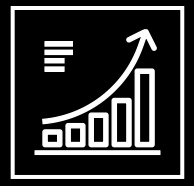
Prime

CCS-A

Resiliência de Segurança Cibernética

Resiliência

Sistema Resiliente:
Aquele que volta às condições normais.



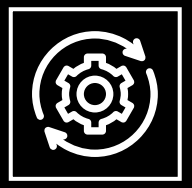
Concentra-se em como voltar ao desempenho total após uma degradação.

Esperar que os sistemas funcionem o tempo todo não é razoável.

Uma boa parte da implementação da resiliência é implementar a redundância em ativos.

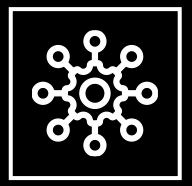
Redundância

Garante que os ativos não tenham um único ponto de falha.



Garante a operação na falta de hardware, software e quando a segurança é violada.

É fundamental um fornecimento de peças de reposição.



Itens críticos para funções críticas facilitam a continuidade.

Diversidade na Redundância

- Uniformidade:
  -  Pode aumenta a eficiência em reposição de peças;
  -  Mas aumenta o risco em falhas comuns.
- Diversidade em sistemas permite operar com diferentes:
  -  Tecnologias;
  -  Fornecedores;
  -  Processos;
  -  Controles.

Tecnologias

- Diversidade em tecnologia mitiga o risco de segurança.
- É preciso usá-las de maneira sobreposta para um segurança profunda.

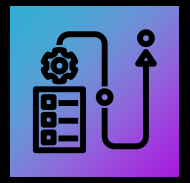
Firewalls;

Switches e roteadores;

Hosts bastiões na DMZ.

- Diversidade diminui as chances de um invasor ter controle total do ambiente.

Fornecedores



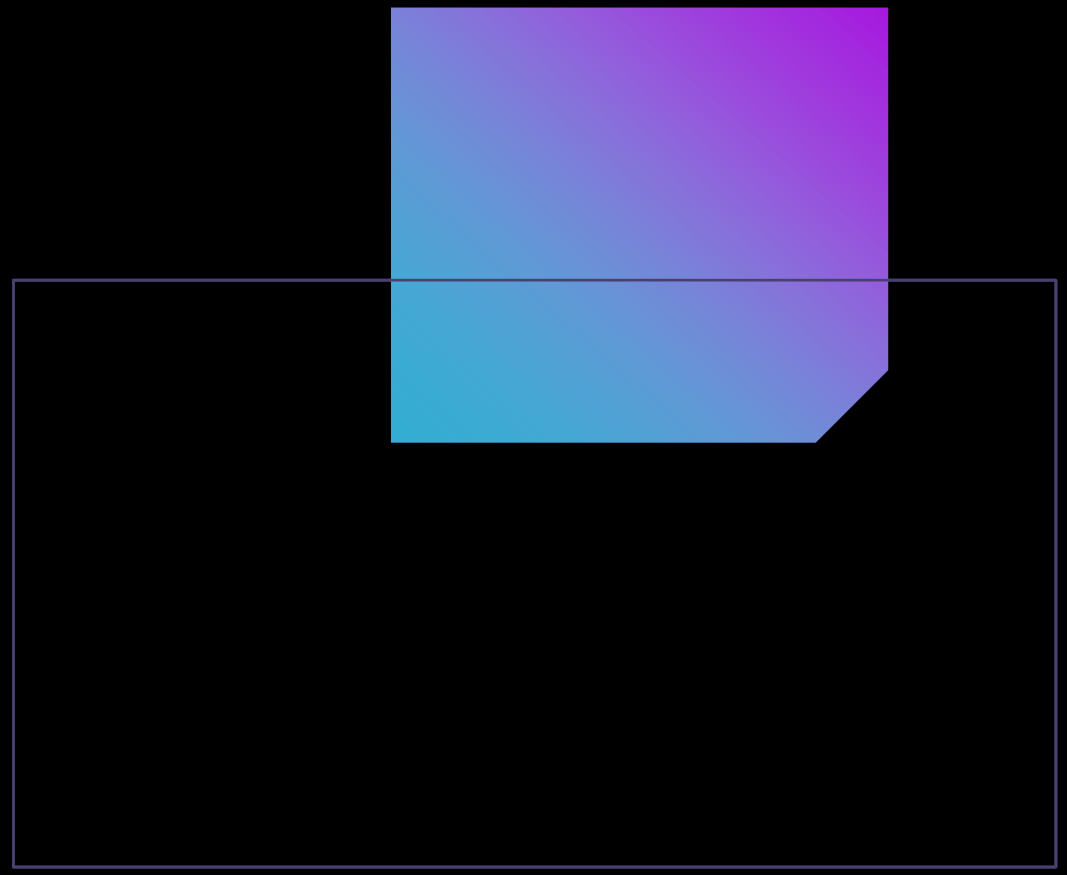
Diferentes fornecedores abordam diferentes metodologias e tecnologias.

Se vários fornecedores buscarem se defender, a vida do invasor fica mais difícil.

Diversidade nesse aspecto evita formas específicas de pontos únicos de falha e proporciona mais recursos defensivos.

Criptografia

- A diversidade também pode existir no mundo criptográfico.
  - Exemplo: Cifras TLS.
- Se a criptografia for quebrada, o mesmo crack não funcionará em cada uso de criptografia.
- A diversidade permite a remoção de uma configuração se algo é afetado, enquanto oferece alternativas.



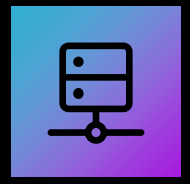
Controles

- Defesa em profundidade é um princípio de várias camadas sendo usadas para garantir a captura de um risco.
- Use uma combinação de controles em desktops e servdores:
  - Firewalls;
  - Antivírus;
  - Antimalwares;
  - Para ACLs, monitoramento etc.

Redundância em Disco

Redundância de disco ajuda a proteger contra pontos de falhas nos discos rígidos do servidor.

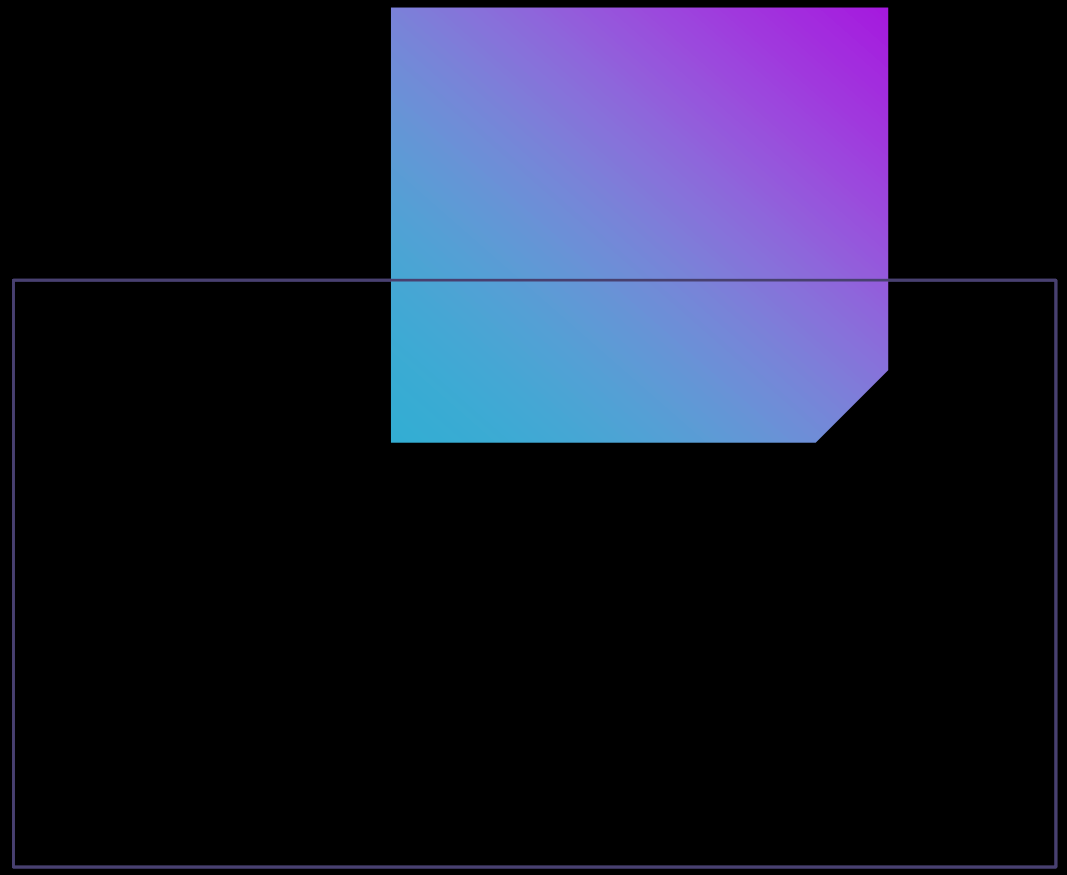
Existem duas soluções, como o RAID e Multipath.



A construção lógica do disco pode conter vários elementos de armazenamento físico.

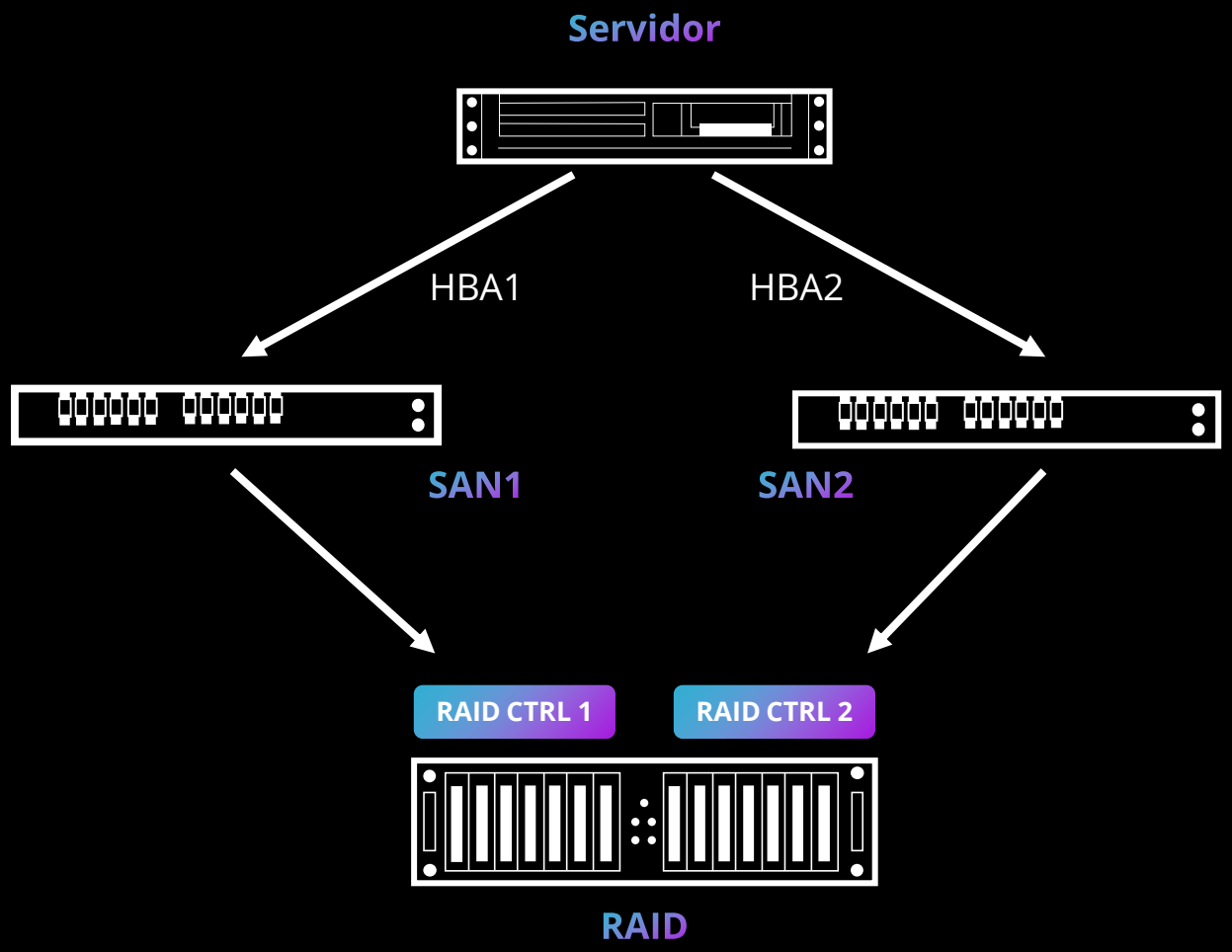
Níveis de Redundant Array of Inexpensive Disks (RAID)

- Aumenta a confiabilidade no armazenamento em disco.
- Pode aumentar a velocidade de recuperação de dados.
- Existem várias abordagens RAID:
  - RAID 0 (Discos distribuídos);
  - RAID 1 (Discos espelhados);
  - RAID 2 (Código de correção de erros em nível de bit);
  - RAID 3 (Byte-striped com verificação de erros);
  - RAID 4 (Unidade de paridade dedicada);
  - RAID 5 (Block-striped com verificação dos erros).



Multipath

- Existem várias interfaces para vários tipos de sistemas de armazenamento.
- Multipath - Redundância no caso de um problema com algum dos adaptadores.

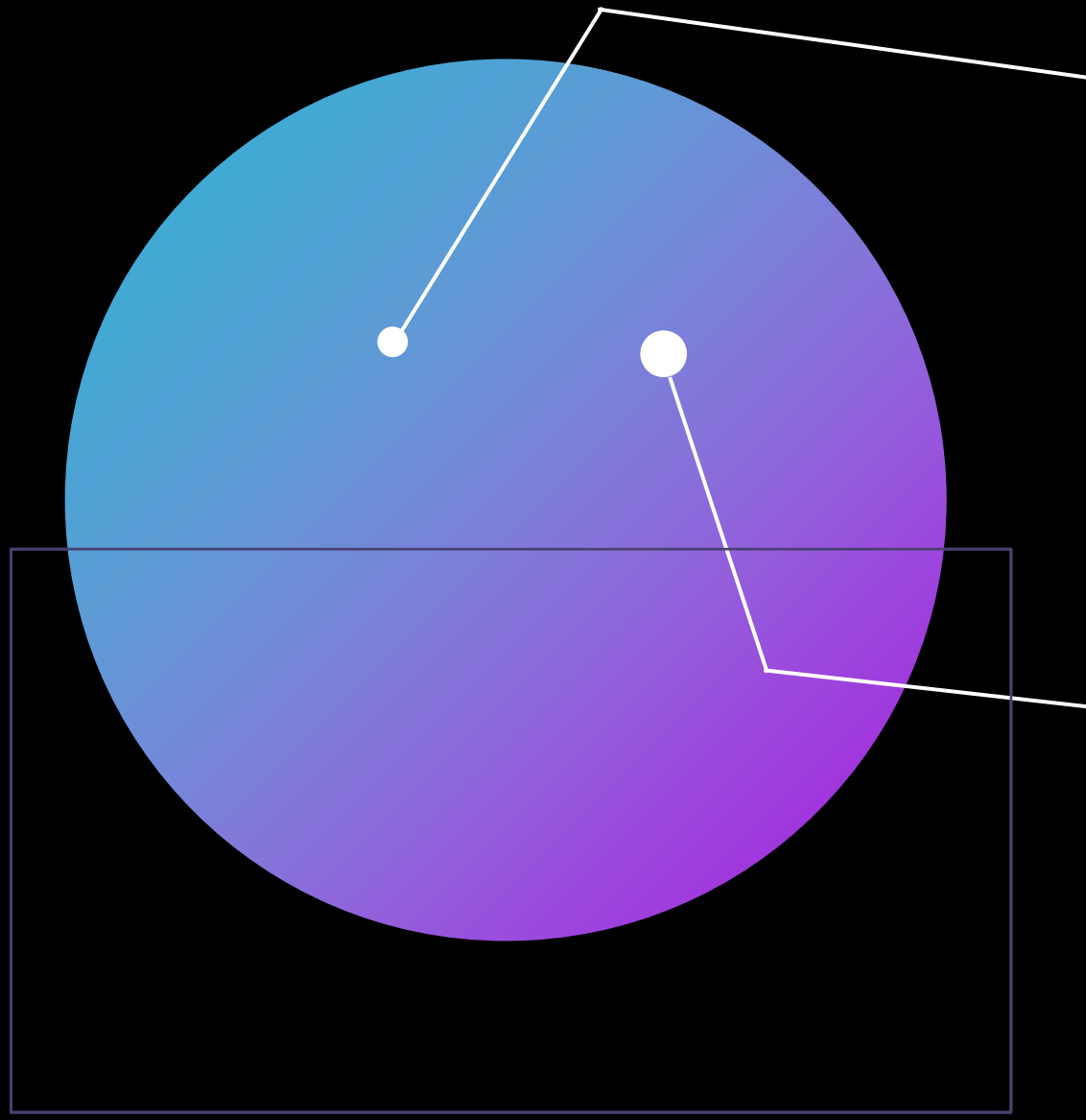


Redundância em Rede

- É um ponto de falha também e precisa de redundância.
- Há tecnologias críticas para redundância.
- Pode ser resiliente sob cargas e problemas de conectividade.
- Mas, para isso, é importante ter uma rede:
  -  Arquitetada;
  -  Com vários caminhos independentes;
  -  Com elementos projetados para aumentar a redundância.
- É preciso considerar dois elementos:
  -  Balanceamento de carga;
  -  Agrupamento da Placa de Interface de Rede (NIC).

Balanceamento de Carga

- Técnica comum usada na tolerância a falhas.
- Distribuição na carga de processamento em dois ou mais sistemas.
- A operação não cai totalmente.
- Frequentemente utilizado para sistemas com:
  - Sites Web;
  - Grandes sites de transferências de arquivos;
  - IRC, chats, e-mails etc.



Agrupamento de Placas de Interface de Rede (NIC)

Permite consolidar a largura de banda de várias placas de rede.

Acelerar o processamento de pacotes com NICs atuando como um.

Benefícios:

- Agrupamento NIC permite que o servidor tenha redundância e maior largura de banda.

Redundância em Energia

- Na falha de energia, é um método que fornece energia a ativos críticos (servidores e roteadores).
- Interrupções ocasionais precisam ser gerenciadas, como:

Fontes de alimentação;

Geradores;

Fontes duplas;

Distribuição de energia gerenciada.

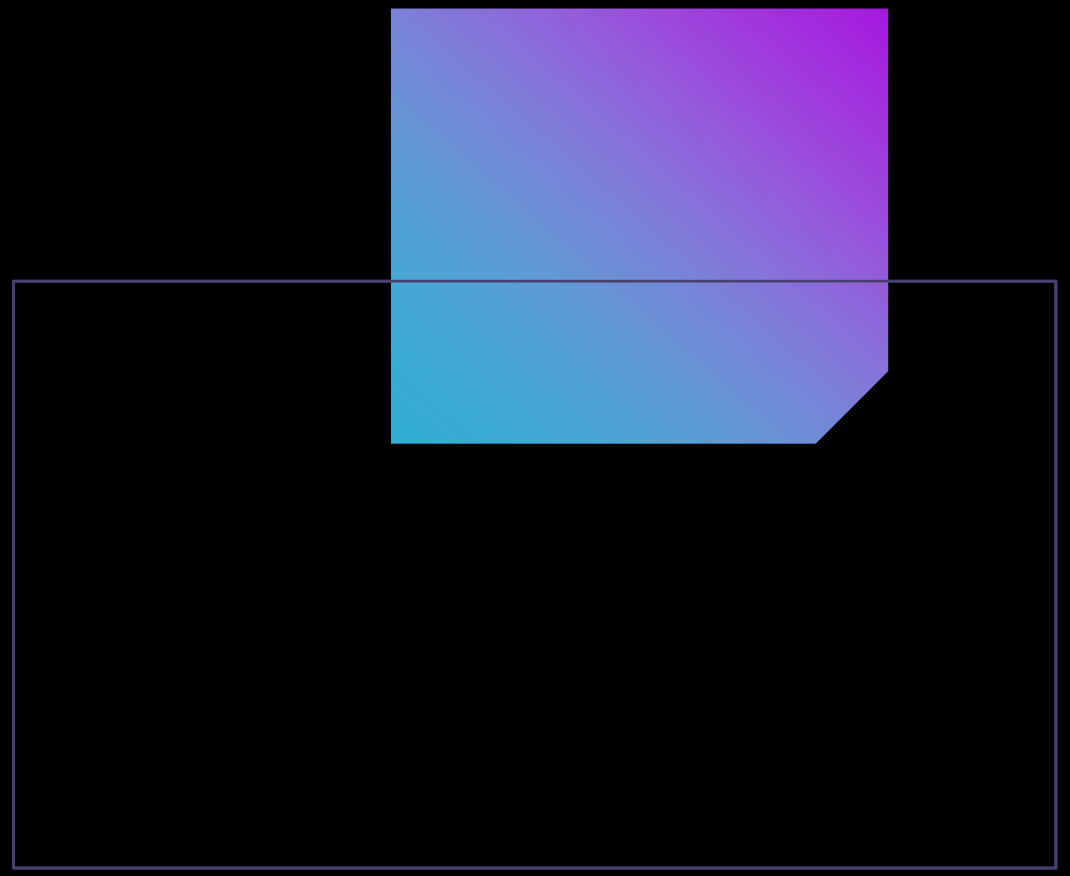
Fonte de Alimentação Ininterrupta (UPS)

Sistemas de fornecimento de energia de emergência.

Não têm uma grande capacidade de backup de bateria.

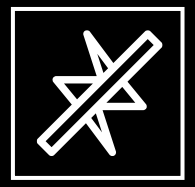
A maioria dos UPSs é projetada e classificada para 20 minutos.

- Suficiente para iniciar geradores de backup.

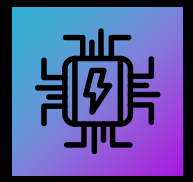


Gerador

Fornece energia quando fontes normais são perdidas. Ativadas manualmente ou automaticamente.



Suficiente para cobrir serviços durante uma queda de energia.



Circuitos separados que fornecem energia apenas a componentes desejados.

É necessário gerenciar reabastecimento (diesel).

Fonte Dupla

RESILIÊNCIA DE SEGURANÇA CIBERNÉTICA

Fontes de alimentação individuais são fracas.

Redundância na fonte é essencial.

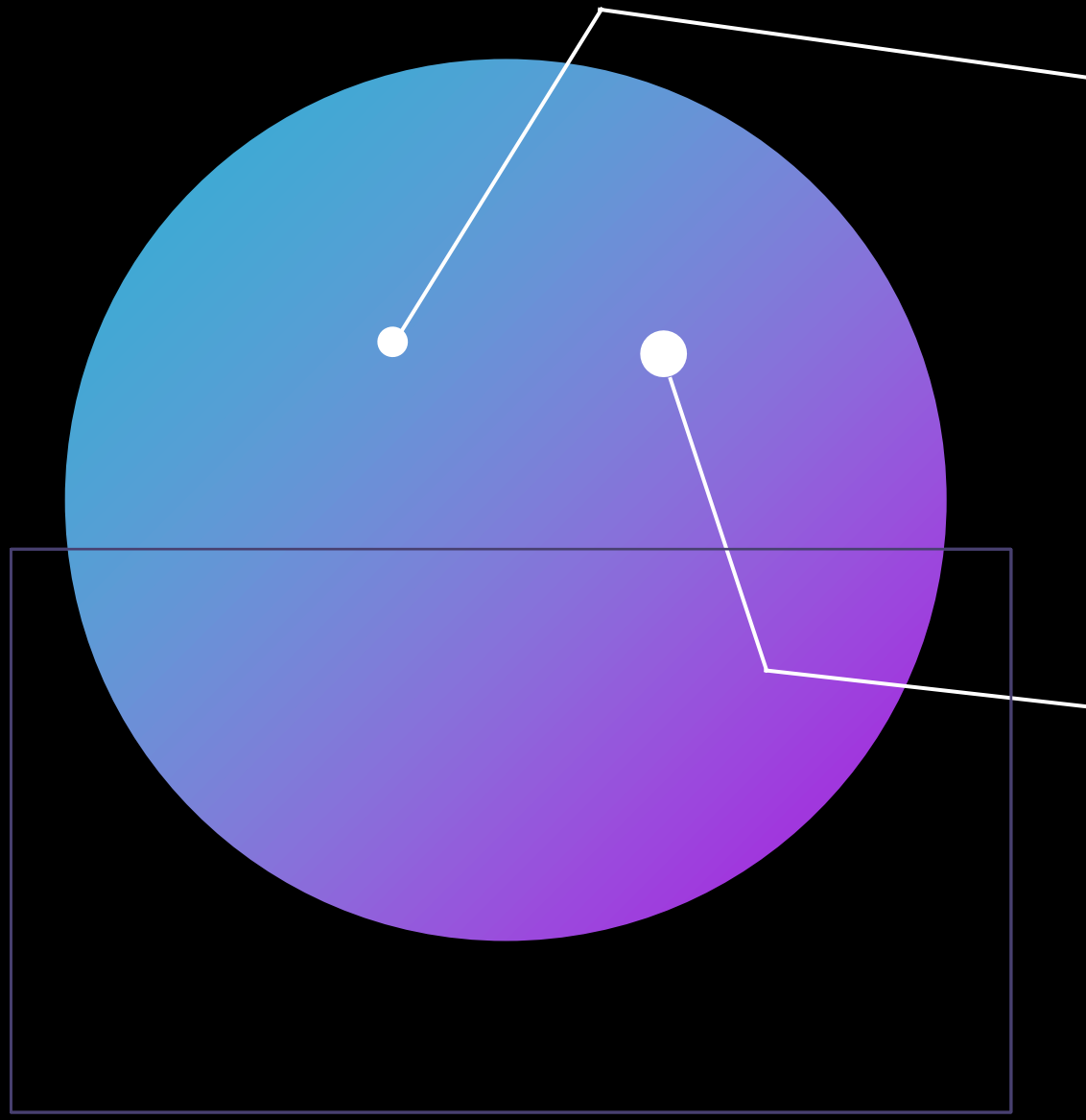
No caso de perda dos suprimentos, uma fonte dupla pode ter uma carga funcionando. *Hot swappable.*

Unidades de Distribuição de Energia Gerenciadas (PDUs)

- Permite ligar ou desligar remotamente a energia.
- Salas de servidores precisam de HVAC especial.
  - PDU recebe energia muito maior.
- PDU converte a energia com eficiência e gerencia o calor.
- Oferece ampla capacidade de monitoramento.

Redundância com Replicação

- Forma simples de redundância.
  - Fontes duplas;
  - Array de discos;
  - Backups;
  - Operações de Continuidade de Negócios.
- Forma comum: Redes de área de armazenamento e tecnologias de máquina virtual.



Rede de Área de Armazenamento (SAN)

Rede dedicada que conecta elementos de computação e armazenamento com replicação.

Modelo antigo de dados armazenados em discos conectados a uma máquina = Modo de falha.

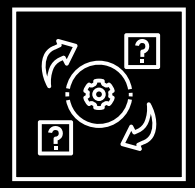
SAN – Proporciona o armazenamento de dados independente de qualquer computador.

VM

- Permite replicar unidades de processamento.
- Permite que várias cópias de uma instância seja utilizada em um hardware diferente.
- Funciona como um Servidor Web extra.
- Revolucionou as operações de computação.
- Fornece independência de hardware para imagens operacionais.

Redundância Local x Nuvem

É preciso considerar a localização.

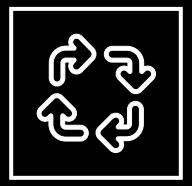


Fatores que serão empregados dependem de onde o sistema está empregado.

Refletir sobre = Gerenciamento da redundância X Riscos.

Alta Disponibilidade

Capacidade de manter a disponibilidade e o processamento, apesar da interrupção.



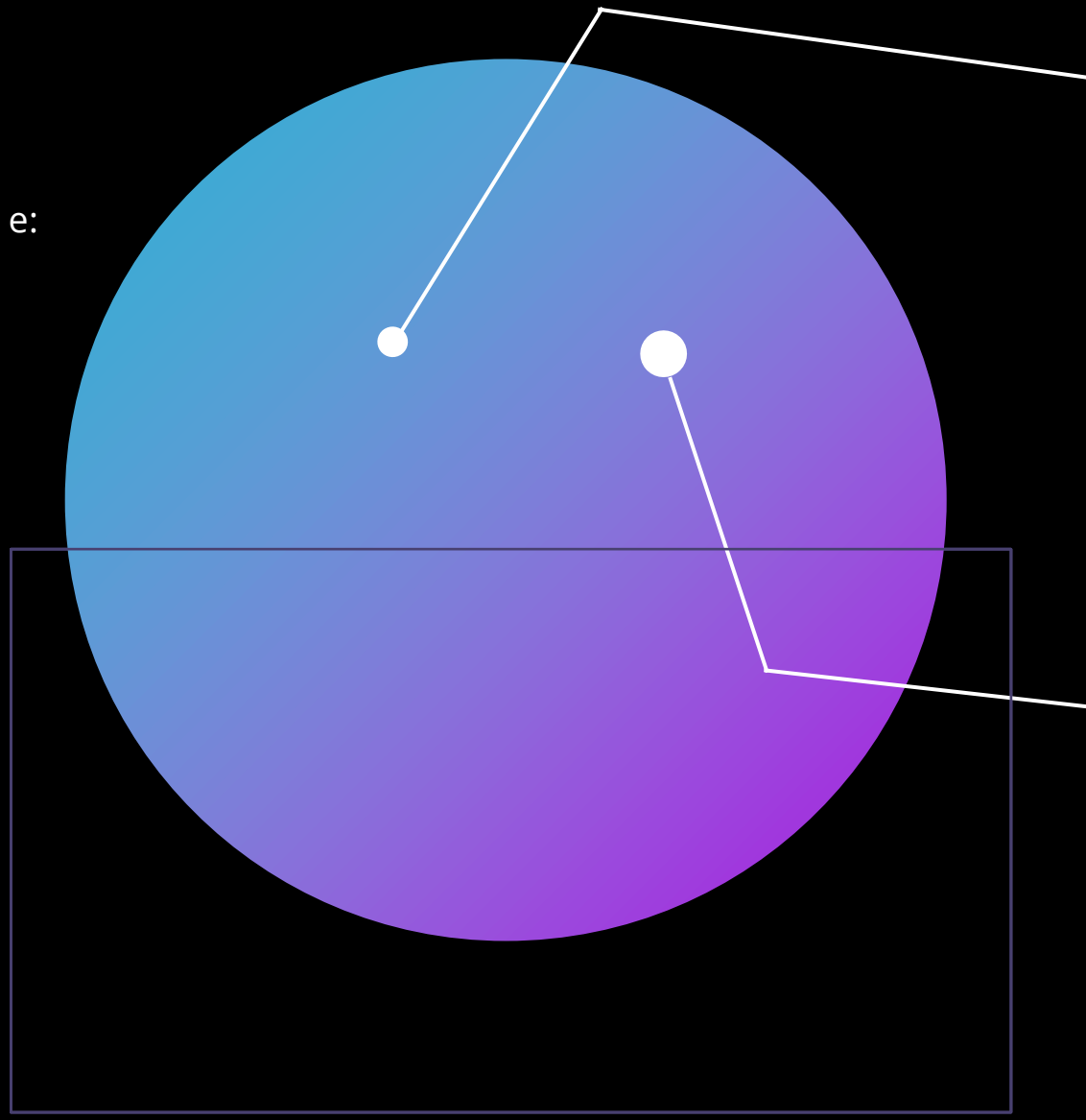
Requer energia, sistemas e até hardwares redundantes, se não em outro local.

Vai além da redundância.

- Requer tanto os dados como os serviços disponíveis.

Escalabilidade

- Permite acomodação (em *farms*) de cargas de trabalho maiores e:
  - Adição de recursos;
  - Fortalecimento do hardware;
  - Adição de nós.
- Se não escalar, pode acarretar em:
  - Indisponibilidade;
  - Queda de velocidade e taxa de transferência.
- Não é a mesma coisa que elasticidade (dinâmico e horizontal)!



Tipos de Backup

- Disponibilidade de backups = Elemento-chave no BC/DR.
- Essencial quando a segurança falha.
- Backup de Dados é um elemento crítico.
- O que considerar:


Frequência dos backups;


Extensão dos backups;


Processo de realização dos backups;


Responsável pela criação dos backups;


Local do armazenamento;


Tempo de armazenamento;


Quantas cópias.

Tipos de Backup

- Objetivo: Fornecer dados válidos/não corrompidos em caso de corrupção ou perda.
- Quatro formas principais de backups:
  - Completo;
  - Incremental;
  - Diferencial;
  - Instantâneo.

Completo

Todos os arquivos e volumes são copiados para a mídia de armazenamento.

A restauração é simples.

- Leva um tempo considerável;
- O bit de arquivo é apagado.

Diferencial

- Backup dos arquivos que foram alterados desde o último backup completo, que contenha o bit de arquivamento.
- Um backup completo precisa ser feito de tempos em tempos.
- Requer duas etapas para o restore:
  - Carregamento do último backup completo;
  - Restauração do backup diferencial para atualização dos arquivos.
- Vantagem: Menos armazenamento e tempo.

Incremental

- Variação do backup diferencial.
- Backup dos arquivos que foram alterados desde o último completo ou incremental.
- Só backups de arquivos com bit de arquivamente.
- Depende de backups completos.
- Requer mais trabalho.

Voltar ao último backup completo;

Recarregar o sistema com os dados;

Atualizar o sistema com **cada** backup incremental desde o último completo.

- Vantagem: Menos armazenamento e tempo.

Resumo das Backup

	Completo	Diferencial	Incremental
Quantidade de espaço	Grande	Médio	Médio
Restauração	Simples	Simples	Trabalhoso

Ordem de Restauração

- Processo de Restore é para restaurar a cópia de backup.
- Permite restaurar e organizar as partes mais importantes para o backup.
- Requer:

Planejamento;

Coordenação e testes contínuos.

Backup Online vs. Offline

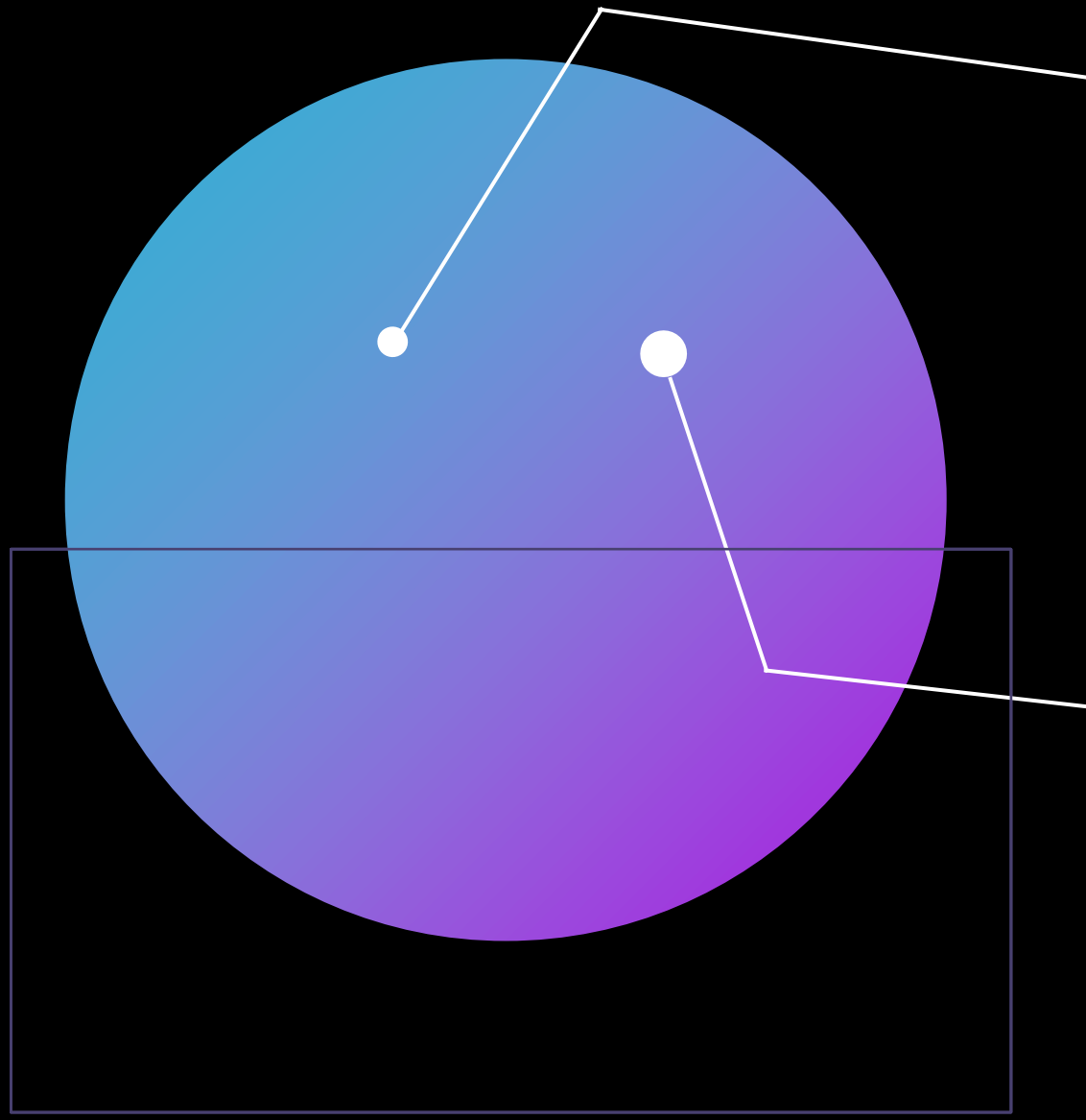
- Online:
  - Acessível pela Internet;
  - Flexibilidade na recuperação, pois é acessível o tempo todo.
- Offline:
  - Armazenados em um sistema offline e não acessível a todo o momento;
  - Sem separação geográfica dos arquivos originais.

Snapshots

Cópia de um VM em um determinado momento.

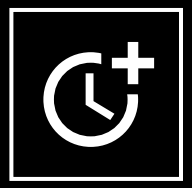
Vantagens:

- Facilidade de cópia e restauração;
- Assemelha-se ao clique de um botão, com uma restauração instantânea.



Imagem

Estrutura de backup de uma imagem completa de um sistema.



Leva mais tempo e consome mais espaço.

Fornece captura completa do sistema, como dados excluídos e não persistentes.

Fornece níveis extras de garantia com uma rápida recuperação, caso haja falhas.

Não Persistência

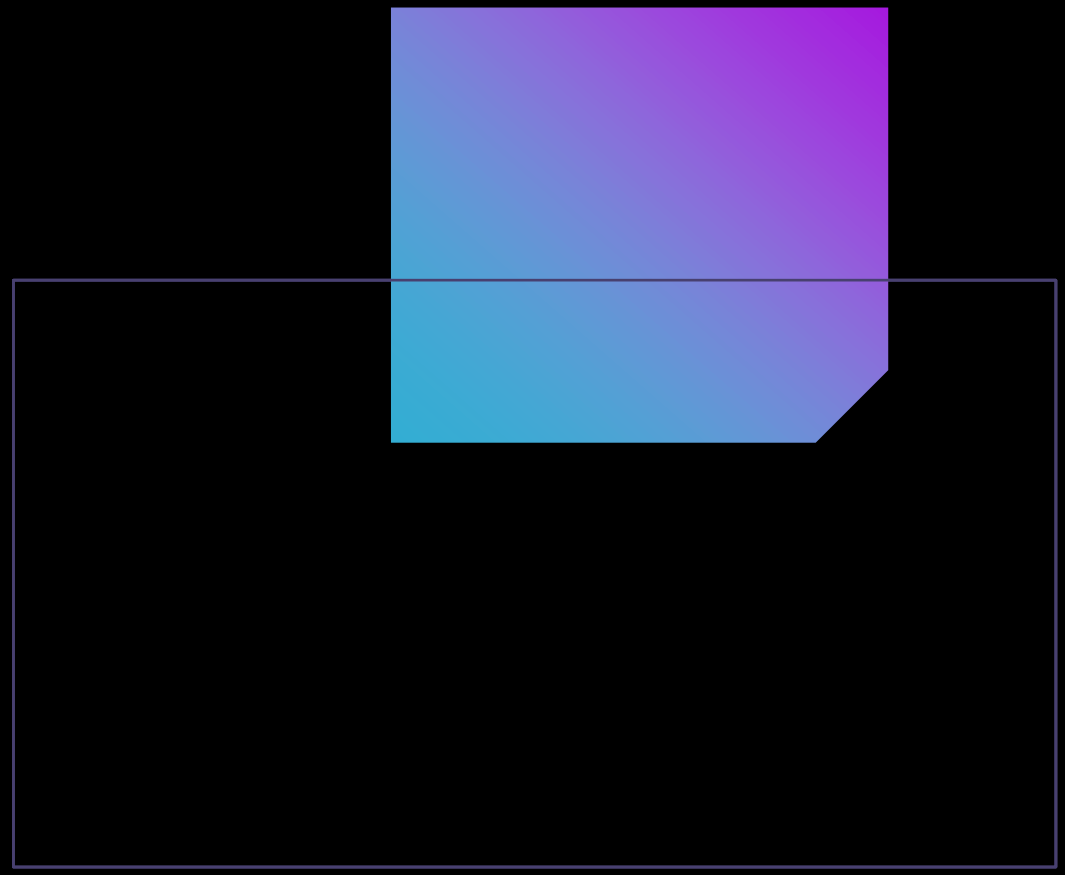
- Itens do sistema que não são permanentes, como conteúdo da memória após o computador ser desligado.

Registro do Microsoft Windows.

- A não persistência precisa ser gerenciada adequadamente.
- Instantâneos - Cópia do sistema em um momento, para utilizá-los como ponto de recuperação.

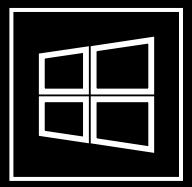
Reverter Para Estado Conhecido

- Capacidade de recuperar para um estado conhecido após um boot.
  - Exemplo: Deep Freeze e Recurso do Windows System Restore.
- Backups só trazem de volta os dados e o sistema.
- Drivers, configurações e patches é mais complicado.
- SOs podem reverter para uma configuração anterior conhecida após um patch com erro, por exemplo.



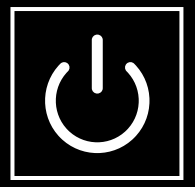
Última Configuração Válida

Meio de reverter para um estado conhecido.



Opção oculta a partir do Windows 10.

Varia de acordo com o tipo de problema.



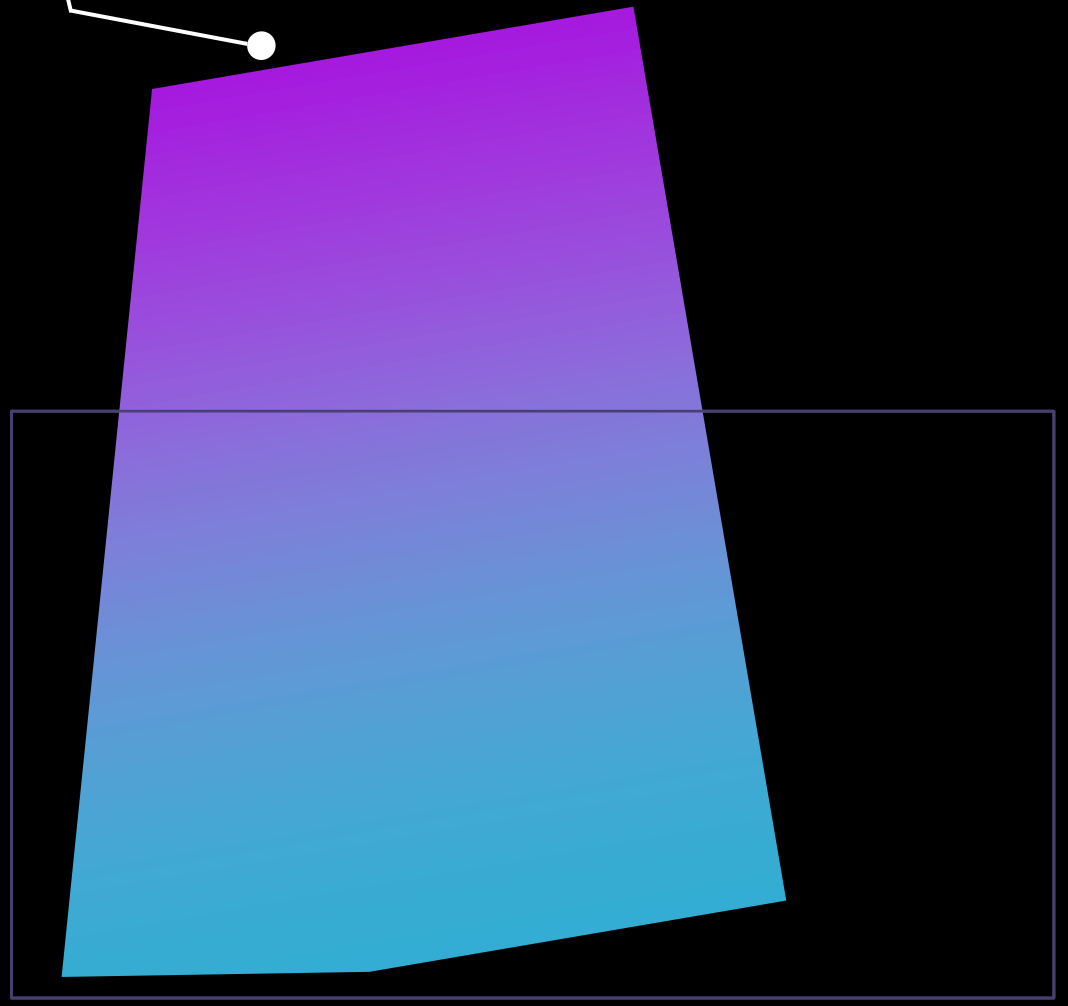
Três falhas seguidas na inicialização = Opções de recuperação no Windows.

Mídia de Inicialização Ao Vivo

Meio de iniciar um sistema com uma configuração e estado conhecidos.

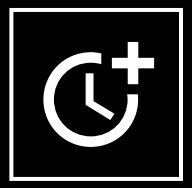
Com DVD ou USB é possível iniciar com uma imagem inicializável completa do SO.

Comum em investigações forenses.



Imagem

Estrutura de backup de uma imagem completa de um sistema.



Leva mais tempo e consome mais espaço.

Fornece captura completa do sistema, como dados excluídos e não persistentes.

Fornece níveis extras de garantia com uma rápida recuperação, caso haja falhas.

Unidade de Fita

Forma mais antiga de armazenamento de dados.

Armazena em uma estrutura longa e sequêncial de leitura/gravação.

Tende a criar problemas de desempenho.

Para armazenamento em massa, ainda é viável por conta do custo e desempenho.

Unidade de Disco

- Pode ser:
  -  Disco rígido físico.
  - 

 Dispositivo de memória de estado sólido.
- No caso do backup, é comum para um único computador.
- Para PCs de cliente, pode fazer sentido.
- É rápido e pode ser feito com unidades removíveis.

Cópia

Formato mais simples de backup e não limpa o bit de arquivamento.

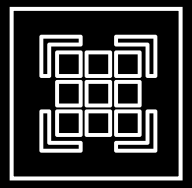
Usuários escolhem pela facilidade ou por um pedido pontual.

Pode executar sabendo que não atrapalhará sua estratégia de backup regular.

Os métodos anteriores (fita/disco) são mais adequados para backups em grande escala.

Dispersão Geográfica

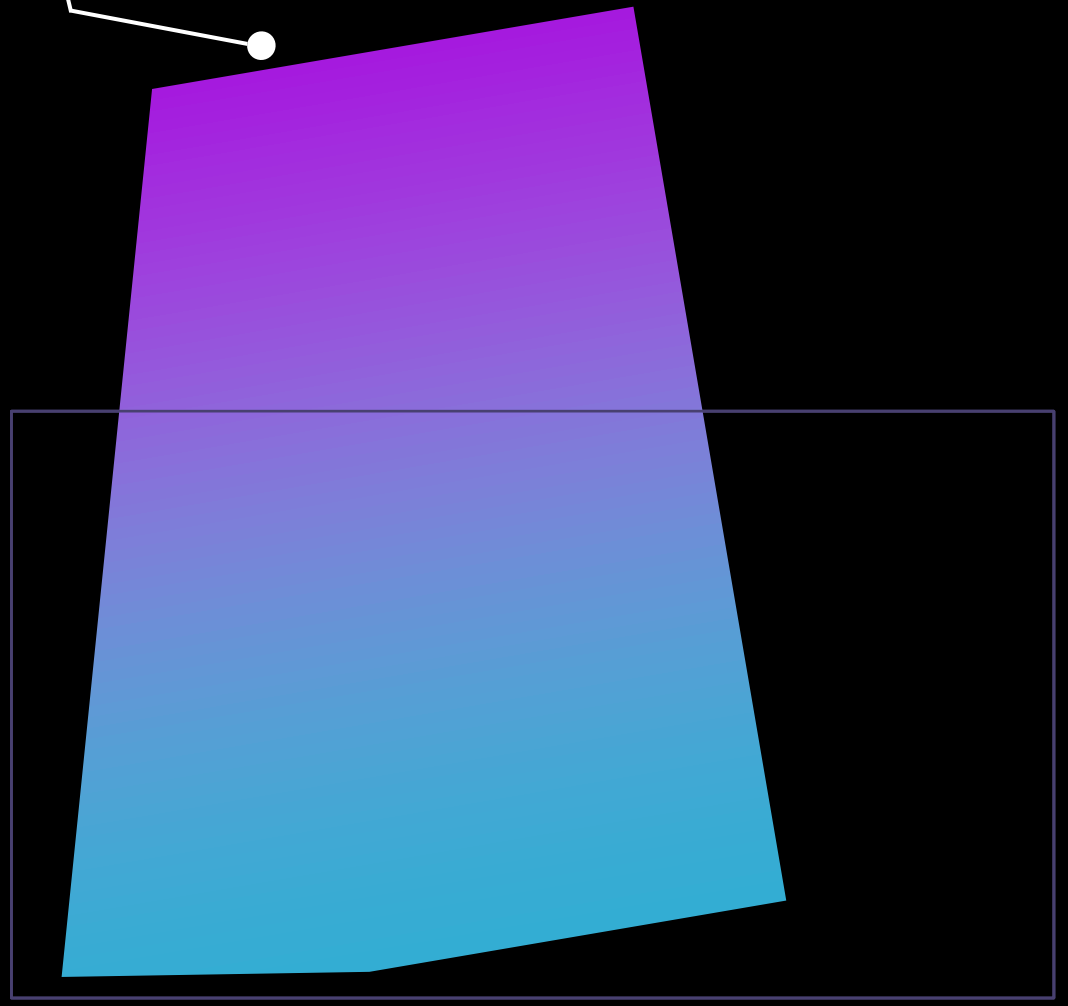
Considere as despesas com o armazenamento de backups.



Manter tudo em um mesmo lugar não é uma boa ideia.

A cópia mais recente pode ser armazenada mais próximo do recurso e longe o suficiente de desastres.

A própria instalação de armazenamento deve ser reforçada contra possíveis ameaças.

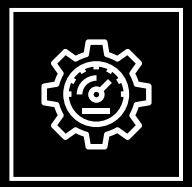


Armazenamento Anexado à Rede (Network-Attached Storage -NAS)

- Conexão de rede para armazenamento externo centralizado.
- Geralmente configuradas em uma solução tolerante a falhas, como uma matriz RAID.
- Pode ser gerenciado por:
  - Conexão USB;
  - Ethernet.
- Não transfere dados com rapidez para operações normais.
- Suporta protocolos de compartilhamento SMB e NFS.
- Segurança redobrada por conta da centralização de dados.
- Implemente esquema de autenticação, permissões, criptografia, firewall e antivírus.

Rede de Área de Armazenamento (SAN)

Rede de alta velocidade para armazenamento (mais rápido que o NAS).



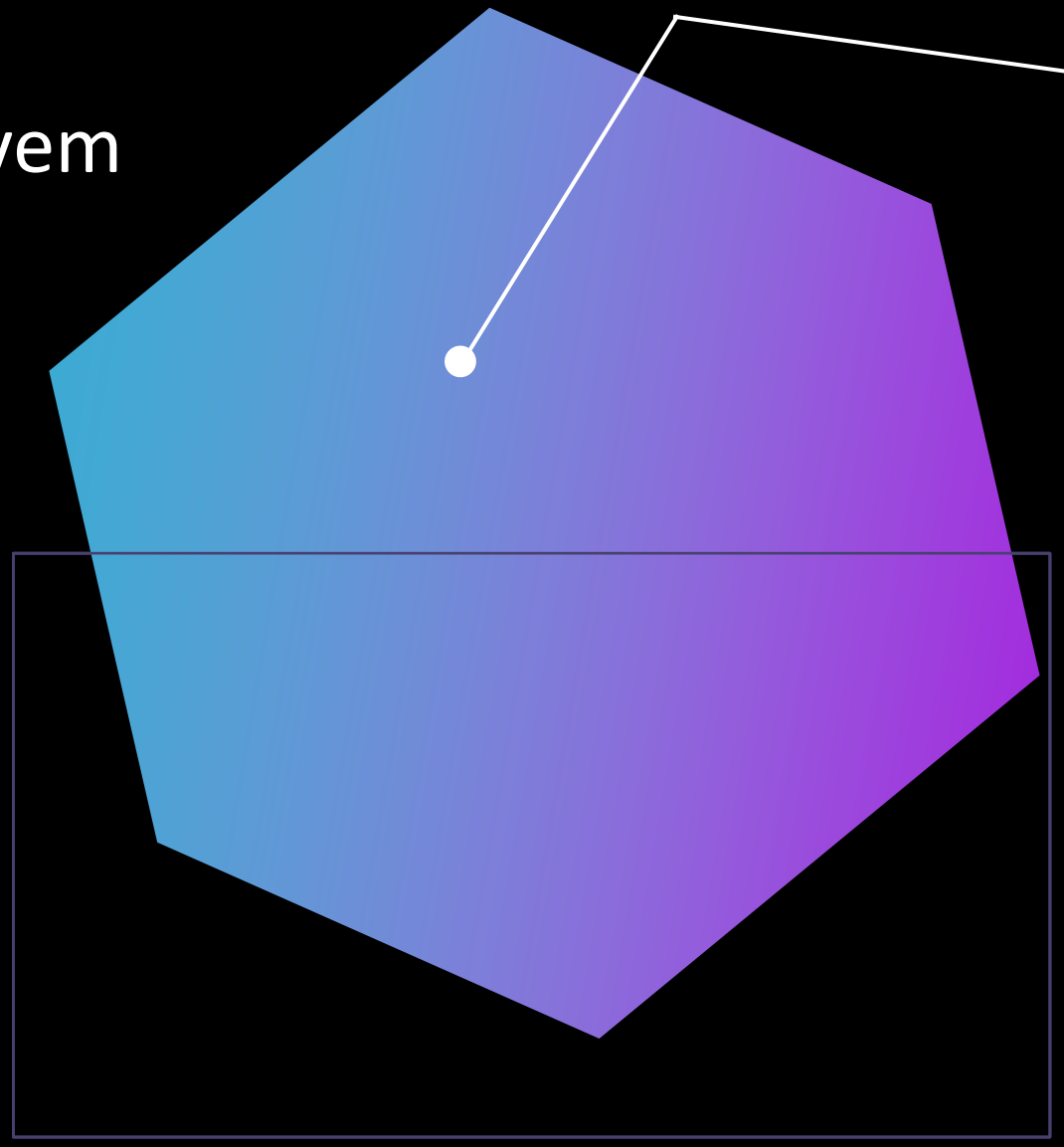
Otimizada para vários tipos de armazenamento como tamanho e taxas de dados e formato.

Exemplo da tecnologia para uso complexo, como Fibre Channel, iSCSI etc.

Permite backups eficientes, eficazes, gerenciáveis e flexíveis.

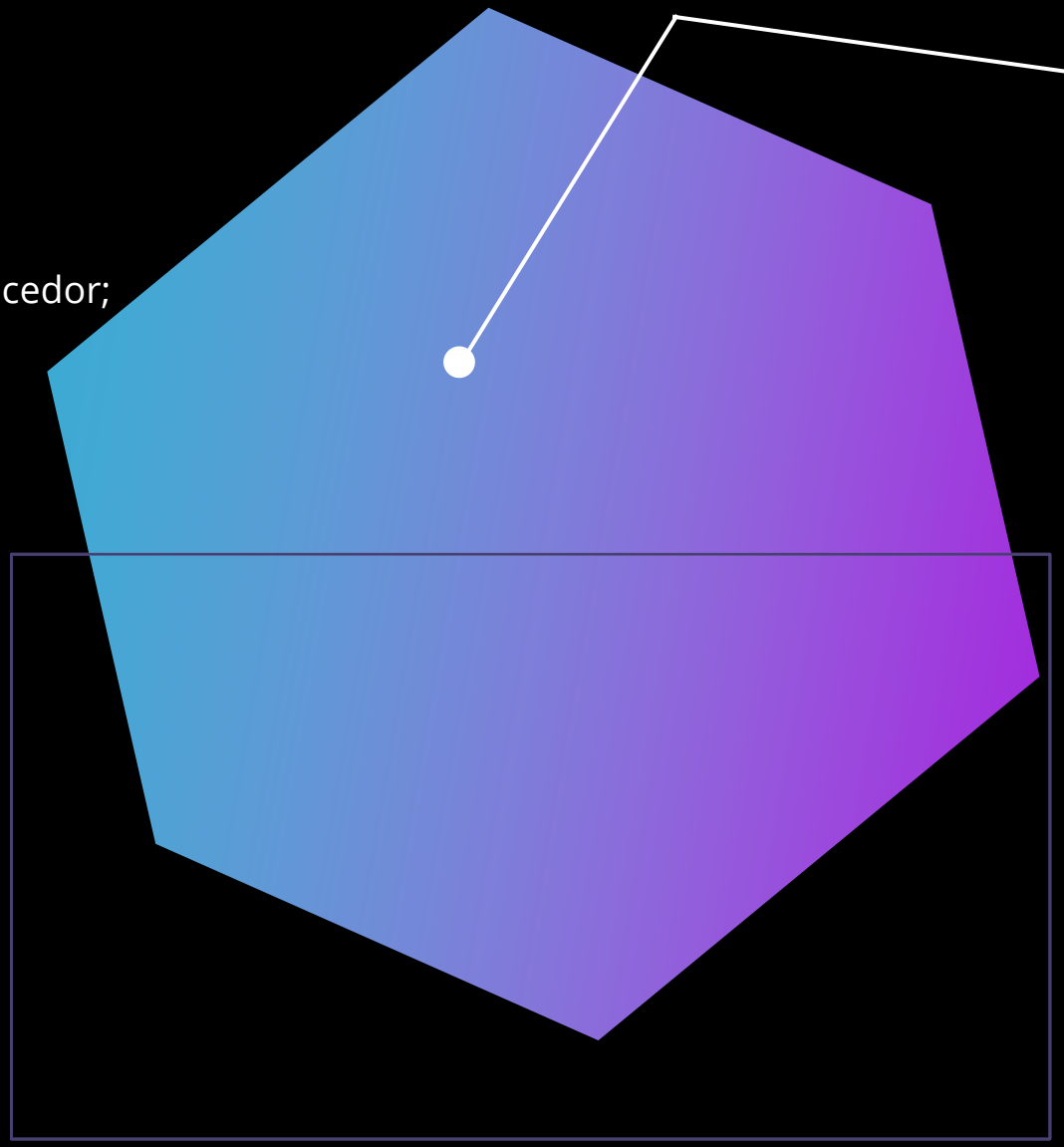
Vantagem: Armazenamento na Nuvem

- Pode ser usada como armazenamento de backup de dados.
- Vantagens:
  - Fora do local;
  - Várias cópias redundantes;
  - Disponível via Web.



Desvantagem: Nuvem

- Desvantagens:
  - Backup em outro local (segurança);
  - Protegida apenas pelo acordo entre usuário e fornecedor;
  - Contratos geralmente favorecem o fornecedor.
- Exemplos:
  - Dropbox;
  - Box;
  - OneDrive;
  - Drive;
  - iCloud.



Armazenamento Externo

Armazenados em um local separado do local onde ficam os sistema.

Alivia o risco de perda dos backups, como um incêndio ou inundação.

Nuvem pode ser uma boa resolução para esses problemas, incluindo a privacidade.

Considerações de Distância

Backups externos podem gerar problemas de logística.

Locais externos precisam estar longe o suficiente para não serem afetados.

Se o seu servidor e seu provedor de nuvem está localizado no mesmo lugar e são atingidos por um desastre natural, seus dados ficam indisponíveis.

OBRIGADO!

RESILIÊNCIA DE
SEGURANÇA CIBERNÉTICA