Gestão da Continuidade do Negócio

Gestão da Continuidade do Negócio

Unidade 5-Gestão da continuidade do negócio

- 5.1-Objetivo
- 5.2-Termos e Definições
- 5.3-Ciclo PDCA
- 5.4-Plano de Recuperação de Desastre em TI
- 5.5-Política GCN
- 5.6-ITIL-Gerenciamento de Continuidade de Serviço de TI (GCSTI)

Gestão da Continuidade do Negócio

Evite impactos negativos, mantenha a reputação de sua organização e garanta a continuidade e o sucesso de seus negócios!

Gestão da Continuidade do Negócio - GCN

- Gestão da Continuidade de Negócios (GCN) é uma abordagem integrada que envolve a mobilização de toda a organização para gerenciar crises e recuperar as operações após a ocorrência de qualquer evento que cause uma ruptura operacional.
- Um plano de continuidade (PCN) descreve as ações e processos necessários para recuperar as operações em caso de ruptura. Um plano de recuperação de desastres em TI (PRD) descreve os procedimentos para recuperar os sistemas e componentes de infraestrutura em caso de desastre.

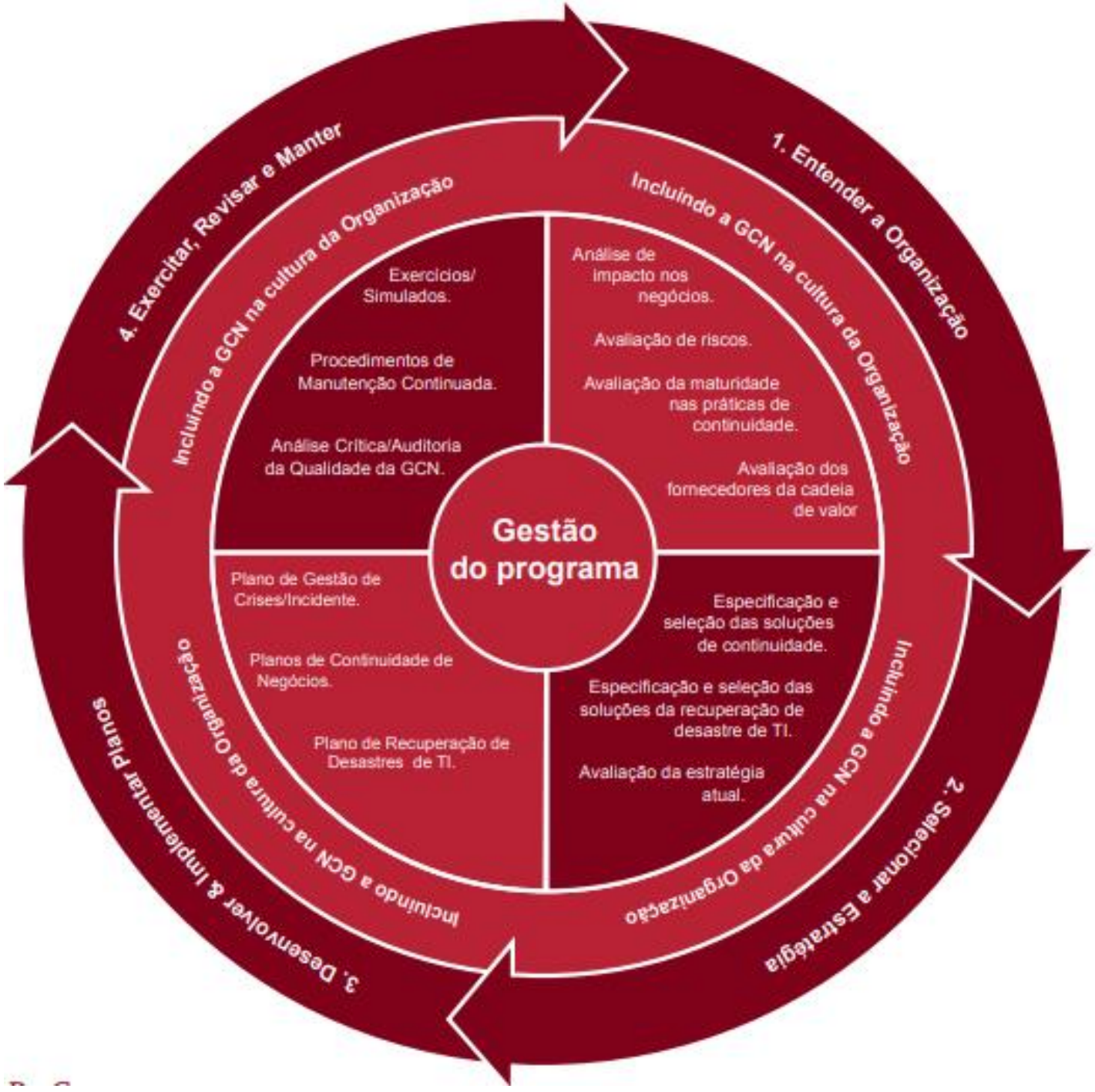
Gestão da Continuidade do Negócio - GCN

Gestão da Continuidade do Negócio - GCN

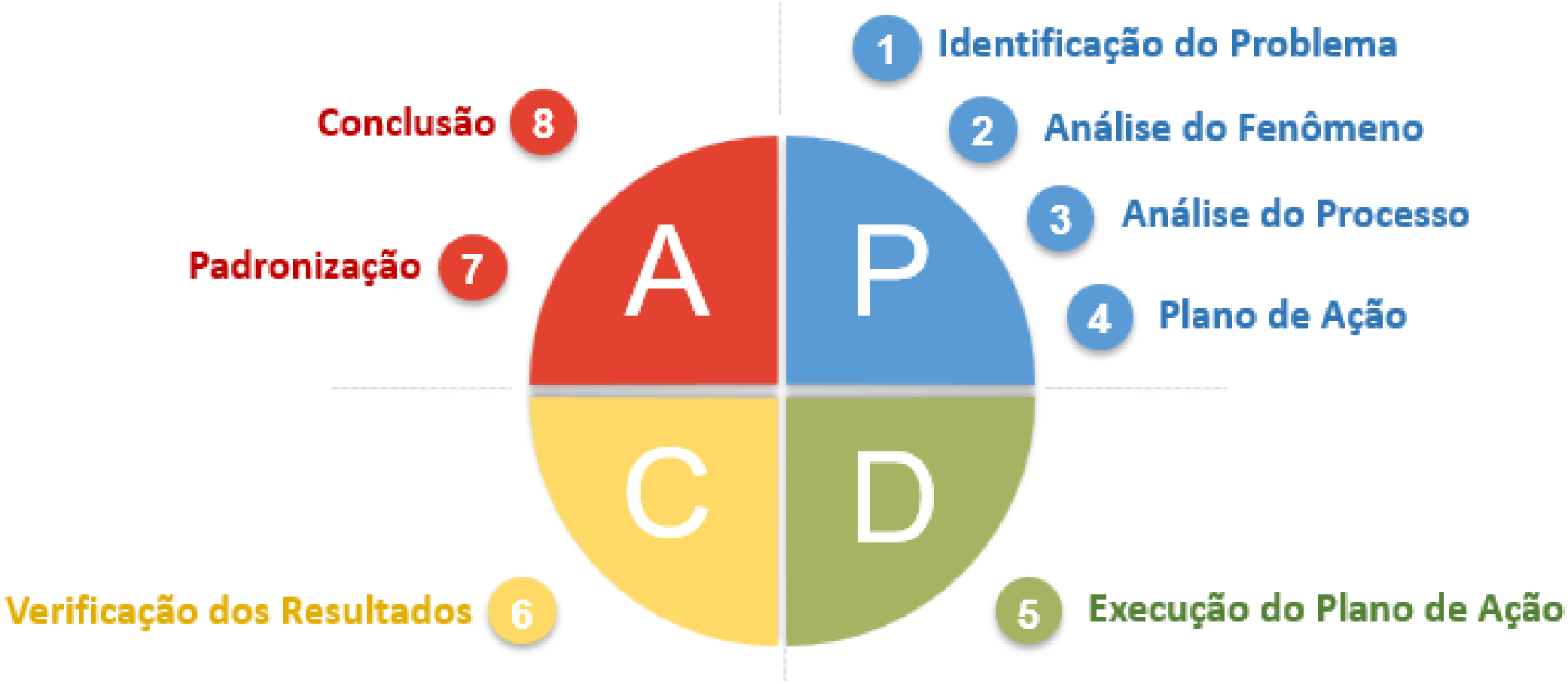
- Já o Plano de Gestão de Crises (PGC) endereça todos os elementos necessários à atuação coordenada durante a crise, a tomada de decisão de contingência e acionamento das equipes. Juntos, esses planos são os mecanismos necessários para garantir que uma organização possa se recuperar de forma eficaz após um desastre.
- As organizações que não possuem planos de contingência estão sujeitas a impactos significativos e atraso no processo de recuperação após um evento de catástrofe. Muitas destas organizações podem nunca se recuperar. As organizações, portanto, precisam assegurar a existência de planos adequados para facilitar a recuperação.

Gestão da Continuidade do Negócio - GCN

Gestão da Continuidade do Negócio



Gestão da Continuidade do Negócio



Gestão da Continuidade do Negócio

As organizações devem assegurar que seus programas de GCN possuam robustez necessária para garantir a recuperação eficaz. Os benefícios de um programa bem estruturado incluem:

1. Salvaguardar seu negócio, marca, reputação e demonstrar que sua empresa está apta a responder de forma oportuna e eficaz frente a incidentes, proporcionando uma vantagem competitiva.
2. Minimizar as perdas e os impactos financeiros, operacionais e de imagem relacionados a um evento de desastre.
3. Entender o que é crítico e essencial e identificas os objetivos de recuperação para os recursos que suportam o negócio de forma a concentrar os esforços de recuperação de forma inteligente e eficaz.
4. Identificar as vulnerabilidades e riscos que a organização está exposta e mitigá-los de forma apropriada.
5. Minimizar custos adicionais desnecessários com esforços e investimentos não planejados.
6. Reduzir potencialmente custos de seguro ao demonstrar que os riscos são gerenciados de forma eficaz.
7. Demonstrar aos acionistas que seu investimento na organização é seguro e está protegido contra casualidades.
8. Ajudar a garantir a segurança dos colaboradores, clientes e parceiros em suas instalações.

Gestão da Continuidade do Negócio - Objetivo

- Gestão da Continuidade Negócios é um processo de gestão holístico que identifica ameaças potencias a uma organização e os impactos às atividades comerciais se estas ameaças se concretizem.
- Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização, e suas atividades de valor agregado.

Gestão da Continuidade do Negócio - Objetivo

- O propósito de um plano de continuidade de negócios, é permitir que uma organização recupere ou mantenha suas atividades em caso de uma interrupção das operações normais de negócios.
- Os PCN são ativados para dar suporte às atividades críticas necessárias para cumprir os objetivos da organização. Eles podem ser executados integral ou parcialmente e em qualquer etapa da resposta a um incidente.

Gestão da Continuidade do Negócio - Objetivo

- O conteúdo e os componentes dos PCN variam de organização para organização e possuem diferentes níveis de detalhe, dependendo da escala, ambiente, cultura e complexidade técnica da organização.
- Algumas organizações de grande porte podem necessitar de documentos separados para cada uma de suas atividades críticas, enquanto as organizações menores podem ser capazes de abordar todos os aspectos críticos em um único documento.

Gestão da Continuidade do Negócio
Termos e Definições

Relembrando....

Gestão da Continuidade do Negócio

- O Plano de Continuidade de Negócios - PCN (do inglês Business Continuity Plan - BCP), estabelecido pela norma ABNT NBR 15999 Parte 1, é o desenvolvimento preventivo de um conjunto de estratégias e planos de ação de maneira a garantir que os serviços essenciais sejam devidamente identificados e preservados após a ocorrência de um desastre, e até o retorno à situação normal de funcionamento da empresa dentro do contexto do negócio do qual faz parte.

Gestão da Continuidade do Negócio

- O **SGCN**, é um padrão mundial mais abrangente para a continuidade, definido pelas **ISO 22301** e **ISO 27301** que, além de definirem os processos tradicionais de GCN, acompanha e analisa a eficiência destes programas, garante o seu alinhamento com os objetivos e metas corporativos e envolve todos os stakeholders que participam ou são impactados por este sistema, criando assim um ciclo de melhoria contínua.

Gestão da Continuidade do Negócio

- A responsabilidade da implementação do plano de continuidade de negócios é dos dirigentes da organização.
- A equipe de gerência da segurança pode auxiliar nessa tarefa, na criação, manutenção, divulgação e coordenação do plano de contingências.

Gestão da Continuidade do Negócio

Ciclo de vida responsabilidades do PCN

- Tomando como referência a ISO 22301, cláusulas 8.4 e 8.5, o ciclo de vida de um PCN pode ser descrito por estes passos gerais:
  - **Elaboração:** definição de cenários sob os quais um evento de interrupção pode ocorrer, e o que fazer para tratar tais incidentes potencialmente catastróficos.
  - **Teste:** realização exercícios e simulações para assegurar que planos, pessoas e recursos funcionarão adequadamente durante um evento de interrupção.
  - **Execução:** quando um evento de interrupção atinge a organização, impactos devem ser minimizados e processos de negócio devem ser retomados e recuperados como definido nos objetivos do PCN.
  - **Atualização:** análises críticas devem ser realizadas após testes ou ativações de um plano, de forma que o plano possa ser corrigido e melhorado.

Gestão da Continuidade do Negócio

- Sob o ponto de vista do PCN, o funcionamento de uma empresa deve-se a duas variáveis:
  - Processos: as atividades realizadas para operar os negócios da empresa;
  - Componentes: todas as variáveis utilizadas para realização dos processos: energia, telecomunicação, informática, infraestrutura, pessoas, etc.. Todas elas podem ser substituídas ou restauradas, de acordo com suas características.
- O Plano de Continuidade de Negócios é constituído pelos seguintes planos:
  - Plano de Contingência,
  - Plano de Administração de Crises (PAC),
  - Plano de Recuperação de Desastres (PRD) e
  - Plano de Continuidade Operacional (PCO).

Gestão da Continuidade do Negócio

- Todos estes planos têm como objetivo principal a formalização de ações a serem tomadas para que, em momentos de crise, a recuperação, a continuidade e a retomada possam ser efetivas, evitando que os processos críticos de negócio da organização sejam afetados, o que pode acarretar em perdas financeiras.
- No que diz respeito à necessidade de atualizações, o Plano de Continuidade de Negócios deve ser revisado periodicamente, porque mudanças significativas em componentes, atividades ou processos críticos de negócio podem fazer com que novas estratégias e planos de ação sejam previstos, evitando assim com que eventuais desastres desestabilizem profundamente o andamento regular do negócio da empresa.

Gestão da Continuidade do Negócio

- Desastre pode ser entendido como qualquer situação que afete os processos críticos do negócio de uma organização.
- Consequentemente, algumas ocorrências podem ser caracterizadas como sendo desastres para uma determinada empresa, mas não como tal em outra empresa.

Gestão da Continuidade do Negócio

- Um Plano de Continuidade de Negócios eficiente e eficaz exige três condições essenciais:
  - **Análise de Risco**: o que de ruim pode vir a acontecer? (principais ameaças)
  - **Análise de impacto**: de que forma eventuais ameaças podem impactar o negócio?
  - **Planejamento Estratégico**: se uma ameaça se apresentar, quais atitudes e ações se fariam necessárias para a retomada das operações?

A Estrutura do Plano de Continuidade de Negócios

- Via de regra, um Plano de Continuidade de Negócios é estruturado em quatro subplanos menores, ligados entre si e cada qual para um estágio diferente. Já citados anteriormente, vamos a eles:
  - **Plano de Contingência** (Emergência): deve ser utilizado em último caso, quando todas as prevenções tiverem falhado. Define as necessidades e ações mais imediatas.
  - **Plano de Administração ou Gerenciamento de Crises** (PAC): define funções e responsabilidades das equipes envolvidas com o acionamento das ações de contingência, antes durante e após a ocorrência.
  - **Plano de Recuperação de Desastres** (PRD): determina o planejamento para que, uma vez controlada a contingência e passada a crise, a empresa retome seus níveis originais de operação.
  - **Plano de Continuidade Operacional** (PCO): seu objetivo é reestabelecer o funcionamento dos principais ativos que suportam as operações de uma empresa, reduzindo o tempo de queda e os impactos provocados por um eventual incidente. Um exemplo simples é a queda de conexão à internet.

Gestão da Continuidade do Negócio

- Em suma, o Plano de Continuidade de Negócios tem como finalidade central criar normas e padrões para que, em situações adversas, as empresas possam recuperar, retomar e dar prosseguimento aos seus mais cruciais processos de negócio, evitando que eles sofram danos mais profundos que provoquem perdas financeiras.

Controles p/ Gestão da Continuidade do Negócio

Controles p/ Gestão da Continuidade do Negócio

ANÁLISE DE IMPACTO NOS NEGÓCIOS (BIA)

- Quantitativo
- Qualitativo

INSPEÇÃO FÍSICA DE AMBIENTES;

TREINAMENTOS E CONSCIENTIZAÇÃO EM GCN – EXECUTIVA E OPERACIONAL.

Controles p/ Gestão da Continuidade do Negócio

PLANOS DE CONTINUIDADE DE NEGÓCIOS (PCN):

- Plano de Contingência Operacional – Negócios;
- Plano de Recuperação de Desastres - TI;
- Plano de Gestão de Crises;
- Plano de Resposta a Incidentes;
- Plano de Comunicação Interna;
- Plano de Comunicação Externa;
- Plano de Testes, Simulações e Exercícios.

Gestão da Continuidade do Negócio

O **MTPD** – Most tolerable period of disruption, trata-se do período que um processo PODE FICAR INTERROMPIDO em estado de Continuidade/Contingência.

MBCO - Minimum Business Continuity Objectives - Objetivos de Continuidade de Negócio Mínimos.

RPO = antes do incidente

RTO = depois do incidente

DRP (Disaster Recovery Plan)

CAPEX, é uma sigla que em inglês significa **capital expenditure**). É aquilo que a empresa adquire fisicamente, por exemplo um computador. Já **OPEX** (operational expenditure) refere-se às despesas operacionais.

Gestão da Continuidade do Negócio

Gestão da Continuidade do Negócio


Action (Agir)
Plan (Planejar)
1 Identificação do Problema
2 Análise do Fenômeno
3 Análise do Processo
4 Plano de Ação
5 Execução
6 Verificação
7 Ação
8 Padronização
A
P
C
D
Check (Verificar)
Do (Executar)

Ciclo PDCA

- **PDCA** (do inglês: ***PLAN*** - ***DO*** - ***CHECK*** - ***ACT*** ou ***Adjust***) é um método iterativo de gestão de quatro passos, utilizado para o controle e melhoria contínua de processos e produtos.
- É uma ferramenta baseada na repetição, aplicada sucessivamente nos processos buscando a melhoria de forma continuada para garantir o alcance das metas necessárias à sobrevivência de uma organização.
- Pode ser utilizada em qualquer ramo de atividade, para alcançar um nível de gestão melhor a cada dia.
- Seu principal objetivo é tornar os processos da gestão de uma empresa mais ágeis, claros e objetivos.

Plano de Recuperação de Desastre em TI

- Um Plano de Recuperação de Desastre de TI (DRP – Disaster Recovery Plan) eficaz para minimizar as interrupções nas redes e restaurar rapidamente a normalidade das atividades.
- A chave para recuperação de desastres de TI ou de rede é a preparação. Por isso é preciso desenvolver um Plano de Recuperação de Desastres com uma documentação abrangente de ações bem planejadas a serem adotadas antes, durante e após um evento catastrófico.

Plano de Recuperação de Desastre em TI

- O DRP é a ferramenta principal das organizações para proteger sua infraestrutura de TI, determinar a estabilidade organizacional e recuperação sistemática de desastres.
- Para garantir a continuidade do negócio e disponibilidade de recursos críticos durante as ocorrências, o plano deve ser documentado e testado com antecedência.
- Isso ajudará a acelerar o processo quando ocorrer um real desastre ou emergência.

Plano de Recuperação de Desastre em TI

- Os principais objetivos do Plano de Recuperação de Desastres incluem:
  - Minimizar a interrupção das operações comerciais;
  - Minimizar o risco de atrasos;
  - Garantir um nível de segurança;
  - Garantir sistemas de backup confiáveis;
  - Ajudar na restauração das operações com velocidade.

Plano de Recuperação de Desastre em TI

Em qualquer organização que se prepara para a recuperação de desastres para responder às variadas circunstâncias e problemas, os três pontos principais a serem considerados são:

- 1- Prevenção:
  - Medidas de segurança que possam barrar os desastres antes que ocorram. Como é o caso de backup e recuperação na nuvem, que evitam que os dados estejam vulneráveis a desastres naturais e outros acidentes que possam ocorrer na sua empresa.
- 2- Antecipação:
  - Planejar e desenvolver medidas adequadas para combater desastres inevitáveis. Contratar um serviço de recuperação de desastres no caso de um ataque de hackers para ter certeza que todos os dados serão recuperados.
- 3- Mitigação:
  - Gerenciar os desastres assim que ocorrem e, dessa forma, minimizar os seus impactos negativos. Um serviço de recuperação de desastres garantirá tempos adequados de retorno as atividades, sem prejuízos para as operações e os negócios.

Política GCN

- O **SGCN**, é um padrão mundial mais abrangente para a continuidade, definido pelas **ISO 22301** e **ISO 27301** que, além de definirem os processos tradicionais de GCN, acompanha e analisa a eficiência destes programas, garante o seu alinhamento com os objetivos e metas corporativos e envolve todos os stakeholders que participam ou são impactados por este sistema, criando assim um ciclo de melhoria contínua.

ITIL - Gerenciamento de Continuidade de Serviço de TI

Gerenciamento de continuidade de serviço de TI

- Este pode ser um assunto extremamente complexo quando se trata de sua aplicação, mas igualmente necessário para manter o recurso funcionando.
- A continuidade de serviço de TI é responsável pela habilidade de recuperação necessária para os serviços de TI e seus componentes de apoio em um evento de desastre. Dentre estes eventos temos:
  - Incêndios
  - Enchentes
  - Terrorismos
  - Tempestades
  - Vandalismos
  - Blackouts e apagões

ITIL - Gerenciamento de Continuidade de Serviço de TI

- Como o processo de disponibilidade foca na operação normal do negócio, cabe ao gerenciamento de continuidade de serviço de TI se preocupar com desastres.
- Este processo auxilia na introdução de medidas de redução de riscos e opções para a recuperação dos serviços.
- Seu propósito:
  - Apoiar o processo de continuidade do negócio;
  - Gerenciar riscos que podem afetar seriamente os serviços de TI;
  - Garantir a provisão no mínimo SLA.

ITIL - Gerenciamento de Continuidade de Serviço de TI

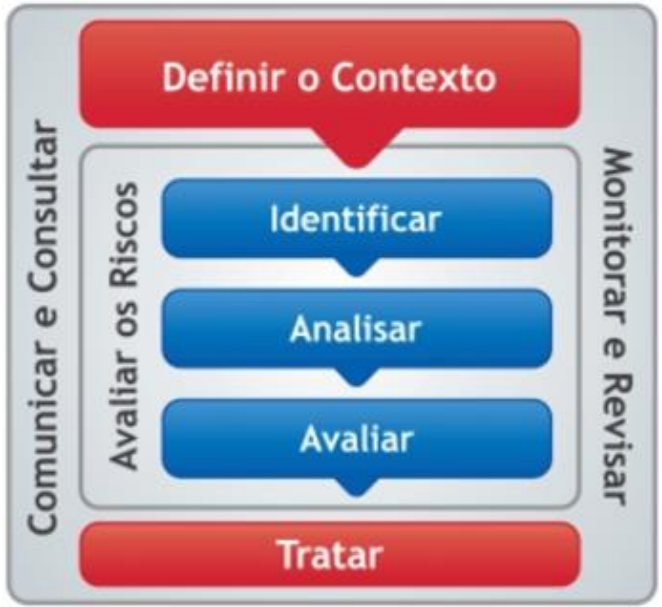
- Suas Definições:
  - Definir e manter planos de continuidade de serviços de TI
  - Realizar regularmente análise de impacto
  - Análise de gerenciamento de riscos
  - Orientar as outras áreas sobre continuidade e recuperação dos serviços de TI
  - Assegurar a implantação dos mecanismos adequados
  - Avaliar o impacto de todas as mudanças nos planos de continuidade de serviços de TI
  - Manutenção contínua nos planos

ITIL - Gerenciamento de Continuidade de Serviço de TI

- Análise de impacto:
  - Ao criar um modelo de análise de impacto, devemos levar em conta:
  - Serviços críticos do negócio de TI
  - Impactos causados pela indisponibilidade
  - Cenários de impacto
  - Obrigações da empresa perante a lei vigente
  - Tempo em que a empresa aguentaria sem os serviços e TI
  - Requisitos para recuperação
  - Determinar o tempo mínimo e máximo dos níveis de serviços a serem recuperados
  - Definir quais processos de negócio devem ser recuperados por completo

ITIL - Gerenciamento de Continuidade de Serviço de TI

- Análise de riscos:
  - Para determinar os requisitos de continuidade é importante ter um entendimento da probabilidade que um evento de desastre ou outra interrupção maior no serviço poderá de fato ocorrer. Isto é feito por meio de uma avaliação de riscos.
  - A avaliação determina as ameaças e o quanto a organização está vulnerável à elas.
  - A Avaliação também pode ser usada em outros processos como gerenciamento de disponibilidade e gerenciamento de segurança da informação.



ITIL - Gerenciamento de Continuidade de Serviço de TI

Ameaça	Vulnerabilidade	Probabilidade	Efeito/impacto	Contramedida
Enchente	As instalações da TI estão no subsolo do prédio da empresa.	Média	Estrago da água, falta de acesso a sala de servidores.	Colocar o datacenter em andar seguro.
Blackout elétrico	A empresa está situada em uma ilha e os cabos de energia que alimentam a cidade passam por debaixo da ponte.	Média	Perda de dados, perda de controles de segurança.	Utilizar gerador de energia. Utilizar estação elétrica auxiliar.
Falha no servidor de aplicativo ERP (SAP)	Um hacker pode invadir a rede e danificar os dados.	Alta	Parada dos processos de faturamento, vendas, etc.	Fazer backup dos dados.

Gestão da Continuidade do Negócio