Auditoria e Qualidade de Sistemas

Prof. Edgard Davidson C. Cardoso

Auditoria de Sistemas

PLANO DE CONTINGÊNCIA

Contextualização

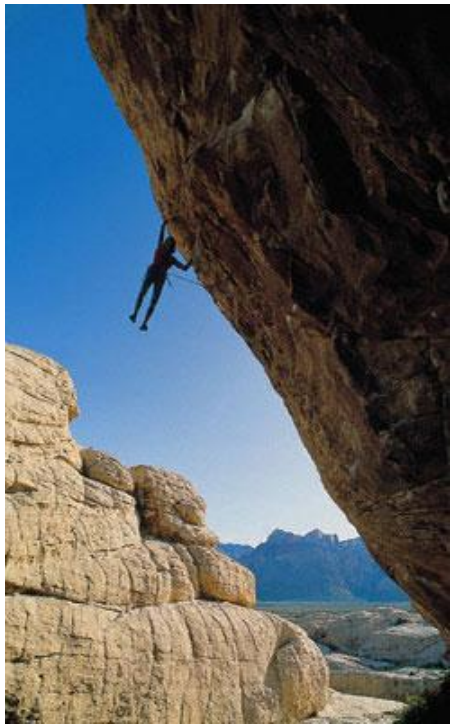
- Crescimento da dependência das organizações em relação aos seus sistemas de informação.
- Os SI apresentam um papel extremamente importante nas atividades críticas das corporações.
- Muitas atividades não poderiam ser executadas com eficácia – se é que poderiam ser realizadas – sem o apoio dos computadores.

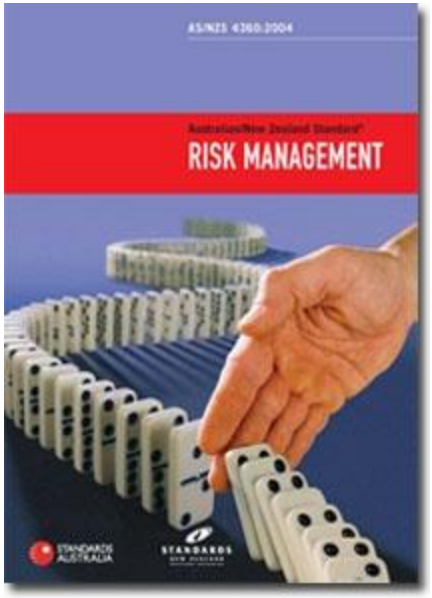
Contextualização

- Queda de energia elétrica, greves de pessoal, desastre naturais, danos intencionais, tudo isso pode representar efeitos desastrosos nos sistemas computacionais.

- Casos de ataques terroristas como o do WTC ilustram o fato de que organizações podem ser seriamente comprometidas se não apresentarem um plano de continuidade do serviço exeqüível e pronto para o uso.

Quem Acredita em “Gerenciar Riscos” ?

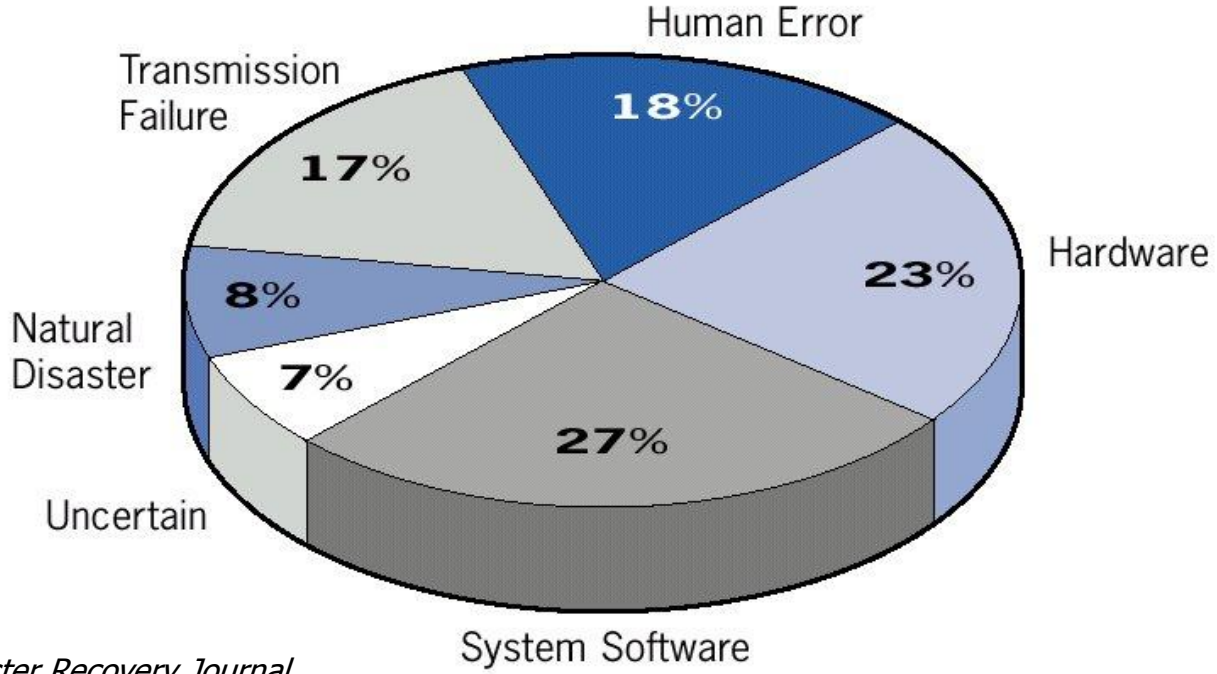




una

Padronizando Conceitos

Evento: Fato de origem voluntária ou não que apresenta risco de **dano**. Também denominado “Fator de Risco”



Fonte: Disaster Recovery Journal

Padronizando Conceitos

- **Risco**: é a medida para um fator de incerteza
- **Avaliação**: considera a pior situação, no pior momento, no cenário mais pessimista
- **Cenário**: consistente com a realidade da Organização
- **Controle**: deveria ser proativo, preditivo e corretivo

Padronizando Conceitos

- **Dano**: Conseqüência nociva acarretada por um Evento.
- **Impacto** de resultado prejudicial. Justifica a Contingência.

Causas	Percentual
Falha Humana	50 a 80 %
Greves	10 a 17 %
Forças da Natureza	10 a 15 %
Sabotagem	3 a 4 %
Alagamento	2 a 3 %
Estranhos à Organização	1 a 3 %

Causas de **Danos** a Sistemas de Informação
Fonte: Adaptado de Forcht, K.A., Computer Security Management, p. 66

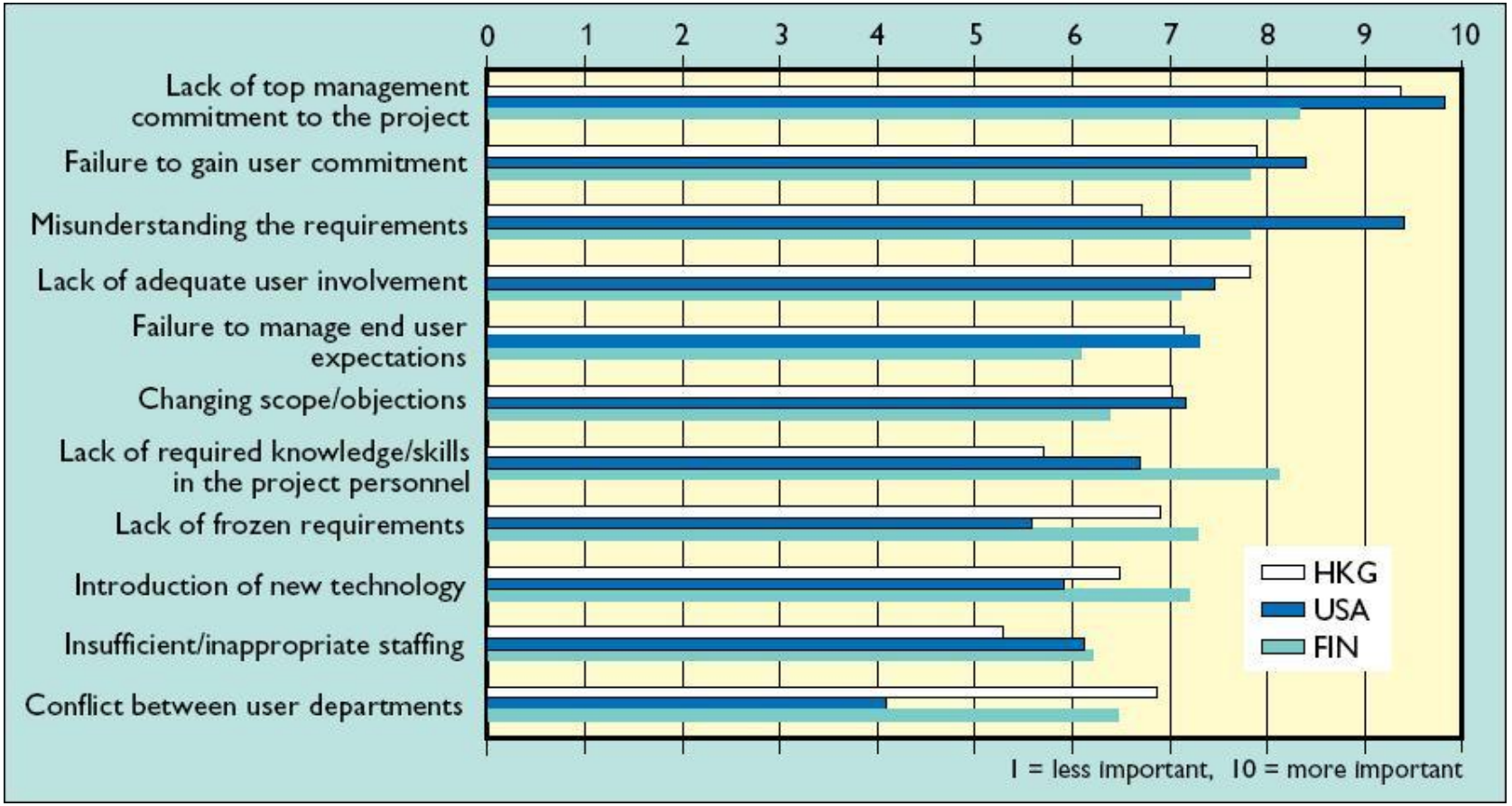
Risco – Conceitos Básicos

- É um mal que pode advir de um certo processo ou evento futuro.
  - Exemplos: desastres naturais, acidentes, processos legais...
- Qualquer negócio ou projeto está exposto a riscos;
- Projetos na área de TI são vistos como “The ultimate risky business”.

Risco – Aprofundando

- Um item de risco é uma propriedade de um projeto que, ignorado, pode aumentar a chance de fracasso.
  - Exemplos em TI:
    - Mudanças no faturamento ou custo previsto;
    - Nível de especialização necessário;
    - Competição inesperada.

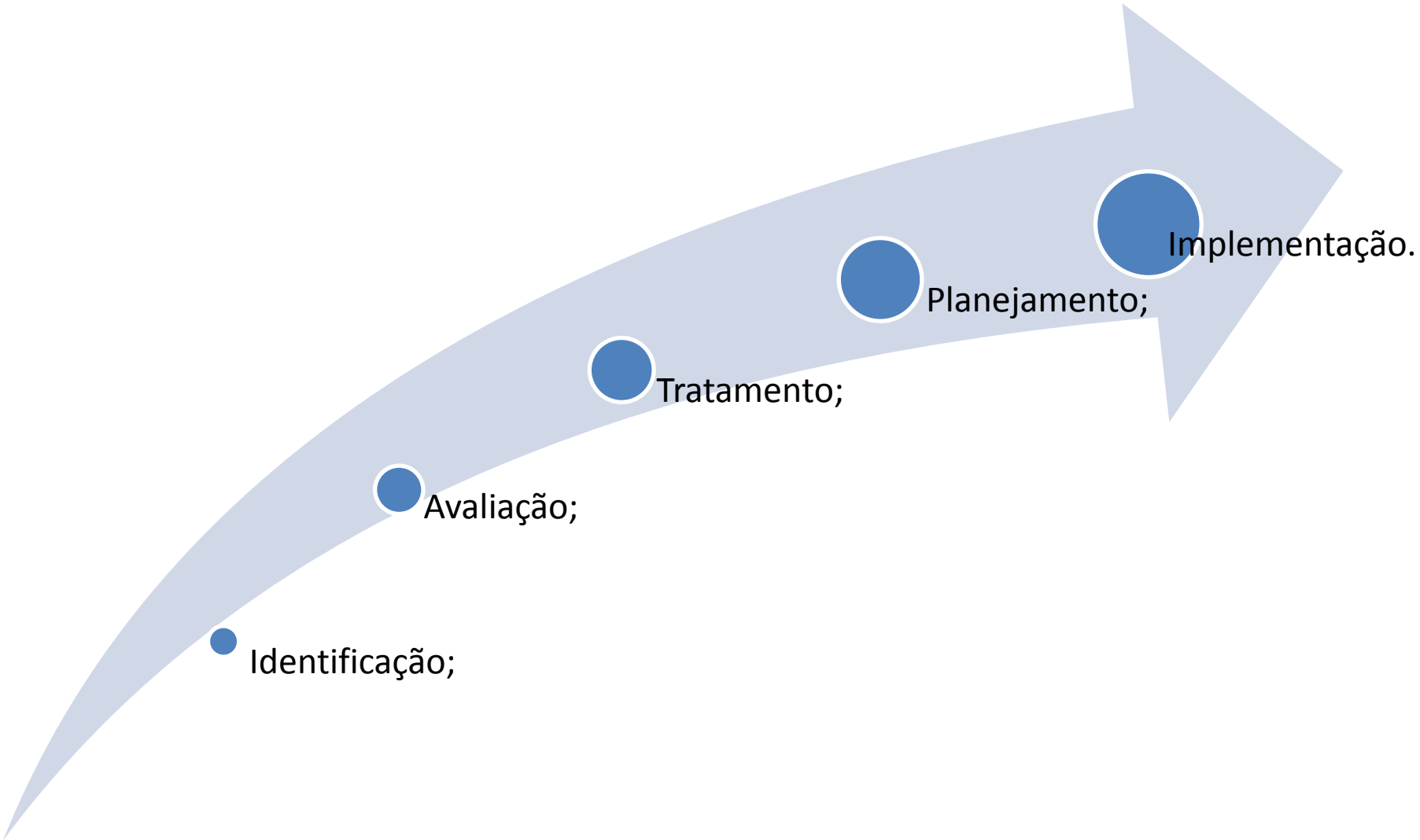
Risco em TI – Fatores Principais



Gerenciamento de Riscos

- Conjunto de medidas e procedimentos que visam medir, avaliar e desenvolver estratégias para tratar riscos.

Gerenciamento de Riscos – Etapas



Identificando Riscos

- Descobrir quais riscos existem;
- Análise da fonte;
  - Acionistas do projeto, empregados da companhia, clima em um aeroporto;
- Análise do problema:
  - Falta de investimento, pouca capacidade técnica, raio atingindo o avião.

Analisando Riscos

- Cálculo da vulnerabilidade associada a um risco;

  onde:

$$E = P \times L$$

  - E: vulnerabilidade (exposure);
  - P: probabilidade de o risco se tornar um problema;
  - L: prejuízo (loss) associado ao risco.

Tratando os Riscos

- Existem quatro técnicas principais para gerenciar riscos:
  - *Risk Avoidance;*
  - *Risk Reduction;*
  - *Risk Retention;*
  - *Risk Transfer;*

Risk Avoidance

- A solução mais óbvia é evitar o risco completamente;
  - "O avião não voa";
  - O projeto não é realizado;
- Sem riscos, mas também sem ganhos.

Risk Reduction

- Adotar medidas que reduzem a severidade dos prejuízos;
  - Máscaras de oxigênio, saídas de emergência;
  - Metodologias incrementais de desenvolvimento de software.

Risk Retention

- Aceitar os prejuízos quando os riscos se concretizam;
- Utilizada quando adotar medidas contra o risco é mais caro que aceitá-lo;
- Riscos muito baixos, mas com conseqüências catastróficas.

Risk Transfer

- Transferência da responsabilidade pelo prejuízo para outros;
- Normalmente feita por contratos;
  - Companhias seguradoras.

Riscos x Impactos

- Fatores de Risco são aleatórios e imprevisíveis, comparando-se ao efeito de uma onda, cuja intensidade e dano estarão vinculados ao cenário de ocorrência quando se concretiza

- Impactos são previsíveis, de acordo com o conhecimento do ambiente onde se manifestam e vinculados aos Eventos que se concretizaram, podendo ser contidos através de medidas de mitigação, independente do cenário

Exemplos de Riscos em TI

- Dependências de fatores externos:
  - Informações e dados fornecidos pelo cliente;
  - Serviços terceirizados;
  - Disponibilidade de pessoal treinado;
  - Reuso de projetos anteriores.

Exemplos de Riscos em TI

- Requisitos:
  - Falta de visão clara do produto;
  - Discordância quanto aos requisitos;
  - Prioridades indefinidas;
  - Novos nichos de mercado com necessidades desconhecidas;
  - Requisitos em mudança constante.

Exemplos de Riscos em TI

- Gerenciamento:
  - Planejamento inadequado;
  - Falta de clareza quanto a decisões de projeto;
  - Compromissos impossíveis de serem mantidos;
  - Prazos mal estabelecidos;
  - Falta de comunicação.

Exemplos de Riscos em TI

- Conhecimento:
  - Treinamento inadequado;
  - Fraca compreensão de métodos, ferramentas e técnicas;
  - Novas tecnologias.

Riscos em Sistemas Computacionais

- Falhas de hardware;
- Bugs no software;
  - Decorrentes de falhas na especificação ou na implementação;
  - Podem expor informações vitais da empresa a acessos indesejados.

O quê é um Plano de Contingência de Negócios PCN ?

- Metodologia que desenvolve estratégias alternativas para execução de processos[1] ou sistemas[2], minimizando os possíveis impactos acarretados pela sua interrupção, imposta por qualquer tipo de evento e que pode acarretar algum tipo de perda, financeira ou não.

1: PCN com foco para Continuidade dos Negócios
2: PCN com foco em Componentes de Tecnologia de Informação

Padronizando Conceitos

BIA (Business Impact Analysis): é a Análise de Impacto nos Negócios, acarretada pela indisponibilidade de um Processo (atividade) ou Componente (recurso por ele utilizado)

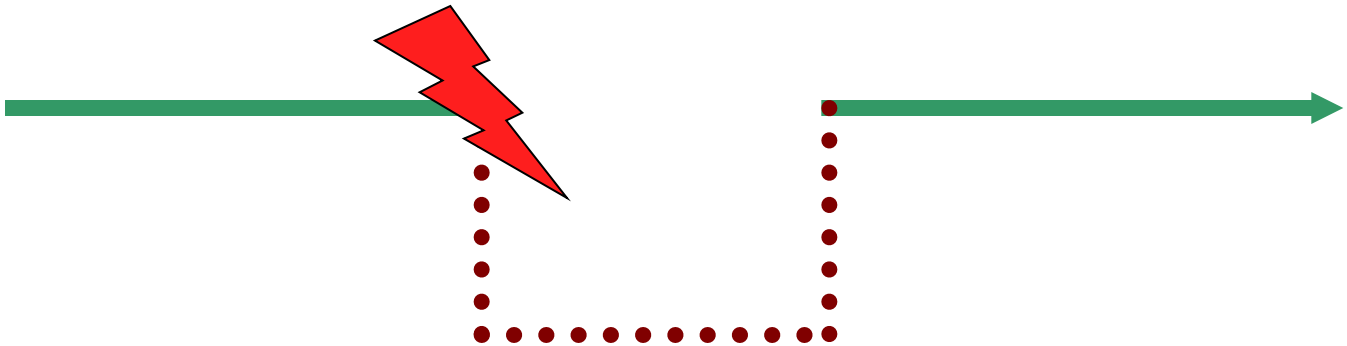
- Oferece uma métrica para a criticidade
- Avalia igualmente Processos ou Componentes
- Apresenta variáveis de custos tangíveis, custos intangíveis e períodos de tempo
- Identifica recursos mínimos necessários
- Seu resultado evidencia a importância das variáveis em função de perdas e prazos de tolerância à interrupções

Padronizando Conceitos

Disaster Recovery Plan (DRP): Plano de Recuperação de Desastres. É a documentação das atividades necessárias para restauração ou substituição dos recursos (Componentes) utilizados pelos Processos de Negócios

- Indica responsabilidades
- Orienta funções
- Define locais
- Indica o RTO (Recovery Time Objectives) – Objetivos de Prazos para Recuperação
- Indica o RPO (Recovery Point Objective) – Objetivos de Pontos de Recuperação

Como Funciona ?



Um **Plano de Recuperação de Desastres (PRD)** visa a reposição/restauração de um dos Componentes que suportam os PNs (p.e: a troca de um Servidor de Rede).

Padronizando Conceitos

Operational Contingency Plan (OCP): Plano de Contingência Operacional. Documenta procedimentos e atividades alternativas para serviços de TI ou Processos de Negócios

- Monitora e controla Fatores de Risco
- Indica responsabilidades e/ou substitutos
- Indica onde será realizado
- Indica como será executado
- É orientado pelos resultados obtidos pelo BIA, especialmente no que tange às variáveis de tempo e custos

Como Funciona ?

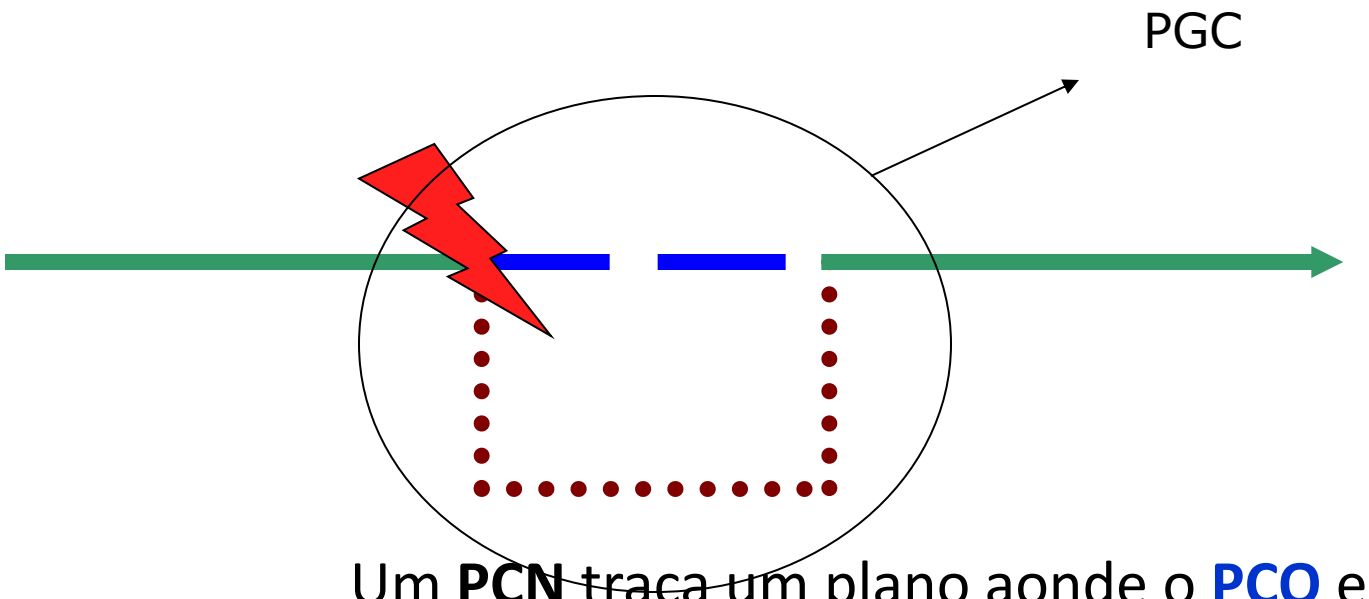
O **Plano de Contingência (PCO)** permite a execução do Processo de Negócio, mesmo que um Componente encontre-se indisponível.
(p.e.: como trabalhar sem telefonia ?).

Padronizando Conceitos

Business Continuity Plan (BCP): Plano de Continuidade de Negócios. É o conjunto de procedimentos documentados pelo PRD e pelo PCO, monitorado por um Plano de Gerenciamento de Crises (PRD) que facilita sua gestão e atualização.

- Orienta resposta aos Impactos mais prováveis
- Considera os principais (críticos) processos da organização
- Consolida responsabilidades, locais e prazos
- Indica parâmetros de RTO e RPO, evidenciados pelo BIA
- Evidencia elementos para auditoria e atendimento de requistos legais ou normativos

Como Funciona ?



Um **PCN** traça um plano aonde o **PCO** e o **PRD** são executados simultaneamente, garantindo a continuidade do PN e a reposição/restauração do Componente paralelamente

Justificando o PCN

- Quais são os principais negócios da minha organização?
- Quais são os fatores de risco operacionais que podem afetar seriamente os negócios da organização?
- Qual seria o impacto nas receitas geradas pelos negócios da empresa se um ou mais fatores de risco acontecesse?
- Como a empresa está preparada para lidar com o inevitável ou uma ameaça?

Justificando o PCN

- O que proteger (Quais processos?);
- Do que proteger (Quais desastres?);
- Com o que proteger (Que Processos e recursos adotar?);
- Grau de exposição (Quanto o(s) processo(s) está(ão) exposto(s) a um desastre?);
- Estimativa de Impacto de um Desastre (Qual a conseqüência de um desastre?);
- Estratégia de Continuidade (Como manter a capacidade produtiva no caso de um desastre?).

PCN - Limitação

- Um PCN responde a um desastre pré-definido;
- Um PCN não tem capacidade de responder o todo e qualquer desastre;
- Recomenda-se que seja considerado o conceito de “pior cenário possível”;

Fases PCN

Etapa Inicial	Etapa de Requisitos e Estratégia	Etapa de Implementação	Etapa de Operações
Início do Gerenciamento de Continuidade dos Negócios	Análise de Impacto no Negócios	Organização e Planejamento	Educação e Consciência
	Análise de Riscos	Implantação do Plano de Recuperação	Auditorias
	Estratégia de Continuidade de Negócios	Procedimentos de Desenvolvimento	Testes
		Teste Inicial	Gerenciamento de Alterações
			Treinamento

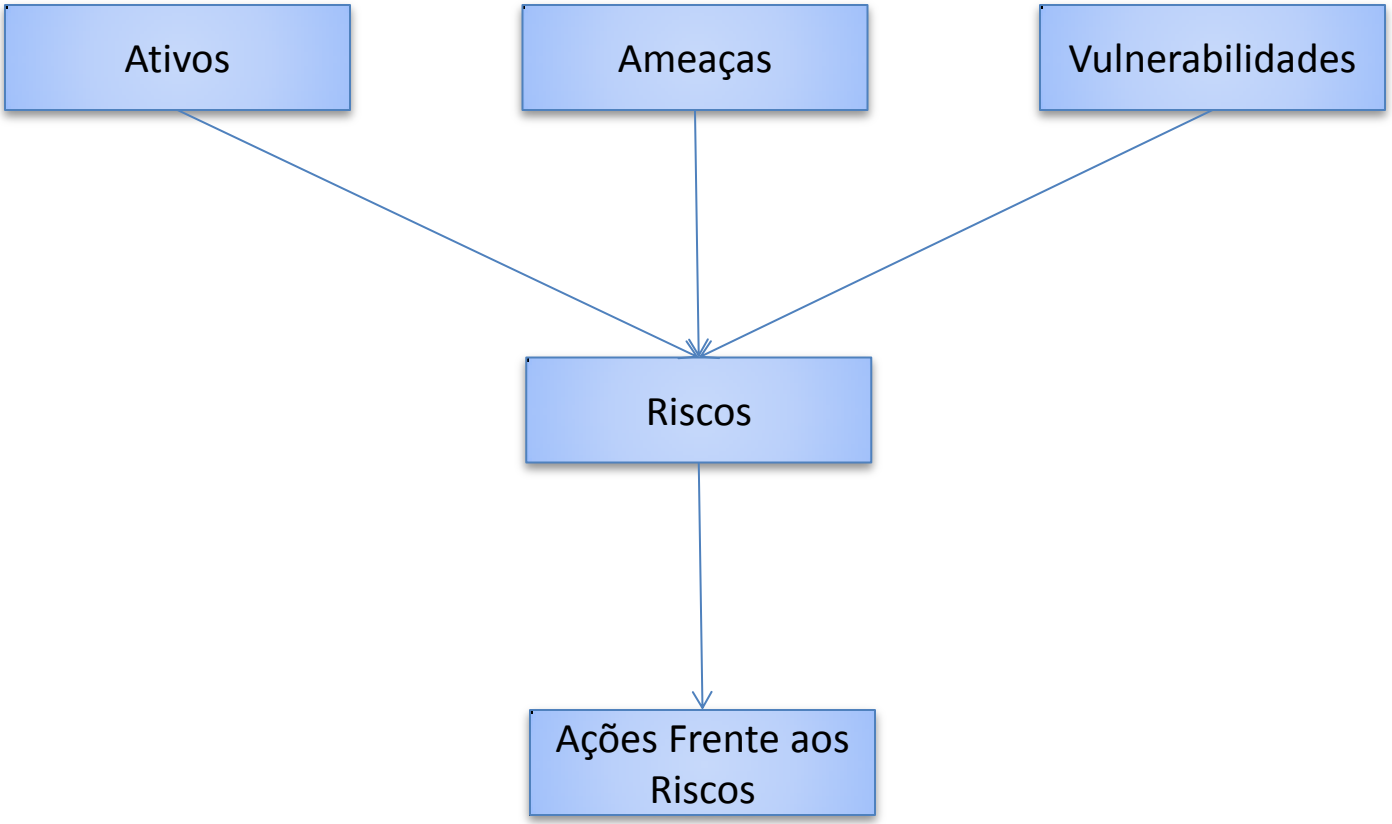
Etapa Inicial

- A única forma de implantar um gerenciamento de continuidade efetivo é através da identificação dos processos críticos do negócio e da análise e coordenação da infra-estrutura e serviços de TI que os suportam.
- A organização do processo cobre todo o processo e está formada pelas seguintes atividades:
  - Definição de políticas
  - Definição de termos de referência e alcance
  - Recursos alocados
  - Definição da organização do projeto e estrutura de controle
  - Contrato do projeto e plano de qualidade

Etapa de Requerimentos e estratégia

- Etapa que fornece a base do gerenciamento de continuidade e é um componente crítico para determinar a reação de uma empresa durante as interrupções do negócio ou desastres e o custo implicado.
  - Análise de impacto no negócio. Processos críticos do negócio
  - Danos potenciais ou perdas. Grau de dano ou perda e como será escalado
  - Habilidades do pessoal e instalações necessárias para ativar as funções críticas
  - Prejuízos financeiros e custos adicionais
  - Avaliação do risco, Identificação dos riscos
  - Avaliação dos níveis de vulnerabilidade e risco
  - Estratégia de continuidade do negócio
  - Medidas de redução de riscos, Eliminação de pontos de falha
  - Maiores controles de segurança física e lógica, Opções de recuperação

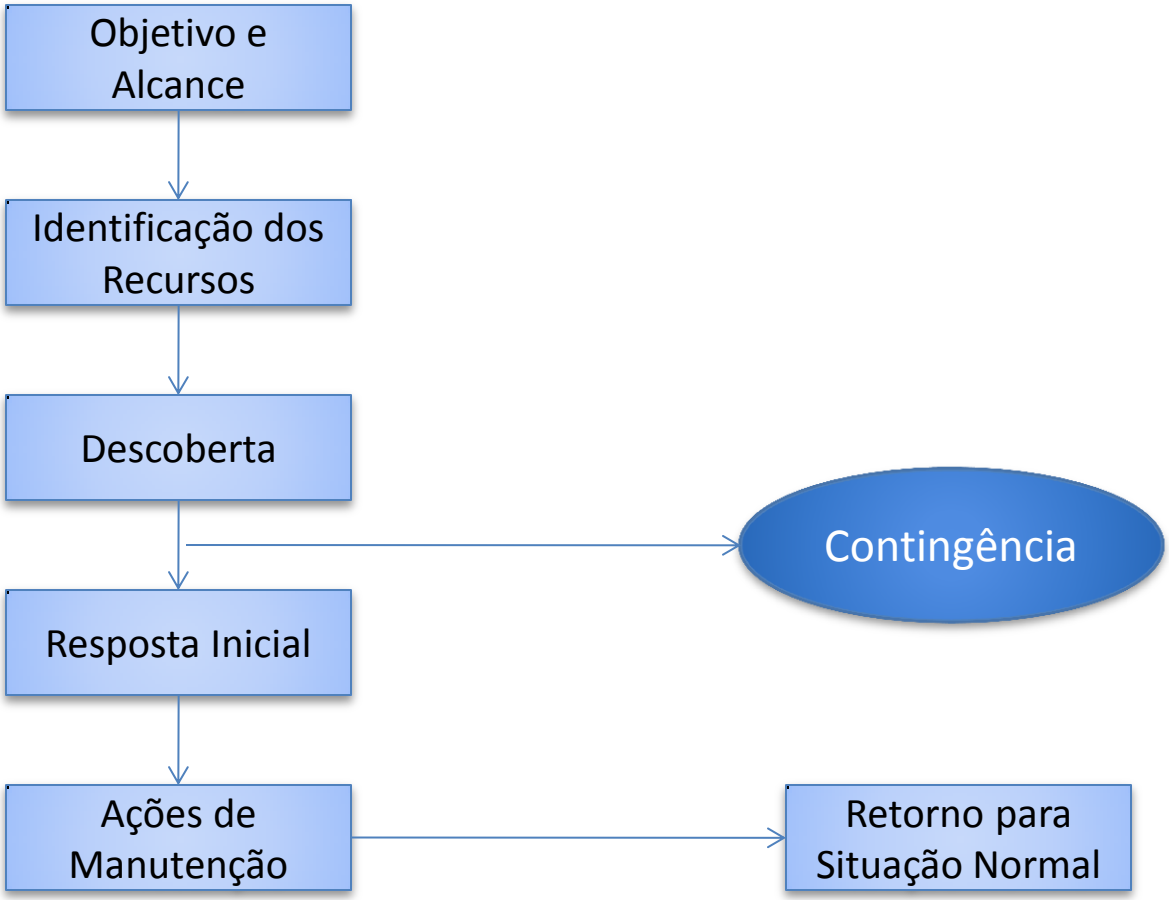
Etapa de Requerimentos e estratégia



Etapa de Implantação

- Esta etapa está formada pelos seguintes processos:
  - Estabelecer a organização e desenvolver o plano de implantação.
  - Implantar contratos de espera.
  - Implantar medidas de redução de riscos.
  - Desenvolver planos de recuperação de TI.
  - Desenvolver os procedimentos.
  - Realização de testes iniciais

Etapa de Implantação



Etapa de Operação

- Depois de finalizar a implantação é necessário garantir que o processo seja mantido como parte do negócio. Isto é conseguido graças ao gerenciamento operacional, incluindo:
  - Educação e conhecimento
  - Capacitação
  - Revisão
  - Prova
  - Controle de alterações
  - Garantia de qualidade

LEMBRETE

- Erros tendem a se repetir...

DICA

- É fácil fazer difícil. Difícil é fazer fácil !