

SEGURANÇA E PROTEÇÃO DE DADOS

Prof. Priscilla Cunha

pcunha@uni9.pro.br



INTRODUÇÃO

- Já cansamos de falar em nossas aulas da informatização das empresas e de seus sistemas... Hoje em dia, as empresas podem ter sistemas que necessitam funcionamento 24x7x365.

- Para isso é preciso que as mesmas tenham equipamentos de apoio sempre disponíveis e funcionando, pois as empresas estão altamente dependentes de suas informações e processos, que na maioria das vezes se encontram armazenadas no Data Center.

- A disponibilidade dos recursos de tecnologia da informação, ou seja, redes de computadores, servidores, sistemas e aplicações é muito importante para que a empresa não tenha as suas tarefas comprometidas, para garantir a sua disponibilidade.

- Quanto maior a disponibilidade que a empresas precisar ter, maior dependência de seus recursos ela terá.
- Para isso, equipamentos de apoio como nobreaks, geradores, aparelhos de ar condicionado e equipamentos de redes devem ter capacidade ociosa, além de equipamentos de reserva para o caso de falhas.

- Sistema de tolerância a falhas
 - Alta confiabilidade
 - Alta disponibilidade
 - Mantém o ambiente funcionando mesmo que falhas ocorram
 - Feito com duplicação de recursos
 - Alto custo

- Por falha devemos entender como sendo a ocorrência de um problema ou defeito. Elas são inevitáveis, sempre podem ocorrer e temos que estar preparados para isso.

- Algumas falhas comuns no ambiente de TI:
 - Problemas no fornecimento de energia;
 - Problema de acesso à rede por falhas de um equipamento (switch, roteador);
 - Problemas de conexão com a internet por falha do provedor;
 - Problema de hardware dos servidores (fonte, discos, placa de rede, memória, etc.);



DISPONIBILIDADE

- A disponibilidade dos ambientes de TI deve estar de acordo com a necessidade da empresa, e pode ser medida com o esquema dos 9's
- A disponibilidade aumenta quando aumentamos nossos recursos redundantes

Disponibilidade	Sistema	Indisponibilidade / ano
90%	Um 9	≈ 876h
99%	Dois 9's	≈ 87h
99,9%	Três 9's	≈ 9h
99,99%	Quatro 9's	≈ 50min
99,999%	Cinco 9's	≈ 5min

Níveis de Tolerância a Falhas

- Disponibilidade básica
 - Sistemas / serviços que podem ter o seu processo interrompido durante um período curto e que não causam impactos significativos para os principais processos da empresa. Podem ser enquadrados dentro da categoria dos três noves, que possibilitariam uma parada de até um dia comercial durante o ano.

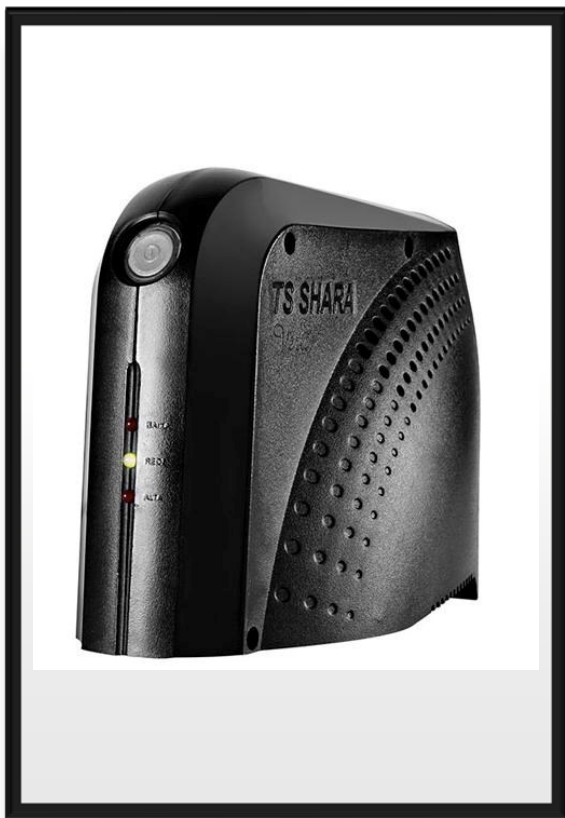
- Alta disponibilidade
 - Sistemas / serviços que precisam funcionar com um período muito baixo de indisponibilidade e, são críticos para a empresa. Para esse tipo de ambiente, o sistema / equipamento deve continuar a operar com toda a sua funcionalidade, mesmo com a presença de algum tipo de falha, e podemos conseguir isso com a existência de um equipamentos / recursos redundantes.


- Disponibilidade contínua / longa duração
 - Sistemas / serviços que precisam de disponibilidade no mínimo quatro nozes, ou seja, 99,99%, chegando, às vezes, ao absurdo de nove nozes 99,99999999, ou seja, pode ficar parado alguns segundos durante o ano ou mês. Aqui podemos pensar em sistemas / serviços cuja interrupção afete milhares de pessoas ao redor do mundo, como um satélite.

- Podemos ter redundância usando múltiplas unidades de hardware que aumentarão a disponibilidade de um recurso qualquer, utilização de múltiplas versões de software ou até mesmo múltiplas cópias de dados.

- Em muitos casos faz-se necessário que sejam implementadas medidas que farão os dados e as informações coexistirem simultaneamente em dois lugares diferente e ao mesmo tempo

- Alguns itens com os quais devemos nos preocupar quando pensamos em tolerância a falhas e alta disponibilidade:
 - Estabilizador;
 - No-break;
 - Gerador;
 - Servidores reserva;
 - Fontes e memórias reserva;
 - Switchs e roteadores reserva;
 - Link de internet duplicado, de outro fornecedor;
 - Ar condicionado reserva.





PLANO DE CONTINUIDADE DO NEGÓCIO - PCN

- As empresas, como estamos discutindo desde o começo do semestre, dependem mais e mais a cada dia de suas informações e ambientes computacionais.
- Porém, desastres podem acontecer de forma a deixar os ambientes completamente indisponíveis, e um plano de como manter as atividades da empresa funcionando é essencial, senão as empresas deixam de existir.

- Por mais que se invista em altíssima disponibilidade e redundância, sabemos que sempre podemos nos deparar com situações altamente críticas e irreversíveis.
- O mais importante para a empresa é que ela tenha uma forma de continuar suas operações, mesmo que seja de forma parcial, até que todo o restante possa voltar à normalidade.

- Quando falamos em continuidade, estamos nos referindo às atividades a serem realizadas para que a empresa continue operando mesmo em situações de crise e desastre de qualquer natureza e porte.
- As organizações devem garantir que seus programas de continuidade do negócio tenham a capacidade necessária para, em caso de necessidades, assegurar a recuperação da empresa.

- O programa de continuidade das empresas deve ser específico e exclusivo da mesma, refletindo sua realidade de negócio.
- Esse plano deve ser permanente e estar constantemente atualizado, pois os riscos, como vimos anteriormente, mudam.

- As operações de negócio das empresas estão, em sua grande maioria, baseadas em serviços e recursos de Tecnologia da Informação (TI). Este cenário se tornou tão crítico, que foram desenvolvidas boas práticas para alinhar os negócios com a TI. Neste contexto, é preciso entender como a TI:

- Está tratando as falhas, incidentes e desastres que afetam a operação do negócio corporativo;
- Está preparada para reagir, ou preferencialmente prever, eventos que comprometam a operação da organização;
- Qual o impacto (financeiro, institucional e comercial) para a organização no caso de uma parada operacional.

- Para tratar deste assunto, é extremamente relevante observar a importância de um Plano de Continuidade de Negócios (PCN) que tem como objetivo, garantir a continuidade das operações da empresa numa eventual indisponibilidade dos recursos que dão suporte à realização de suas operações (equipamentos, sistemas de informação, instalações, pessoal e informações).

- O PCN protege a empresa como um todo, não se preocupando apenas com a TI. Todos os processos operacionais devem ser englobados aqui, diferenciando quais são mais ou menos críticos, quanto tempo cada um deve levar para ser retomado, entre outras coisas.
- É no PCN que teremos descrito aquilo que é mais importante para a empresa e como fazer para que tudo seja restabelecido.

- A continuidade do serviço envolve a preparação prévia para o caso de problemas, pois criamos estratégias de recuperação das operações da empresa
- É preciso entender quais informações e ativos mantém a empresa em funcionamento

- Para garantir a continuidade deve-se:
 - Levantar todos os processos da empresa e identificar quais são os principais processos
 - Identificar quais são os ativos que mantêm esses processos funcionando
 - Ter planos de backup e restore (veremos em breve)

- Ao elaborarmos o PCN (que deve ser uma ação preventiva), devemos levar em conta o BIA (Business Impact Analysis), que é o impacto que um desastre pode ter em nosso cenário corporativo.
- O PCN será uma espécie de manual, check list da empresa do que fazer e como fazer.

- Devemos, ainda, definir o que deve ser feito para o restabelecimento de cada processo, quem é o responsável, onde se encontram as informações que precisam ser recuperadas, quem são os fornecedores de hardware e software e como tudo deve ser feito.

- Em primeiro lugar vamos nos preocupar com nossos sistemas mais críticos, e depois, de maneira planejada, iremos restabelecendo os demais processos.
- Devemos analisar:
 - tempo de recuperação X necessidade do negócio X o que eu perdi X o que eu tenho de Backup

- Devemos, ainda, saber quanto tempo cada processo pode ficar parado (RTO – Recovery Time Objectives) e até que ponto devemos recuperar as informações de cada processo (RPO – Recovery Points Objectives)

- O PCN contará, ainda, com alguns planos complementares:
 - PAC – Programa de Administração de Crise
 - PRD – Plano de Recuperação de Desastres (foco dele é TI)
 - PCO – Plano de Continuidade Operacional
 - PCC – Plano de Comunicações de Crise
- Um detalhe importante: O PCN deve estar armazenado em local seguro, separado das instalações principais da empresa, de forma a estar disponível em caso de desastres



SITES ALTERNATIVOS

- Caso o site principal da empresa fique totalmente indisponível, é necessário que a mesma continue operando de forma completa ou parcial, ou pelo menos que tenha um local para iniciar as atividades de recuperação
- Sendo assim, o PCN deve considerar a inclusão de um local alternativo

Cold Site

- Local com infraestrutura básica:
 - Água
 - Luz
 - Telefonia
 - Rede
 - Climatização
 - Combate a incêndio
 - Controle de acesso
- Não tem equipamentos de TI
- Não tem mobília
- Não permite testar se tudo vai funcionar



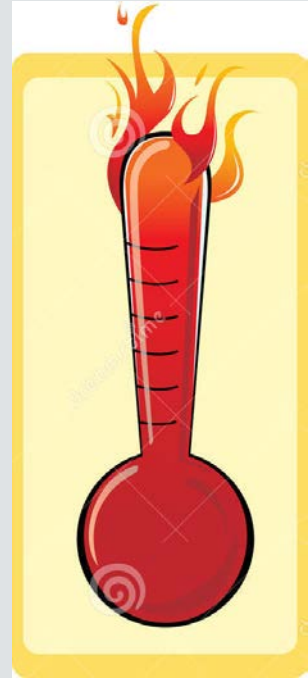
Warm Site

- Local com infraestrutura básica
- Possui os recursos de TI principais (que suportam os principais processos)
- Basta a alocação de alguns recursos e a restauração de algumas informações para um funcionamento básico
- Envolve o processo de restore de backup
- Tem um custo maior



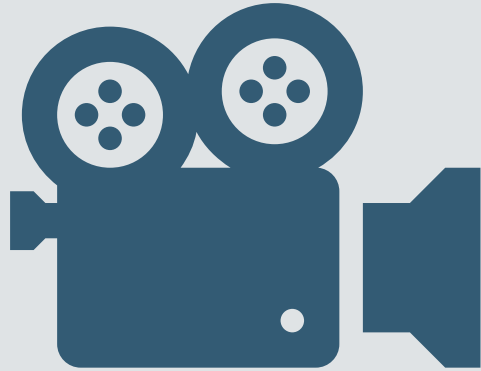
Hot Site

- Site idêntico ao original
- Mesmos recursos de TI
- Mesma infraestrutura
- Replicação real time das informações
- Alto custo
- Alto nível de continuidade





VÍDEOS



- Continuidade e contingência -

<https://www.youtube.com/watch?v=piWYbXYKRpU>



**PARA SABER
MAIS**

- Quanto custa um Data Center fora do ar?
- De acordo com pesquisas internacionais, temos a seguinte tabela de estimativas:

Tipo de negócio	Custo de Downtime por hora (US\$)
Corretagem	6.450.000
Energia	2.817.846
Autorizações de venda a crédito	2.600.000
Telecomunicações	2.066.245
Indústria	1.610.654
Instituições Financeiras	1.495.134
Seguros	1.202.444
Saúde	636.030
Reservas aéreas	90.000



- <https://www.meupositivo.com.br/panoramapositivo/disaster-recovery/>

