAGO TAQUECHI KIRIHARA

ATRIBUIÇÕES

- Promover mecanismos de segurança, tanto nas estações de trabalho, quanto nos acessos remotos, em caso de acionamento do PCN. Resguardar aplicações e dados, evitando que desdobramentos de segurança afetem o acionamento da continuidade.
- Analisar as perdas e mapear a quantidade de dados perdidos, tempo de recuperação desses dados e formular estratégia de recuperação de dados.

10 – PROCESSOS E SISTEMAS CRITICOS

10.1 Processos e sistemas críticos podem ser definidos como um processo de trabalho que, uma vez paralisado por um tempo superior ao definido pelos gestores de negócio, irá afetar sensivelmente as operações, gerando impacto aos clientes. Esse impacto é definido pela seguinte formula:
MTD = RTO + WRT.

10.1.1- MTD (Maximum Tolerable Downtime) = Define a quantidade total de tempo que um processo de negócios pode ser interrompido sem causar quaisquer consequências inaceitáveis. Esse valor deve ser definido pelo Comitê de Desastres. Diferentes funções de negócio terão diferentes MTD's.

10.1.2- RTO (Recovery Time Objective) = Determina a quantidade máxima tolerável de tempo necessária para colocar todos os sistemas críticos novamente on-line (por exemplo, restaurar dados de backup ou consertar uma falha).

10.1.3- WRT (Work Recovery Time) = Determina a quantidade de tempo tolerável necessária para verificar o sistema e/ou a integridade dos dados (verificar os bancos de dados e logs, por exemplo). Quando todos os sistemas afetados pelo desastre são verificados e / ou recuperados, o ambiente está pronto para retomar a produção novamente.

PROCESSO CRITICO	MTD	RTO	WRT
Defeito de Hardware	4 hrs	3 hrs	1 hr
Danos, perda ou corrupção dos servidores, computadores e sistemas operacionais	4 hrs	3 hrs	1 hr
Falha no Backup	10 hrs	8 hrs	2 hrs
Falha humana (imprudencia, negligencia e / ou impericia)	3 hrs	2 hrs	1 hr
Falha no equipamento interno	2 hrs	1 hr	1 hr
Falha estrutural (danos fisicos ao edificio/escritorio)	2:30 hrs	2	30 min
Absenteísmo de funcionários essenciais	1:10 hrs	1 hr	10 min

11 – ANALISE DE IMPACTO DE NEGOCIOS (BIA)

I. Uma análise de impacto de negócios (BIA) prevê as consequências da interrupção de uma função e processos de negócios e reúne informações necessárias para desenvolver estratégias de recuperação.

II. Cenários potencias de perda devem ser identificados durante uma avaliação de risco. As operações também podem ser interrompidas pela falha de um fornecedor de bens ou serviços.

III. A BIA deve identificar os impactos operacionais e financeiros resultantes da interrupção das funções e processos empresariais. Os possíveis cenários e impactos a considerar no caso de interrupção do processo / negocio, incluem:

a) Vendas e renda perdida;
b) Penalidades contratuais;
c) Insatisfação ou deserção do cliente;

d) Danos físicos ao edifício
e) Danos ou quebras de máquinas, sistemas ou equipamentos
f) Acesso restrito a um local ou edifico
g) Paralisação dos serviços públicos (por exemplo, queda de energia elétrica)
h) Danos, perda ou corrupção dos servidores, computadores, sistemas operacionais, aplicativos e dados
i) Absenteísmo de funcionários essenciais

11.1 – TEMPO E DURAÇÃO DA INTERRUPÇÃO

I. A análise de impacto de negócios existe para definir parâmetros sobre o prazo requerido na recuperação dos serviços (indisponibilidade máxima aceitável/objetivo para o tempo de recuperação) e o momento requerido para suas copias de segurança (objetivo para Ponto de recuperação / perda máxima de dados). Parâmetros estes que serão calculados após a elaboração de questionários e tabulação de levantamento de riscos.

II. Os questionários são pensados para obter informações para a elaboração dos:

a) Sistemas /processos críticos de negócios sob responsabilidade da empresa;
b) Levantar o investimento e custeio para implantação das alternativas para evitar a interrupção e /ou recuperar as operações;
c) Impactos a serem considerados;
d) Grau de criticidade dos sistemas/processos críticos;
e) Tempo objetivado e tempo máximo de paralisação, bem como o seu ponto positivo;
f) Decidir sobre as alternativas, recursos e seus custos com base em análise de custo x benefício;

11.2 – CONDUÇÃO DA BIA

I. Para que se dê uma condução correta da BIA, primeiramente se faz necessário a análise da criticidade e após, a avaliação de todos os impactos (financeiro, legal, operacional, administrativo imagem e recursos humanos).

II. A tabela abaixo serve como referência para que se identifique as ameaças, seus impactos, qual o valor sobre o negócio, sua importância e qual o procedimento será adotado para correção desta ameaça.

III. A revisão desta tabela deve ser feita anualmente, ou sempre que houver mudanças significativas das atividades, devendo, nesse caso, o CSI solicitar a revisão.

Ameaças	Impacto	Valor	Importância	Procedimento
Defeito de Hardware	Direto	Alto	1	
Danos, perda ou corrupção dos servidores, computadores e sistemas operacionais	Direto	Alto	1	
Falha no Backup	Direto	Alto	1	
Perda de dados vitais ao negocio	Direto	Alto	1	

Ataques à Sistemas	Direto	Alto	2	
Falha humana (imprudencia, negligencia e / ou impericia)	Direto	Alto	2	
Desatualização de Softwares	Indireto	Médio	3	
Falha no equipamento interno	Direto	Medio	3	
Falha estrutural (danos fisicos ao edificio/escritorio)	Indireto	Baixo	4	
Absenteísmo de funcionários essenciais	Direto	Baixo	4	

11.3 – RELATORIO DA BIA

I. Para verificação do nível de criticidade do risco, será utilizada a seguinte formula:
AMEAÇA + IMPORTANCIA = IMPACTO DE NEGOCIO

II. Para cálculo desta formula, serão utilizados os seguintes parâmetros de pontuação:

- Importância 1 – 15 pontos para cada processo;
- Importância 2 – 10 pontos para cada processo;
- Importância 3 – 07 pontos para cada processo;
- Importância 4 – 03 pontos para cada processo.

III. O resultado desta formula, sinaliza o grau de impacto da não implementação de contingência e/ou sua demora, no caso de desastre ou paralização do serviço.

Resultado	Severidade	Impacto da não impolementação de contigencia
70 a 100	Critico	Alto
40 a 70	Moderado	Médio
10 a 40	Leve	Baixo

12 – PLANO DE ADMINISTRAÇÃO DE CRISES - (PAC)

I. Este plano especifica as ações ante os cenários de desastres. As ações incluem administrar, gerir, eliminar ou neutralizar os impactos inerente ao relacionamento entre os envolvidos e/ou afetados, até a superação da crise.

12.1 – OBJETIVO

I. O objetivo do PAC é garantir a comunicação, gerenciar as crises e viabilizar uma compreensão linear a todos os envolvidos das ações antes, durante e após a ocorrência de um desastre.

II. São objetivos específicos do PAC:

a) Garantir a segurança à vida das pessoas;
b) Orientar os funcionários e demais colaboradores sobre as condutas que serão tomadas;
c) Informar aos clientes com esclarecimentos condizentes com o ocorrido em tempo hábil;
d) Minimizar transtornos sobre os desdobramentos de incidente e estimular o esforço em conjunto para a superação da crise.

12.2 – EXECUÇÃO DO PLANO

I. Na ocorrência de um desastre será necessário entrar em contato com as áreas afetadas para informa-las de seu efeito na continuidade dos serviços e tempo para recuperação. O plano deve incluir ações para redirecionar as chamadas telefônicas recebidas para um segundo número. A equipe de comunicação será responsável por contatar os clientes e demais prejudicados e passar as informações pertinentes.

II. A comunicação ocorrerá da seguinte forma:

a) COMUNICAR AS AUTORIDADES: Deve-se comunicar as autoridades competentes em caso de desastre que envolva risco às pessoas, fornecendo informações de localização, natureza, magnitude e impacto do desastre.
Policia Militar - 190
SAMU – 192
Corpo de Bombeiros – 193
Defesa Civil – 199

b) COMUNICAR OS SETORES RESPONSAVEIS: Além da comunicação aos responsáveis, deverá informar também:
11 Natureza, impacto e abrangência da catástrofe
12 Ações de contingência em andamento
13 Processos / sistemas e serviços cobertos pelo plano de continuidade (serviços essenciais)

c) COMUNICAR FORNECEDORES / PRESTADORES DE SERVIÇOS.
d) COMUNICAR COLABORADORES EXTERNOS.
e) COMUNICAR TODAS AS PARTES ACIMA QUANDO OCORRER O RETORNO DAS OPERAÇÕES À NORMALIDADE

12.3 – ENCERRAMENTO DO PAC

I. Uma vez validado o retorno das funções essências do sistema e sua total estabilidade, bem como a estabilidade do datacenter, se esse for o caso, a Equipe de comunicação entrará em contato com todos os envolvidos descritos neste plano, provendo as informações de retorno e o status dos serviços essenciais, devendo emitir um parecer relatando as atividades realizadas para restabelecimento dos serviços.

13 – PLANO DE CONTIGENCIA – (PC)

13.1 – OBJETIVO

I. Este plano visa estabelecer uma recuperação após um desastre, com o objetivo de assegurar o reestabelecimento dos sistemas essenciais e suas respectivas atividades.

II. Tem como principal objetivo listar os procedimentos definidos para permitir que serviços de processamento e armazenamento de dados continuem a operar, mesmo que com um certo grau de degradação.

13.2 – DEFINIÇÃO DA ESTRATEGIA

I. O plano de contingência, tem como definição três pilares macros, aos quais se baseiam:

a) **PESSOAS:** trata dos recursos humanos envolvidos nas atividades em contingência;
b) **ORGANIZAÇÃO:** trata a disponibilidade e segurança dos recursos estruturais organizacionais para suportar as atividades necessárias em contingência
c) **TECNOLOGIA:** trata dos recursos de hardware e software apoiados em tecnologias e complementam para atender a contingência.

II. Seguindo esta linha, temos como referência quatro grupos, distribuídos da seguinte forma:

a. Contingência de infraestruturas físicas
Compreende as situações de catástrofe, naturais ou não, tais como inundações, desabamentos, incêndios, falhas no fornecimento de energia, entre outros. Em termos gerais, são ocorrências que impeçam o acesso e/ou utilização das instalações, como também danos físicos relevantes a instalações e/ou equipamentos, intencionais ou não.

b. Contingência de pessoas
São aquelas onde os colaboradores chave não estão presentes por motivos de greves, doenças, licenças e etc

c. Contingencia de Infraestruturas Tecnológicas
Compreende as situações de inacessibilidade, falha ou perda de quaisquer recursos de TI, tais como hardware, software, telecomunicações, rede e segurança.

d. Contingência de serviços Externos
Compreende as situações de não prestação de serviço contratado considerado critico aos processos.

13.3 – ETAPAS DA CONTIGENCIA

I. Para que a contingência siga seu fluxo, são recomendadas que essas etapas estejam presentes. São elas:

a) **Diagnostico:** consiste na identificação dos pontos fracos que poderiam ser foco de problemas para o setor de TI da empresa
b) **Analise de riscos:** a partir das vulnerabilidades, deve-se considerar as possíveis ameaças e os fatores que possam levar à concretização desses riscos, como o ataque de vírus e a ausência de um antivírus corporativo.
c) **Definição de prioridades:** identificar os processos vitais da empresa e apontar quais os sistemas que precisam ser recuperados primeiro ou preferencialmente em casos de problemas
d) **Determinação de estratégias:** esse é o caminho para se definir como cada sistema deve ser recuperado (usando softwares ou aplicações), quando e quem são os responsáveis por isso.

13.4 – ENCERRAMENTO DO PLANO DE CONTIGENCIA

I. O plano será encerrado assim que todos os serviços estiverem estáveis e o funcionamento dos sistemas essenciais operando normalmente

II. A equipe responsável pelo retorno deve emitir um parecer relatando as atividades realizadas, que por sua vez deverá fornecer um comunicado de retorno as atividades.

14 – PLANO DE RECUPERAÇÃO DE DESASTRES – (PRD)

I. Este plano descreve os cenários de inoperância e seus respectivos procedimentos, para que, uma vez definindo as atividades prioritárias para restabelecer o nível de operação dos serviços, controlada a contingência e passada a crise, a organização retorne aos seus níveis normais de operação.

II. Para garantir o retorno das operações depois da ocorrência de uma crise ou desastre, são objetivos do plano de recuperação:

a) Avaliar danos aos ativos e conexões do DataCenter e prover meios para sua recuperação.
b) Evitar desdobramento de outros incidentes
c) Reestabelecer o DataCenter dentro do prazo tolerável.

14.1 – EXECUÇÃO DO PLANO DE RECUPERAÇÃO

I. Para que o plano transcorra como planejado, deve-se executar os seguintes passos:

a) A equipe responsável pelos BACKUPS e SERVIDORES, deverá identificar e listar todos os ativos danificados da ocorrência do desastre;
b) A equipe de rede deverá identificar as interrupções de conexões e acessos gerados após o desastre, informando se a abrangência está na rede local, WAN ou com o provedor de serviços;
c) Os responsáveis pelo PRD deverão mapear quais os serviços foram descontinuados contendo as informações de perda de ativo e de conexão;
d) O comitê responsável pelo PRD, após o mapeamento das perdas e impactos elaborará um cronograma de recuperação das aplicações, levando em consideração as seguintes aplicações para recuperação:
   - Substituição dos ativos e equipamentos;
   - Reconfiguração de ativos e equipamentos;
   - Teste de ambiente.

14.1.1 – SUBSTITUIÇÃO DOS ATIVOS E EQUIPAMENTOS

I. Em caso de perda de ativos, deverá ser imediatamente informado a necessidade de aquisição de ativos perdidos que não puderem ser recuperados. A equipe irá mensurar quanto tempo a aquisição irá impactar cada serviço, comunicando se há alguma solução alternativa a ser tomada enquanto é realizada a aquisição. As informações pertinentes à alteração do tempo de recuperação dos serviços serão passadas às equipes de PCO e PAC.

14.1.2 – RECONFIGURAÇÃO DE ATIVOS E EQUIPAMENTOS

I. A equipe responsável deverá verificar que as configurações dos ativos reparados ou substituídos estão em funcionamento pleno. Caso não estejam, prover cronograma estimado para configurar estes ativos.

14.1.3 – TESTE DE AMBIENTE

I. O ambiente principal (local e/ou DataCenter), deverá ser testado antes da recuperação dos dados, a fim de garantir que o processo de recuperação ocorra conforme o planejado. Os testes e recuperações deverão:
   a) Garantir os mesmos níveis de capacidade e disponibilidade dos serviços essenciais antes do desastre;
   b) Garantir a integridade dos dados, que podem estar corrompidos ou defasados;
   c) Validar todas as configurações anteriores;
   d) Suportar o retorno dos sistemas de acordo com a demanda;
   e) Verificar a integridade dos dados e restaurar os backups, caso necessário.

14.2 – ENCERRAMENTO DO PLANO

I. O plano será encerrado assim que os procedimentos de recuperação forem realizados por todas as equipes. Ao termino de todos os procedimentos, as informações de recuperação de serviços serão consolidadas em parecer especifico, informando o horário de reestabelecimento de cada serviço, equipamentos adquiridos e/ou realocados, se for o caso, fornecedores que tiveram de ser acionados procedimentos de recuperação realizados, entre outras informações relevantes

15 – PLANO DE CONTINUIDADE OPERACIONAL – (PCO)

I. Este plano descreve os cenários de inoperância e seus respectivos procedimentos alternativos planejados, definindo as atividades prioritárias para garantir a continuidade dos serviços e restabelecer o funcionamento dos principais ativos que suportam as operações de TI, reduzindo o tempo de queda e os impactos provocados por um eventual desastre.

15.1 – OBJETIVO

I. Garantir ações de continuidade durante e depois da ocorrência de uma crise ou desastre, tratando-se apenas de ações de contingência, destinados a manter a continuidade dos processos de negócios e serviços vitais. É através deste, que as equipes de processos saberão como agir na falta ou na falha de algum componente que o suporte, garantindo assim a continuidade do processo, reduzindo os seus impactos.
II. Prover meios para manter o funcionamento dos principais serviços de TI e a continuidade das operações e sistemas essências;
III. Estabelecer controles, regras e procedimentos alternativos que possibilitem a continuidade das operações de TI durante uma crise ou cenário de desastre;
IV. Definir os formulários, checklist e relatórios a serem entregues pelas equipes ao executar a contingencia.

15.2 – EXECUÇÃO DO PLANO

I. Identificada a ocorrência de um incidente, crise ou desastre, a equipe de operações e backups deve verificar a dimensão do impacto, extensão e possíveis desdobramentos do ocorrido. Após

a avaliação de impacto de desastre, a equipe responsável deverá preencher um questionário para avaliação e decisão sobre o acionamento do plano e início das ações de contingência. Este questionário deve ser divulgado para todas as equipes envolvidas.

II. Dado o aval para o acionamento do plano pelos responsáveis, será convocada uma reunião de emergência com os lideres com o intuito de:
   a) Coordenar prazos e orquestrar as ações de contingência;
   b) Informar as equipes de ações de contingência com a priorização dos serviços essências.

15.3 – PROCEDIMENTOS DE RETOMADA

I. Para que se tenha a retomada do negócio, será necessário a verificação das seguintes etapas:
   a) Estimar o impacto de perda de dados;
   b) Identificar ativos afetados;
   c) Mapear ativos a serem recuperados;
   d) Estimar volume dos dados a serem recuperados;
   e) Tempo de recuperação e possíveis perdas operacionais;
   f) Implantar procedimento de recuperação;
   g) Testar procedimentos realizados;
   h) Repassar os procedimentos aos servidores e verificar melhorias.

15.4 – ENCERRAMENTO DO PLANO

I. O plano será encerrado assim que for validado o funcionamento dos sistemas essências, bem como o DataCenter, se esse for o caso, relatando a sua estabilidade e a sua normalidade. Após esse processo, será emitido um parecer da equipe responsável, informando o que ensejou o acionamento do plano, as atividades realizadas e os recursos que foram utilizadas para então, comunicar a todos os setores a estabilidade do sistema.