Prime

CCS-A

Segurança da Nuvem e Virtualização

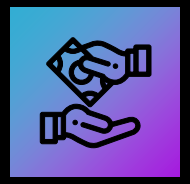
Modelos de Nuvem

- Pode ser criada por entidades internas e externas.
  - Google;
  - Amazon;
  - Provedores menores ou “dentro de casa”.
- A nuvem é comercializada sob os conceitos:
  - Plataforma como Serviço (PaaS);
  - Software como Serviço (SaaS);
  - Infraestrutura como Serviço (IPaaS).
- Para cada uso, os fatores econômicos influenciam.
  - Questões de custo;
  - Contratos: Segurança, backup, suporte, conectividade etc.

Infraestrutura como Serviço (IaaS)

Termo para descrever sistemas em nuvem que são uma solução virtual.

Ao invés de construir um datacenter, permite a contratação de computação em nuvem.



Comercializado sob pagamento por uso.

NUVEM

Plataforma como Serviço (PaaS)

Conjuntos de software que trabalham para fornecer serviços.

Oferta de uma plataforma de computação em nuvem: Heroki, Microsoft Azure, Sales Force etc.

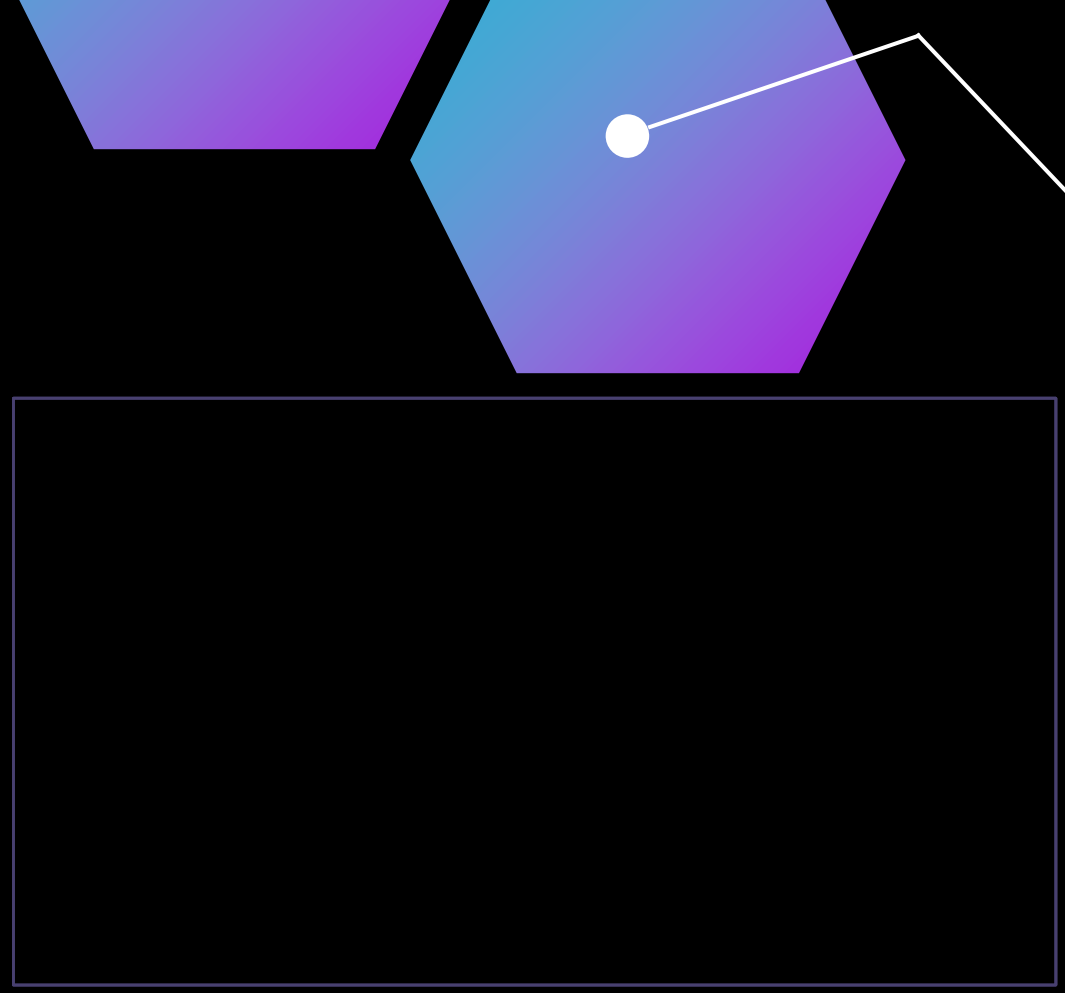
Podem ser entregues por meio da nuvem como plataforma.

Geralmente se concentram em segurança e escalabilidade.

NUVEM

Software como Serviço (SaaS)

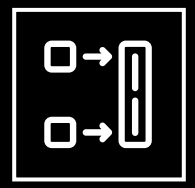
- Software sob demanda, ao invés de instalar nos clientes.
- Oferta de software para usuários finais de dentro da nuvem como Microsoft Office 365 e Adobe Creative Suite etc.
- Vantagens:
  - Atualizações, perfeitas para usuários finais;
  - Integração entre componentes.



NUVEM

Qualquer coisa como Serviço (XaaS)

Novas ofertas de nuvem. Anything as a Service (XaaS), como streaming etc.



Agrupamento do SaaS com o IaaS.

- Surgimento de um item comercializável, como Disaster Recovery.

NUVEM

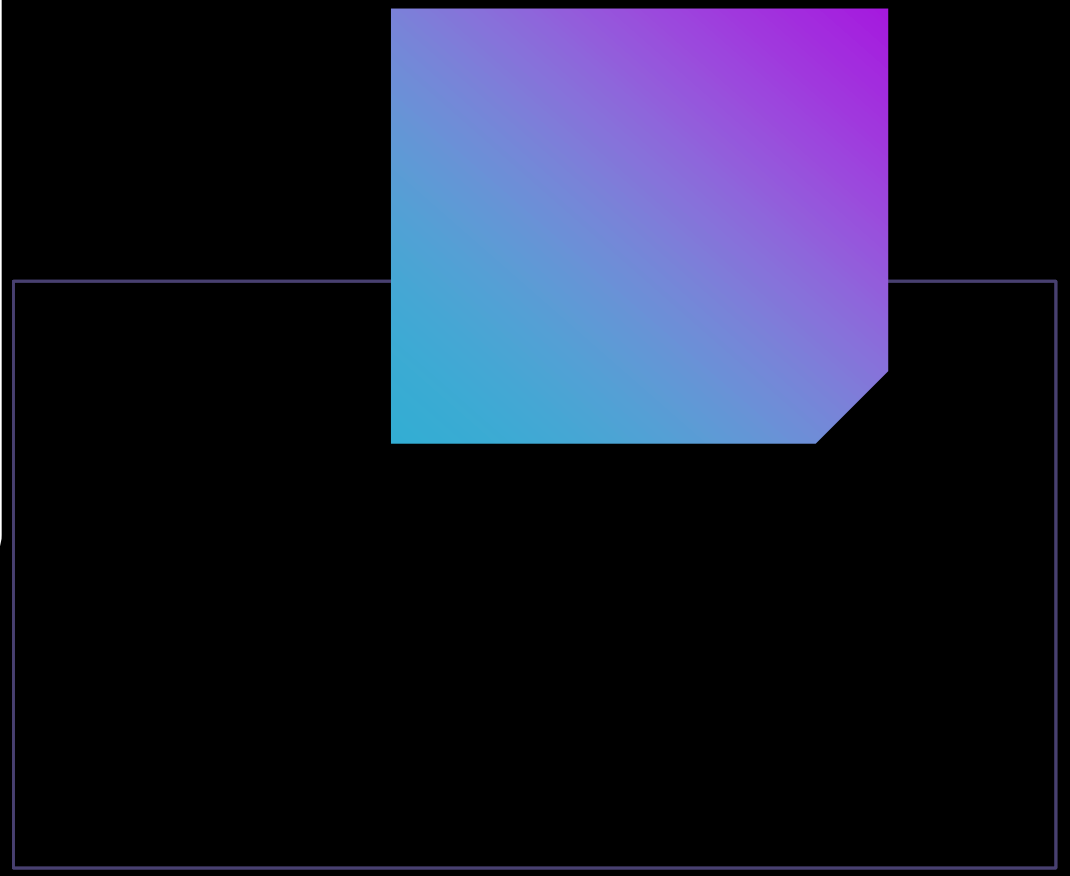
Nível de Controle nos Modelos de Hospedagem

Local Tradicional	Hosting	IaaS	PasS	SaaS	XaaS
Dados	Dados	Dados	Dados	Dados	Dados
Aplicações	Aplicações	Aplicações	Aplicações	Aplicações	Aplicações
Banco de Dados	Banco de Dados	Banco de Dados	Banco de Dados	Banco de Dados	Banco de Dados
Sistema Operacional	Sistema Operacional	Sistema Operacional	Sistema Operacional	Sistema Operacional	Sistema Operacional
Virtualização	Virtualização	Virtualização	Virtualização	Virtualização	Virtualização
Servidores Físicos	Servidores Físicos	Servidores Físicos	Servidores Físicos	Servidores Físicos	Servidores Físicos
Rede e Armazenamento	Rede e Armazenamento	Rede e Armazenamento	Rede e Armazenamento	Rede e Armazenamento	Rede e Armazenamento
Data Center	Data Center	Data Center	Data Center	Data Center	Data Center

NUVEM

Auto Gerenciado

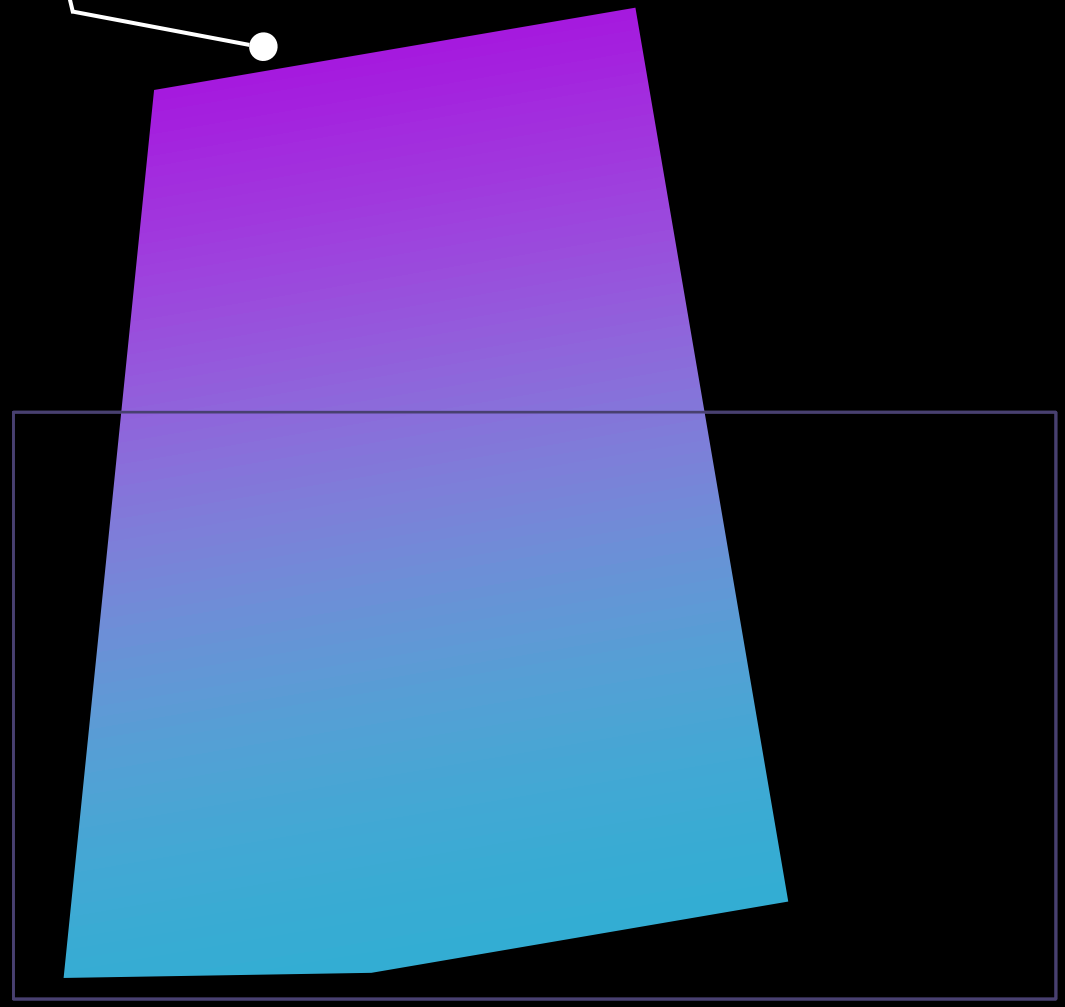
Gerenciado pelo Provedor da Nuvem



Pública

- Serviço de nuvem prestado em um sistema aberto.
- Pouca diferença arquitetônica entre pública e privada.

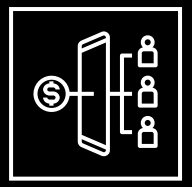
No quesito segurança, as restrições na pública são menores.



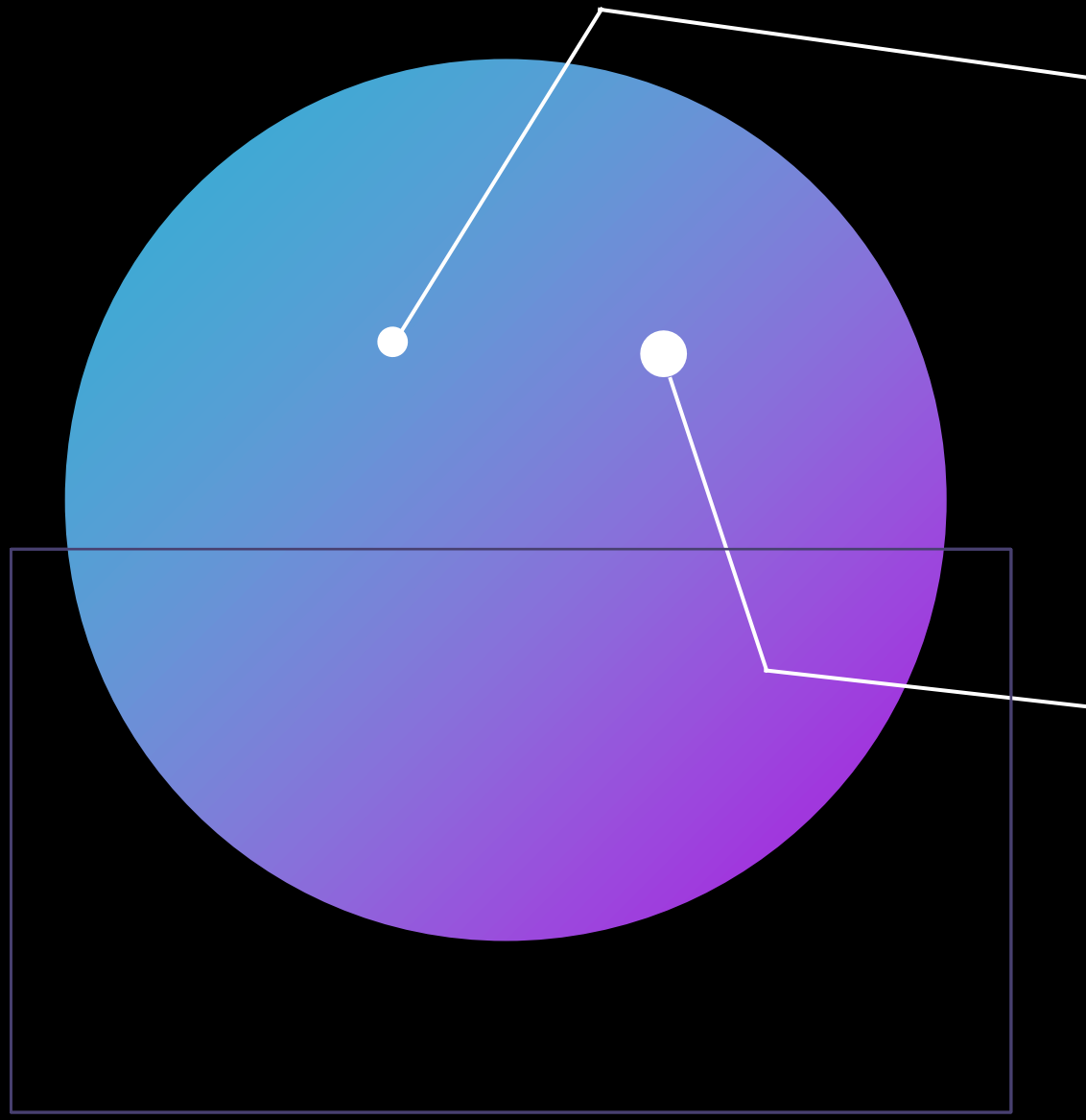
Comunitária

Várias organizações com interesses comuns compartilham um ambiente de nuvem.

- Exemplo: Entidades públicas e empresas.



Mecanismo que atrai pelo compartilhamento de custos.



Privada

- Recomendável para organizações sensíveis ao compartilhamento de recursos.

Mais cara.

Menos exposição;

Permite definir melhor a segurança;

Melhora o processamento;

Permite o manuseio de dados.

Híbrida

- Combinação entre a privada, pública e comunitária.
- Não é uma união, mas uma combinação!
  - Informações confidenciais podem ser armazenadas em uma nuvem privada, e outras podem estar na nuvem comunitária.

Provedores de Serviços em Nuvem (CSP)

- Em vários tamanhos e formas.
- Provedores de mega-nuvem:
  - Amazon;
  - Google;
  - Microsoft;
  - Oracle.
- É preciso levar em conta preços e termos contratuais.
- Se algo não estiver no contrato, não será feito.

Provedor de Serviço Gerenciado (MSP)/
Provedor de Serviço de Segurança Gerenciado (MSSP)

MSP – Controla remotamente a infraestrutura de TI, provisionamento, gerenciamento, monitoramento, backup etc.

MSSP - Terceiro que gerencia serviços de segurança, como IDS, Firewall, patches, gerenciamento de incidentes de SI etc.

Serviços gerenciados fornecem força a uma empresa por uma fração do custo.

Desvantagens dos Serviços Gerenciados:

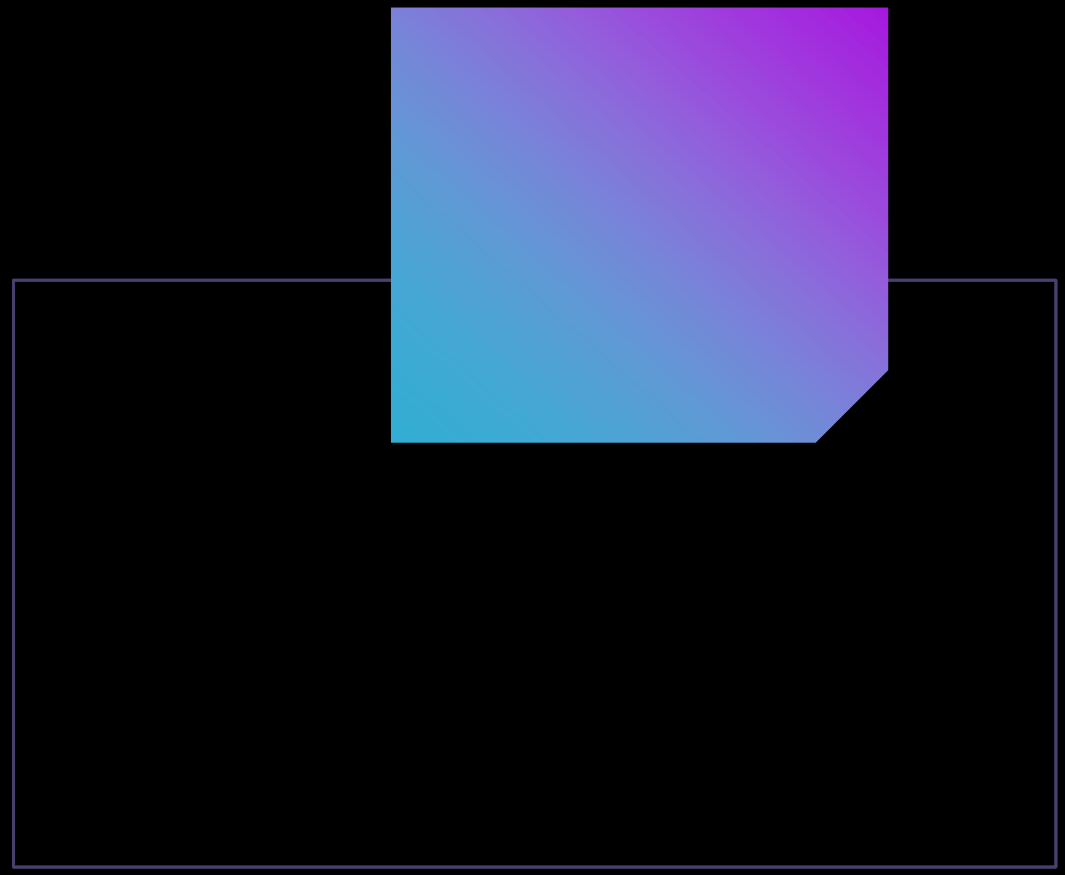
- Falta de flexibilidade;
- Falta de espaço para qualquer mudança.

On-Premises vs. Off-Premises

- On-premises = Sistema reside localmente.
- Pode ser uma máquina virtual (VM), armazenamento ou serviço.
- A organização tem controle do sistema.
- Desvantagens:
  - Requer recursos locais;
  - Não é fácil de escalar.
- "Na nuvem": Sistema distribuído em uma infraestrutura de forma remota e acessível por uma rede.

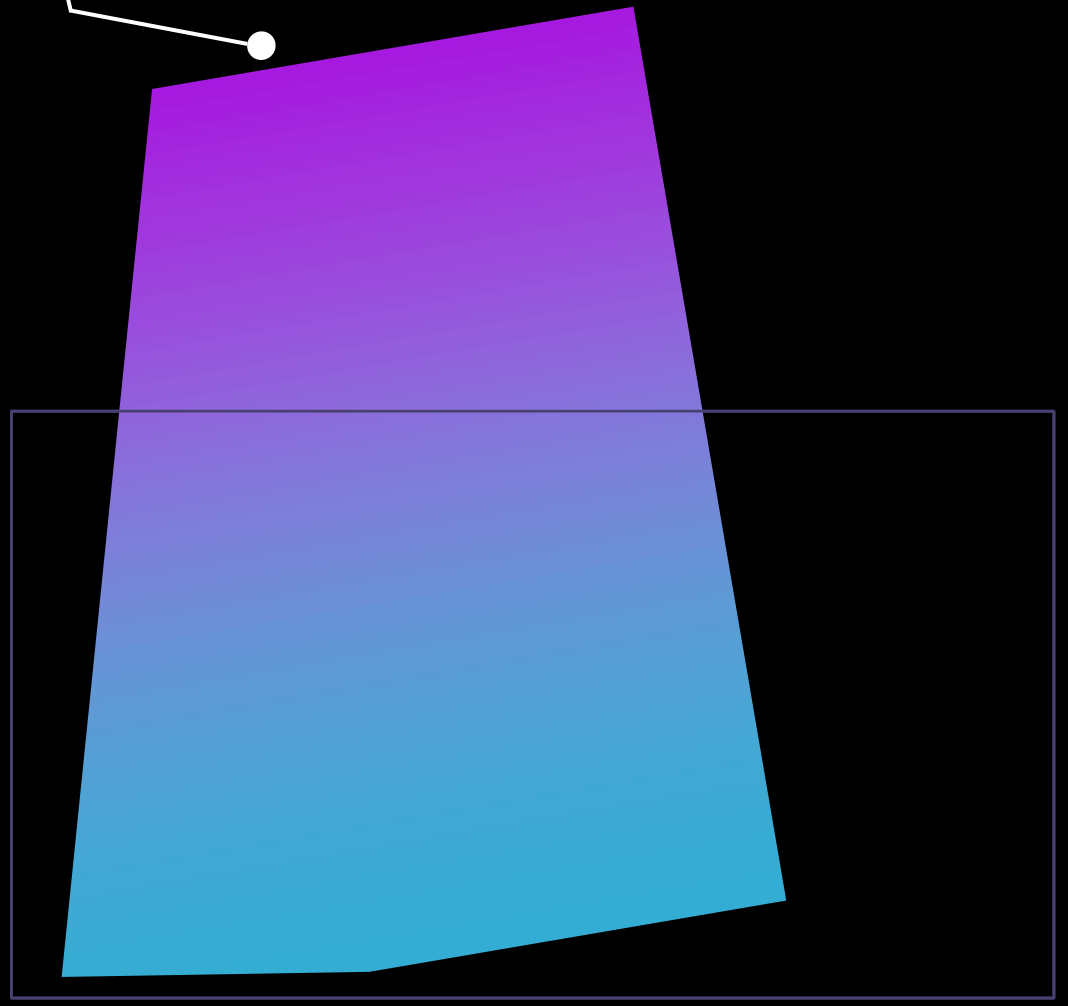
Fog Computing

- Processamento distribuído usando o computador de outra pessoa.
- Desenvolvida pela Cisco em 2014.
- Move parte do trabalho para o ambiente local.
- Gerencia problemas de latência, semelhante à computação de borda.
- Complemento da nuvem, e não um substituto.



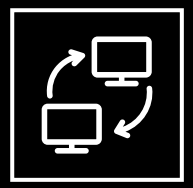
Computação de Borda

- Computação realizada na borda de uma rede (como roteadores e firewalls).
- Economiza banda larga, enfatiza a proximidade com os usuários finais.
- Impulsionada com a Internet das Coisas (IoT).
- Depende da "borda" e de um processamento em nível suficiente.
- Pode gerenciar o fluxo de dados e fazer a computação no trajeto.



Thin Client

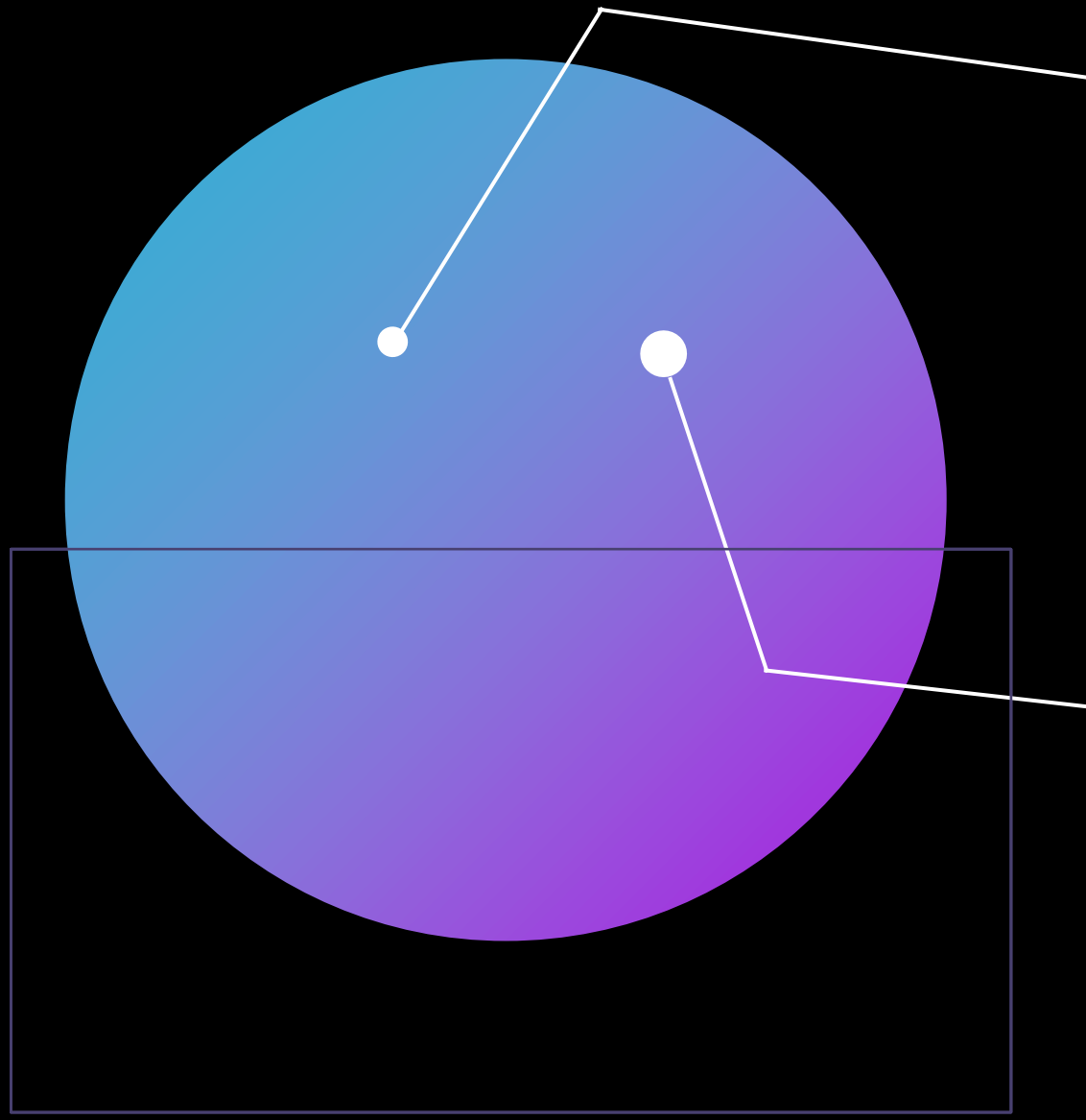
Recursos limitados.



Comunica-se com outra máquina.

Permite o acesso a um servidor com recursos apropriados.

Utiliza computação em nuvem e virtualização.



Contêineres

- Compartilha o kernel do S.O. do sistema host, deixando-o mais leve. Várias instâncias S.O. em uma único hardware.
- Podem compartilhar um S.O., mas separam:
  -  Threads de memória;
  -  CPU;
  -  Armazenamento.
- Evolução do conceito de VM, como o Docker.
- Um ambiente inteiro agrupado em um pacote:
  -  Aplicativo e suas dependências;
  -  Bibliotecas;
  -  Arquivos de configuração.
- Elimina as diferenças entre os ambientes de desenvolvimento, teste e produção.

NUVEM

Microsserviços/API

- API - Meio para especificar como alguém interage com um software.
- Se ele usa a API REST, a interface definida é um conjunto de quatro ações em HTTP:

GET;

POST;

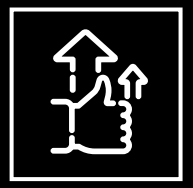
PUT;

DELETE.

- Microsserviços - Dividem o sistema em pequenos módulos. Muito útil para equipes ágeis.

Infraestrutura Como Código

Uso de arquivos de definição legíveis por máquina.



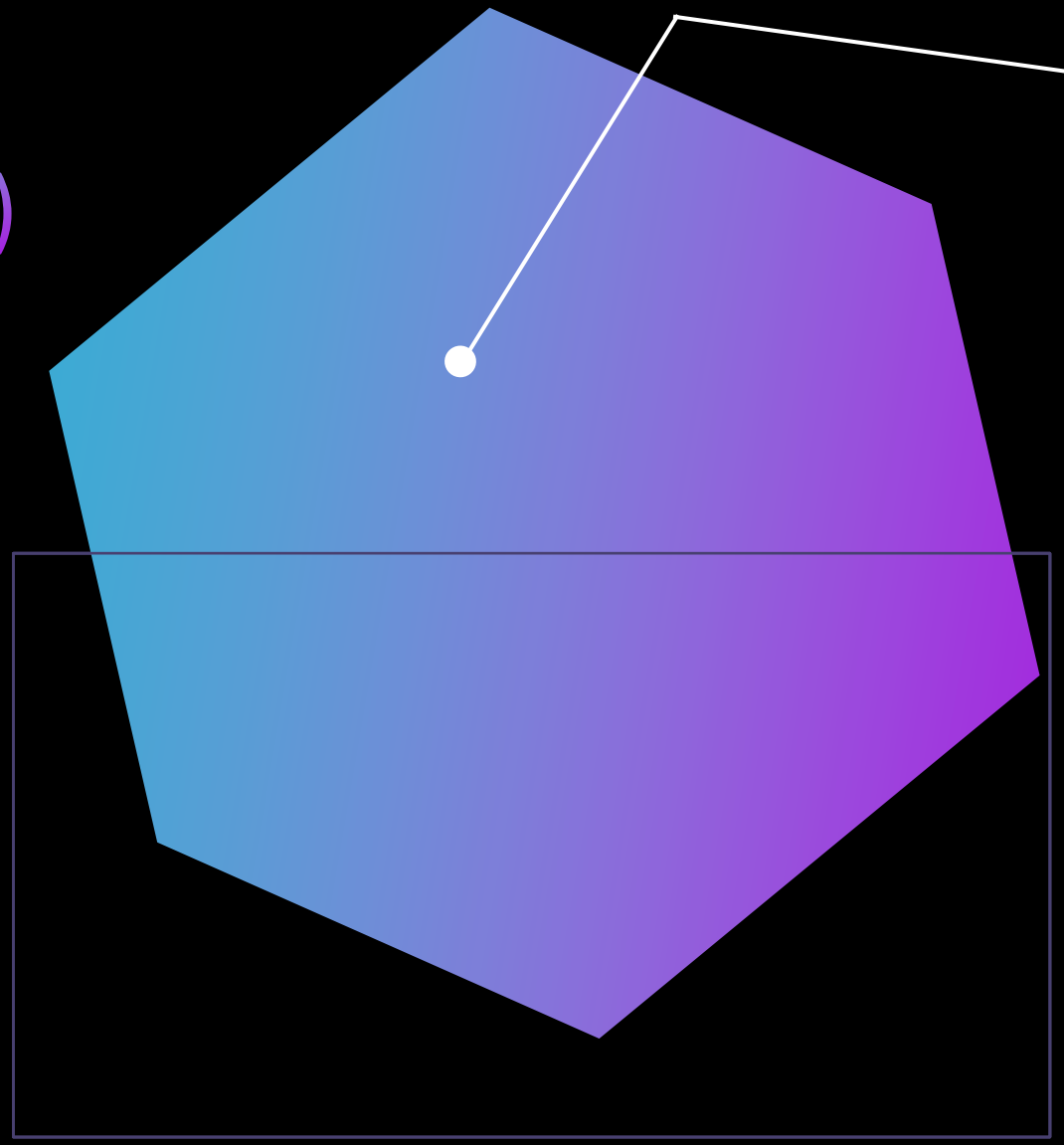
Vantagens:

- Flexibilidade;
- Escalabilidade.

Permite gerenciar hardware físico de forma programática.

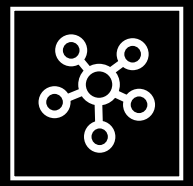
Rede Definida por Software (SDN)

- Forma de **gerenciar a configuração** do dispositivo de rede a partir de um ponto central.
  - Alterações na rede via software.
- Cria e controla uma rede virtual ou tradicional com:
  - Flexibilidade;
  - Programabilidade.
- Depende da função de rede (NFV): virtualiza serviços de rede, como roteadores, firewalls etc.



Visibilidade Definida por Software (SDV)

Para um dispositivo de rede operar com dados, ele deve ver o fluxo de dados.



Monitora o ambiente de rede com a capacidade de responder a incidentes de segurança em tempo real.

Vantagens:

- Flexibilidade no projeto por meio da malha SDN;
- Capacidade de reconfiguração em tempo real.

Arquitetura Sem Servidor

- Não precisa investir em hardware de servidor;
- Simplesmente cria uma instância de um serviço na nuvem (BD);
- Elasticidade e escalabilidade;
- Vantagens:
  - Provedores de nuvem podem fazer alterações por scripts automatizados;
  - Oferece suporte à integração de serviços.

NUVEM

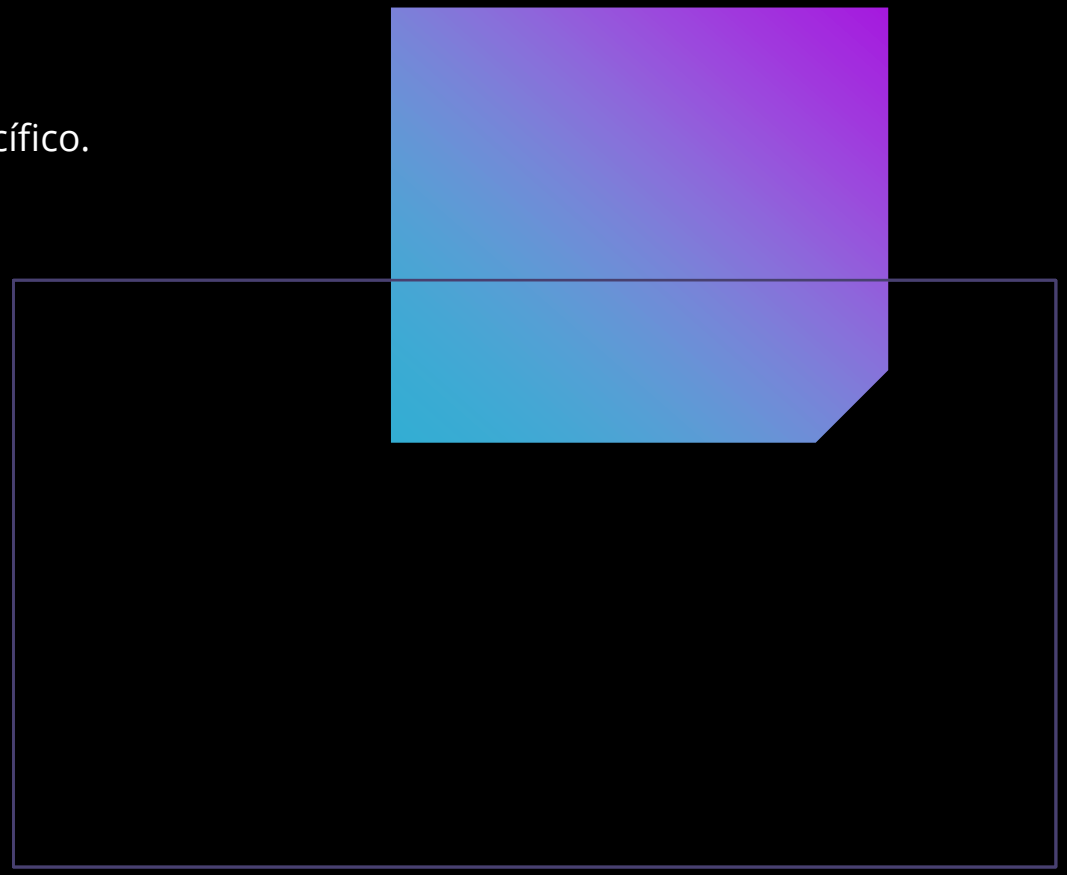
Integração de Serviços

- Permite que dados locais interajam com dados em nuvem.
- Conexão da infraestrutura e software como um serviço específico.
- Como se tudo estivesse conectado no mesmo local.
- A infraestrutura em nuvem consegue integrar serviços com um gateway de trânsito.

Scripts pré-projetados, de maneira mais escalável.

Economia de custos (muitos clientes);

Confiabilidade por conta da repetibilidade e reprodutibilidade.



NUVEM

Gateway de Trânsito

- Fornece um link seguro e privado para estender sua rede local para sua rede em nuvem.
- Conexão para interconectar nuvens privadas virtuais (VPCs) e redes locais.
- Vantagens:
  -  Definir e controlar a comunicação entre recursos na rede;
  -  Definir e controlar a comunicação entre recursos da própria infraestrutura.
- Implementados para dar suporte ao ambiente de nuvem.

NUVEM

Políticas de Recursos

- Quem pode criar ou ver uma VM, BD, aplicativo Web?
- Gerenciamento de recursos é feito através da política de recursos.
- Cada provedor tem uma maneira de interação com um menu de serviços.
- Com essa política, você pode:

Definir o que, onde e como os recursos são provisionados;

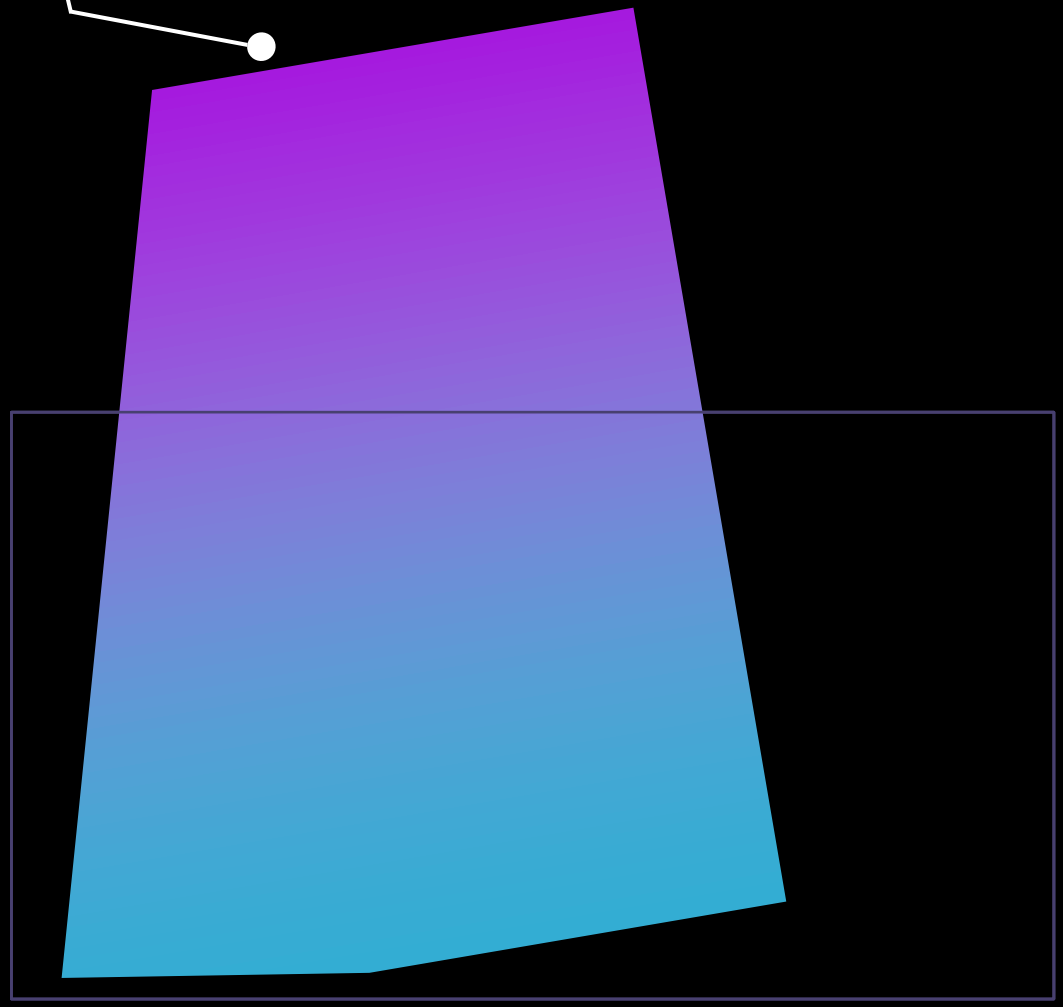
Definir restrições;

Gerenciar recursos;

Gerenciar custos (licenciamento).

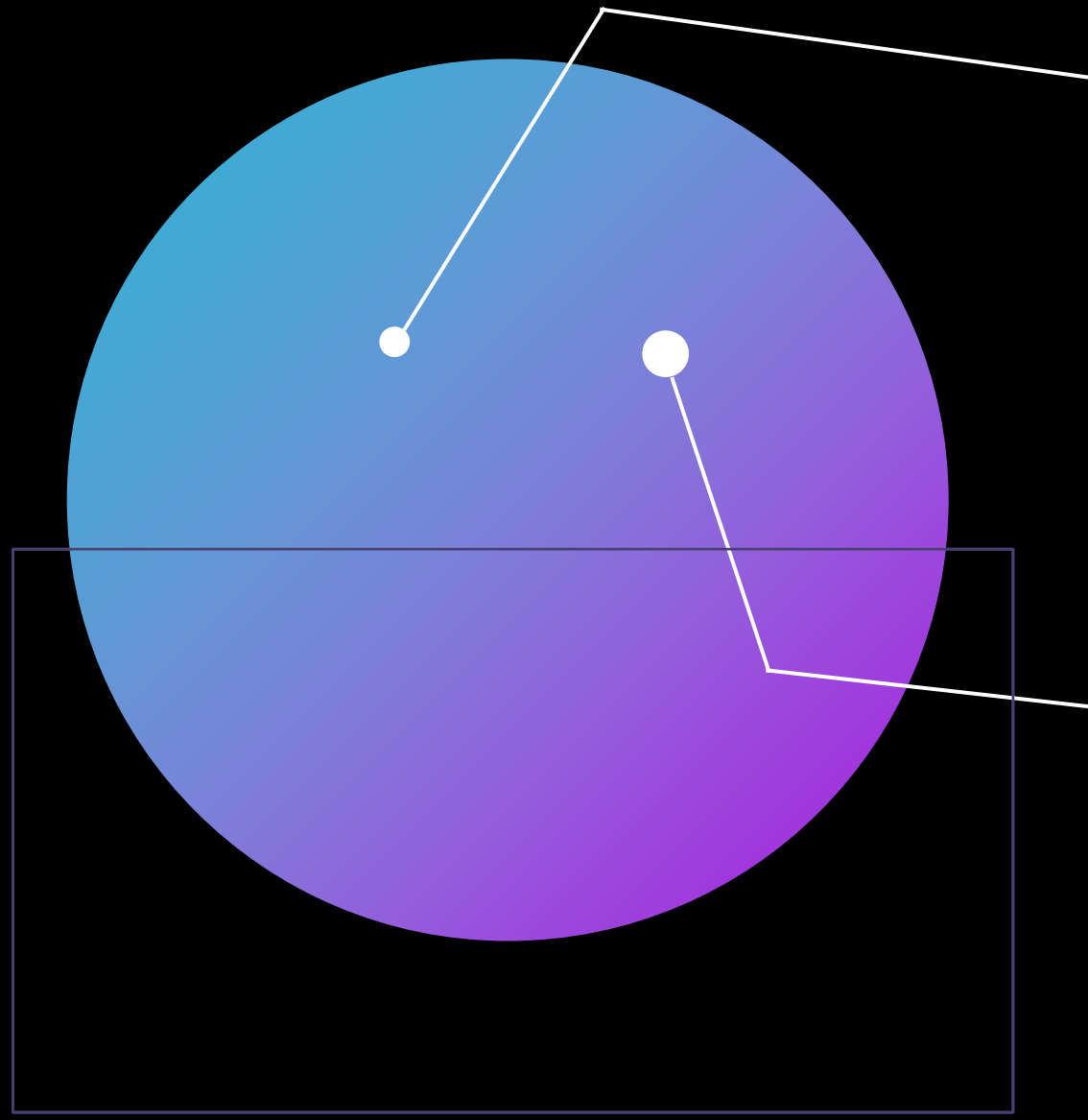
Virtualização

- Permite que um computador tenha mais de um sistema operacional.
- Capacidade de hospedar vários SOs em um único hardware.
- É preciso habilitar um Hypervisor em um computador host.
- Programa de baixo nível onde vários SOs são executados em um host.
- Vantagens:
  - Separação do software e hardware;
  - Economia e sustentabilidade.
- Máquinas virtuais = SOs convidados.



Hypervisor Tipo I

- Hypervisor sendo executados direto no hardware.
- Velocidade e eficiência. Controla os convidados.
- Exemplos de *bare-metal*:
  - KVM;
  - Xen;
  - Microsoft Windows Server Hyper-V;
  - Plataformas VMWare vSphere/ESXi.

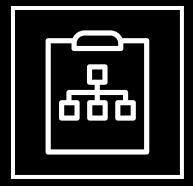


Hypervisor Tipo II

- Executados em cima de um sistema operacional host.
- Exemplos:
  -  VirtualBox (Oracle);
  -  VMware Player.
- Projetados para um número limitado de VMs.

Prevenção de Expansão de Máquinas Virtuais (VM) Sprawl

Disseminação e desorganização por falta de uma estrutura organizacional.



VMs são arquivos com uma cópia das estruturas de disco e memória. A criação delas pode ser **descontrolada.**

Expansão da VM = Estrutura desorganizada devido a facilidade de se criar uma VM.

Uma ferramenta de gerenciamento permite que os administradores gerenciem VMs e evitem a expansão.

Proteção Contra Fuga de VM

- Alguém acessando o SO do host a partir do SO convidado da VM.
- Software, malware ou invasor podem escapar de um VM.
- Uma fuga pode proporcionar ataques.
- Ambientes de VM de grande escala têm módulos específicos.
  - Conseguem detectar fuga;
  - Fornecem proteção para outros módulos.

OBRIGADO!

NUVEM