Prime

CCSF

Tipos de Backup e Outros Aspectos de Resiliência

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;


Realização dos backups;


Responsável pela criação dos backups;


Local do armazenamento;


Manutenção dos backups;


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 softwares são copiados para a mídia de armazenamento.

A restauração é simples.

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

Incremental

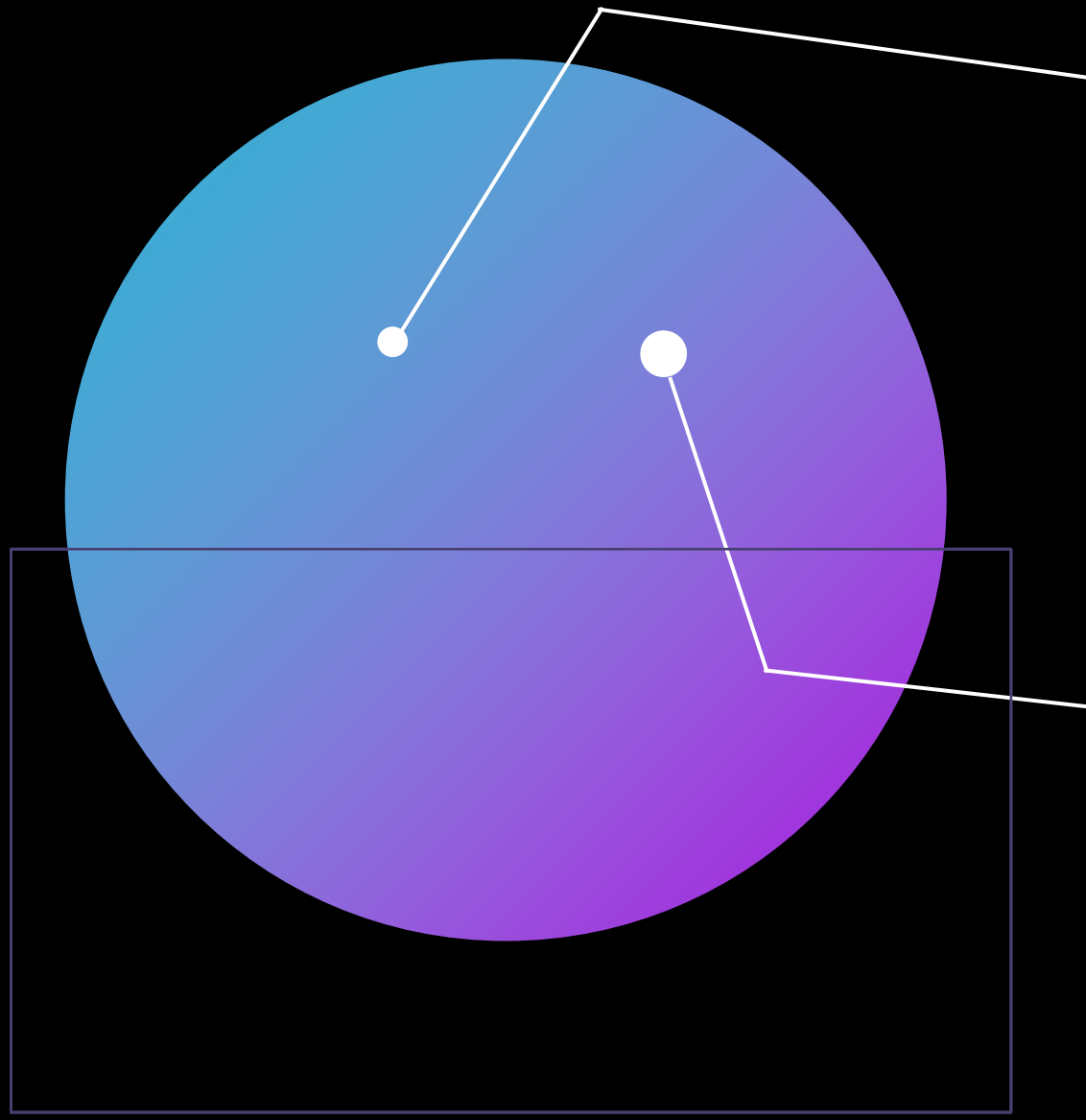
- Variação do backup diferencial.
- Backup dos arquivos que foram alterados desde o último completo ou incremental.
- Depende de backups completos.
- Requer mais trabalho.
  - Voltar ao último backup completo;
  - Recarregar o sistema com os dados;
  - Atualizar o sistema com cada backup incremental desde o último completo.
- Vantagem: Menos armazenamento e tempo.

Instantâneo

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.



Diferencial

- Backup dos arquivos que foram alterados desde o último backup completo.
- Um backup completo precisa ser feito de tempos em tempos.
- Requer duas etapas:

Carregamento do último backup completo;

Execução do backup diferencial para atualização dos arquivos.

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

Fita

Forma mais antiga de armazenamento de dados.

Armazena em uma estrutura longa.

Tende a criar problemas de desempenho.

Para backups, ainda pode funcionar.

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.

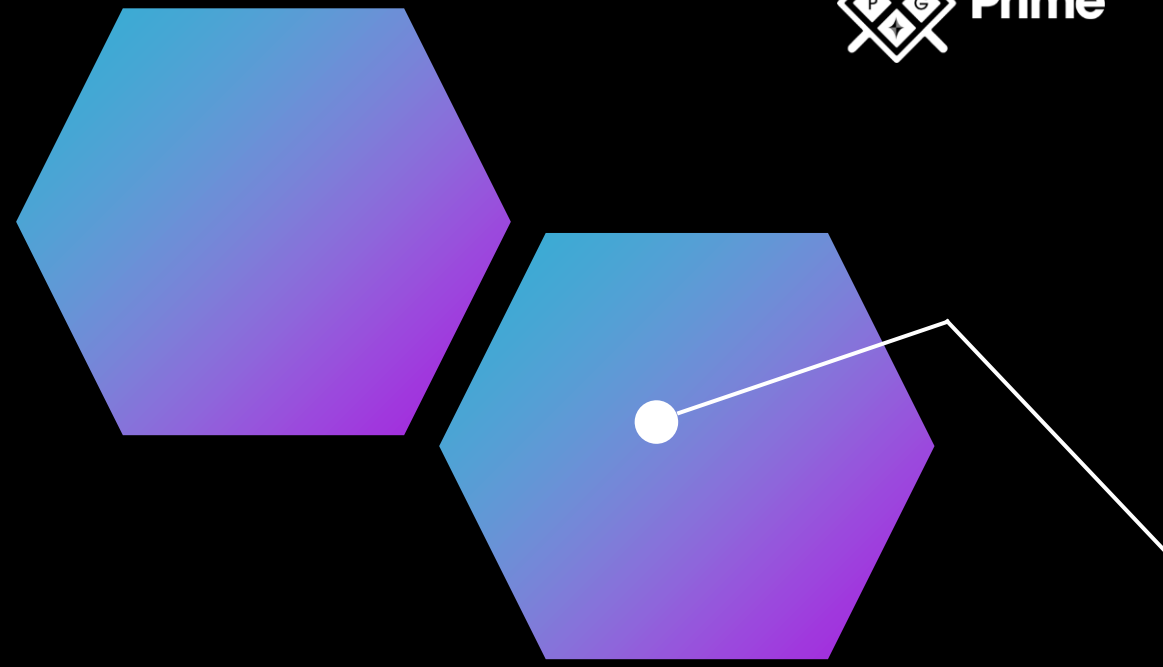
Cópia

Formato mais simples de backup.

Usuários escolhem pela facilidade.

Interrompido quando o escopo se expande para conjuntos de dados.

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

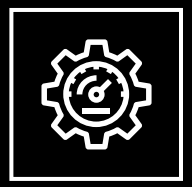


Armazenamento Anexado à Rede

- Conexão de rede para armazenamento externo.
- Pode ser gerenciado por:
  - Conexão USB;
  - Ethernet.
- Não transfere dados com rapidez para operações normais.

Rede de Área de Armazenamento (SAN)

Conecta elementos de computação e armazenamento.



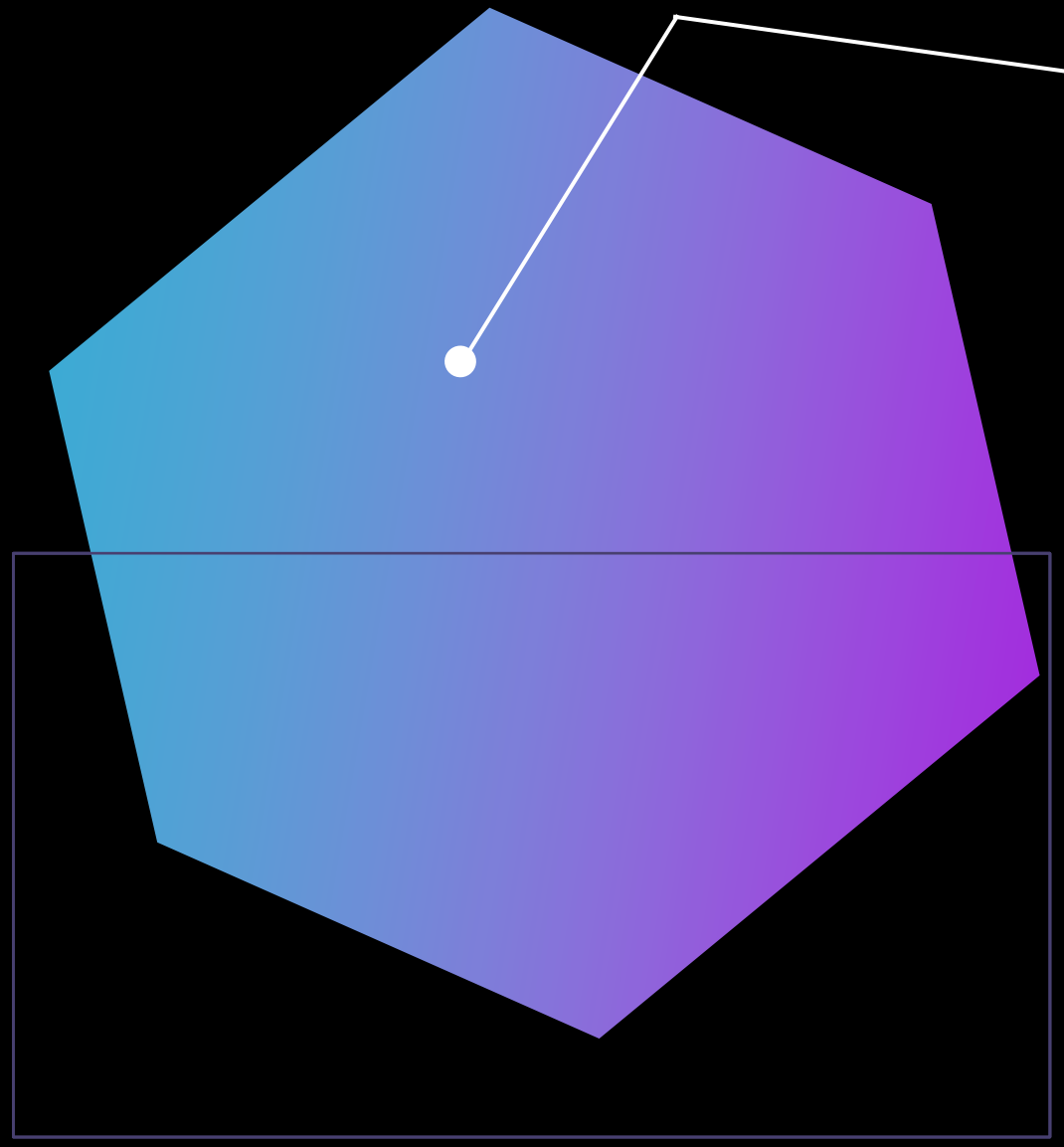
Otimizada para os tipos de armazenamento necessários.

Exemplo da tecnologia para uso complexo.

Permite backups eficientes e eficazes.

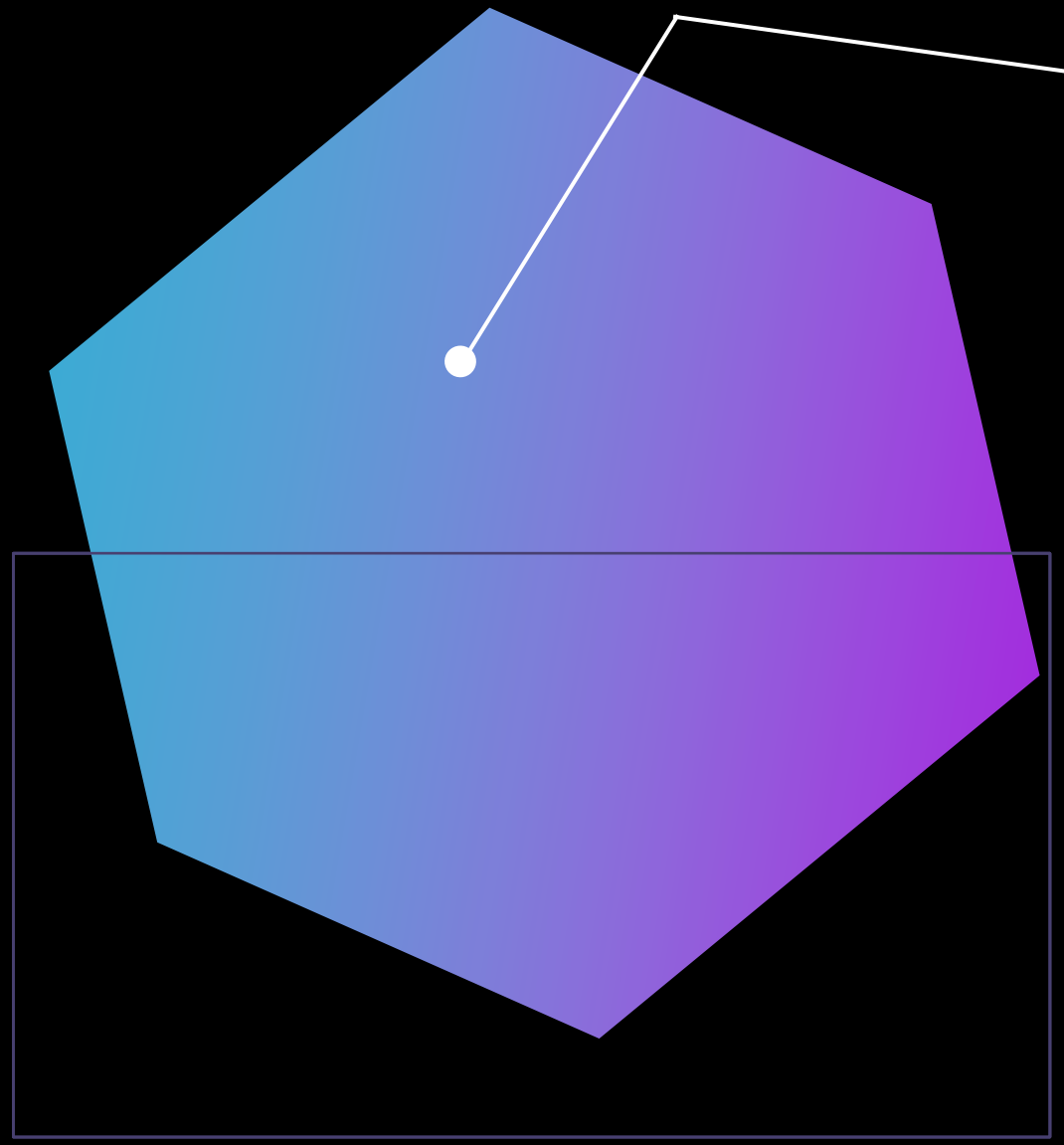
Nuvem

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



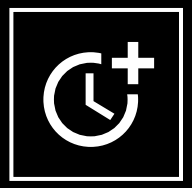
Nuvem

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



Imagem

Estrutura específica do arquivo de backup.



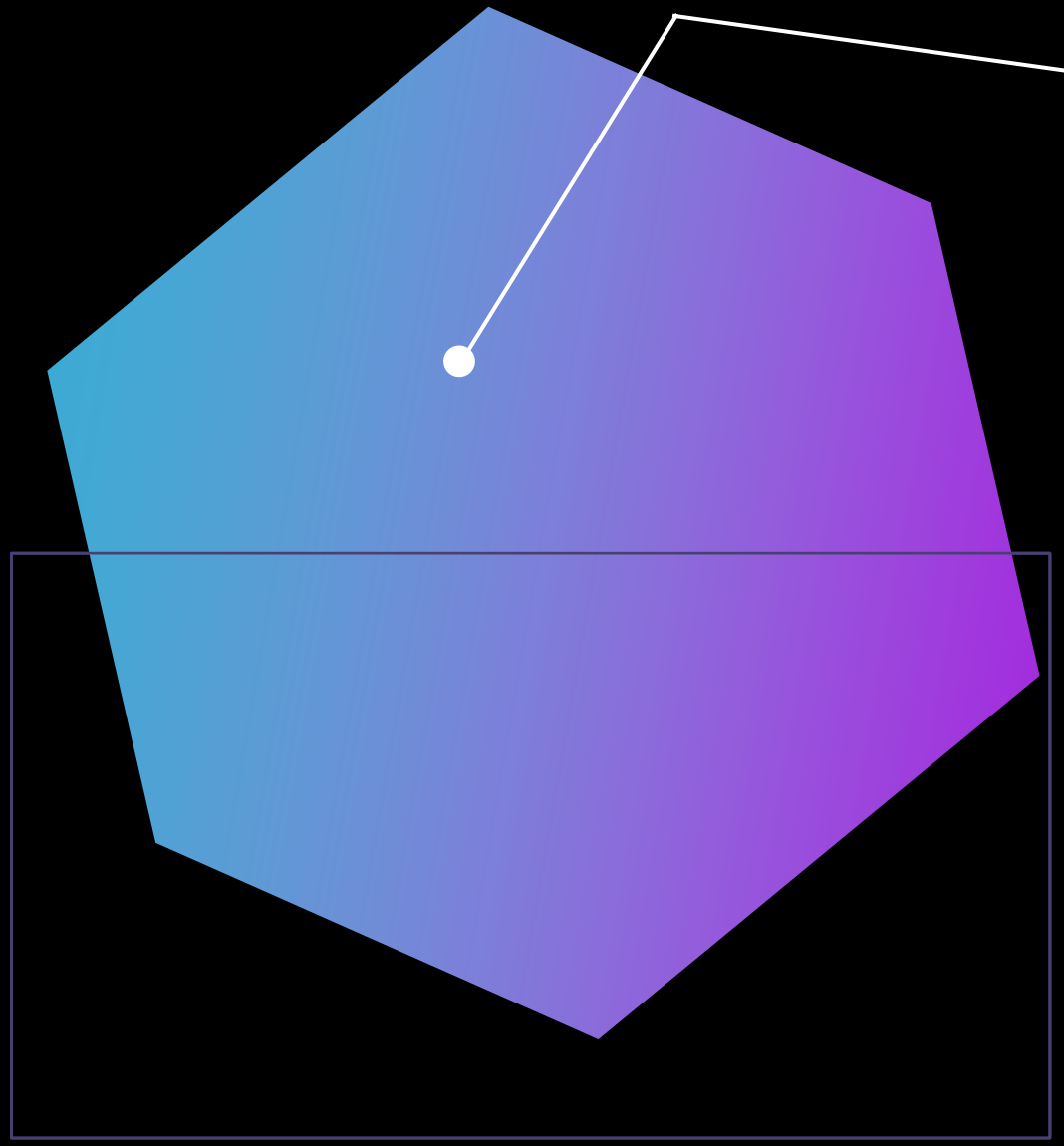
Leva mais tempo e espaço.

Fornece captura completa do sistema.

Fornece níveis extras de garantia.

Online vs. Offline

- Online:
  - Armazenados em um local acessível pela Internet;
  - Flexibilidade na recuperação.
- Offline:
  - Armazenados em um sistema offline;
  - Fornecem separação geográfica.



Armazenamento Externo

Armazenados em um local separado do sistema.

Alivia o risco de perda dos backups.

Nuvem pode ser uma boa resolução para esses problemas.

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.

Não Persistência

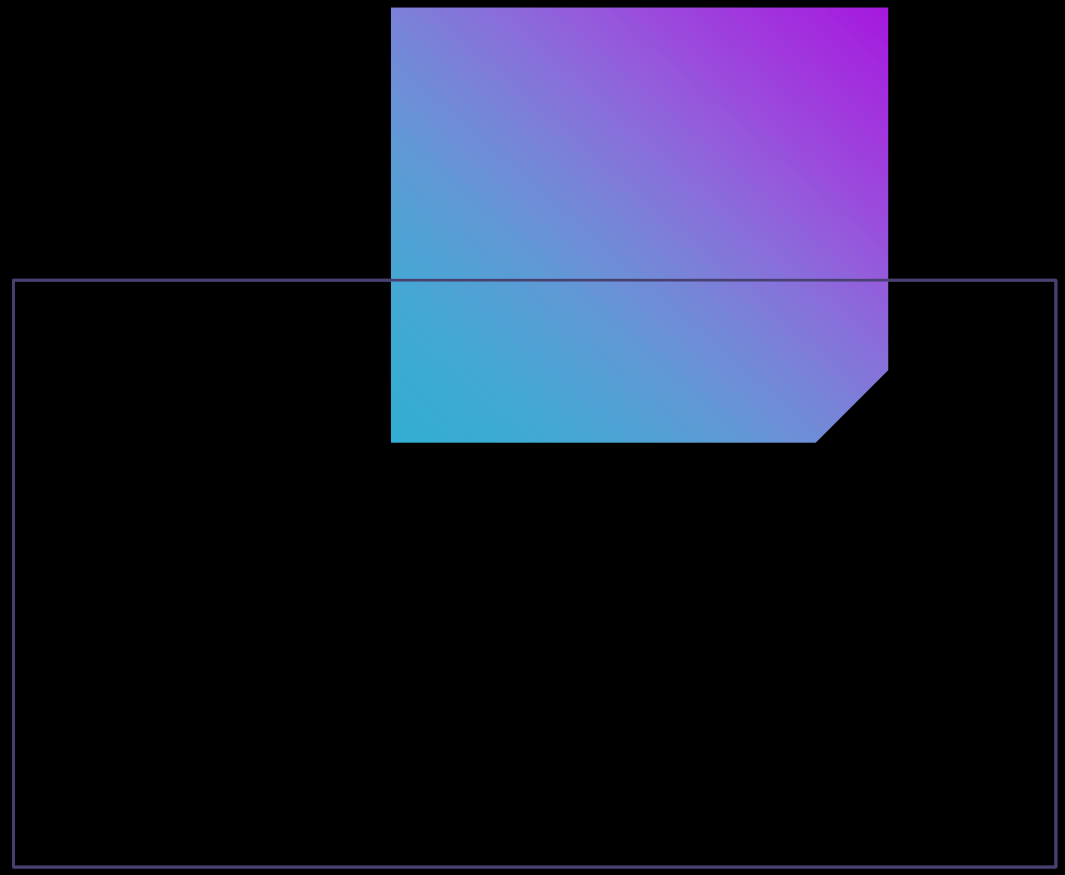
- Itens do sistema que não são permanentes, podendo ser alterados.

Microsoft Windows.

- Possuem mecanismos embutidos.
- 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.
  - Exemplo: OSS.
- Trazer a configuração de um sistema é algo complexo.
- SOs podem reverter para uma configuração anterior conhecida.



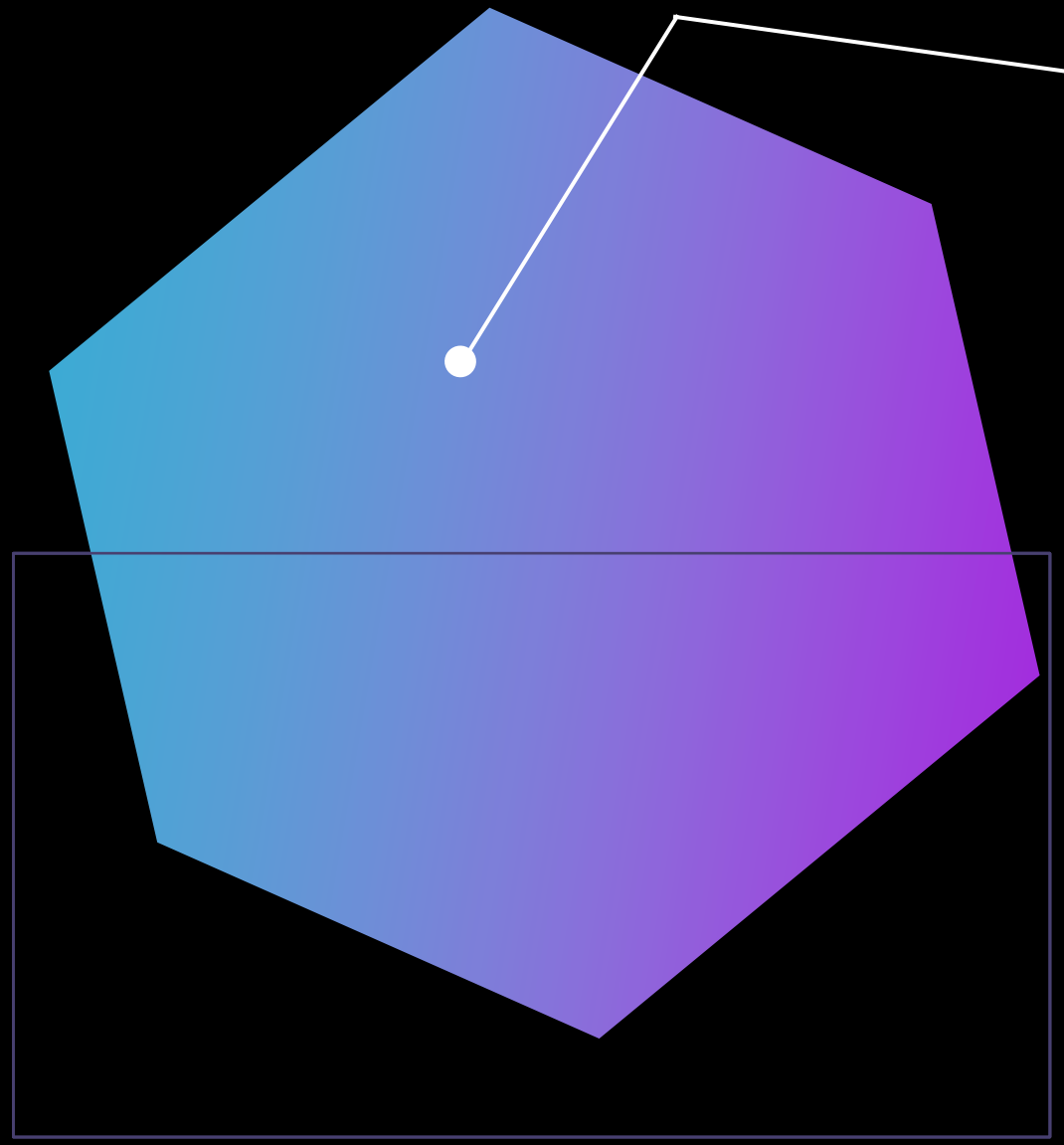
Última Configuração Válida

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 = Opções de recuperação no Windows.

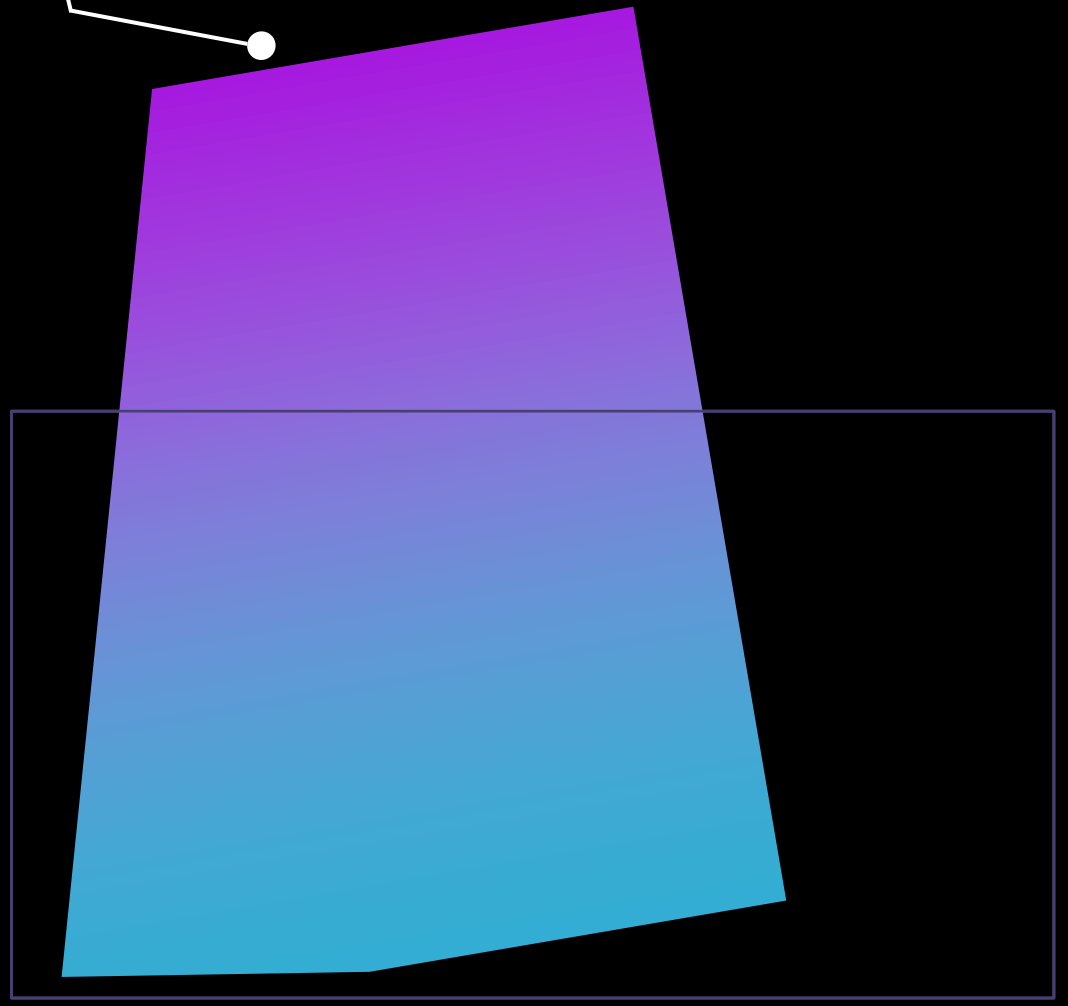


Mídia de Inicialização Ao Vivo

Meio de iniciar com uma configuração e estado conhecidos.

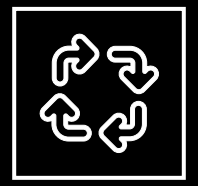
Contém uma imagem completa do SO.

Comum em investigações forenses.



Alta Disponibilidade

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



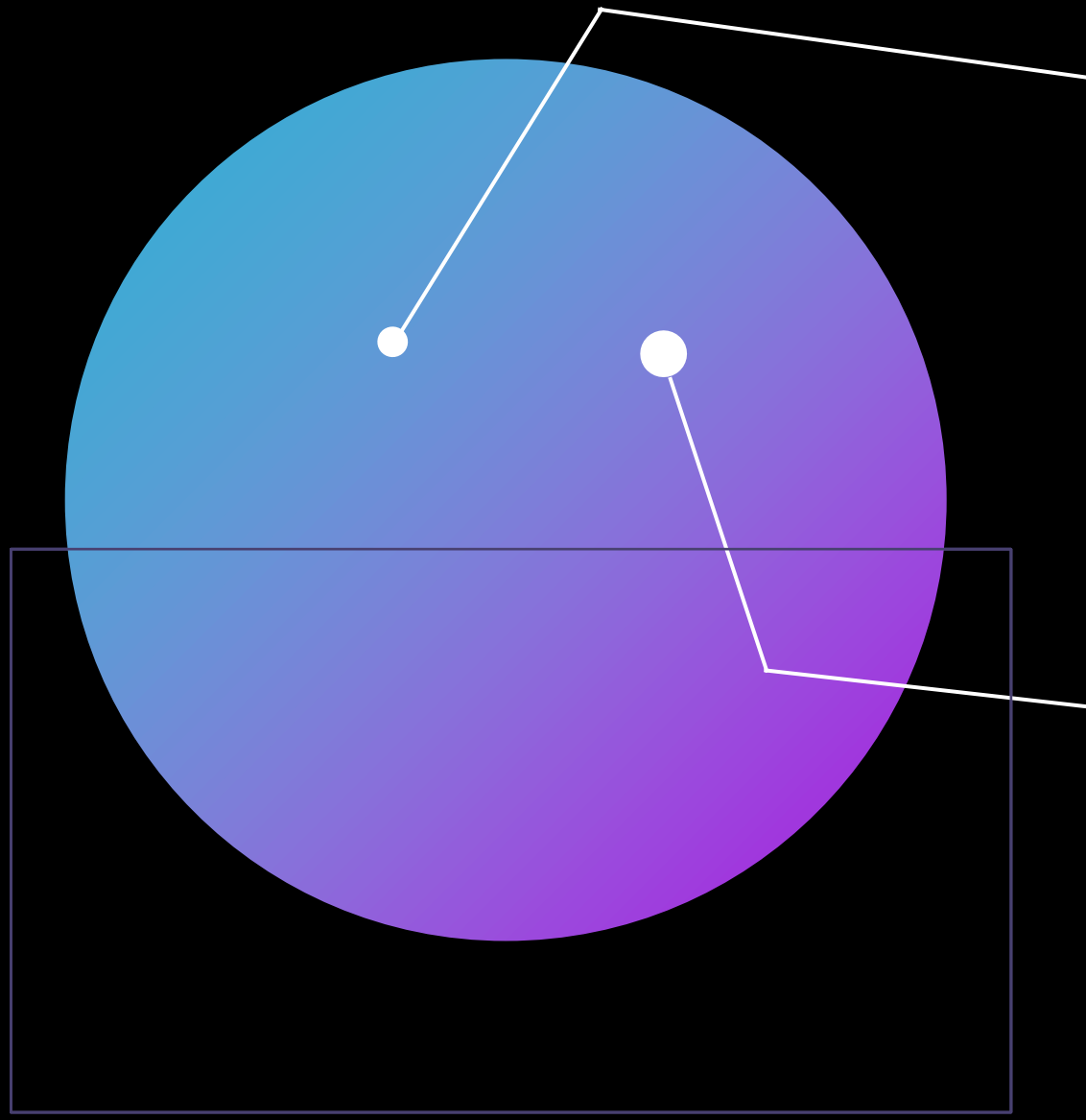
Requer sistemas redundantes.

Vai além da redundância.

- Dados e serviços precisam ser disponíveis.

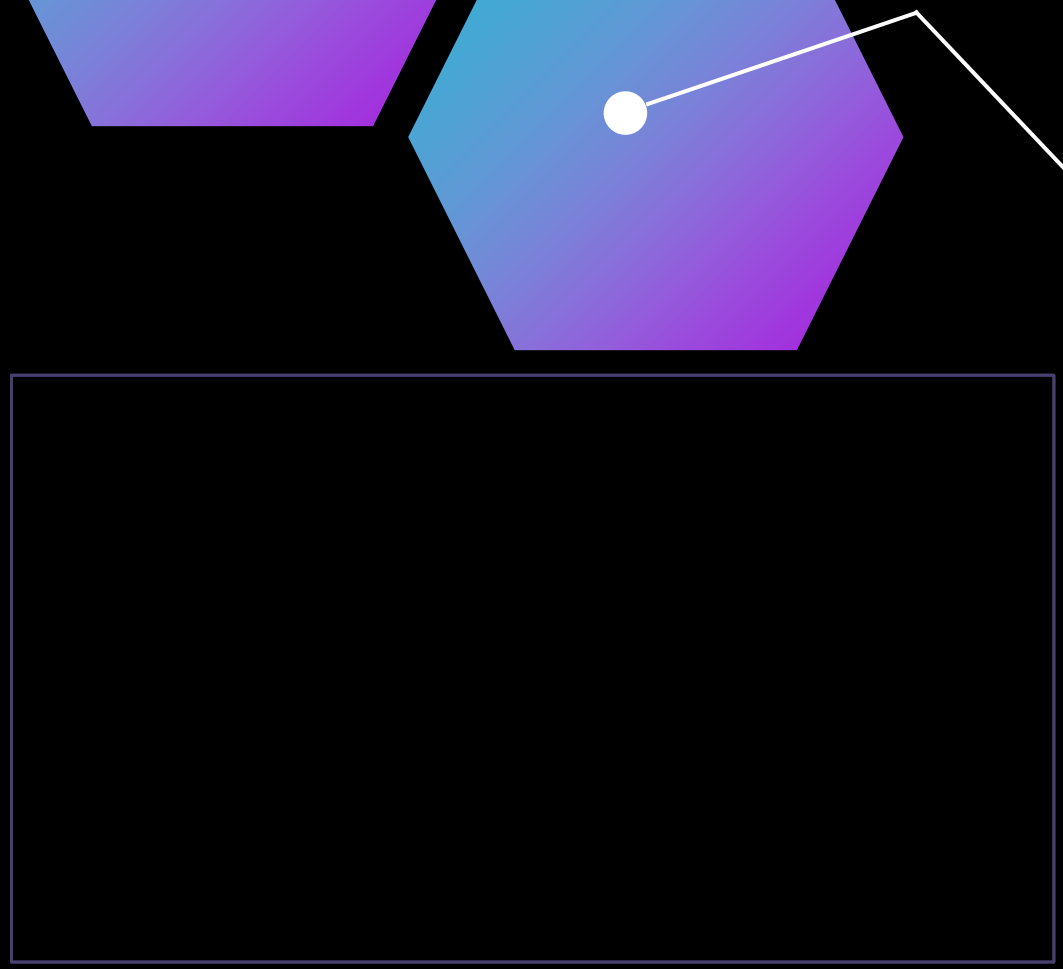
Escalabilidade

- Permite acomodação de cargas de trabalho maiores e:
  - Adição de recursos;
  - Fortalecimento do hardware;
  - Adição de nós.
- Afeta a:
  - Disponibilidade;
  - Taxa de transferência.
- Não é a mesma coisa que elasticidade!



Ordem de Restauração

- Projetada para obter uma cópia alternativa.
- Permite restaurar e organizar as partes mais importantes para o backup.
- Requer:
  - Planejamento;
  - Coordenação.



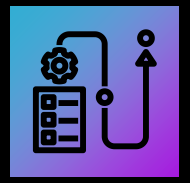
Diversidade

- Monocultura:
  - Aumenta a eficiência dos patches;
  - 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.
  -  Firewalls;
  -  ACLs;
  -  Hosts bastiões.
- Diversidade aumenta as chances de capturar um invasor.

Fornecedores



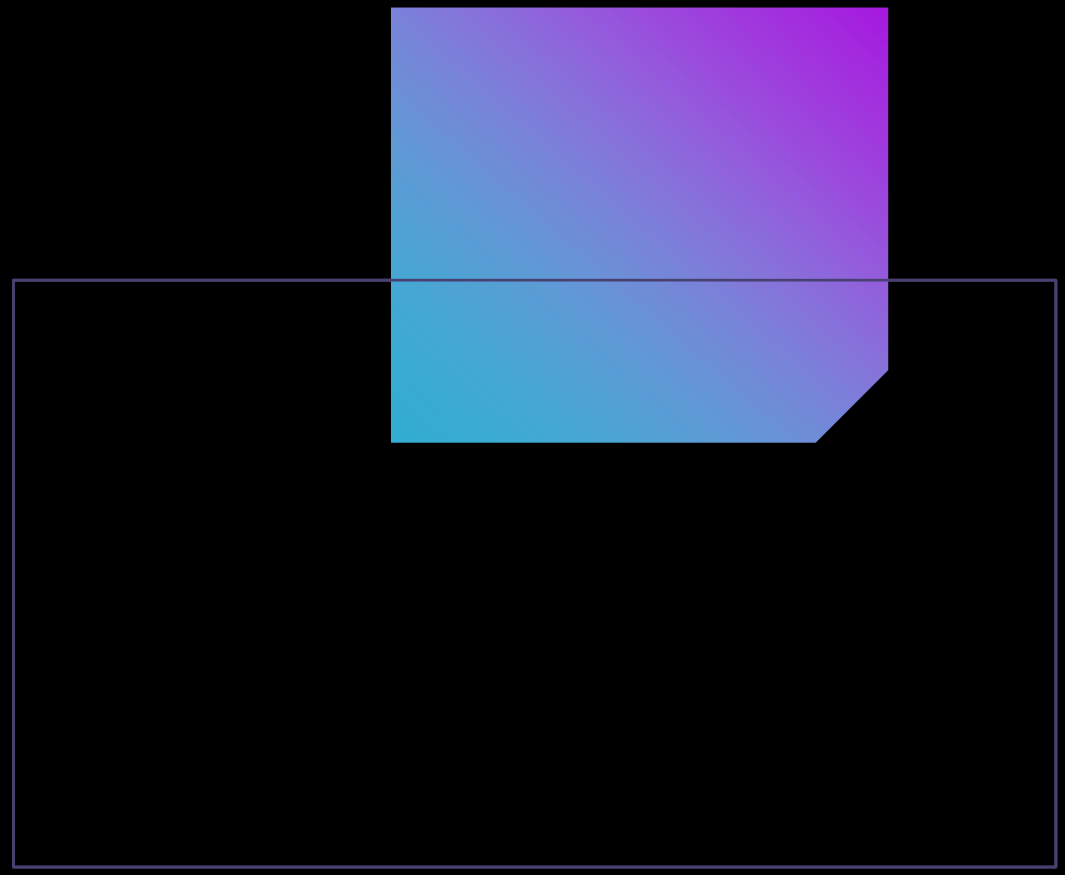
Diferentes fornecedores abordam diferentes metodologias.

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.

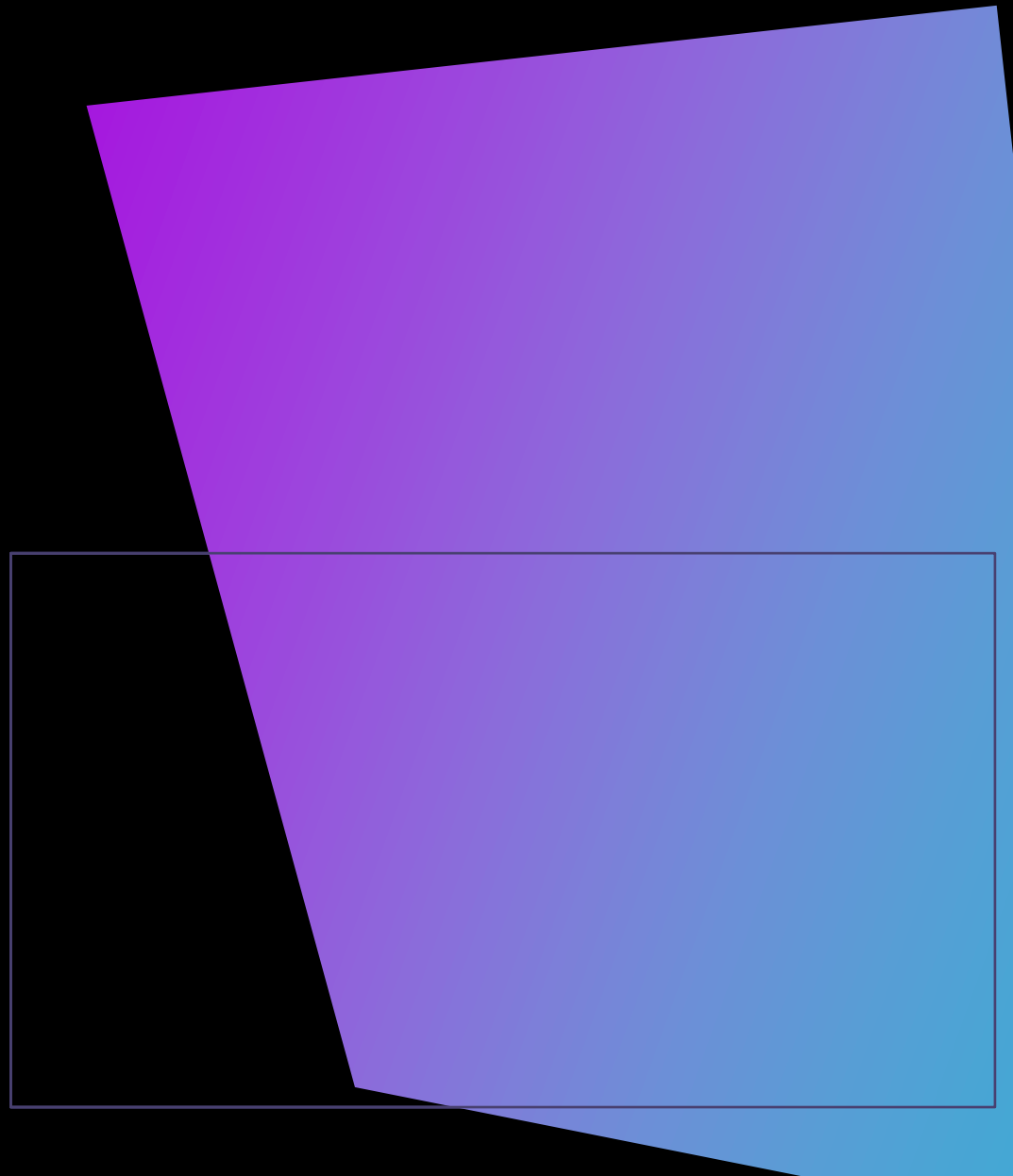
Criptografia

- A diversidade também pode existir no mundo criptográfico.
  - Exemplo: Cifras TLS.
- Um mesmo servidor com host diferente pode ocasionar diferentes opções de criptografia, mas ainda é seguro.
- 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.
- Redes modernas empregam:
  - Firewall;
  - Sub-Rede rastreada (DMZ);
  - Hosts bastiões;
  - ACLs.



OBRIGADO!

TIPOS DE BACKUP E OUTROS ASPECTOS DE RESILIÊNCIA