


# **Plano de Contingência**

## **Plano de Continuidade do Negócio - PCN**

A series of horizontal lines in teal and light blue colors, with varying lengths and offsets, creating a modern, layered effect across the width of the slide.

# Plano de Continuidade do Negócio - PCN



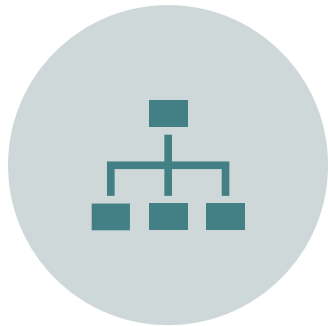
As empresas, como estamos discutindo desde o começo do semestre, dependem mais e mais a cada dia de suas informações e ambientes computacionais.



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.



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.



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.



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.



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

# Como Montar o Plano de Contingência

## Mapear os pontos fracos da empresa

- Fazer uma lista dos pontos fracos e possíveis focos de crise na empresa.
- Dividir os diferentes cenários de crise de acordo com as consequências que cada um pode trazer.

## Definir prioridades

- Definir quais são as atividades e processos principais da empresa, para saber o que deve ser mantido e/ou restabelecido primeiro.
- Classificar essas atividades e processos como “essencial”, “importante” ou “não essencial”.



## Elaborar plano de ação

Listar as ações a serem tomadas para minimizar ou eliminar esses pontos fracos.



## Escrever o plano de contingência

Escrever o documento de política de contingência que deve incluir etapas claras a serem seguidas caso qualquer um dos eventos identificados ocorra.



## Testar o plano de contingência

- Alguns itens que devem ser contemplados em um plano de contingência:
  - O que fazer em caso de falta de energia;
  - O que fazer em caso de parada de link de internet;
  - O que fazer em caso de falhas de hardware e/ou dispositivos de rede;
  - O que fazer em caso de infecção da rede por vírus;
  - O que fazer em caso de ciberataque e vazamento de informações;
  - O que fazer em caso de desastres críticos;
  - Entre outros.

# Plano de Administração de Crises (PAC)



A administração de crise é um trabalho delicado, de muita responsabilidade e que exige muito conhecimento técnico e prático.



Quando falamos do gerenciamento de crises na área da TI, essa tarefa fica bem mais complexa — porém, ainda mais essencial.

# O que é uma crise?



Crise é todo e qualquer evento inesperado que possa comprometer o bom funcionamento da empresa.



Em toda instituição e em todos os setores, existem situações conflituosas e problemáticas que são denominadas de “momentos de crise”.



No setor de TI, as crises podem estar relacionadas, por exemplo, à perda de dados, à invasão dos arquivos por fonte externa, a problemas internos de manutenção e/ou utilização dos equipamentos e sistemas, entre outros.

Situações de crise podem ser ocasionadas por vários fatores, como já vimos ao tratar de análise de riscos: desastres naturais, acidentes, pessoas mal intencionadas e falhas são os mais comuns.

Elas podem vir acompanhadas de interrupções que afetam o funcionamento da empresa, causando grandes prejuízos



# Plano de Administração de Crises (PAC)



O PAC é um documento que define as responsabilidades dos membros das equipes envolvidas com o acionamento da contingência antes, durante e depois da ocorrência do incidente, além de definir os procedimentos a serem executados pela mesma equipe no período de retorno à normalidade.



O principal objetivo do Plano de Administração de Crises (PAC) é definir os procedimentos a serem executados até o retorno normal das atividades da organização.



Ele define o "passo a passo" o funcionamento das equipes antes, durante e depois da ocorrência do incidente.



Trata-se da capacidade de atuar diante dos momentos mais delicados de forma eficiente, analisando o quanto antes os sinais de que algo está errado e tomando, desde o princípio, todas as medidas possíveis para amenizar suas consequências e resolver a situação o quanto antes.

# Comitê de gestão de crises

- O comitê deve se reunir periodicamente, pelo menos uma vez por semestre e a cada novo evento significativo, para analisar os planos e os cenários adversos que podem influenciar a empresa.
- **Atribuições do comitê de gestão de crises:**
  - Saber quais as partes da estrutura da empresa são essenciais e não podem parar.
  - Conhecer bem as instalações e serviços da empresa, nas diversas unidades.
  - Estabelecer a função principal de cada envolvido.
  - Reunir-se para discutir e treinar, pelo menos semestralmente, uma eventual situação de risco.
  - Ter autoridade e autonomia para falar e agir em nome da empresa.
  - Ter sempre um plano B para cada procedimento de crise do PAC.

---

Crises geram prejuízos significativos, incluindo multas, indenizações, honorários legais, despesas com material e muito mais.

---

Tais custos não são cobertos por seguros e afetam funcionários, clientes e fornecedores.

---

Planejar para crises é essencial, e não há uma abordagem única, já que cada empresa precisa de uma estratégia personalizada.

---

É crucial reunir uma equipe estratégica que represente a organização.

---

O Plano de Ação de Crise (PAC) deve ser ágil, tranquilo, versátil e baseado na aprendizagem com erros anteriores. O PAC deve responder a perguntas-chave para direcionar a resolução da crise de forma eficaz.

# Plano de Recuperação de Desastres (PRD)

- O Plano de Recuperação de Desastres (PRD), com foco em Tecnologia da Informação (TI), é um componente essencial da gestão de riscos e continuidade de negócios de uma organização. Ele é projetado para garantir que os sistemas de TI críticos e os dados da empresa possam ser restaurados e recuperados em caso de desastres ou interrupções significativas.
- Alguns pontos-chave sobre o PRD:

- **Objetivo:** O objetivo principal de um PRD é minimizar a interrupção dos serviços de TI após um desastre e garantir a rápida recuperação de sistemas essenciais para a continuidade dos negócios.
- **Avaliação de Riscos:** Antes de criar um PRD, é fundamental realizar uma avaliação de riscos para identificar ameaças potenciais que podem afetar a TI, como desastres naturais, falhas de hardware, ciberataques e outros eventos adversos.

- **Definição de Recuperação:** O PRD deve especificar os tempos de recuperação aceitáveis para sistemas e dados críticos. Isso inclui a definição de **RTO (Recovery Time Objective)** e **RPO (Recovery Point Objective)**, que indicam o tempo máximo que uma organização pode tolerar para recuperar dados e sistemas.
- **Procedimentos de Recuperação:** O plano deve detalhar os procedimentos para restaurar sistemas, aplicativos e dados. Isso envolve a identificação de backups, locais de recuperação, responsabilidades da equipe e a sequência de ações a serem tomadas.

- **Testes e Treinamento:** O PRD não é eficaz se não for testado regularmente. Simulações de desastres e treinamentos da equipe de TI são necessários para garantir que o plano funcione quando necessário.
- **Backup e Recuperação de Dados:** O PRD deve incluir estratégias sólidas de backup e recuperação de dados, garantindo que as informações críticas estejam protegidas e possam ser restauradas com eficiência.

- **Local de Recuperação:** É importante determinar um local de recuperação secundário, seja um data center alternativo, nuvem ou outro local remoto, para garantir a continuidade dos serviços de TI, mesmo em caso de falha nas instalações principais.
- **Segurança Cibernética:** Considerações de segurança cibernética são fundamentais. Um PRD deve incluir medidas para proteger os sistemas de TI durante e após um desastre, incluindo proteção contra ataques cibernéticos.



- **Comunicação e Notificação:** Um plano eficaz deve incluir procedimentos de comunicação para informar a equipe, partes interessadas e clientes sobre a situação e as ações em andamento.
- **Documentação Adequada:** Todo o PRD deve ser documentado de forma clara e atualizada regularmente. Isso garante que a equipe saiba o que fazer em caso de um desastre.
- **Melhoria Contínua:** Um PRD não é um documento estático. Deve ser revisado e atualizado conforme as necessidades da organização e as ameaças evoluem.

# Plano de Continuidade Operacional (PCO)

- O Plano de Continuidade Operacional (PCO) é um conjunto de estratégias e procedimentos que visam manter a operação de uma organização durante eventos disruptivos, como desastres naturais, crises de segurança cibernética ou interrupções significativas.
- O PCO é projetado para garantir que as funções críticas do negócio continuem a operar com o mínimo de interrupções, minimizando o impacto nos clientes e partes interessadas. Ele aborda a continuidade dos processos de negócios, a recuperação de sistemas e dados essenciais e a manutenção da operacionalidade em situações adversas.

# Plano de Comunicações de Crise (PCC)

- O Plano de Comunicações de Crise (PCC) é um conjunto de estratégias e diretrizes para gerenciar a comunicação durante eventos de crise.
- Define como a organização se comunicará interna e externamente, incluindo a identificação de porta-vozes, mensagens-chave e canais de comunicação.
- O PCC visa garantir que as informações sejam transmitidas de maneira clara, rápida e eficaz durante situações adversas, mantendo a transparência e protegendo a reputação da organização.

# 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

- **O que é Plano de contingência?**
  - <https://www.youtube.com/watch?v=piWYbXYKRpU>
- **O que é Plano de Contingência - 4 minutos Sobre Negócios**
  - [https://www.youtube.com/watch?v=RQrItKWw\\_aM](https://www.youtube.com/watch?v=RQrItKWw_aM)



# Para saber mais

- **Cinco passos para estabelecer um plano de Disaster Recovery**
  - <https://inovti.com.br/cinco-passos-para-estabelecer-um-plano-de-disaster-recovery/>
- **Qual a importância de sua empresa ter um plano de Disaster Recovery**
  - <https://www.penso.com.br/qual-a-importancia-de-sua-empresa-ter-um-plano-de-disaster-recovery/>

# RAID, CLUSTER, BACKUP e DLP

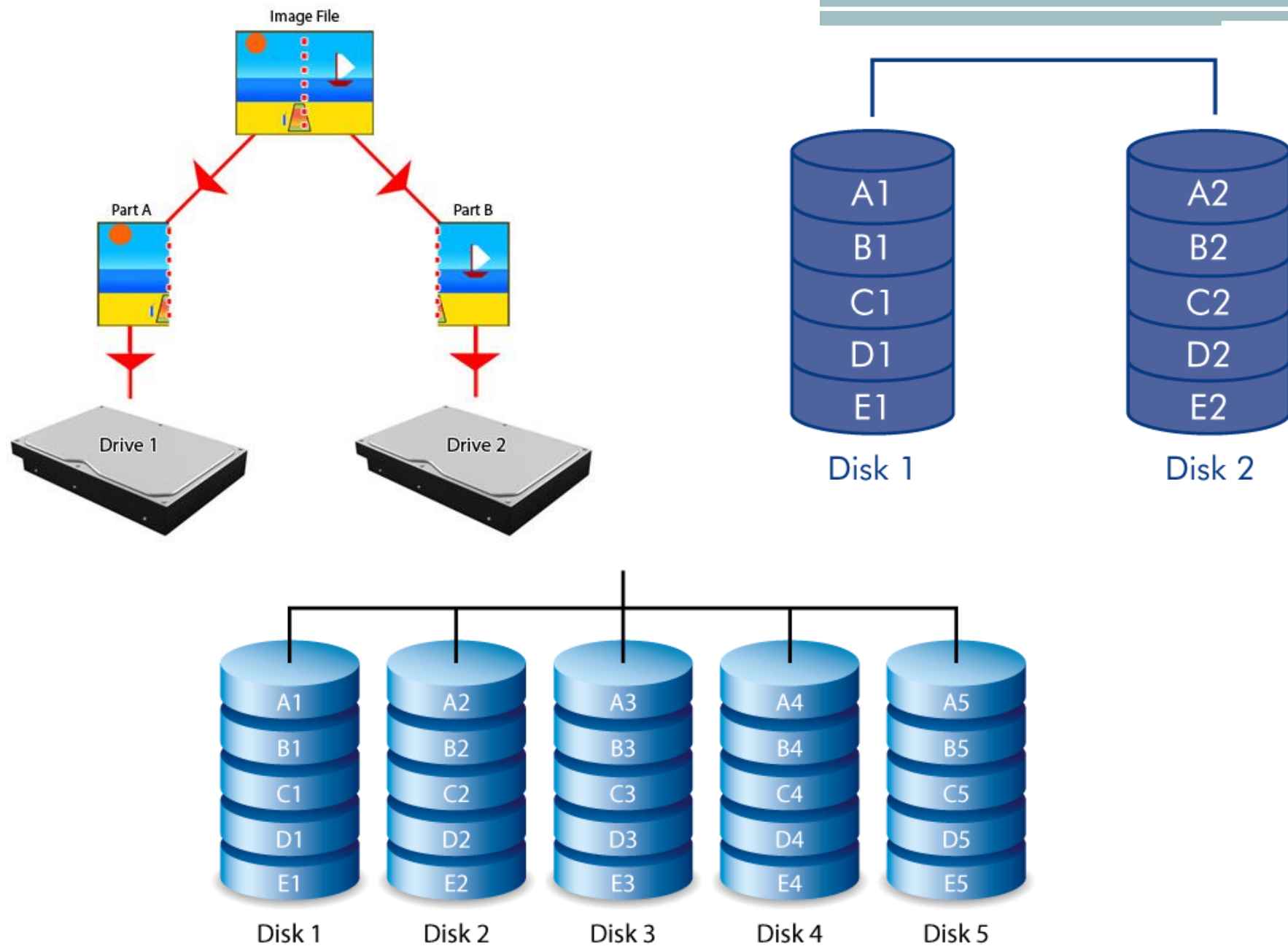
A series of horizontal lines in teal and light blue colors, with varying lengths and offsets, creating a modern, layered effect across the width of the slide.

# RAID

- Redundant Array of Independent Disks (Conjunto Redundante de Discos Independentes)
- Sistema formado por conjunto de discos independentes interligados trabalhando em conjunto.
- Objetivo: implementar redundância e tolerância a falhas de discos.
- Existem vários tipos de RAID, de acordo com o agrupamento dos discos, e os mais usados no mercado são: RAID 0, RAID 1, RAID 1 + 0 e RAID 5.

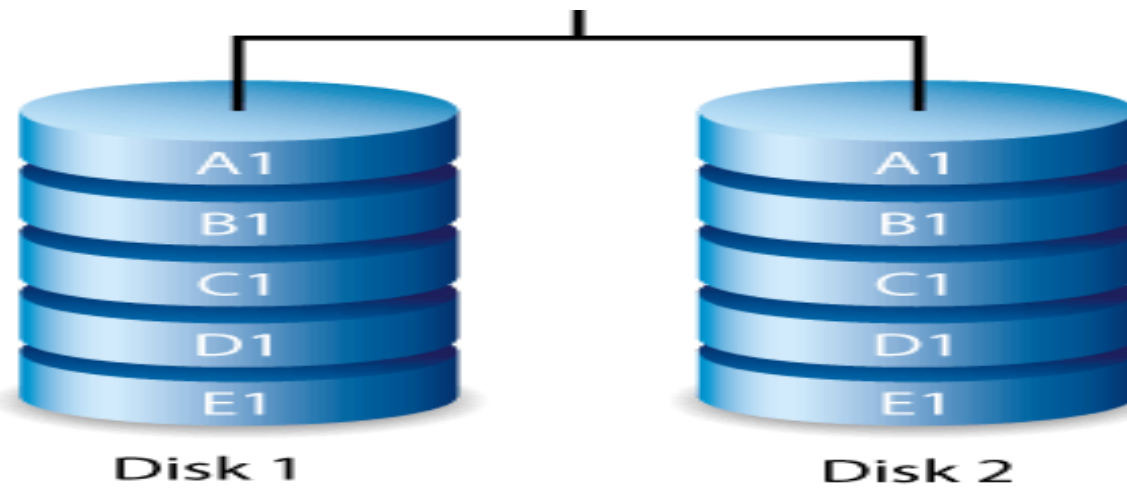
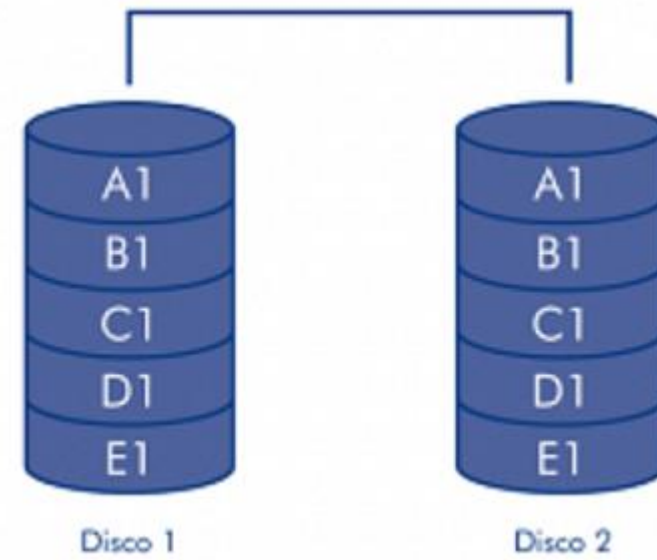
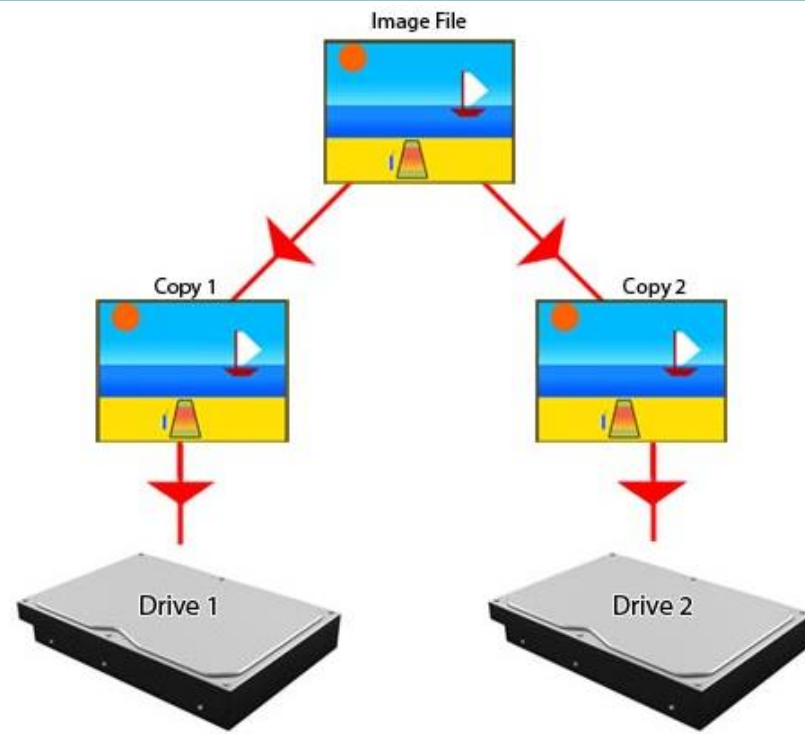
## RAID 0

- Stripping (fatiamento)
- Precisa de no mínimo 2 HDs
- Funcionamento: quando uma informação é armazenada, ela é “fatiada” e distribuída nos HDs
- Vantagem: alta performance na transferência
- Desvantagem: não possui tolerância a falhas (se um disco falhar perdermos todas as informações)
- Não é indicado quando precisamos de segurança dos dados
- Quanto mais discos, maior será a velocidade



## RAID 1

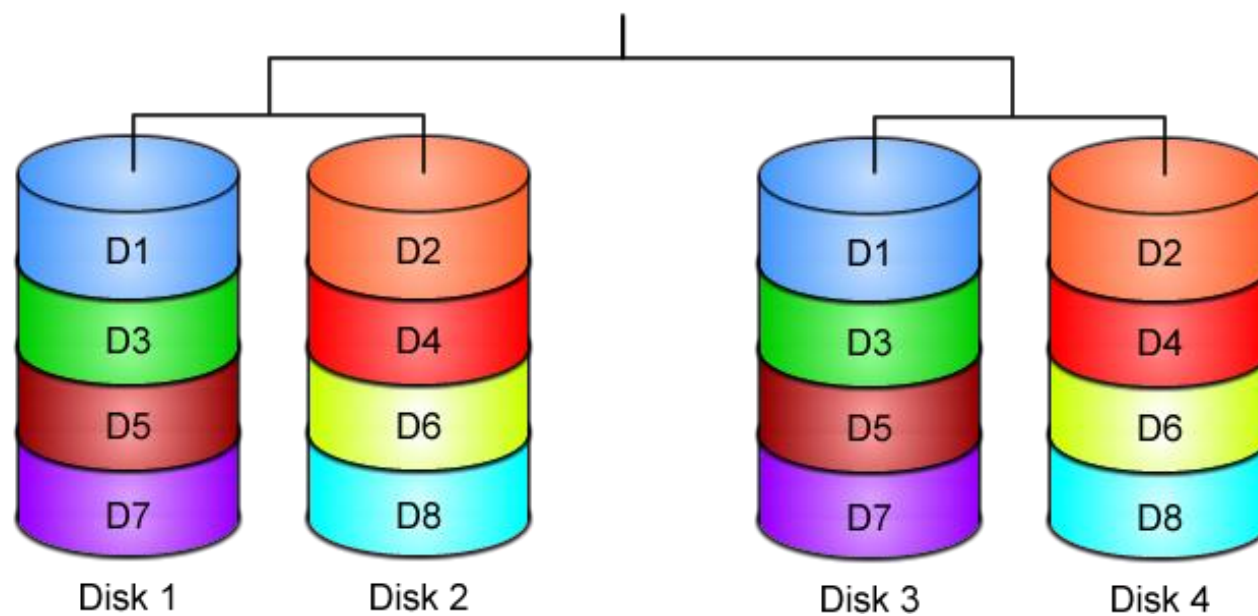
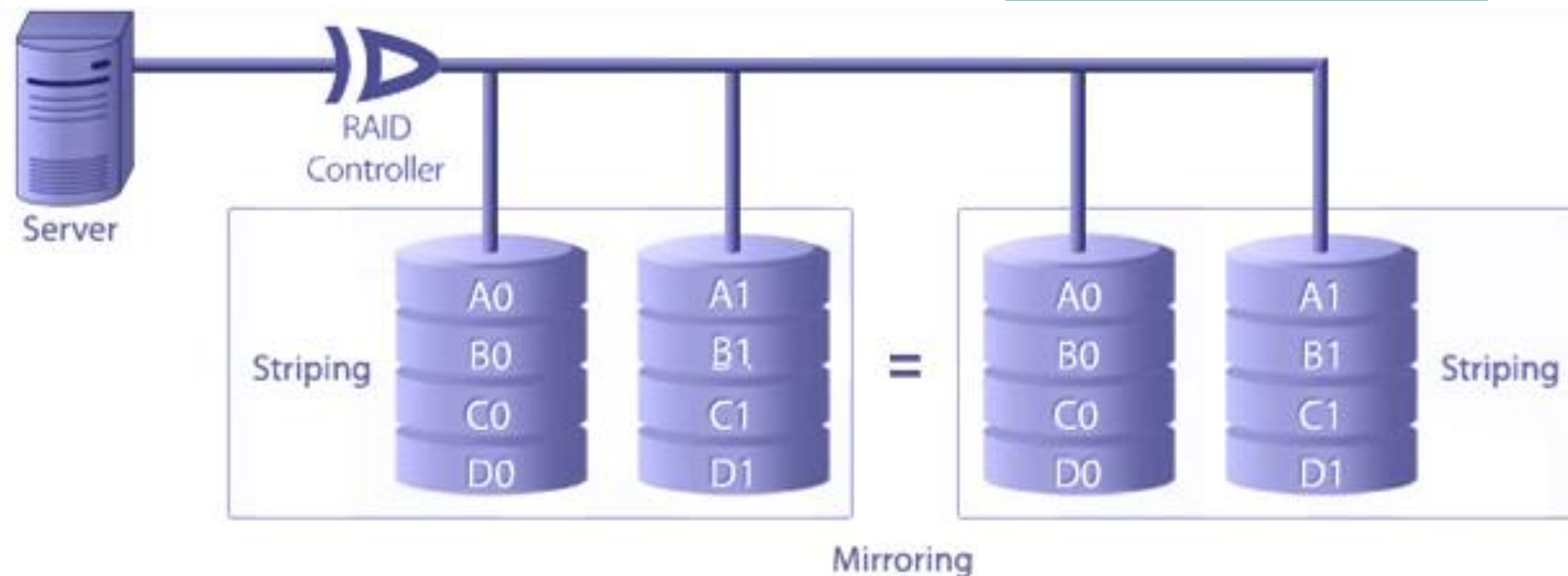
- Mirroring (espelhamento)
- Precisa de 2 HDs
- Funcionamento: a informação é gravada em um disco, e uma cópia fiel da mesma é feita no outro disco
- Vantagem: alta tolerância a falhas
- Desvantagens: baixa performance na transferência e desperdício de 50% da capacidade de armazenamento, já que um disco é usado apenas para espelho e não para armazenar novos dados.



## RAID 0 + 1

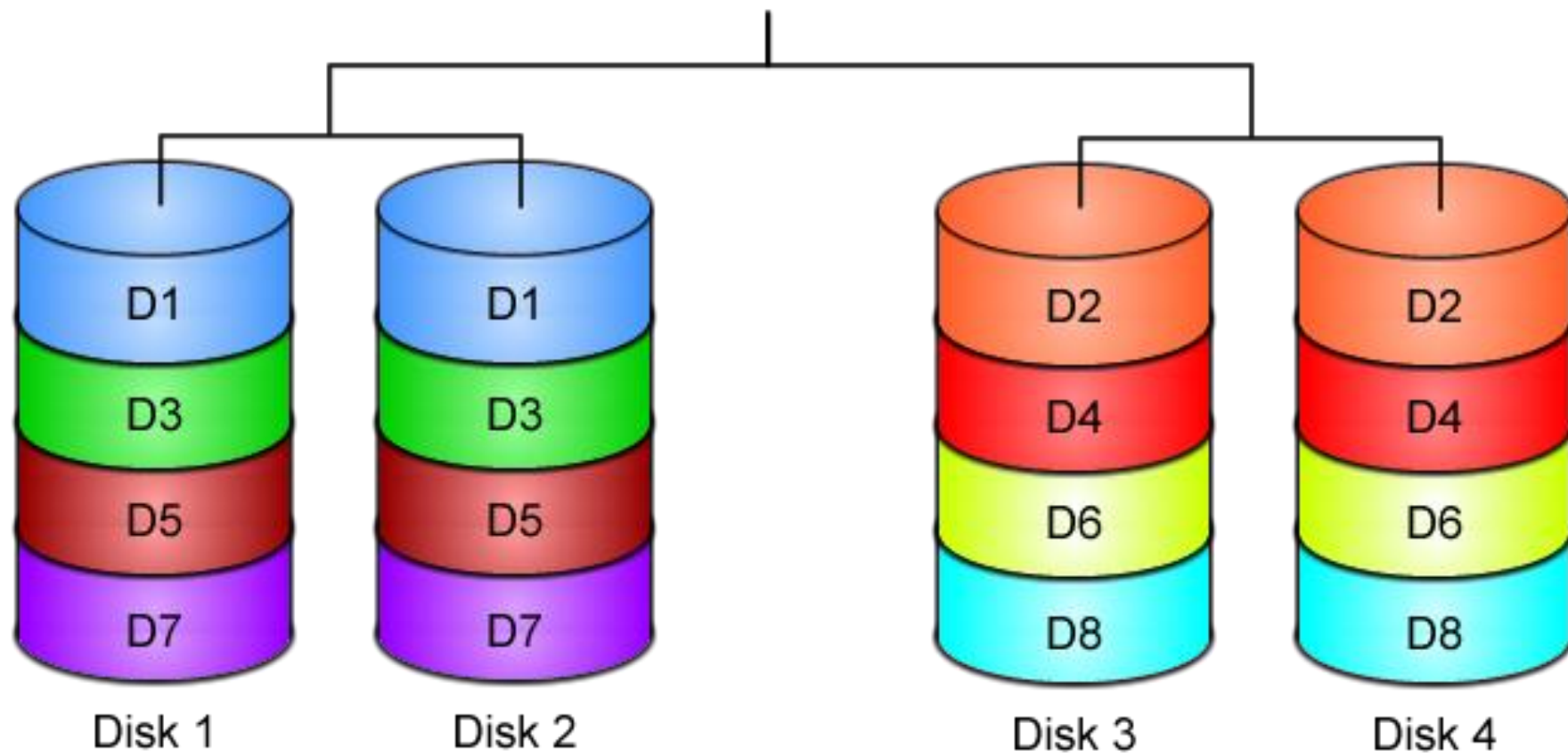
- Combinação dos RAIDs tipo 0 e 1
- Precisa de 4 HDs separados em grupos de 2
- Um dos grupos é implementado como strip (RAID 0) e em seguida é implementado o mirror (RAID 1) no outro conjunto de discos (os discos do primeiro conjunto são espelhados)
- Tem alta tolerância a falhas, exceto no caso de ocorrer a perda de um disco em cada grupo, simultaneamente.





## RAID 1 + 0

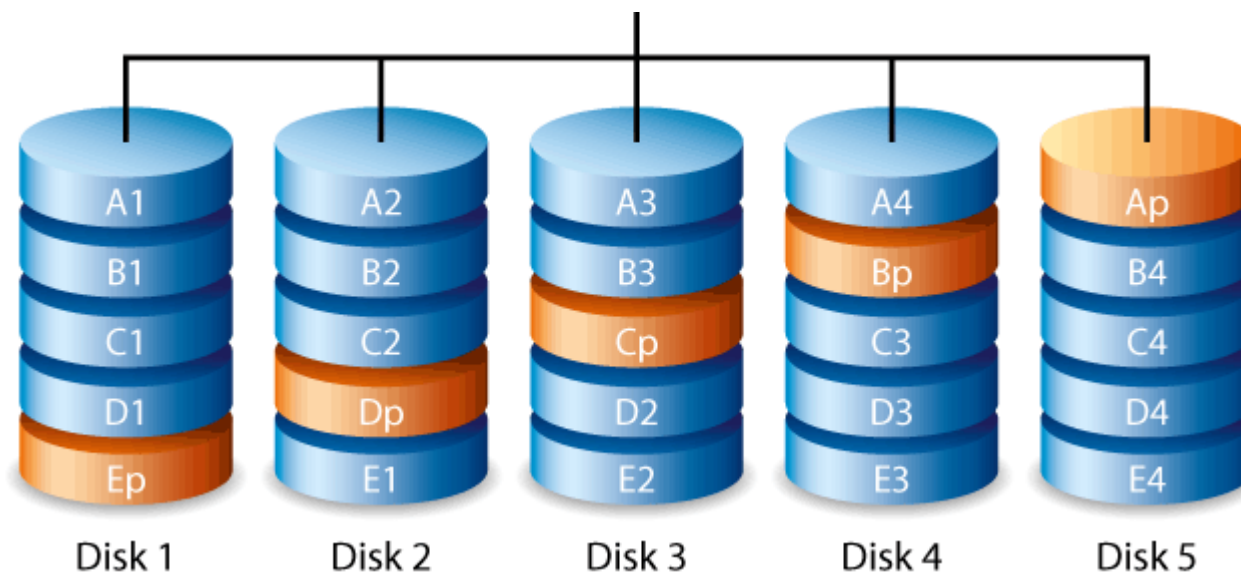
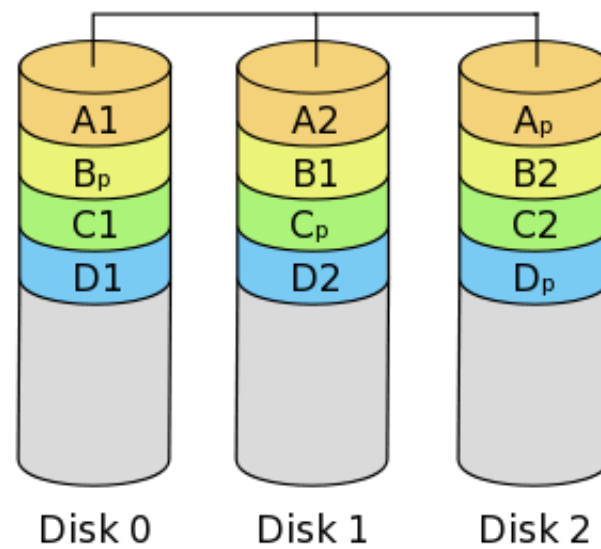
- Também trabalha com os RAIDs 0 e 1
- Precisa de 4 HDs separados em grupos de 2
- Aqui, primeiro a função do RAID 0 (strip) é executada, mas colocando cada parte da informação em um grupo, e em seguida a função do RAID 1 (mirror) é executada, espelhando o disco em seu próprio grupo.
- Agrega o que os 2 tipos de RAID tem de melhor: desempenho e redundância.



## RAID 5

- Usa o conceito de paridade
- Usa, no mínimo, 3 discos, mas pode usar muito mais que isso.
- A informação é gravada em partes, dividida pelos discos, e em um deles é gravada a paridade. Na próxima informação, a distribuição da informação e da paridade ocorre de maneira diferente, ou seja, a paridade de cada informação fica em um disco.
- Se um disco falhar, é possível recriar a informação que estava ali com base na paridade e nos dados que compõem essa informação e que estava espalhados nos demais discos, trazendo redundância e confiabilidade

- Tem alta velocidade de gravação, trazendo alta performance
- Paridade é um método matemático que gera um código a partir dos bits da informação original. A paridade é um valor calculado usado para reconstruir dados após uma falha.



## RAID 15

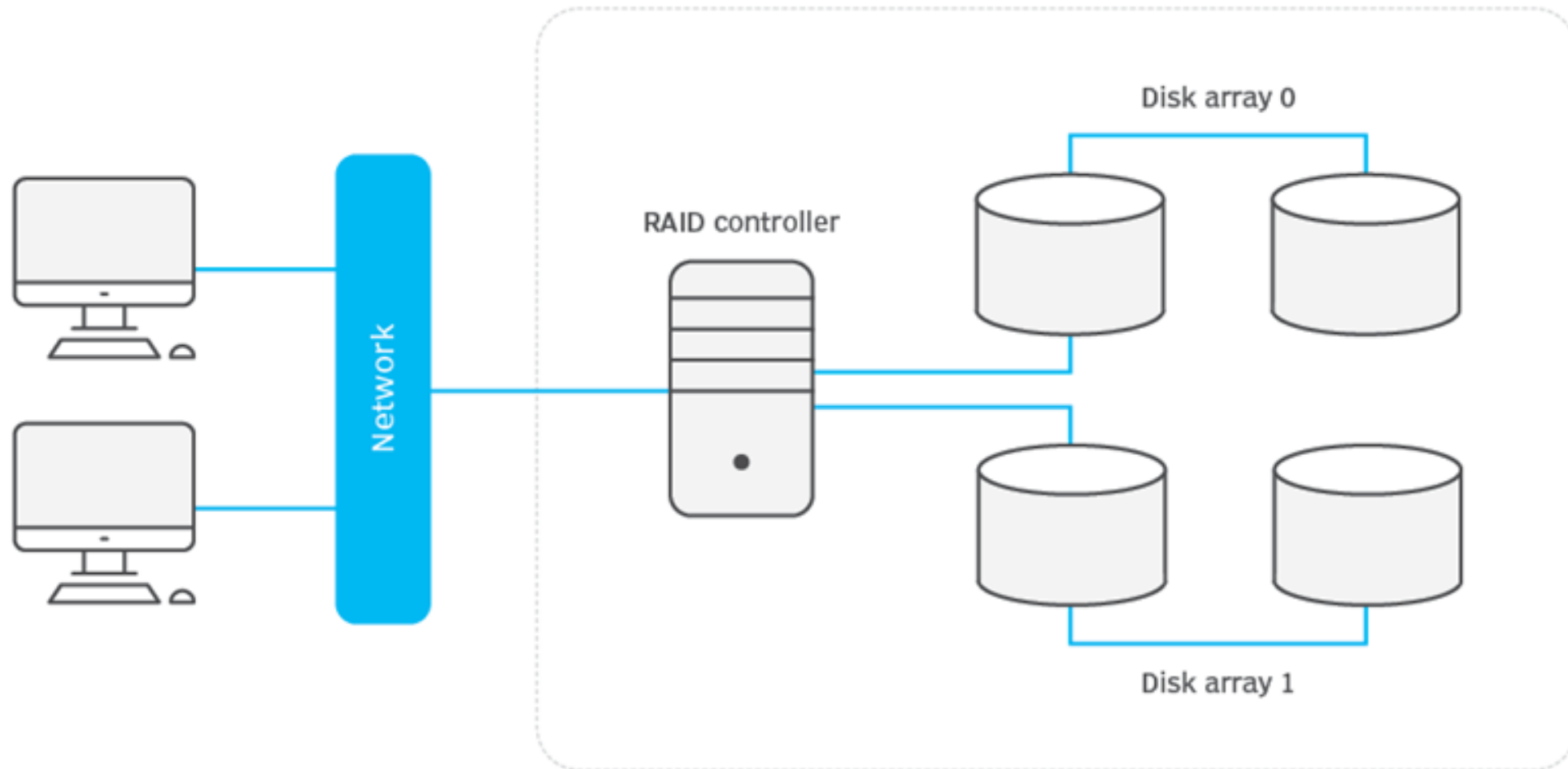
- Tipo de RAID mais usado atualmente, usa o conceito de mirroring (RAID 1) e de paridade (RAID 5) em conjunto
- Visa aumentar o processo de tolerância a falha e a alta disponibilidade
- Precisa de no mínimo 5 HDs, separados em um grupo de 2 e outro de 3 discos
- No primeiro grupo é implementado o RAID 1, no segundo é implementado o RAID 5

## RAID VIA HARDWARE E RAID VIA SOFTWARE

- Podemos implementar RAID via hardware ou via software, cada um com suas vantagens e desvantagens.
- **RAID via hardware:**
  - Método mais usado
  - Funciona independente do SO
  - Possui melhor desempenho
  - Alto custo devido à necessidade da existência de um controlador RAID que é responsável pelo gerenciamento dos discos.

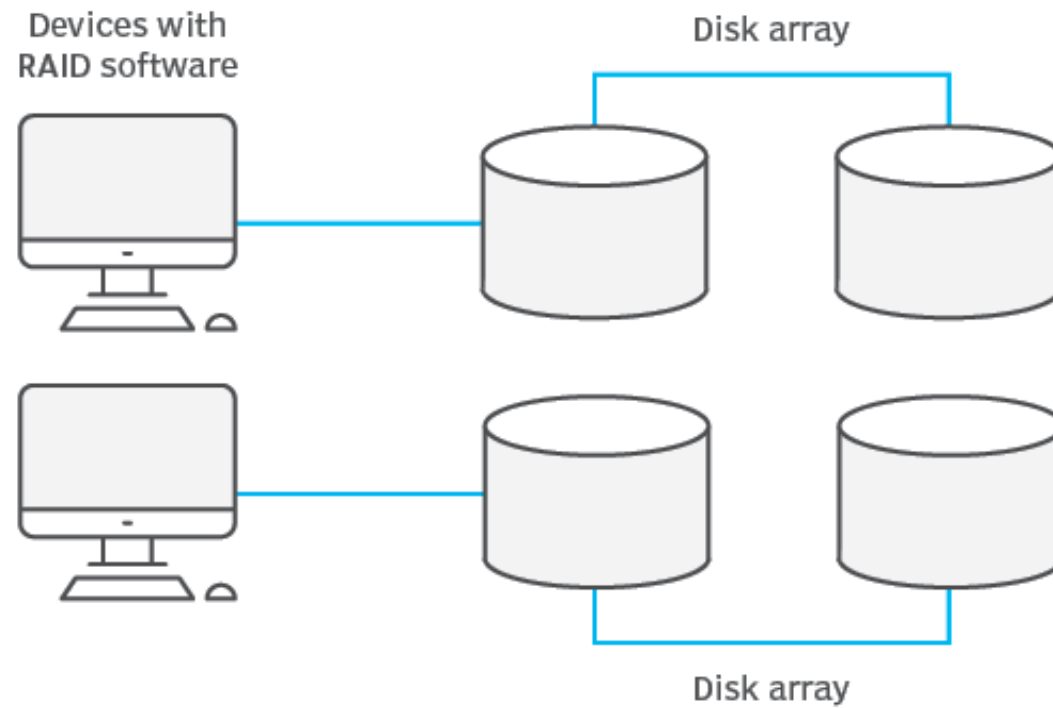


# Hardware RAID



- **RAID via software:**
  - Criado pelo SO da máquina onde está instalado
  - Mais barato
  - Performance menor do que o baseado em hardware, já que o SO se preocupa em controlar os discos além das suas atividades básicas
  - Depende do poder de processamento do computador no qual for implementado.
- Sempre que implementamos qualquer sistema de RAID, o mesmo deve ser testado.

# Software RAID



# VÍDEOS

- **RAID - Introdução ao conceito de RAID**
  - <https://www.youtube.com/watch?v=PMX61TisJgY>
- **RAID - Conhecendo os níveis de RAID**
  - <https://www.youtube.com/watch?v=8V5FoTQpjIE>

# CLUSTER

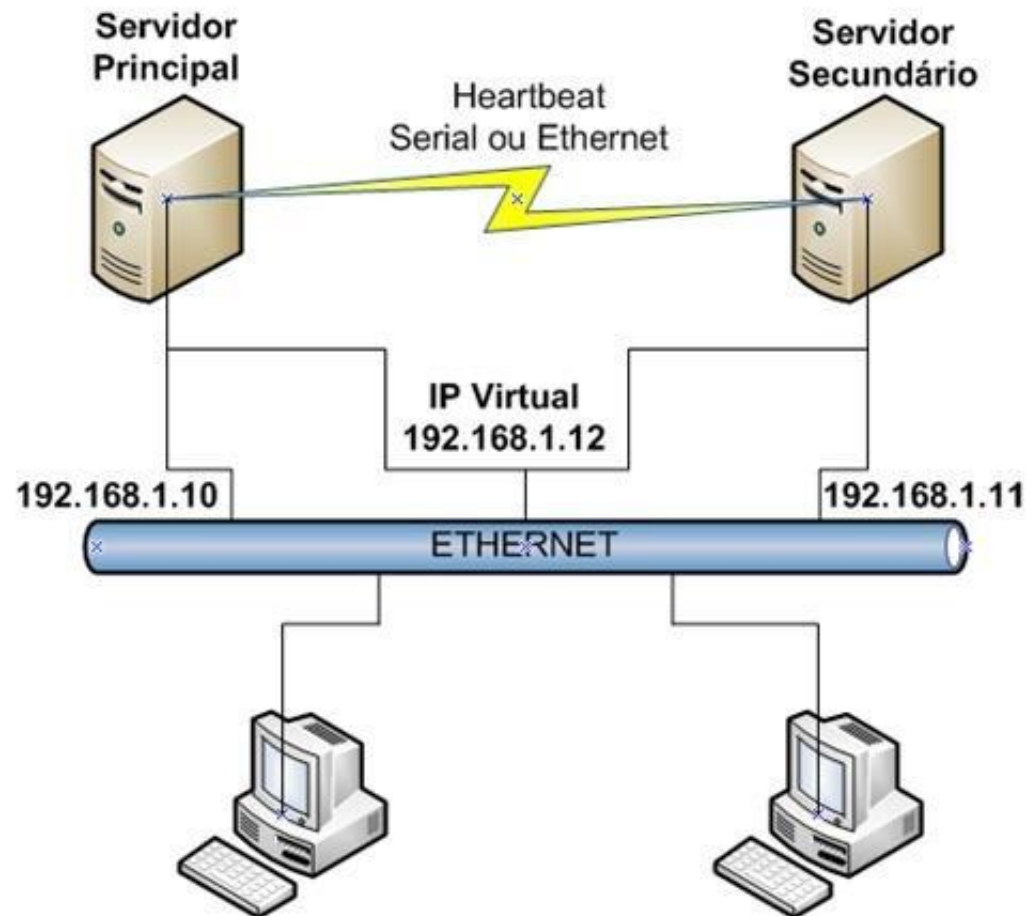
- Sistema que agrega redundância de processamento
- Dois ou mais computadores (servidores) completos são usados trabalhando em conjunto
- Cada computador terá todos seus componentes, placas, discos e processador
- Os computadores devem, obrigatoriamente, estar ligados entre si, seja via placa de rede ou usando um switch
- Uma rede privada é criada entre as máquinas do cluster

- Usa o conceito de ativo e passivo:
  - Ativo: servidor que está funcionando.
  - Passivo: servidor que está em standby.
- Cada máquina do cluster é denominada de nó.
- Novos nós podem ser acrescentados (ou retirados) do cluster sem a parada do mesmo.
- Para o usuário que está acessando, isso é transparente, é como se ele estivesse acessando uma única máquina.
- Depois de configurado e em funcionamento, não necessita de intervenção humana.
- Precisa de um software que faça gerenciamento e montagem do cluster.
- Vantagens: confiabilidade, distribuição de carga e alto desempenho.





# TIPOS DE CLUSTER

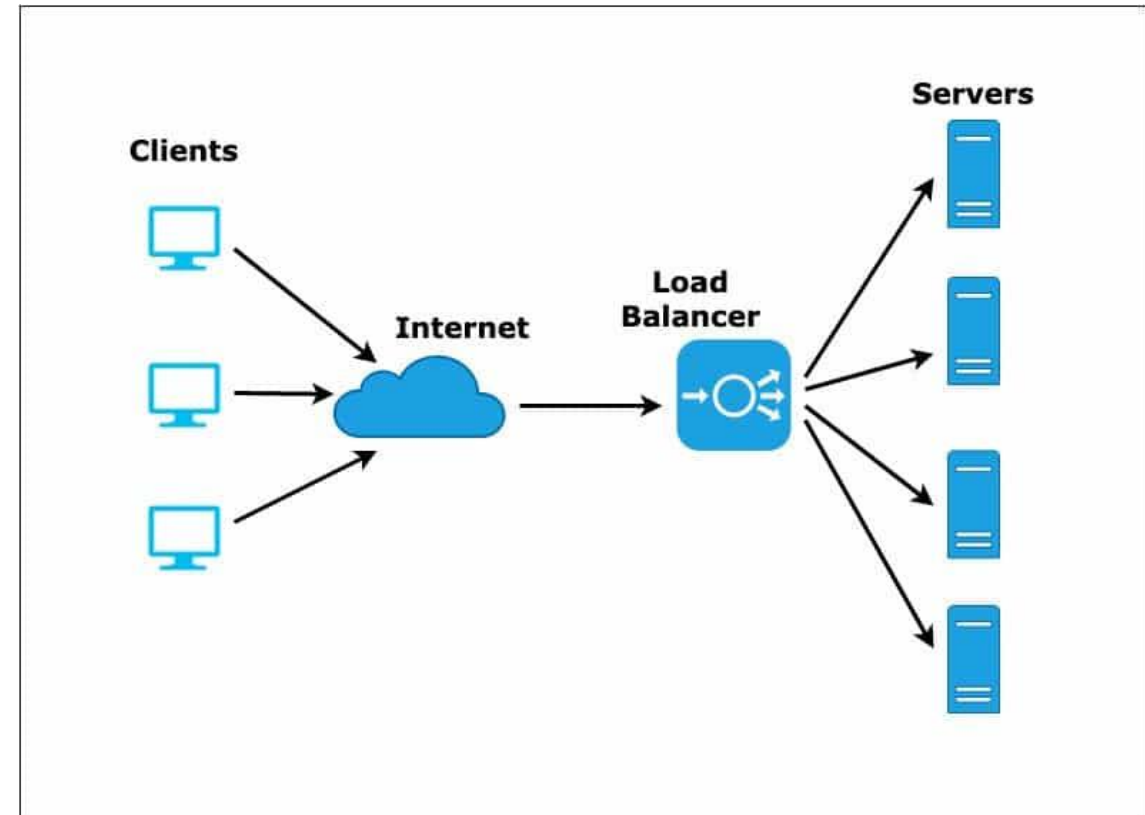


- **Alta disponibilidade - High Availability**
  - Usado quando um serviço ou sistema não pode ficar fora do ar, estando sempre disponível
  - Quando uma máquina do cluster que estava “ativa” apresenta qualquer tipo de falha, seu status passa para “passivo”, e uma máquina que estava “passiva” se torna ativa, assumindo o processamento como se nada houvesse ocorrido



- **Balanceamento de Carga (Load Balancing)**

- Várias máquinas rodam o mesmo serviço juntas, sendo que a carga de processamento é distribuída entre os nós
- Muito usado para serviços / sistemas mais pesados e que precisam de grande poder de processamento
- Caso uma falha em um nó ocorra, o sistema de cluster redistribui o processamento entre as máquinas que continuam ativas



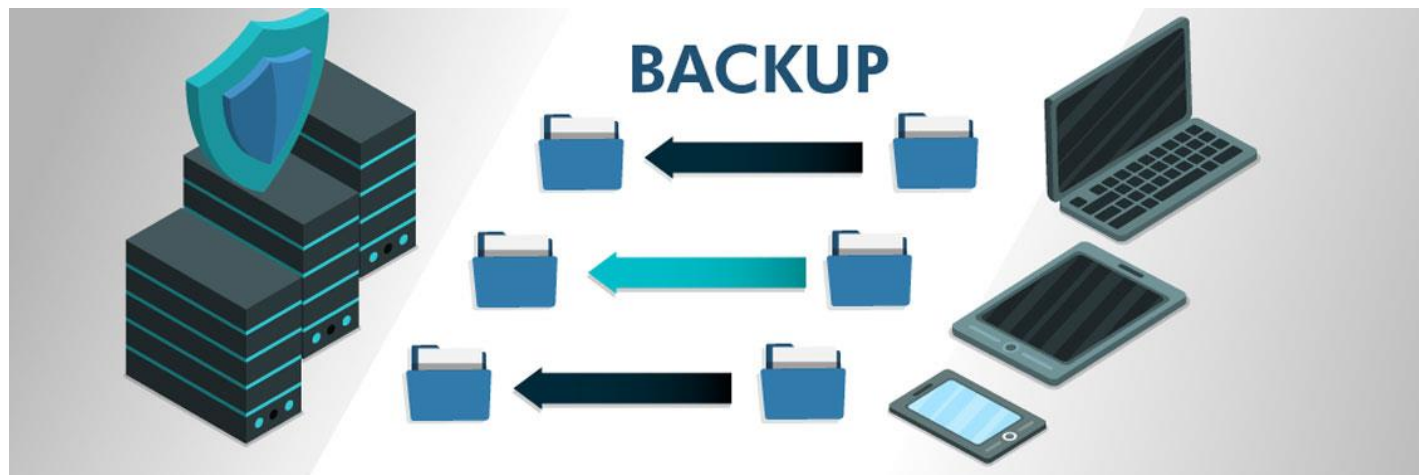
- **Combinação: alta disponibilidade + balanceamento de carga**
  - Combina os dois tipos de cluster anteriormente explicados
  - Usado para sistemas que não podem parar e que sejam muito pesados
- **Termos importantes:**
  - **Nó primário:** máquina que controla o cluster
  - **Failover:** quando uma falha ocorre, o sistema identifica a mesma automaticamente e inicia o processo de troca do nó
  - **Escalabilidade:** capacidade do cluster de ser expandido sem ser tirado do ar para isso
  - **Heartbeat:** consulta que o nó primário manda de tempos em tempos para os demais nós, a fim de ver quem está ativo e quem teve um failover, ficando passivo

# Vídeo

- **Cluster // Dicionário do Programador**
  - <https://www.youtube.com/watch?v=1cVUpoAR2Qc>

# Backup

- Backup é a cópia de segurança de nossas informações, que será usada caso as mesmas sejam perdidas.
- Não podemos nos lembrar dele apenas depois que os problemas ocorreram, pois aí será tarde!
- Mesmo tendo o backup, se ele não for feito corretamente e testado, ele pode não resolver.



- Em geral, os softwares de backup usam um atributo dos arquivos, o atributo “marcado” para verificar se o backup já foi realizado.
- Se esse atributo estiver selecionado (marcado) no arquivo, significa que ele foi alterado e que, depois dessa alteração, nenhum backup dele foi realizado ainda. Ou ainda, que ele foi criado depois de um backup e mais nenhum foi executado depois disso.
- Já se esse atributo estiver desmarcado, significa que ele já teve seu backup realizado e mais nenhuma alteração ocorreu no arquivo depois disso.

- Todo arquivo tem suas propriedades. Quando estamos usando o Windows, se formos em um arquivo e clicarmos com o botão direito, e depois em propriedades, veremos alguns atributos como Nome, Data, Tamanho, e outros atributos particulares de cada tipo de arquivo. Existem, ainda, alguns atributos que não vemos, que são atributos que apenas o SO “enxerga”. Um desses atributos é o atributo MARCADO.
- Toda vez que um arquivo é criado ou alterado, esse atributo MARCADO é selecionado. O atributo MARCADO vai mostrar ao sistema se aquele arquivo já teve o backup realizado (caso o atributo esteja desmarcado) ou se ele foi alterado e não teve o backup realizado (caso o atributo esteja marcado).

# TIPOS DE BACKUP

- **Backup Diário**

- Realizado de acordo com o dia
- Faz o backup de acordo com a Data dos arquivos
- Se o arquivo tem Data de criação ou alteração igual ao dia em que o backup está sendo realizado, ele faz o backup desses arquivos
- Senão, ele os ignora
- Não verifica se o backup já foi realizado ou não. Sua única preocupação é a data de criação ou alteração do arquivo
- Não mexe com o atributo marcado dos arquivos

- **Backup Cópia**

- No software, o gerenciador do backup deve selecionar quais arquivos serão “backupeados”
  - Uma cópia exata desses arquivos será feita todas as vezes que esse tipo de backup rodar
  - Independe de Data de criação, Data de alteração ou atributo marcado dos arquivos
- Tanto o backup diário quanto o cópia são menos usados. A seguir veremos os 3 tipos de backup mais usados.



- **Backup Full (ou Normal ou Completo)**

- Sempre deve ser executado no início do processo de backup e é recomendável que o mesmo seja executado uma vez por semana. Por ser demorado deve ser executado em períodos de menor utilização
- Faz a cópia de todos os arquivos, independentemente de seu atributo marcado estar ou não selecionado
- Ao fim de sua execução, os arquivos que foram backupeados tem o atributo marcado limpo, o que significa que ele já teve seu backup realizado
- Quando algum usuário alterar esse arquivo, o atributo marcado será novamente selecionado. E ao rodar o backup completo a seleção do atributo será limpa novamente. Esse processo é cíclico e sempre ocorrerá.

- **Backup Diferencial**

- Aqui o backup é realizado dos arquivos que foram criados ou alterados após o último backup, ou seja, APENAS os que estiverem com o atributo marcado selecionado, como no incremental
- A diferença é que ele não limpa o atributo marcados dos arquivos, o que o torna acumulativo, ou seja, quando ele rodar de novo vai fazer o backup dos mesmos arquivos
- Também deve ser usado em conjunto com o full
- Realização demorada e restauração rápida

<b>Dia</b>	<b>Hora</b>	<b>Tipo</b>	<b>OBS</b>
<b>Sábado</b>	<b>23h</b>	<b>Full</b>	<b>Todos os arquivos</b>
<b>Segunda</b>	<b>23h</b>	<b>Diferencial</b>	<b>Alterados 2a. feira</b>
<b>Terça</b>	<b>23h</b>	<b>Diferencial</b>	<b>Alterados 2a.f + 3a.f</b>
<b>Quarta</b>	<b>23h</b>	<b>Diferencial</b>	<b>Alterados 2a.f + 3a.f + 4a.f</b>
<b>Quinta</b>	<b>23h</b>	<b>Diferencial</b>	<b>Alterados 2a.f + 3a.f + 4a.f + 5a.f</b>
<b>Sexta</b>	<b>23h</b>	<b>Diferencial</b>	<b>Alterados 2a.f + 3a.f + 4a.f + 5a.f + 6a.f</b>

## • Backup Incremental

- Aqui é realizado o backup dos arquivos que foram criados ou alterados após o último backup, ou seja, APENAS os que estiverem com o atributo marcado selecionado
- Após a realização desse backup, ele limpa o atributo marcado dos arquivos
- Caso o arquivo não possua o atributo marcado, o backup vai ignorar os arquivos e não copiará nada
- Geralmente é usado em conjunto com o backup full
- Realização rápida e restauração demorada

<b>Dia</b>	<b>Hora</b>	<b>Tipo</b>	<b>OBS</b>
<b>Sábado</b>	<b>23h</b>	<b>Full</b>	<b>Todos os arquivos</b>
<b>Segunda</b>	<b>23h</b>	<b>Incremental</b>	<b>Alterados 2a. feira</b>
<b>Terça</b>	<b>23h</b>	<b>Incremental</b>	<b>Alterados 3a. feira</b>
<b>Quarta</b>	<b>23h</b>	<b>Incremental</b>	<b>Alterados 4a. feira</b>
<b>Quinta</b>	<b>23h</b>	<b>Incremental</b>	<b>Alterados 5a. feira</b>
<b>Sexta</b>	<b>23h</b>	<b>Incremental</b>	<b>Alterados 6a. feira</b>

- Ao realizarmos o backup, o processo deve ser controlado e auditado, a fim de garantir que o mesmo está ocorrendo sem problema algum.
- Quando pensamos em backup, sempre devemos planejar o mesmo previamente, ver qual tipo mais se adéqua a nossa necessidade, onde as mídias de backup serão armazenadas, como será o processo de restauração (restore), quem será responsável por cada etapa, etc..
- Uma coisa **MUITO IMPORTANTE** é que as mídias de backup **SEMPRE** devem ser armazenadas longe das informações originais, preferencialmente em outro local distante fisicamente.

## • Restore do Backup

- Processo de recuperação do backup.
- Deve ser um processo devidamente formalizado e identificado, a fim de ser realizado o mais brevemente possível em casos de emergência. O mesmo deve ser tratado como todos os outros processos da empresa.
- As mídias devem ser verificadas constantemente a fim de evitar problemas.
- O prazo de armazenamento, localização, segurança física, controle de acesso aos dados armazenados e treinamentos das pessoas que executarão o processo também devem ser considerados.

- O início do processo de restore deve começar com um registro formal do pedido, e a identificação de quem o está fazendo.<sup>7</sup>
- Isso visa garantir a confidencialidade dos dados de forma que somente as pessoas autorizadas tenham acesso a determinadas informações. (um pedido de restore feito por uma pessoa que não tem autorização à informação pode representar uma vulnerabilidade nos controles de segurança).
- O processo de restore deve gerar um log do que foi realizado e por quem de maneira automática



- **Segregação das Funções de Backup**

- É importante que mais de um funcionário seja responsável pelo processo de backup de uma empresa.
- Ou seja: uma pessoa deve ser responsável pelo backup, outra pela autorização de restore, uma outra pelo restore em si, e mais uma deve ser responsável pelos testes.
- Além disso, devemos contar com mais de uma pessoa conhecendo cada etapa do processo, de forma que sempre tenha alguém apto a realizar cada etapa.

# Vídeo

- **Tipos de backup**
  - <https://www.youtube.com/watch?v=89ediViE9hM>

# O que é Data Loss Prevention? (DLP)

- O termo Data Loss Prevention (DLP) é utilizado na área de Segurança da Informação para se referir a sistemas e metodologias que possibilitam as empresas a reduzir o risco do vazamento de informações confidenciais.
- Os sistemas DLPs são capazes de identificar a perda de dados através da identificação do conteúdo, monitoramento e bloqueio de dados sensíveis, ou seja, identificar, monitorar e proteger os informações confidenciais que podem estar em uso (máquinas dos usuários), em movimento (na rede corporativa) ou armazenadas (banco de dados, servidores, etc) .

# O que é Data Loss Prevention? (DLP)

- Além do termo DLP, alguns fabricantes utilizam variações do termo, como: Data Leak Prevention, Information Leak Detection and Prevention (ILDPA), Information Leak Prevention (ILP), Content Monitoring and Filtering (CMF), Information Protection and Control (IPC) ou Extrusion Prevention System. (Leak significa vazamento).
- Hoje existem 3 tipos de proteção DLP que podemos utilizar em redes corporativas, Network DLP (Data in Motion - DiM), Storage DLP (Data at Rest - DaR ) e Endpoint DLP (Data in Use - DiU).

# Network DLP

- Pode ser uma solução em hardware ou software, sendo instalado em todos os pontos de saída dos dados da rede corporativa para Internet. Os dados serão analisados para identificar informações confidenciais que estão violando as políticas de segurança da empresa.

# Storage DLP

- O Storage DLP se aplica a qualquer sistema que contém dados como compartilhamentos de arquivos, bancos de dados, etc. Este recurso permite descobrir dados sensíveis que estão armazenados e que estão violando as políticas de segurança da empresa.

# Endpoint DLP

- Normalmente é uma solução baseada em um agente que fica instalado nas estações de trabalho e laptops e permite o monitoramento e bloqueio para todos os dados sensíveis que saem através de dispositivos removíveis, como disquetes, CDs, USBs, etc. Fornecendo também a auditoria e proteção dos dados segundo as políticas de segurança da empresa.

# Vídeo – Exemplo de uma ferramenta DLP

- **Safetica Product Video**

- <https://www.youtube.com/watch?v=x5KQdh77-Uk&feature=youtu.be>