



Olá, Professor!  
Peço que realize a **avaliação do conteúdo** com o intuito de manter o nosso material sempre atualizado.

Avalie este  
conteúdo! 🚀 ✨



<https://bit.ly/451BDqS>



# Computação em nuvem



# Fundamentos de computação em nuvem



# — Computação em nuvem

## Conceitos da computação em nuvem



A computação em nuvem oferece serviços pagos com base no uso, desde armazenamento pessoal até terceirização de TI.

- Permite acesso a aplicativos e dados pela internet, sem instalação local, graças a servidores remotos.
- O termo "nuvem" refere-se à interligação de redes, tornando a localização dos dados e aplicativos invisível.
- Usuários podem acessar dados de qualquer lugar, eliminando a necessidade de estar em um local específico.



# — Computação em nuvem

## Utility computing

- Cloud computing é a evolução do utility computing, oferecendo TI sob demanda com baixo custo.
- Utility computing é uma etapa precursora para a computação em nuvem.



## — Utilizando a computação em nuvem

A computação em nuvem permite acesso flexível a dados e programas de qualquer lugar, através de infraestrutura de terceiros.

A infraestrutura em nuvem é redundante e resiliente, garantindo operação contínua mesmo em falhas.

Acesso a serviços em nuvem requer apenas um dispositivo conectado à internet e um navegador.

Oferece vantagens de terceirização de hardware e software, benéficas para empresas de diversos tamanhos.

# — Utilizando a computação em nuvem

## Vantagens da computação em nuvem

**Economia**

**Escalabilidade**

**Elasticidade**

**Atualização constante**

**Implantação rápida**

**Acesso global**

**Disponibilidade**

**Segurança**

## — Utilizando a computação em nuvem

### Desvantagens da computação em nuvem

**Perda de controle**

**Interrupção dos serviços  
em nuvem**

**Segurança**



# — Principais provedores de computação em nuvem



**Amazon Web Services  
(AWS)**



**Microsoft Azure**



**Google Cloud Platform**



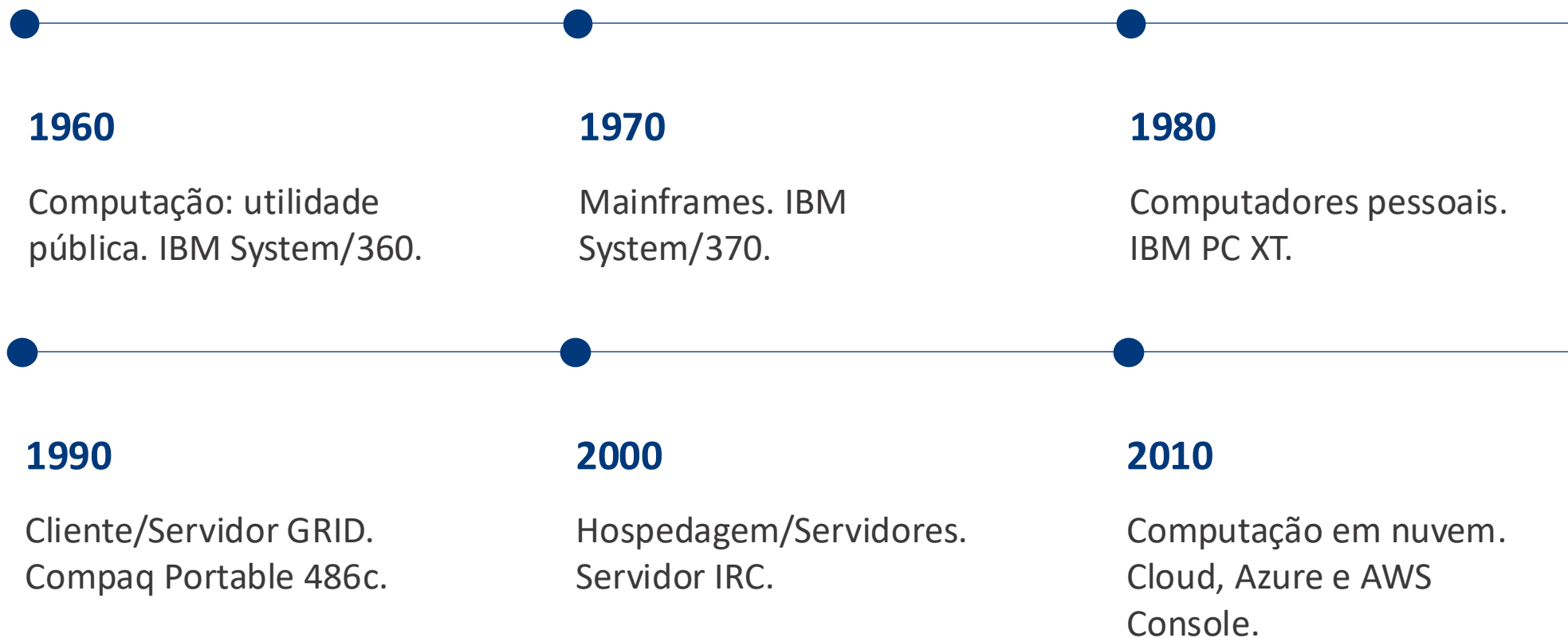
**IBM Cloud**



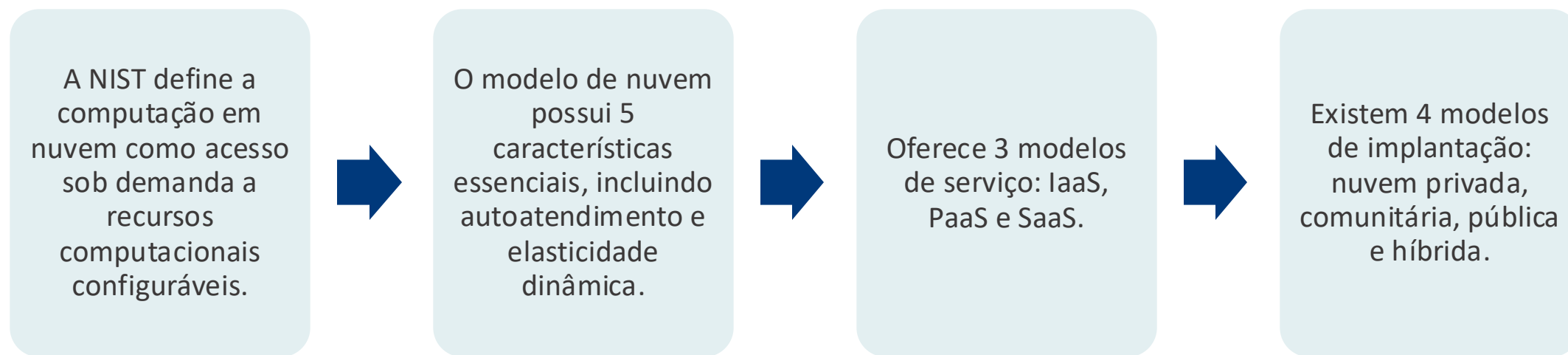
**Oracle Cloud**

# — Evolução histórica

Linha do tempo da evolução da tecnologia até a computação em nuvem:



## — Essência da computação em nuvem



# — Características essenciais da computação em nuvem

A computação em nuvem possui cinco características essenciais e determinantes para a tecnologia, são elas



On-demand self-service (autoatendimento sob demanda)



Broad network access (amplo acesso à rede)



Resource pooling (agrupamento de recursos)



Rapid elasticity (elasticidade dinâmica)



Measured service (serviço mensurável)

# — Características essenciais da computação em nuvem

## Camadas e atores na computação em nuvem

- Camada de infraestrutura: Fornece servidores, sistemas de armazenamento e rede.
- Camada de plataforma: Oferece serviços de aplicação para desenvolvimento e implementação.
- Camada de aplicação: Disponibiliza aplicações como serviços para os usuários.



### Aplicação

- Aplicações como serviço
- Usuários de serviços



### Plataforma

- Desenvolvimento de aplicações
- Prestadores de serviços



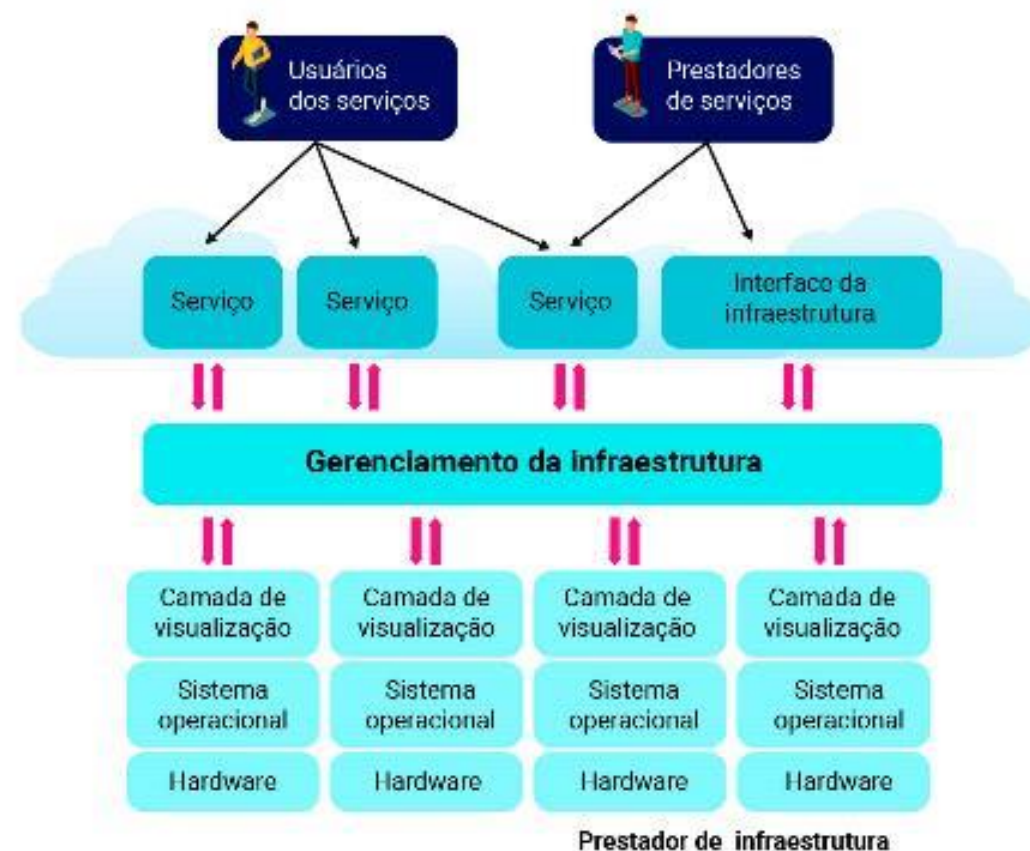
### Infraestrutura

- Serviços de rede e armazenamento
- Prestadores de infraestrutura

# — Características essenciais da computação em nuvem

## Camadas e atores na computação em nuvem

- Provedores de serviço: Desenvolvem e disponibilizam serviços na nuvem.
- Usuários da nuvem: Utilizam os serviços disponíveis na nuvem.
- Provedores de infraestrutura: Fornecem a infraestrutura necessária como serviço para os provedores de serviço.





# — Modelos de serviços para computação em nuvem

## Principais modelos de serviços

A computação em nuvem distribui os recursos na forma de serviços e podemos dividir em três cenários principais:

### **Infraestrutura como Serviço (IaaS)**

O usuário gerencia aplicativos e máquinas virtuais, o provedor cuida da infraestrutura do datacenter.

### **Plataforma como Serviço (PaaS)**

O usuário desenvolve aplicativos, o provedor fornece recursos de hardware e software.

### **Software como Serviço (SaaS)**

O usuário utiliza aplicativos, o provedor gerencia toda a pilha de aplicativos.

# — Modelos de serviços para computação em nuvem

## Principais modelos de serviços



# — Modelos de serviços para computação em nuvem

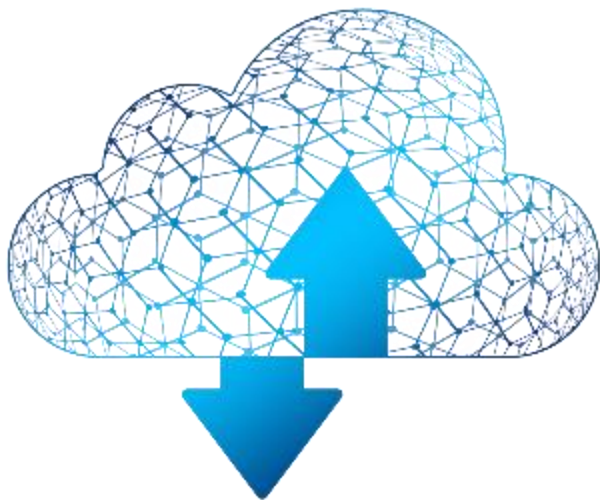
## Outros modelos de serviços

- **DRaaS (Recuperação de Desastres como Serviço):** Focado na segurança da informação, envolve a replicação de servidores, dados e aplicações.
- **CaaS (Comunicação como Serviço):** Oferece soluções de comunicação, como VoIP, mensagens e streaming de vídeos, como serviço.
- **FaaS (Função como Serviço), DBaaS (Banco de Dados como Serviço), MaaS (Malware como Serviço):** Outros modelos de serviços que aproveitam a capacidade infinita da nuvem.



# — Nuvens públicas e privadas

## Modelos de implantação para computação em nuvem



Três modelos principais na nuvem definem local de dados e interação do usuário.

- Exploraremos os modelos detalhadamente e outros mais simples.
- Nuvem: público, privado e híbrido, cada um com características únicas.
- Esses modelos moldam como a computação em nuvem é implantada e utilizada.

## — Public cloud – nuvem pública

- Nuvem pública: Provedores oferecem recursos para o público via internet.
- Acesso aberto a qualquer usuário, pagamento conforme uso.
- Menos controle dos usuários sobre seus dados.
- Exemplos: AWS, Azure, Google Cloud.



## — Public cloud – nuvem pública

As vantagens desse modelo são:

**Preço**

**Facilidade de contratação,  
configuração e  
infraestrutura**

**Escalabilidade**

**Performance**



## — Public cloud – nuvem pública

Algumas desvantagens são:

**Segurança**

**Controle feito por  
terceiros**

**Requisitos legais**

## — Private cloud – nuvem privada



Nuvem privada: Ambiente exclusivo para um único usuário ou empresa.

Localizado atrás do firewall do usuário, pode ser **on premise** ou **off premise**.

Oferece benefícios da nuvem pública, mas sem compartilhamento.

Ideal para dados sensíveis e organizações com rigoroso controle interno.

## — Private cloud – nuvem privada

Algumas vantagens desse modelo são:

**Disponibilidade**

**Customização de  
infraestrutura**

**Suporte exclusivo**

**Segurança**

## — Nuvens híbridas e outros tipos

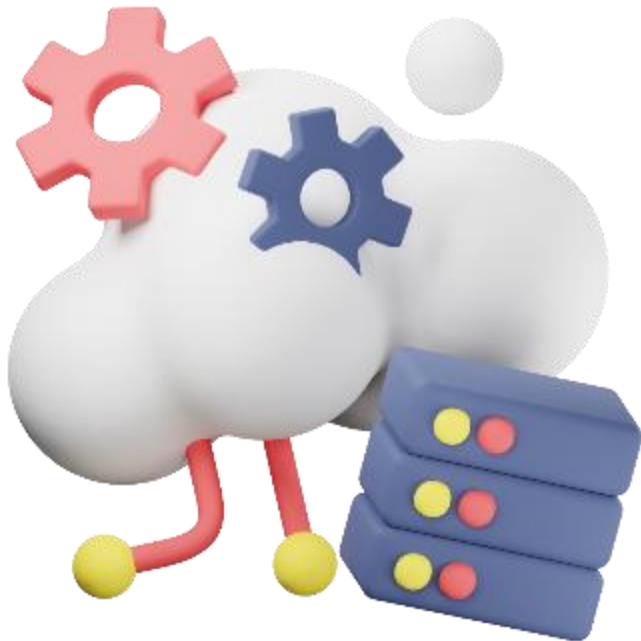
### Hybrid cloud – nuvem híbrida

- Nuvem híbrida: Combina serviços da nuvem pública e privada.
- Permite manter dados cruciais na nuvem privada e outros na pública.
- Melhora performance e controle, reduz tempo de escalabilidade.
- Flexibilidade e versatilidade para atender demandas internas.



## — Nuvens híbridas e outros tipos

### Community Cloud – nuvem comunitária



- Nuvem comunitária: Compartilhada por empresas com interesses comuns.
- Pode ser administrada internamente ou por terceiros.
- Semelhante à nuvem pública, mas com número reduzido de usuários.
- Configurável de acordo com os objetivos das organizações.

## — Nuvens híbridas e outros tipos

### Distributed Cloud – nuvem distribuída

- Nuvem distribuída: Acionada em diferentes localidades, com servidores conectados a uma rede central.
- Maximiza disponibilidade de recursos e reduz latência.
- Ideal para garantir alta performance e acessibilidade.





# — Infraestrutura on premise x em nuvem

## Aspectos de infraestrutura de TI on premise e em nuvem

### On Premise

- Em Nuvem Servidores locais e alto investimento inicial.
- Manutenção interna e controle total.
- Escalabilidade limitada e custos fixos.



### Em Nuvem

- Serviços terceirizados e custos variáveis.
- Manutenção gerenciada e escalabilidade facilitada.
- Menos controle direto, mas responsabilidade compartilhada.

# — Infraestrutura on premise x em nuvem

## Tipo de servidor

### On Premise

O servidor é físico, pois existe um servidor principal instalado na empresa na qual os computadores estão conectados.



### Em Nuvem

Os dados e os serviços estão na nuvem, ou seja, estão guardados em um provedor de nuvem, uma empresa especializada com poder computacional disponível para alugar.

# — Infraestrutura on premise x em nuvem

## Forma de acesso

### On Premise

O acesso aos dados só é possível se o computador estiver devidamente configurado e interligado ao servidor principal.



### Em Nuvem

O acesso é realizado pela plataforma disponibilizada pelo provedor de nuvem.

## — Infraestrutura on premise x em nuvem

### Flexibilidade de armazenamento

#### On Premise

A capacidade de armazenamento é contratada inicialmente por um volume específico e, no caso de uma necessidade de crescimento, será necessário adquirir softwares e hardwares, além de uma equipe de TIC para realizar a instalação.



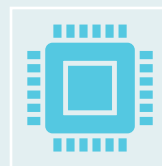
#### Em Nuvem

Ao se contratar os recursos do provedor de nuvem, é possível aumentar ou diminuir o espaço consumido. Assim, a flexibilidade se torna mais rápida e mais barata.

# — A importância da virtualização



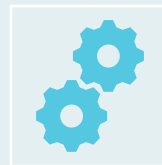
A computação em nuvem transforma como empresas acessam recursos de TI pela internet.



Provedores gerenciam infraestrutura e serviços, acessíveis remotamente de vários dispositivos.



A virtualização, junto com outras tecnologias, é essencial para a computação em nuvem.



Novo modelo integra tendências como serverless computing e software como serviço.

# — A importância da virtualização

## Virtualização

- Virtualização permite rodar múltiplos sistemas em uma única máquina.
- Compartilha recursos e é gerenciada por um hypervisor.
- **Existem tipos:** bare-metal (hardware direto) e hosted (software).
- Escolha depende das necessidades e compatibilidade de hardware.

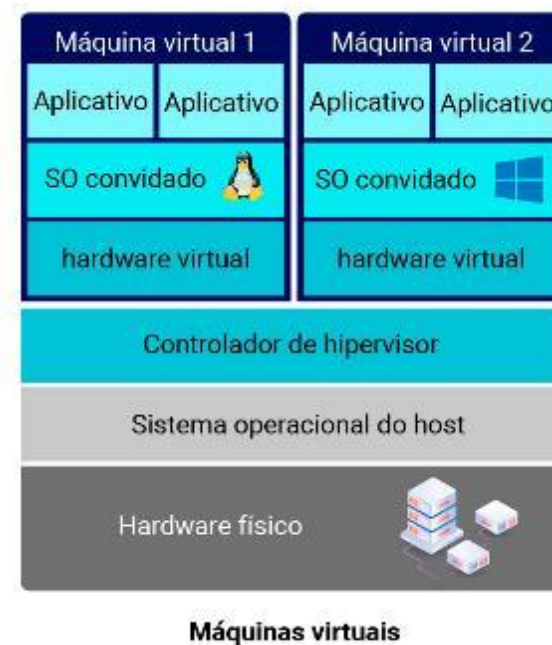
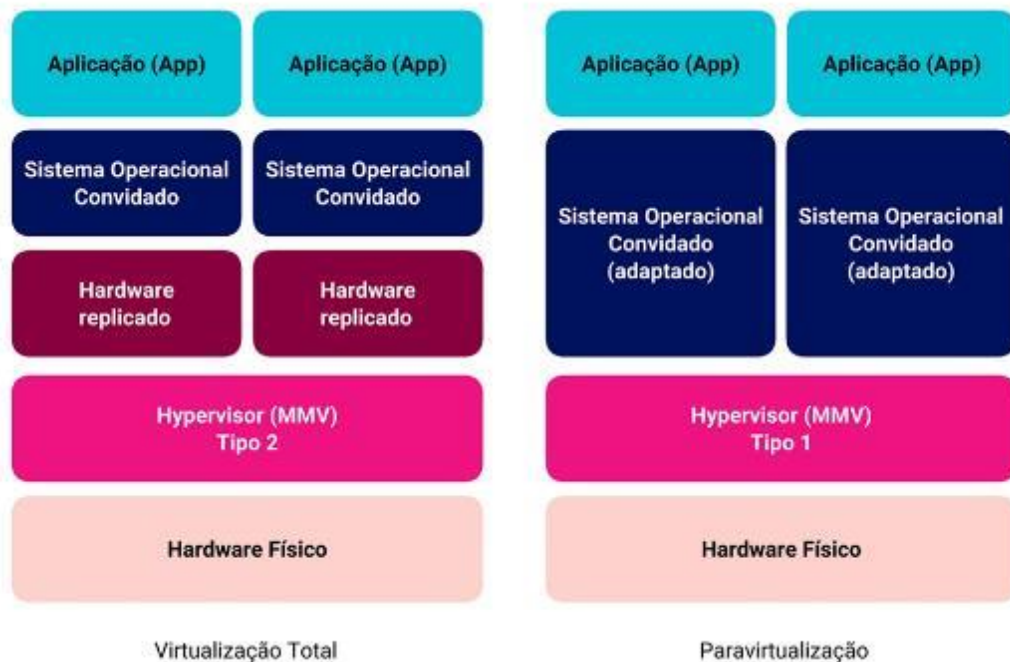




# — A importância da virtualização

## Virtualização

Os hypervisores tipo 1 e tipo 2 irão definir dois tipos de virtualização: paravirtualização e virtualização completa.



# — Virtualização baseada em contêineres

## Containerização



Containerização é método para executar aplicativos distribuídos sem VMs completas.



Contêineres compartilham kernel, são mais leves e consomem menos recursos que VMs.



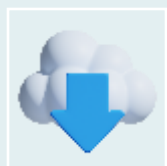
Evolução desde Unix V7 nos anos 70 até Docker na computação em nuvem.



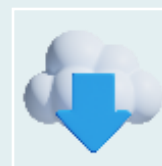
Contêineres isolados, independem de sistemas operacionais, facilitando implantação de aplicativos.

# — Serverless computing e ASP

## Computação sem servidor (serverless computing)



Serverless computing permite hospedar funções sem configurar servidores.



Baseado no conceito de Function as a Service (FaaS).



Elimina a necessidade de gerenciamento de servidores, focando em eventos e execução de funções.



Nasceu com a plataforma Zimki em 2006 e é uma nova arquitetura na computação em nuvem.

# — Serverless computing e ASP

## Computação sem servidor (serverless computing)

Entre os diferenciais dessa solução, podemos destacar:

### **Baixo custo**

São cobradas por uso: isso significa que você só vai pagar aquilo que realmente está utilizando.

### **Redução de código**

É menos complexa, sem a necessidade de ter um sistema back-end de várias camadas.

# — Serverless computing e ASP

## Computação sem servidor (serverless computing)

Confira a diferença entre as tecnologias



Máquinas virtuais



Contêineres



Sem servidor

# — Serverless computing e ASP

## Provedor de serviços de aplicação (ASP)



Provedor de Serviços de Aplicação (ASP) oferece software e aplicativos via internet.



Os usuários alugam aplicativos de terceiros, em vez de possuir software e hardware.



Pagamento de assinatura conforme a necessidade, reduzindo custos e complexidade.



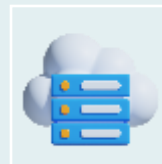
Exemplos incluem webmail e serviços de armazenamento de documentos online.

# — Computação em grade e utility computing

## Grid computing



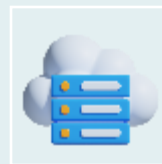
Grid computing: Agrupa servidores para formar uma grande infraestrutura de computação.



Divide e distribui partes de programas para milhares de computadores.



Possibilita o compartilhamento dinâmico de recursos geograficamente distribuídos.



Melhora a eficiência, processamento paralelo e confiabilidade. Distingue-se de clusters por seu gerenciamento descentralizado.

# — Computação em grade e utility computing

## Utility computing



Utility computing é um modelo sob demanda que permite contratar recursos de TI conforme necessidade.

- Comparado às empresas públicas de água e eletricidade, o cliente paga pelo que consome.
- Potencializa otimização de infraestrutura e reduz custos fixos não utilizados.
- Oferece capacidade temporária de processamento e armazenamento de dados.



# Arquitetura de computação em nuvem



## — Aspectos da infraestrutura de TI

- **Infraestrutura On Premise:** Recursos de TI mantidos internamente pela organização, custos iniciais altos, gestão complexa, menos escalabilidade.
- **Computação em Nuvem:** Recursos fornecidos por provedores via internet, escalável, custos iniciais baixos, gerenciamento simplificado, custo de manutenção reduzido.



# — Aspectos da infraestrutura de TI

## Infraestrutura em nuvem

As três principais camadas de serviço da infraestrutura em nuvem típica consistem em:



**Camada de servidor**



**Camada de  
armazenamento**



**Camada de rede**

# — Aspectos da infraestrutura de TI

## Características da infraestrutura em nuvem



Na computação em nuvem, a arquitetura é essencial para atender a requisitos como segurança e confiabilidade.



A arquitetura descreve as características e funções do serviço, enquanto a implementação se concentra na criação do serviço.



A arquitetura define como os elementos funcionais estão organizados e como a computação em nuvem opera.



Elementos principais incluem usuários geograficamente dispersos, provedores de serviços e canais de comunicação.

# — Aspectos da infraestrutura de TI

## Componentes da infraestrutura em nuvem

Principais componentes da arquitetura em nuvem:

**Hardware do servidor**

**Virtualização**

**Modelos de serviço**

**Gerenciamento de nuvem**

**Redes em nuvem**

**Segurança em nuvem**

# — Aspectos da infraestrutura de TI

## Grandes grupos de componentes da arquitetura

Os grandes grupos que podemos inserir os componentes da arquitetura são:



**Front end**

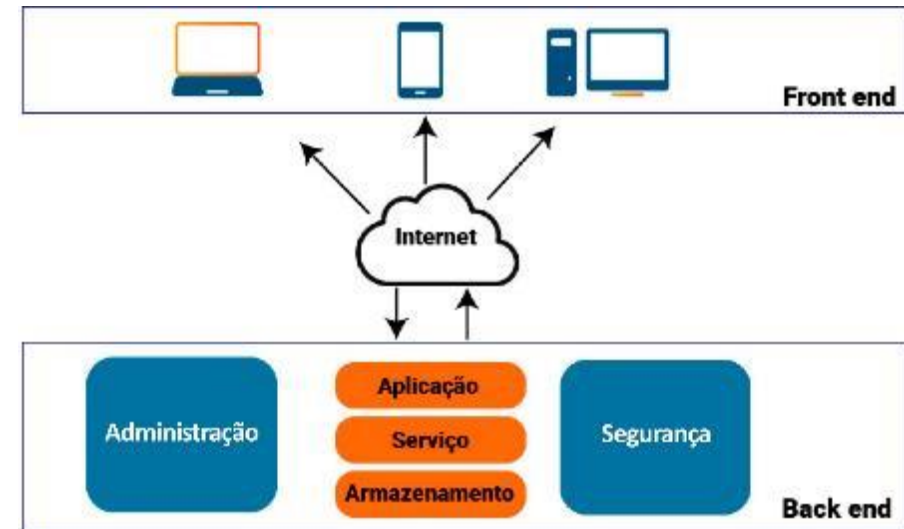
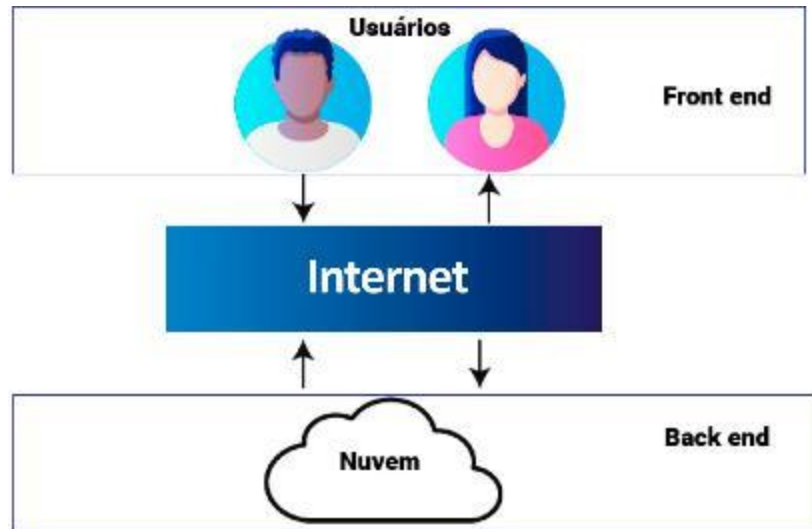


**Back end**

# — Aspectos da infraestrutura de TI

## Grandes grupos de componentes da arquitetura

Componentes da arquitetura de computação em nuvem:

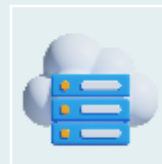


# — Infraestrutura dos datacenters

## Organização física dos datacenters



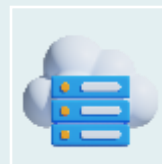
Datacenters abrigam servidores e dispositivos de armazenamento de forma segura.



Redes de alto desempenho interconectam servidores e dispositivos de armazenamento.



Componentes de rede no back end incluem switches, roteadores e modems.

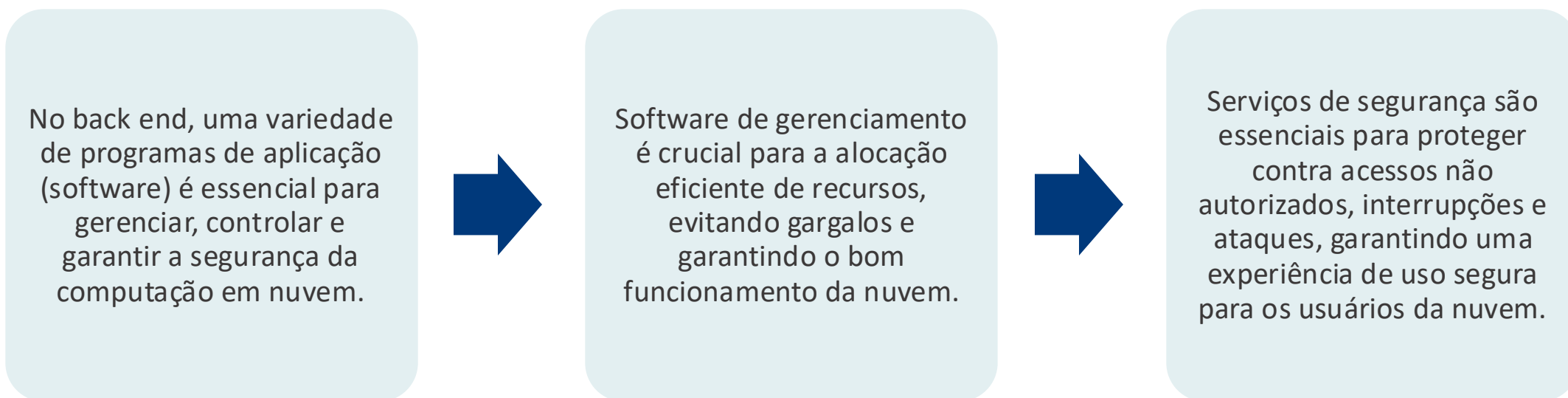


Alguns provedores de serviços de nuvem também oferecem serviços de rede, aliviando os usuários da tarefa de manutenção da rede.



# — Infraestrutura dos datacenters

## Organização lógica dos datacenters



# — Camada de servidores

## Conceitos

- A camada de servidores hospeda serviços e dados em infraestruturas de TI.
- Ela requer monitoramento, gerenciamento, otimização de desempenho e segurança.
- Ferramentas de administração de servidor são essenciais.
- Garantir o funcionamento eficaz da camada de servidores é fundamental.

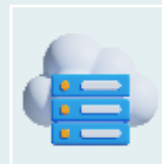


# — Camada de servidores

## Administração de camada de servidores



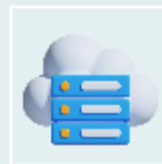
Administração de servidores envolve monitoramento, segurança, configuração e automação.



Ferramentas de gerenciamento, configuração e monitoramento são essenciais.



Controle de acesso, documentação e segurança são componentes importantes.



Automatização de tarefas, como backup, é fundamental para a eficiência.

## — Camada de servidores

### Plataforma de administração de camada de servidores

Os principais provedores possuem soluções que permitem criação, administração e gerenciamento de servidores:



**Amazon Web Services  
(AWS)**



**Microsoft Azure**



**Google Cloud  
Platform**



**Microsoft Azure**

## — Serviços em nuvem



Serviços em nuvem envolvem recursos de software e hardware entregues pela internet.



Isso permite aos usuários acessar computação, armazenamento e serviços de aplicativos sem gerenciar infraestrutura.



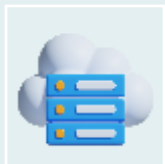
Exemplos incluem armazenamento, computação, infraestrutura, plataforma, análise e desenvolvimento na nuvem.



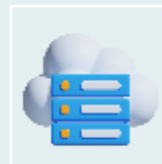
Os serviços em nuvem oferecem flexibilidade e escalabilidade aos usuários de TI.

# — Tipos de serviços em nuvem

## Serviço de computação em nuvem



Serviço de computação em nuvem oferece acesso remoto a recursos de computação pela internet.



Provedores de serviços mantêm servidores remotos, proporcionando escalabilidade e flexibilidade.



O back end (provedor) inclui servidores, armazenamento, máquinas virtuais e segurança.



O serviço é acessado por meio do front end (interface do usuário), coordenando as ações do usuário com os recursos do back end.

# — Tipos de serviços em nuvem

## Serviço de armazenamento



Serviço de armazenamento na nuvem permite o armazenamento e acesso a dados remotos pela internet.



Oferece flexibilidade e escalabilidade, permitindo que empresas adicionem ou removam recursos conforme necessário.



Melhora a segurança ao armazenar dados em servidores seguros acessíveis apenas por usuários autorizados.



Utiliza discos rígidos (HD), unidades de estado sólido (SSD) e, mais recentemente, memória Optane para armazenamento de dados.

# — Tipos de serviços em nuvem

## Serviço de compartilhamento

- Compartilhamento de dados em sistemas de nuvem é gerenciado por protocolos como CIFS e NFS.
- Esses protocolos permitem compartilhar recursos, como armazenamento de dados.
- A infraestrutura de nuvem usa servidores potentes com processadores Intel Xeon ou AMD Opteron.
- O compartilhamento de dados em nuvem é essencial para atender às necessidades de armazenamento.





# — Tipos de serviços em nuvem

## Emprego de novas tecnologias

Servidores utilizam GPUs (placas de vídeo) para aumentar o poder de processamento.

Tecnologias específicas, como o Google Tensor Processing Unit (ASICs), são usadas para tarefas de inteligência artificial na nuvem.

Essas inovações aprimoram o desempenho e a eficiência dos servidores.

As novas tecnologias oferecem soluções avançadas para diversas necessidades de processamento de dados.

# — Solução IaaS

## IaaS (Infraestrutura como Serviço)

### Cenário de elasticidade

O IaaS (Infraestrutura como Serviço) fornece equipamentos de computação e infraestrutura para criar aplicativos e serviços na nuvem.

Inclui servidores virtuais, sistemas de armazenamento, ferramentas de gerenciamento de dados e balanceamento de carga.

Também pode envolver software, como plataformas de orquestração de nuvem, para gerenciar vários provedores de serviços de nuvem.

Oferece benefícios como escalabilidade, alta disponibilidade, elasticidade e suporte para cenários multicloud e cloud híbrido.

# — Solução IaaS

## IaaS (Infraestrutura como Serviço)

### Cenário de balanceamento de carga



Elasticidade no IaaS permite adicionar recursos rapidamente para atender às demandas.



Ideal para empresas que buscam agilidade e economia na gestão de recursos.



Facilita licenciamento e remoção ágil de recursos, reduzindo custos operacionais.



Oferece flexibilidade para dimensionar vertical ou horizontalmente, otimizando a eficiência dos recursos.

# — Solução IaaS

## IaaS (Infraestrutura como Serviço)

### Cenário de alta disponibilidade

Ações que podem ser tomadas para permitir a alta disponibilidade:

**Replicação de dados**

**Balanceamento de carga**

**Uso de redundância**

**Monitoramento contínuo**

**Atualizações frequentes**

# — Solução IaaS

## Cenário multcloud e cloud híbrido

### Cenário Multicloud

- Uso de vários provedores em um ambiente.
- Orquestração centralizada com Kubernetes ou OpenStack.



### Cenário de Cloud Híbrido

- Combina nuvem pública e privada.
- Usa servidores físicos e serviços de nuvem como S3 e Elastic Load Balancer.
- Suporta sistemas de gerenciamento de dados, como MongoDB.

# — Edge computing

## O que é edge computing?

- Edge computing é processamento de dados localmente, reduzindo latência, melhorando segurança e economizando largura de banda.
- Ideal para IoT ao processar dados localmente e enviar apenas o necessário para a nuvem.



# — Edge computing

## Quando usar edge computing?



Necessitar processar dados onde são gerados, para maior eficiência.



Tiver aplicações iot que exigem decisões rápidas e ações imediatas.



Precisar de análise de dados em tempo real e serviços de resposta rápida.



Quiser reduzir problemas de largura de banda ao processar localmente.

# — Edge computing

## Edge computing e serverless

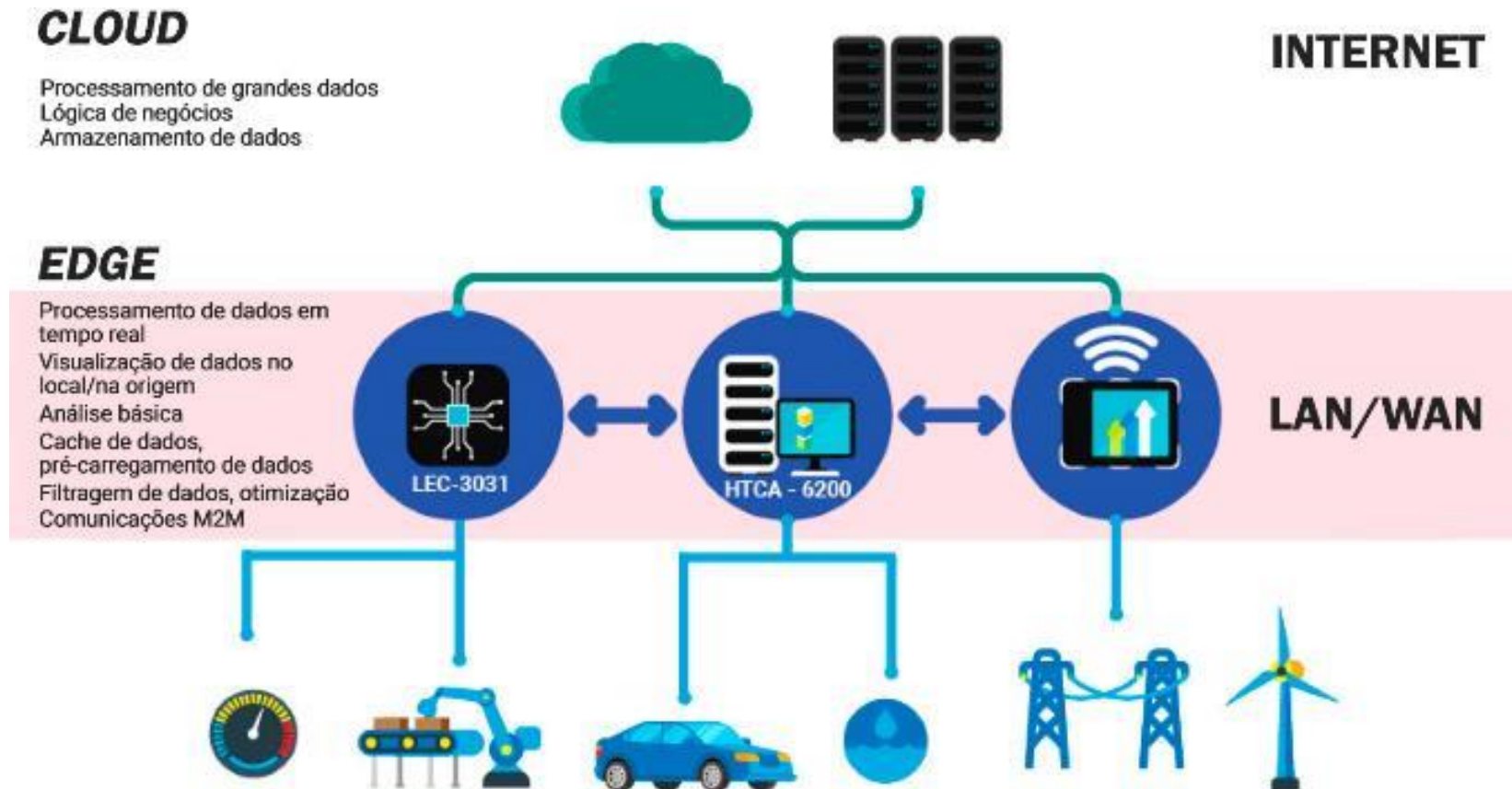
- Serverless separa infraestrutura, permitindo foco em código.
- Ideal para ambientes altamente distribuídos como edge computing.
- Permite construir e executar funções de edge computing com eficiência.
- Reduz complexidade e acelera o desenvolvimento de aplicações em ambientes de edge computing.





# — Edge computing

## Edge computing e serverless



# — Migração para nuvem

Quando migrar para a nuvem?

Quando sua infraestrutura  
está ultrapassada

Quando você precisa  
escalar rapidamente

Quando você precisa  
acessar de qualquer lugar

Quando você precisa  
economizar dinheiro

Quando você precisa de  
maior segurança

# — Migração para nuvem

## Estratégia para migração

**Rehost (Re-hospedar)**

**Replatform  
(Replataforma)**

**Repurchase (Recompra)**

**Refactoring/Re-  
architecting  
(Refatorar/Rearquitetar)**

**Retire (Aposentar)**

**Retain (Reter)**

**Relocate (Realocação)**

# Segurança em computação em nuvem



# — Características essenciais

NIST define serviços de nuvem por 5 características essenciais:

**On-demand self-service**

**Broad network access**

**Resource pooling**

**Rapid elasticity**

**Measured service**

# — Modelos de Serviço

NIST destaca três modelos de serviço possíveis:

## **Software as a service (SaaS)**

Provedor oferece aplicativos na nuvem, gerenciando infraestrutura, com configuração mínima pelo cliente.

## **Platform as a service (PaaS)**

Permite aos clientes desenvolverem e implantarem seus aplicativos na nuvem, sem gerenciar a infraestrutura subjacente.

## **Infrastructure as a service (IaaS)**

Oferece recursos de processamento, armazenamento e rede, permitindo que o cliente implante softwares e sistemas, mas não gerencie a infraestrutura subjacente.

# — Modelos de Implantação

A publicação 800-145 do NIST relaciona ainda **quatro modelos de implantação** para os serviços em nuvem.



**Private cloud**



**Community cloud**



**Public cloud**



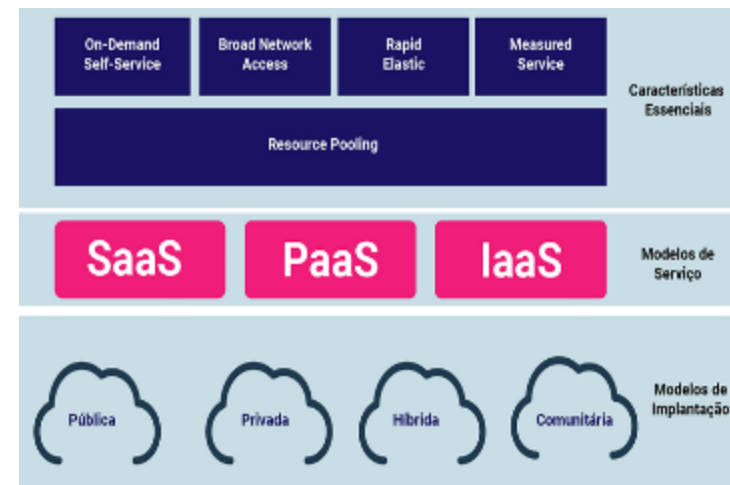
**Hybrid cloud**

# — Mercado de Serviço de Nuvem

Existem 3 principais provedores de serviços em nuvem:  
AWS, Azure e GCP. Exemplos de empresas que os utilizam:

- Netflix na AWS
- Mercedes-Benz na Azure
- Home Depot na GCP

Esses provedores oferecem vários modelos de serviço em nuvem.





# — Necessidades de Segurança



Segurança na nuvem é crucial, com dados dispersos globalmente.



A segurança da informação abrange confidencialidade, integridade e disponibilidade.



"Segurança da nuvem" aplica princípios de segurança ao ambiente de nuvem.



Controle varia com o modelo de serviço; comparação com data centers tradicionais.

## — Necessidades de Segurança



Muitas organizações relutam em adotar a nuvem pública devido a preocupações de segurança.



A responsabilidade pela segurança não é binária; pode ser compartilhada entre o provedor e a organização cliente.



Grandes provedores de nuvem investem significativamente em segurança, superando muitas organizações locais.



Isso se deve à necessidade de manter alta confiança dos clientes e justifica o retorno dos investimentos, garantindo eficiência e conformidade global.

# — Modelo de Responsabilidade Compartilhada



O modelo de responsabilidade compartilhada define obrigações de segurança do provedor e da organização cliente.

- A responsabilidade pela segurança não é binária, mas sim compartilhada entre provedores e clientes de serviços em nuvem.
- Dependendo do modelo de serviço (IaaS, PaaS, SaaS), a divisão de responsabilidade varia.
- Geralmente, a responsabilidade aumenta à medida que se passa de SaaS para PaaS e IaaS.

# — Modelo de Responsabilidade Compartilhada

- Em IaaS, o cliente cuida da segurança acima do sistema operacional.
- Em PaaS, o cliente se responsabiliza pela segurança de suas aplicações e dados.
- Em SaaS, o provedor gerencia tudo, e o cliente lida apenas com permissões de dados.



# — Serviço de Máquinas Virtuais



Serviços em nuvem incluem IaaS, que oferece máquinas virtuais, bancos de dados, contêineres e serverless.



Configuração de máquinas virtuais envolve seleção de tamanho, sistema operacional, armazenamento e rede.



Os clientes implantam aplicativos e realizam a manutenção contínua, incluindo atualizações.



Provedores de nuvem variam na implementação de VMs, mas o conceito básico é compartilhado com os clientes.

## — Serviço de Containerização



Contêineres são uma abordagem de virtualização mais leve do que máquinas virtuais.



Cada contêiner inclui tudo necessário para executar um aplicativo.



Vários contêineres podem ser implantados em um único host, escalando facilmente.



Contêineres compartilham o kernel do sistema operacional e usam recursos de forma eficiente.

## — Serviço de Containerização

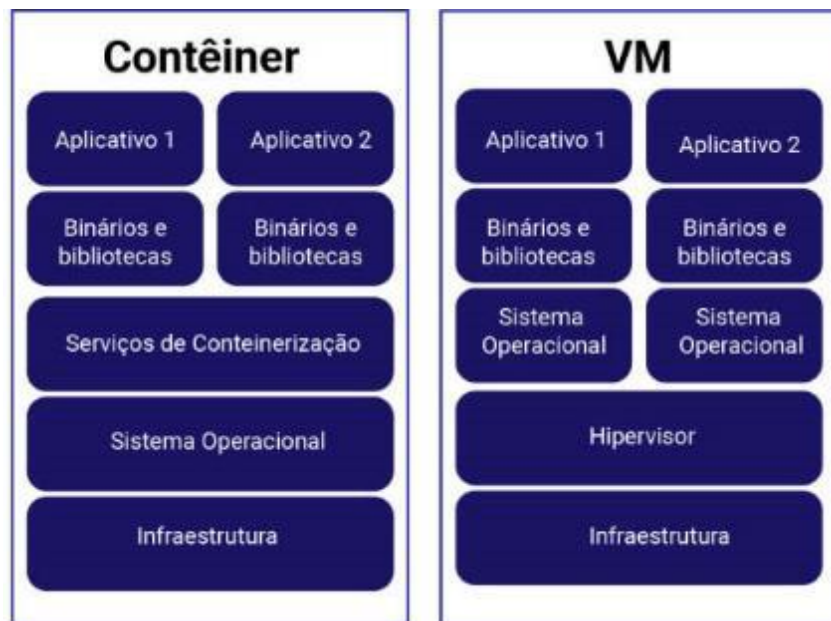
Os contêineres têm os seguintes benefícios em relação às VMs:

**Portabilidade**

**Espaço reduzido**

**Velocidade**

# — Serviço de Containerização



A imagem compara arquiteturas de contêineres e máquinas virtuais, destacando as diferenças.

- **Docker** é um padrão para encapsular contêineres amplamente adotado pela indústria.
- **Kubernetes** é um projeto de código aberto para orquestrar, implantar e gerenciar contêineres.
- Ambos são amplamente usados na computação em nuvem para desenvolvimento e produção.



# — Funções como Serviço (abordagem serverless)



Serverless (função como serviço): desresponsabiliza o cliente pela infraestrutura, focando na execução de código e eventos.



**Implementação simplificada:** importa código, configura CPU/memória e define gatilhos para execução.

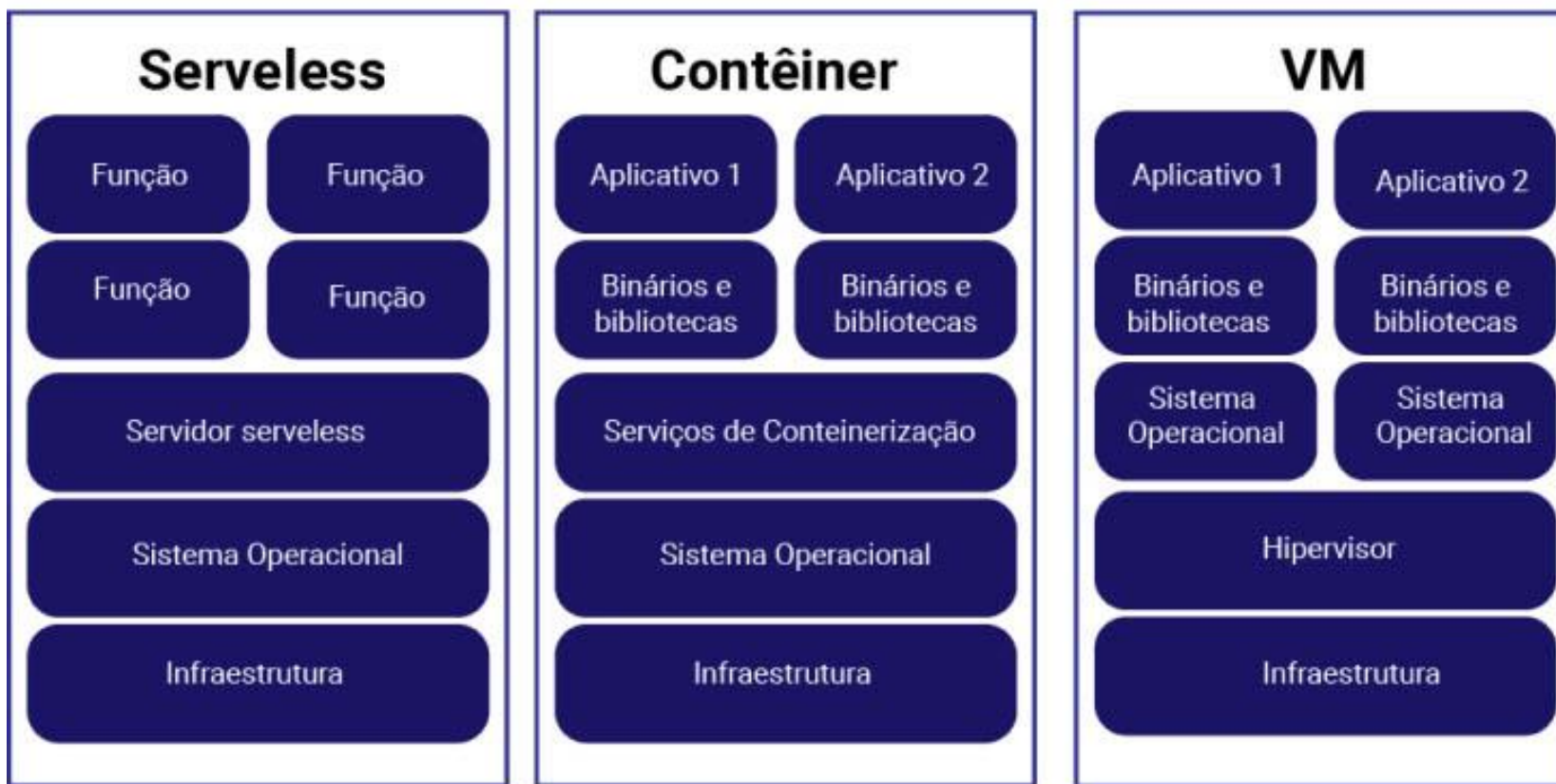


**Abordagem orientada a eventos:** desenvolvedores criam, executam e gerenciam funções como pacotes de aplicativos.



Serverless difere de contêineres e máquinas virtuais, às vezes classificado como faas, um novo tipo de serviço.

## — Funções como Serviço (abordagem serverless)



Comparação entre serverless, contêiner e máquina virtual.

## — Serviço de Base de Dados Gerenciadas



Serviços de banco de dados gerenciados simplificam o provisionamento e manutenção de bancos de dados.

- Provedores cuidam da segurança, atualizações, alta disponibilidade, backups e criptografia.
- Clientes selecionam o tipo de banco, máquina, acesso à rede e configuram instâncias.
- Vantagens incluem responsabilidade do provedor em manutenção, segurança, backups e auditoria.

# — Serviço de Armazenamento

- Armazenamento em nuvem: Categorias incluem arquivo, objeto e bloco.
- **Principais ameaças:** lista de controle de acesso, criptografia, auditoria, backups, gerenciamento de acesso e identidade.
- Armazenamento de objeto em "buckets" com API, para arquivos.
- Armazenamento de bloco permite montar volumes com sistemas de arquivos.



## — Serviço de Rede



Serviços de rede em nuvem incluem DNS, CDN, VPN, WAF e proteção contra DDoS.



Redes virtuais compartilham responsabilidades de segurança entre cliente e provedor.



CDNs armazenam conteúdo globalmente para acesso rápido e proteção contra ataques DDoS.



Provedores de nuvem oferecem soluções avançadas de proteção contra DDoS, como AWS Shield, Azure DDoS Protection e Google Cloud Armor.

# — Serviço de Monitoramento e Auditoria

- Monitoramento e auditoria são cruciais para a segurança na nuvem.
- Monitoramento envolve registro de eventos, como login de usuário e ações tomadas.
- A trilha de auditoria documenta todas as ações e é armazenada em um repositório central de logs.
- Alertas baseados em regras pré-configuradas, como logins de administradores, fazem parte do serviço de monitoramento.



## — Apresentando a Cloud Security Alliance (CSA)



A Cloud Security Alliance (CSA) é uma organização global que promove práticas de segurança em ambientes de computação em nuvem.

- A CSA oferece orientações de segurança em 14 domínios, abrangendo desde conceitos de nuvem até tecnologias relacionadas.
- Esses domínios incluem governança, conformidade, segurança de aplicativos, criptografia de dados e muito mais.

# — Conceitos e Arquiteturas de Computação em Nuvem



O domínio "Conceitos e Arquiteturas de Computação em Nuvem" define uma estrutura conceitual para a computação em nuvem.



A CSA descreve a nuvem como um modelo operacional e conjunto de tecnologias para gerenciar recursos compartilhados.



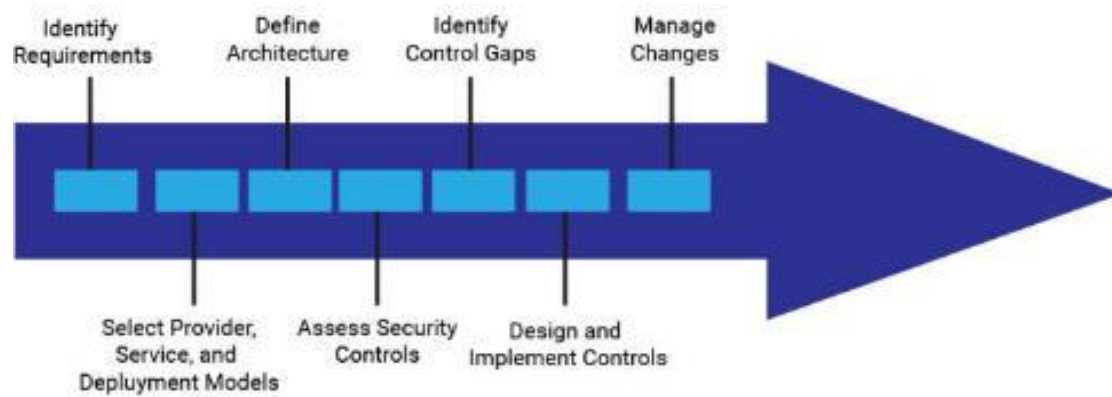
Abstração e orquestração são técnicas-chave para criar uma nuvem, permitindo a coordenação de recursos virtualizados.



Outros conceitos importantes incluem segregação, isolamento e multilocação, garantindo a divisão de recursos entre diferentes grupos ou unidades.



# — Conceitos e Arquiteturas de Computação em Nuvem



A arquitetura recomendada pela CSA ajuda provedores a adaptar serviços em nuvem ao mundo real.

- A visão funcional da computação em nuvem inclui camadas baseadas na funcionalidade.
- A CSA fornece recomendações de segurança e um processo de gestão.
- Há 13 outros domínios nas orientações de segurança da CSA, abrangendo questões estratégicas e táticas de segurança na nuvem.

# — Domínios de Governança

## Governança e gestão de risco empresarial

- A governança e gestão de risco empresarial aborda como as organizações lidam com riscos ao adotar a computação em nuvem.
- Isso inclui avaliar riscos com provedores de nuvem, acordos legais, responsabilidades na proteção de dados e questões jurisdicionais.



# — Domínios de Governança

## Governança e gestão de risco empresarial

### Aspectos legais

Problemas legais na nuvem incluem regulamentos, privacidade, segurança e conformidade.

### Compliance e gerenciamento de auditorias

Garantir e comprovar conformidade em uso da nuvem, abrangendo avaliação de impacto nas políticas internas e regulamentos.

### Governança da informação

Governança de dados na nuvem abrange controle e responsabilidade dos dados, incluindo segurança e confidencialidade.

# — Domínios de Operação

## Plano de gestão e continuidade do negócio

- Proteção do plano de gestão e de todas as interfaces administrativas usadas para acessar a nuvem, incluindo consoles da web e APIs.
- Observa as garantias para a continuidade dos negócios nas implantações em nuvem.



# — Domínios de Operação

## Segurança da infraestrutura



Seus aspectos incluem a segurança dos níveis inferiores da pilha de serviços, hardware para processamento, memória e armazenamento, rede, e software para orquestração do pool de recursos.

# — Domínios de Operação

## Virtualização e containerização

- Segurança na virtualização abrange hipervisores, contêineres e redes definidas por software.
- Impactos da virtualização são fundamentais para arquitetar a segurança na nuvem.
- Protege recursos abstraídos, como computação, rede e armazenamento.



# — Domínios de Operação

## Resposta a incidentes



- Detecção, resposta, notificação e remediação de incidentes de formas apropriadas.
- Estabelece os limites de responsabilidade por ações compartilhadas entre provedor e cliente.

# — Domínios de Operação

## Segurança das aplicações

- Proteção dos softwares aplicativos que estão sendo executados ou implantados na nuvem.
- Na prática, inclui questões como saber se é apropriado migrar ou projetar um aplicativo para ser executado na nuvem.





# — Domínios de Operação

## **Criptografia e segurança de dados**

Implementação dos mecanismos de segurança e criptografia de dados e toda a garantia de gerenciamento de chaves.

## **Gerenciamento de acessos, privilégios e identidades**

Gerenciamento de identidades apoiado nos serviços de diretório para fornecer controle de acesso. Identidades, privilégios e acessos (IAM) são profundamente impactados pela computação em nuvem.

## **Tecnologias relacionadas**

Tecnologias estabelecidas e emergentes que tenham estreito relacionamento com a computação em nuvem, incluindo Big Data, Internet das Coisas (IoT), computação móvel etc.

# Segurança em computação em nuvem



# — Tipos de modelo

## Modelo de responsabilidade compartilhada



Modelo de responsabilidade compartilhada na nuvem divide tarefas entre cliente e provedor.



Provedor cuida da infraestrutura física, enquanto o cliente é responsável por dados, dispositivos e permissões.



Responsabilidades variam de acordo com o tipo de serviço de nuvem (IaaS, PaaS, SaaS).



Cliente sempre mantém responsabilidade sobre informações, dispositivos e identidades na nuvem.

# — Tipos de modelo

## Modelos de nuvem



**Nuvem privada**



**Nuvem pública**



**Nuvem híbrida**



**Várias nuvens ou  
multicloud**



**O modelo baseado  
em consumo**

## — Tipos de serviço de nuvem

### **Infraestrutura como serviço e o modelo de responsabilidade compartilhada**

IaaS oferece controle flexível na nuvem. Provedor cuida do hardware, cliente gerencia sistemas, redes e mais.

### **Plataforma como serviço e o modelo de responsabilidade compartilhada**

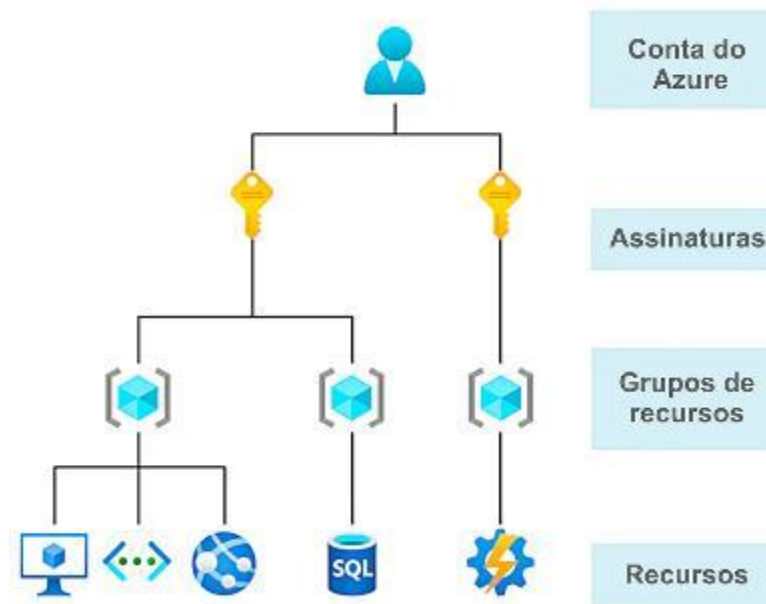
PaaS equilibra controle e simplicidade. Provedor lida com infraestrutura, cliente mantém aplicações.

### **Software como serviço e o modelo de responsabilidade compartilhada**

No SaaS, o provedor lida com a maioria das responsabilidades; cliente cuida dos dados e acesso.

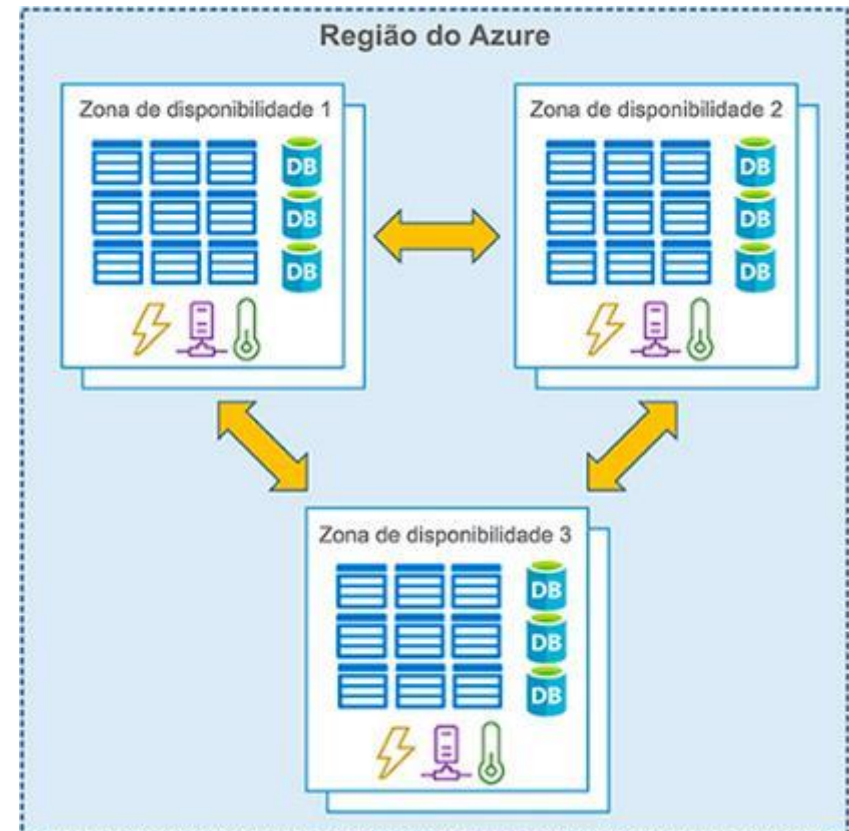
# — O que é Microsoft Azure?

- **Contas Azure:** contas Azure gerenciam recursos e limites de custos. A conta gratuita oferece produtos e crédito por 12 meses.
- **Datacenters globais** e regiões mantêm dados.
- **Zonas de disponibilidade** garantem alta disponibilidade.

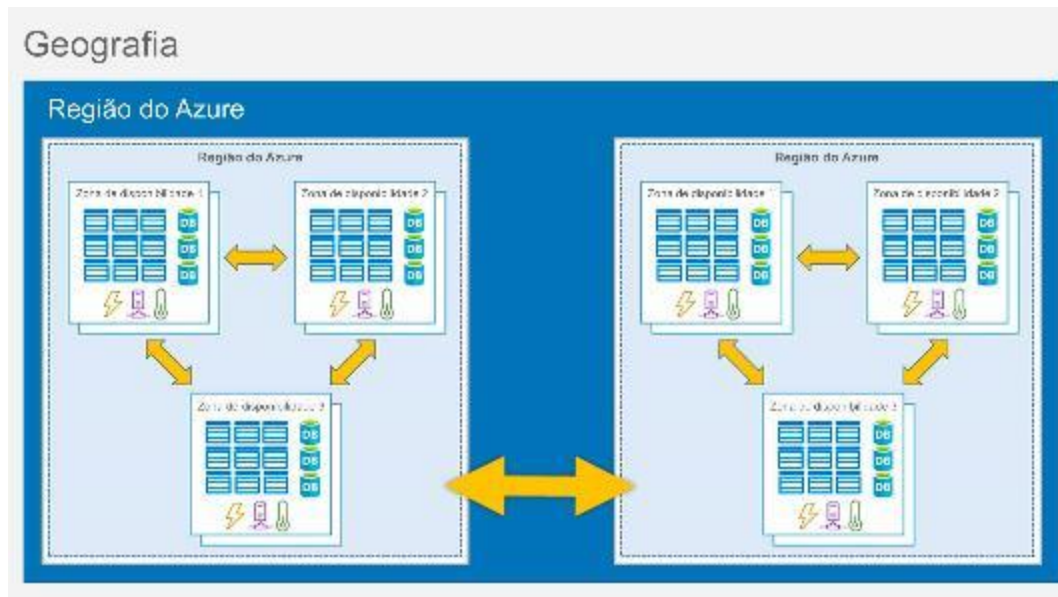


# — O que é Microsoft Azure?

Zonas de disponibilidade do Azure.



# — O que é Microsoft Azure?



**Pares de Regiões:** Emparelhamento de regiões reduz interrupções de desastres.

- **Recursos e grupos de recursos do Azure:** Recursos do Azure são organizados em grupos.
- **Assinaturas do Azure:** Assinaturas gerenciam recursos, cobrança e acesso.



# — Serviços de computação e rede do Azure

## Máquinas virtuais do Azure

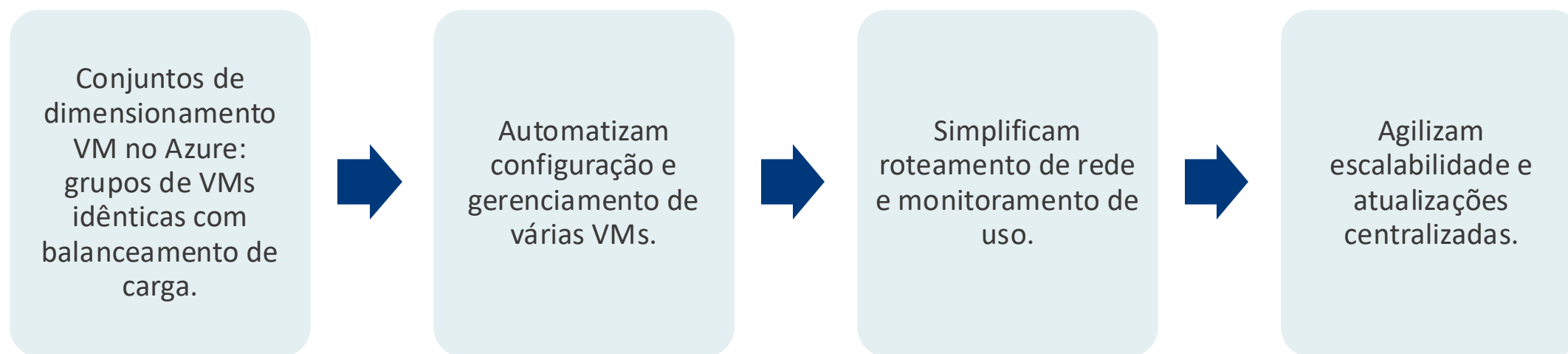
- Máquinas virtuais Azure oferecem VMs na nuvem com controle total do SO.
- Permitem personalizar software e configurações de hospedagem.
- Proporcionam infraestrutura como serviço (IaaS).
- Ideal para executar software personalizado em servidores virtuais.



# — Serviços de computação e rede do Azure

## Máquinas virtuais do Azure

### Conjuntos de escala de máquinas virtual

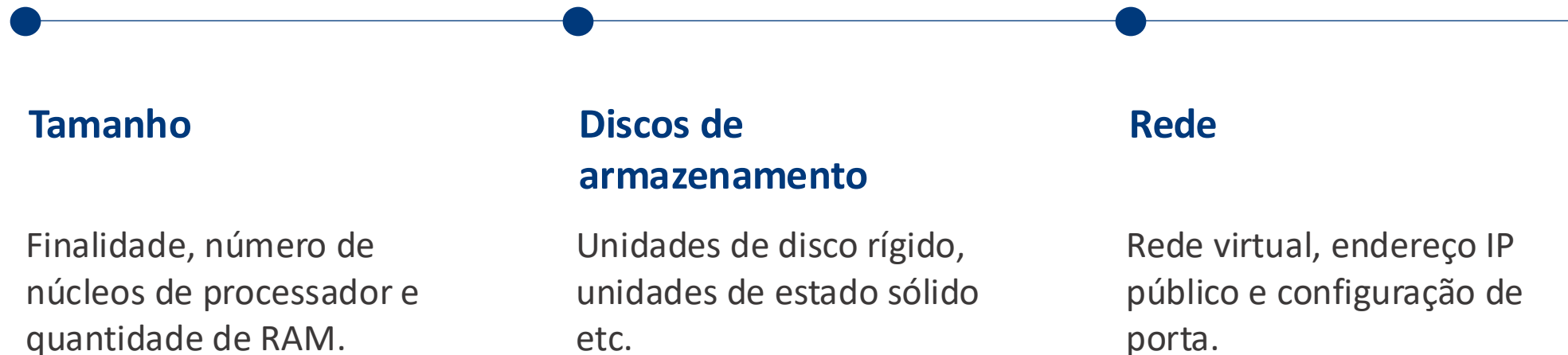


# — Serviços de computação e rede do Azure

## Máquinas virtuais do Azure

### Recursos da máquina virtual

Ao provisionar uma VM, você também terá a oportunidade de escolher os recursos associados a ela, incluindo:



# — Serviços de computação e rede do Azure

## Área de trabalho virtual do Azure (Azure Virtual Desktop)

- Azure Virtual Desktop: serviço de virtualização de área de trabalho em nuvem.
- Oferece Windows hospedado na nuvem em várias localizações.
- Funciona em diversos dispositivos e sistemas operacionais.
- Suporta multissessão no Windows 10/11 Enterprise, proporcionando experiência consistente.



# — Serviços de computação e rede do Azure

## Área de trabalho virtual do Azure (Azure Virtual Desktop)

### Contêineres do Azure



Contêineres do Azure: ambiente de virtualização leve e ágil.

- Diferem de máquinas virtuais, não requerem gerenciamento de SO.
- Permitem criar, dimensionar e interromper dinamicamente.
- Azure Container Instances: oferta PaaS para executar contêineres sem gerenciar VMs.

# — Serviços de computação e rede do Azure

## Área de trabalho virtual do Azure (Azure Virtual Desktop)

### Azure Functions



Azure Functions: Computação sem servidor controlada por eventos.



Elimina a necessidade de manter máquinas virtuais ou contêineres em execução.



Ideal para responder a eventos, temporizadores ou mensagens de outros serviços do Azure.



Enfoca apenas no código do serviço, não na infraestrutura subjacente.

# — Serviços de computação e rede do Azure

## Área de trabalho virtual do Azure (Azure Virtual Desktop)

### Serviço de aplicativo do Azure

Serviço de Aplicativo Azure: Criação de aplicativos web, back-ends, APIs sem gerenciar infraestrutura.

Oferece dimensionamento automático, alta disponibilidade e suporta Windows e Linux.

Possibilita implantações contínuas do GitHub, Azure DevOps, ou repositórios Git.

Gerencia infraestrutura, protege endpoints, escala para alto tráfego e garante alta disponibilidade.

## — Serviços de computação e rede do Azure

### Área de trabalho virtual do Azure (Azure Virtual Desktop)

#### Redes virtuais

**Redes virtuais privadas (VPNs)**

**Gateways VPN**

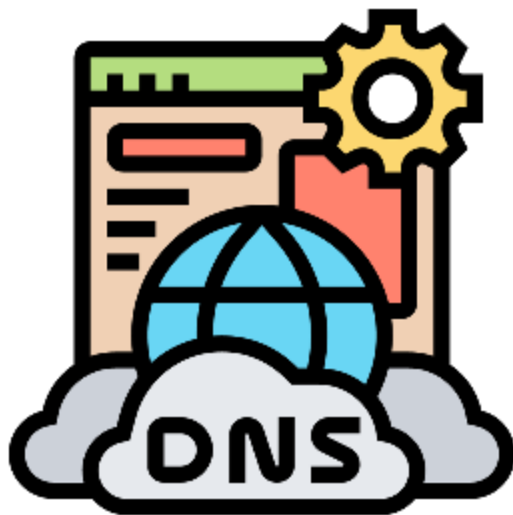
**Azure ExpressRoute**



## — Serviços de computação e rede do Azure

### Área de trabalho virtual do Azure (Azure Virtual Desktop)

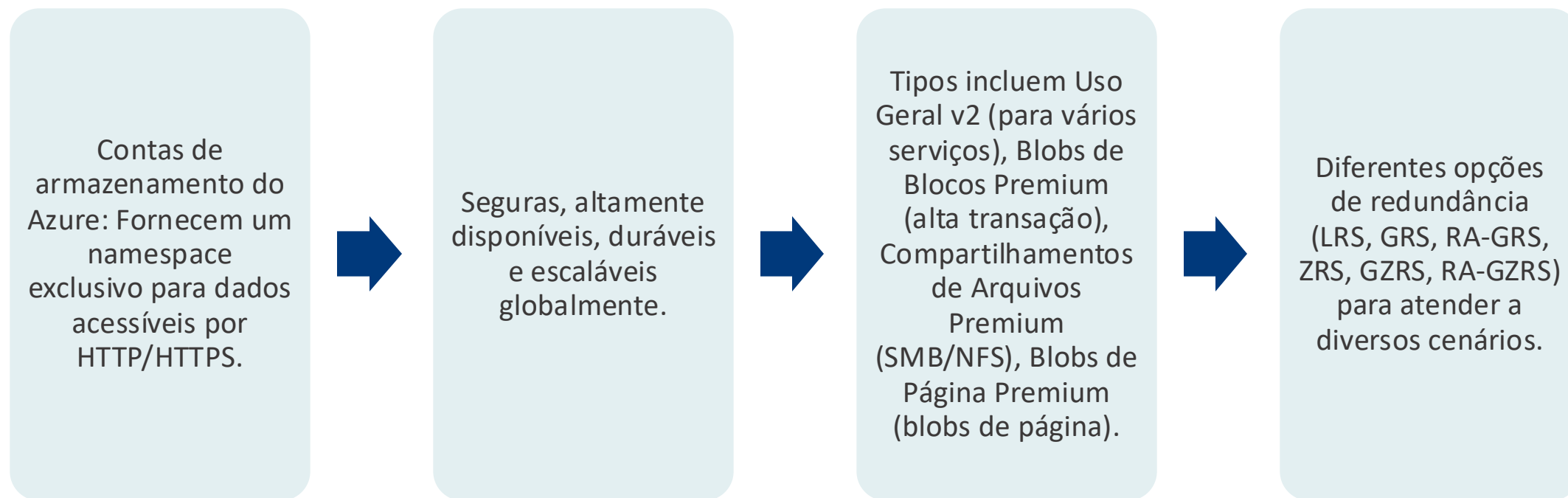
#### DNS do Azure



DNS do Azure: Serviço de hospedagem de domínios DNS no Azure.

- Gerenciamento de registros DNS com as mesmas credenciais e ferramentas do Azure.
- Benefícios incluem confiabilidade, desempenho, segurança e personalização de redes virtuais.
- Oferece registros de alias e facilidade de uso.

## — Os serviços de armazenamento do Azure



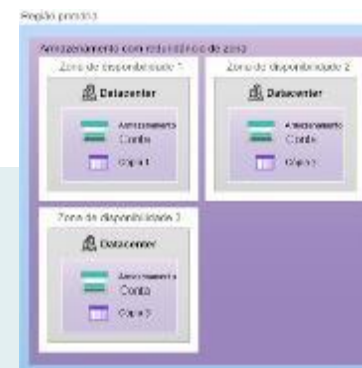
# — Os serviços de armazenamento do Azure

## Redundância de armazenamento do Azure

### Redundância na região primária



**Armazenamento com redundância local**



**Armazenamento com redundância de zona**

# — Os serviços de armazenamento do Azure

## Redundância de armazenamento do Azure

### Redundância em uma região secundária

Armazenamento com Redundância Geográfica (GRS):  
Replicação de dados em múltiplas cópias para alta durabilidade e recuperação.

Réplicas síncronas ocorrem três vezes no mesmo datacenter e na mesma região (LRS).

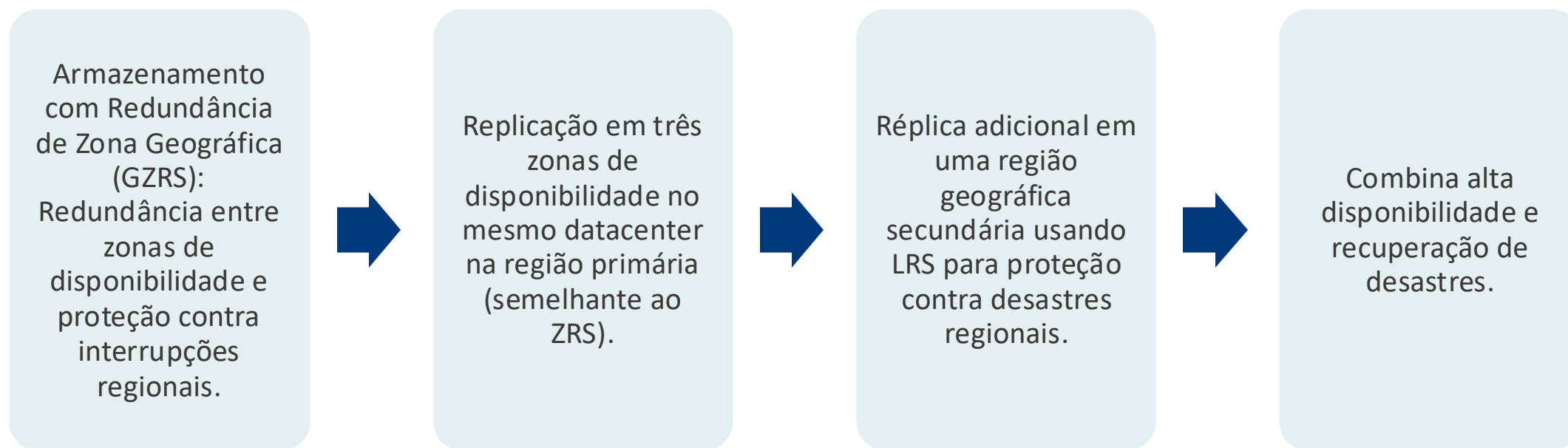
Réplica assíncrona é realizada em um único datacenter na região secundária (LR).

GRS oferece durabilidade de pelo menos 16 noves (99,999999999999999%) durante um ano.

# — Os serviços de armazenamento do Azure

## Redundância de armazenamento do Azure

### Armazenamento com redundância de zona geográfica

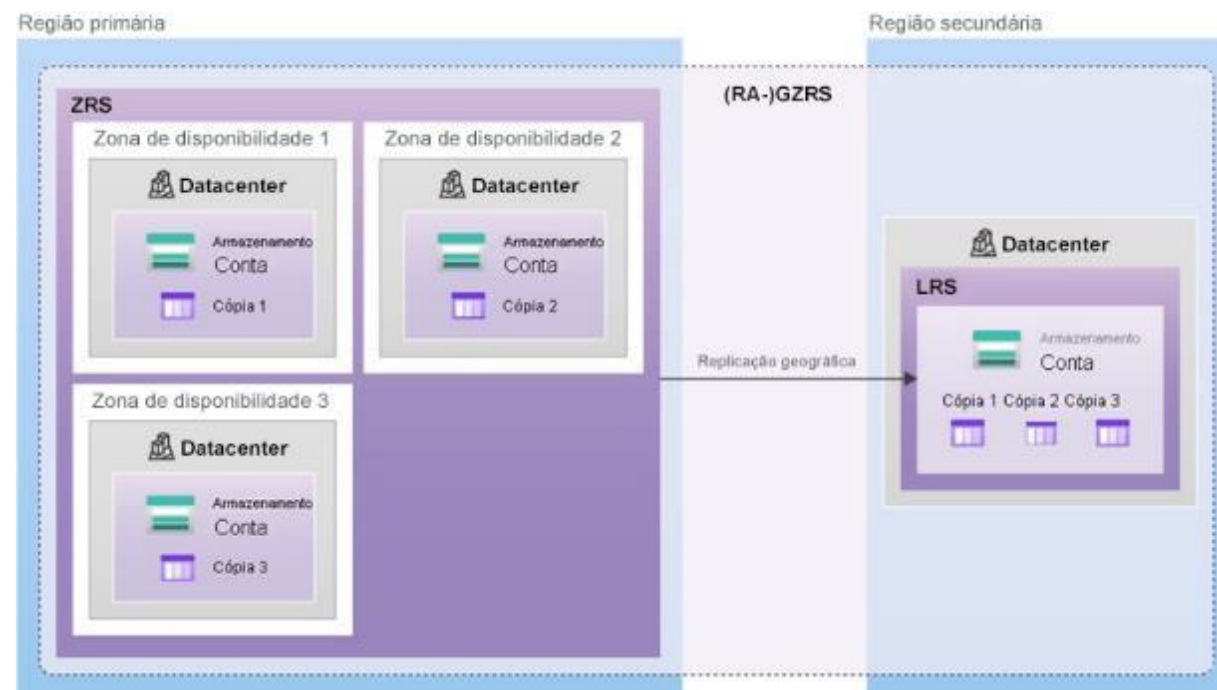


# — Os serviços de armazenamento do Azure

## Redundância de armazenamento do Azure

### Armazenamento com redundância de zona geográfica

Região secundária e redundância de zona geográfica.



# — Os serviços de armazenamento do Azure

## Serviços de armazenamento do Azure



**Blobs do Azure**



**Arquivos do Azure**



**Filas do Azure**



**Azure Disks**

# — Os serviços de armazenamento do Azure

## Serviços de armazenamento do Azure

### Armazenamento de blob



Armazenamento de Blob Azure:  
Armazena objetos na nuvem, como  
textos, imagens, vídeos e dados  
binários.



Ideal para dados não estruturados e  
suporta grande volume de  
transferências simultâneas.



Usado para imagens, documentos,  
streaming, backup, análise de dados,  
etc.



Oferece camadas de acesso: quente  
(frequente), frio (menos frequente,  
>30 dias) e aos arquivos (raro, >180  
dias).



# — Os serviços de armazenamento do Azure

## Serviços de armazenamento do Azure

### Armazenamento de blob

#### Arquivos do Azure (Azure Files)

Os arquivos do Azure são um tipo de armazenamento em nuvem que possui compatibilidade com os protocolos SMB ou NFS, usando a familiar tecnologia de compartilhamento de arquivos.

#### Armazenamento de filas (Azure Queues)

É um tipo de armazenamento usado para armazenar mensagens em grande escala. Após o armazenamento, é possível acessá-las de qualquer local por meio de autenticação HTTP ou HTTPS.

# — Identidade e segurança do Azure

## Serviços de diretório do Azure

- Serviços de Diretório do Azure: Oferece gerenciamento de identidade e acesso.
- Azure AD é um serviço de diretório em nuvem da Microsoft.
- Fornece autenticação, logon único, gerenciamento de aplicativos e dispositivos.
- Detecta tentativas de conexão suspeitas e oferece recursos de segurança avançados.



# — Identidade e segurança do Azure

## Controle de acesso baseado em função (RBAC)



Controle de Acesso Baseado em Função (RBAC) do Azure: Sistema de autorização para gerenciar acesso a recursos na nuvem.



Refina o controle sobre quem tem acesso, o que podem fazer e a quais áreas têm acesso.



Usado para segmentar o gerenciamento de recursos, permitindo que diferentes grupos acessem apenas os recursos relacionados às suas funções.



Integrado ao Azure Resource Manager para gerenciar com precisão as permissões dos usuários em grupos de recursos.

# — Identidade e segurança do Azure

## Defesa em profundidade



Defesa em Profundidade: Estratégia de segurança com camadas de proteção em torno dos dados.



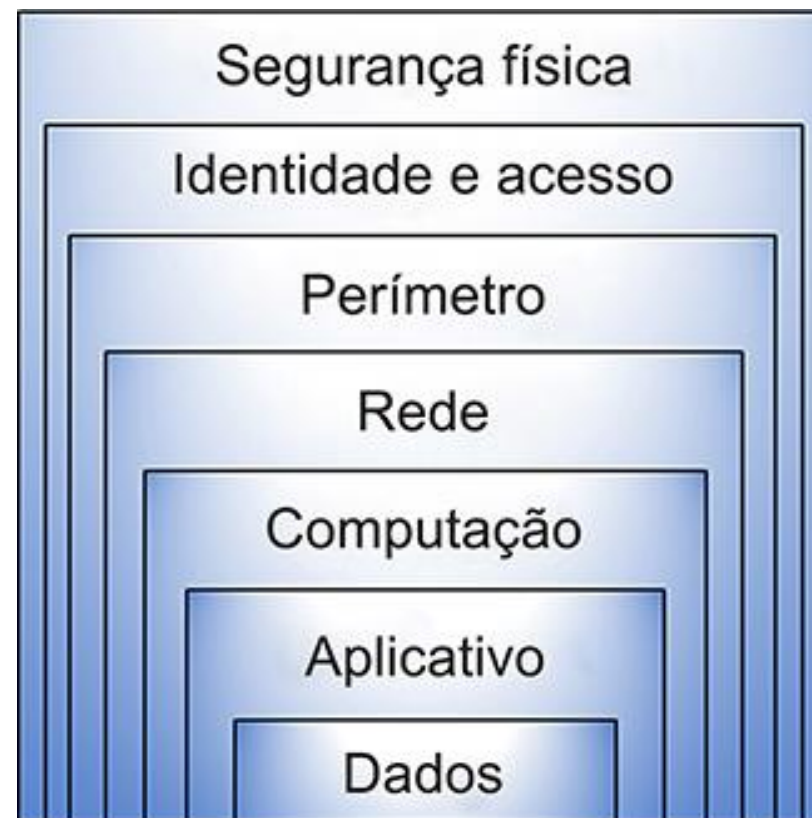
Inclui segurança física, identidade, perímetro, rede, computação, aplicativos e dados.



Protege os dados no centro, abordando todas as possíveis ameaças em vários níveis.



Garante uma proteção abrangente e resiliente contra ameaças de segurança.



# — Gerenciamento de custos no Azure

## Fatores que podem afetar os custos no Azure



Os custos no Azure são afetados por vários fatores, como o tipo de recurso, consumo e manutenção.



A localização geográfica da implantação, o tipo de assinatura e o uso de soluções de terceiros no Azure Marketplace também impactam os custos.



Azure desloca custos de CapEx para OpEx, permitindo alugar recursos conforme necessário.



A otimização de custos é fundamental para garantir um uso eficiente dos recursos na plataforma Azure.

# — Gerenciamento de custos no Azure

## Calculadoras de preço e custo total de propriedade

### Calculadora de preço



Calculadora de Preço Azure: Ferramenta online para estimar custos de recursos no Azure.

- Oferece cenários de exemplo, estimativas salvas, FAQs e orçamentos personalizados.
- Ajuda a planejar e entender os custos detalhados de provisionamento de recursos na plataforma Microsoft Azure.

# — Gerenciamento de custos no Azure

## Calculadoras de preço e custo total de propriedade

### Calculadora de TCO



Calculadora de TCO (Custo Total de Propriedade): Projetada para migração de infraestrutura local para o Azure.



Gerencia custos atuais e futuros, identificando recursos locais (servidores, bancos de dados, armazenamento, tráfego).



Oferece um orçamento baseado no custo atual e uma previsão de economia de 1 a 5 anos na nuvem do Azure.



Auxilia na tomada de decisões ao avaliar os benefícios financeiros da migração para a nuvem.

# — Gerenciamento de custos no Azure

## Calculadoras de preço e custo total de propriedade

### Gerenciamento de custos

Gerenciamento de Custos no Azure: Monitora e gerencia os custos de recursos na plataforma.



Permite criar alertas com base nos gastos e definir orçamentos para automação do gerenciamento.



Exemplo: Estabelecer um orçamento de R\$ 20.000,00 e configurar um alerta para quando 80% desse valor for atingido, recebendo um aviso por e-mail.



A análise de custo fornece visualização rápida dos custos em várias perspectivas, como por ciclo de cobrança, região e recurso, facilitando o controle financeiro.



# — Gerenciamento de custos no Azure

## Calculadoras de preço e custo total de propriedade

### Gerenciamento de custos



# — Gerenciamento de custos no Azure

## Finalidade das marcas (tags)



A finalidade das marcas (tags) é associar metadados a recursos ou grupos de recursos no Azure.



Permitem a organização e classificação de recursos, facilitando a identificação e o gerenciamento.



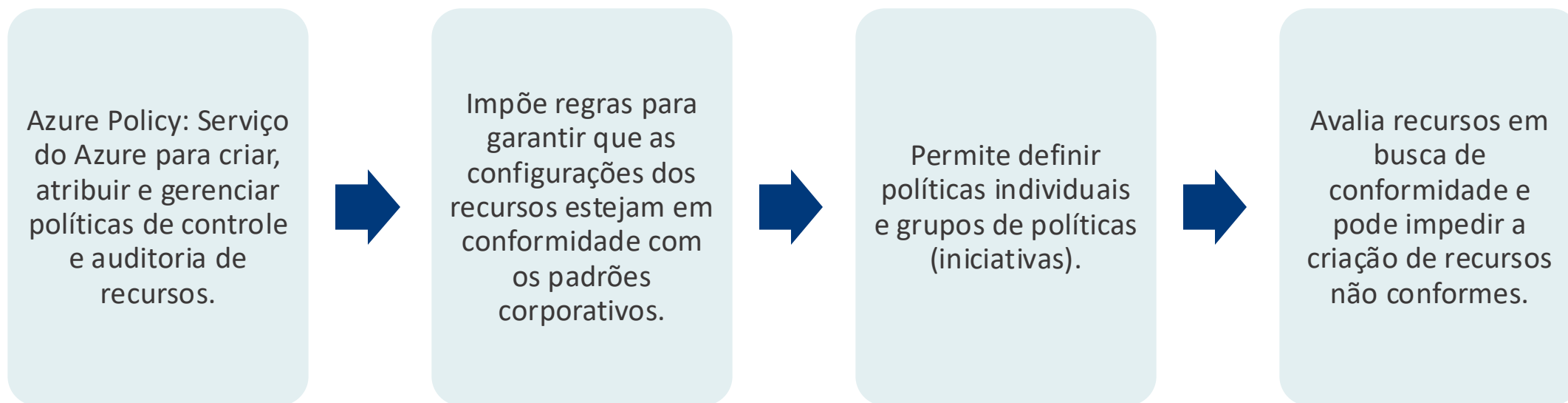
Exemplo: Usar tags para categorizar máquinas virtuais por departamento (RH, Almoxarifado) e facilitar a filtragem e geração de relatórios financeiros específicos por marca/setor.



Simplificam a gestão e organização de recursos, tornando mais fácil a identificação e análise de custos e uso.

# — Os recursos e ferramentas de governança e conformidade no Azure

## Azure Policy



# — Os recursos e ferramentas de governança e conformidade no Azure

## Bloqueio de recursos (Locks)

- Bloqueio de Recursos (Locks): Importante na governança de recursos do Azure.
- Dois tipos de bloqueios: "Exclusão" (Delete) que impede a exclusão e "ReadOnly" que permite leitura e modificação, mas impede exclusão.
- Controla quem pode ou não excluir ou alterar recursos, garantindo maior controle e segurança na gestão de recursos na nuvem.



# — Os recursos e ferramentas de governança e conformidade no Azure

## Portal de confiança do serviço (Service Trust)



Portal de Confiança do Serviço (Service Trust Portal): Fornece acesso a informações sobre práticas de segurança, privacidade e conformidade da Microsoft relacionadas ao Azure.



Contém documentos de conformidade legal, como NIST e ISO 27001, para casos em que é necessário demonstrar a conformidade regulatória.



Oferece recursos e ferramentas relacionados à governança e boas práticas no Azure.

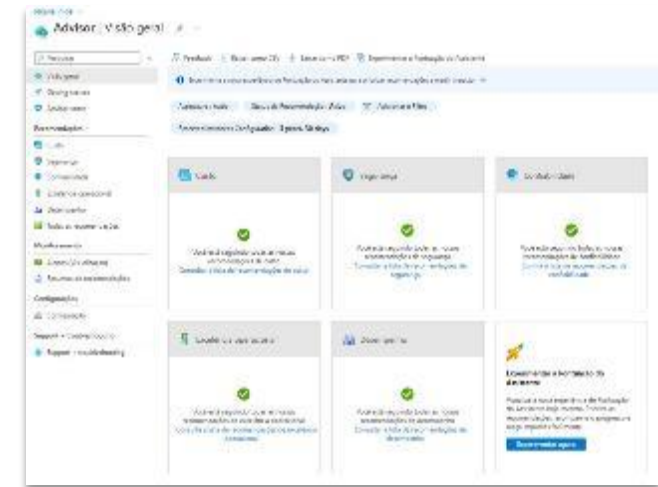


Essencial para acesso a documentação que atesta a conformidade do Azure com normas regulatórias e para fins de relatórios de conformidade.

# — Ferramentas de monitoramento do Azure

## Assistente do Azure (Azure Advisor)

- Azure Advisor monitora recursos e fornece recomendações para melhorar confiabilidade, segurança, desempenho, excelência operacional e redução de custos no Azure.
- Ajuda na otimização e economia na nuvem com recomendações claras e ação imediata, adiável ou ignorável.



# — Ferramentas de monitoramento do Azure

## Assistente do Azure (Azure Advisor)

### Integridade do serviço do Azure

Integridade do Serviço Azure: Ajuda na tomada de decisão em relação à infraestrutura, com três serviços combinados:

**Status do Azure**

**Integridade do serviço**

**Resource health**

# — Ferramentas de monitoramento do Azure

## Assistente do Azure (Azure Advisor)

### Azure Monitor



Azure Monitor: Coleta, analisa e visualiza dados de recursos para monitoramento proativo.



Monitora recursos no Azure, em ambientes locais e em várias nuvens, como AWS e Google Cloud.



Fornecer visibilidade e insights abrangentes para garantir o desempenho e a integridade de recursos em diversas plataformas.



# — Migrações para o Azure

## Processos e ferramentas para a migração



Migrações para Azure oferecem um serviço completo de migração, modernização e otimização.



Inclui etapas de descoberta, avaliação e dimensionamento de recursos locais.



Possui uma estrutura extensível que permite a integração de ferramentas de terceiros para suporte a vários casos de uso.



Oferece uma plataforma unificada, uma variedade de ferramentas e suporte para avaliação, migração e modernização de recursos na nuvem Azure.

# — Migrações para o Azure

## Processos e ferramentas para a migração

### **Plataforma de migração unificada**

Essa funcionalidade oferece um único portal para iniciar, executar e acompanhar sua migração para o Azure.

### **Variedade de ferramentas**

As ferramentas das migrações incluem itens como o Migrações para Azure, descoberta, avaliação e ferramenta de Migração do Servidor.

### **Avaliação, migração e modernização**

No hub de Migrações para Azure, você pode avaliar, migrar e modernizar servidores, bancos de dados e aplicativos web, por exemplo

## — Serviço de aplicativo



Azure App Service simplifica a criação de aplicativos web e móveis na nuvem.



Suporta várias linguagens e sistemas operacionais.



Oferece manutenção de infraestrutura, CI/CD, segurança rigorosa e integração com ferramentas de desenvolvimento.



Suporta Kubernetes, servless e é gerenciado pela Microsoft.

# — Serviço de aplicativo

## Planos de serviço no Azure (service plan)

- Planos de serviço no Azure determinam o poder computacional para aplicativos.
- Cada plano oferece recursos específicos, como armazenamento e escalabilidade.
- Escolha um plano alinhado às necessidades do seu aplicativo.
- Personalize o plano com recursos adequados, como certificados e escala automática.



## — Serviço de aplicativo

### Planos de serviço no Azure (service plan)

Alguns tipos de plano de serviço e o número máximo de aplicativos que ele suporta:

Tipo do plano de serviço de aplicativo	Máximo de aplicativos
B1, S1, P1v2, I1v1	8
B2, S2, P2v2, I2v1	16
B3, S3, P3v2, I3v1	32
P1v3, I1v2	16
P2v3, I2v2	32
P3v3, I3v2	64

# Ambiente de computação em nuvem – AWS



## — Opções de computação na AWS



### **Máquinas Virtuais (VMs) no Amazon EC2**

Opção tradicional para infraestrutura virtualizada, semelhante a servidores físicos.



### **Containers no Amazon ECS e Amazon EKS**

Oferecem escalabilidade, consistência e empacotamento de aplicativos com containers.



### **Computação sem servidor no AWS Lambda**

Abstrai hardware, sistema operacional e infraestrutura, ideal para focar no código das aplicações sem gerenciar servidores.

## — Máquinas virtuais – Amazon EC2



Amazon EC2 fornece capacidade computacional escalável em formato de máquinas virtuais (instâncias).



Permite configurar rapidamente servidores virtuais, escolher sistemas operacionais, e instalar aplicativos.



Oferece um processo simplificado em comparação com implantações on-premise, economizando tempo e recursos.

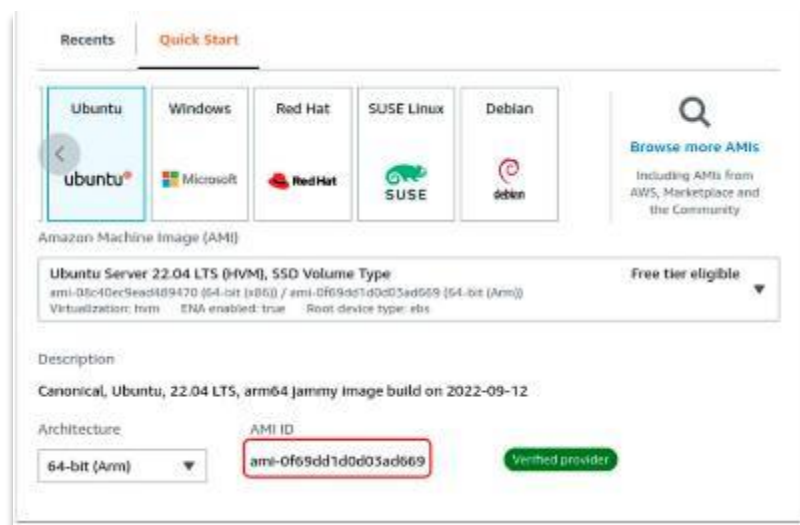


Permite desligar instâncias quando não forem mais necessárias para economizar custos.



# — Máquinas virtuais – Amazon EC2

## Amazon Machine Image (imagens de aplicações e sistema operacional)



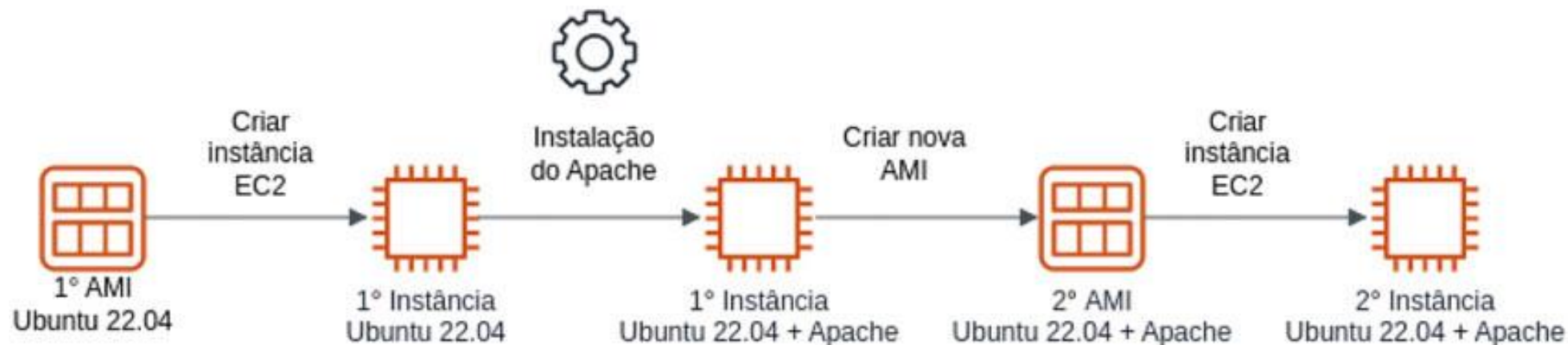
Amazon Machine Images (AMI) são imagens prontas para uso, incluindo sistema operacional e aplicativos.

- A AWS oferece um catálogo de AMIs, incluindo opções recomendadas pela AWS.
- AMIs podem ser customizadas e reutilizadas, permitindo criar imagens personalizadas para cenários específicos.
- Ao criar uma AMI, é importante nomeá-la para facilitar a identificação, e os snapshots associados a ela podem resultar em custos de armazenamento.

## — Máquinas virtuais – Amazon EC2

Amazon Machine Image (imagens de aplicações e sistema operacional)

Ciclo de criação e reuso de uma AMI customizada:



# — Máquinas virtuais – Amazon EC2

## Tipos de instâncias EC2



Instâncias EC2 combinam vCPUs, memória, rede, armazenamento e, às vezes, GPUs.



Os tipos de instâncias são otimizados para diferentes casos de uso e seguem uma nomenclatura específica (ex.: m5.large, t4g.small).



As famílias de instâncias incluem M (geral), T (baixo custo), C (computação), R (memória), G (gráficos), I (E/S intensiva), entre outras.

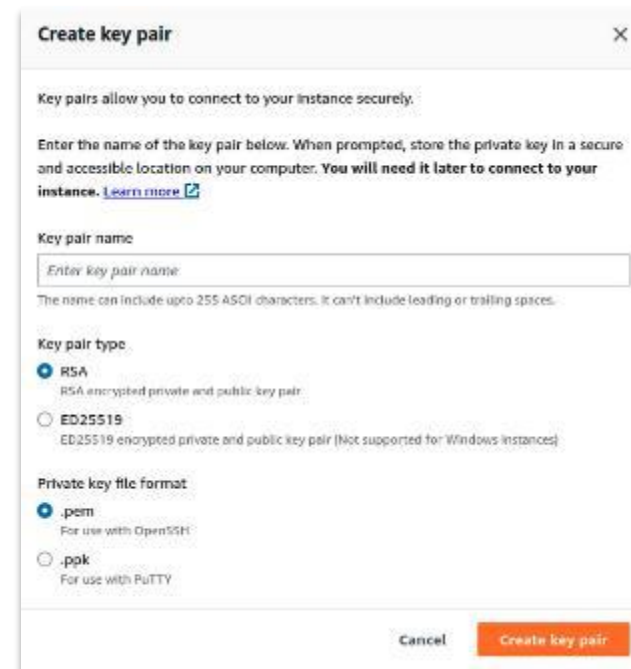


As letras após o número da geração podem indicar detalhes como processadores Intel (i), ARM (a) ou outras características específicas.

# — Máquinas virtuais – Amazon EC2

## Par de chaves

- Um par de chaves EC2 consiste em uma chave pública e uma chave privada.
- A chave pública é armazenada na instância, e a chave privada é usada para se conectar à instância (SSH no Linux) ou descriptografar senhas (Windows).
- A chave privada deve ser mantida com segurança, pois oferece acesso à instância.



The screenshot shows the 'Create key pair' dialog box in the AWS Management Console. It includes a title bar with a close button, an explanatory text about key pairs, a text input field for the key pair name, and two sections for selecting options: 'Key pair type' (with RSA and ED25519 options) and 'Private key file format' (with .pem and .ppk options). At the bottom, there are 'Cancel' and 'Create key pair' buttons.

**Create key pair** [X]

Key pairs allow you to connect to your instance securely.

Enter the name of the key pair below. When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** [Learn more](#)

Key pair name

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

☒ **RSA**  
RSA encrypted private and public key pair

☐ **ED25519**  
ED25519 encrypted private and public key pair (Not supported for Windows instances)

Private key file format

☒ **.pem**  
For use with OpenSSH

☐ **.ppk**  
For use with PuTTY

Cancel Create key pair

# — Máquinas virtuais – Amazon EC2

## Rede e firewall de EC2



O Amazon VPC (Virtual Private Cloud) permite a execução de recursos da AWS em uma rede virtual dedicada à sua conta.



Você pode controlar se uma instância receberá um endereço IP público da Amazon e associá-lo a uma instância.



O security group (SG) age como um firewall virtual para controlar o tráfego de entrada e saída de instâncias EC2.



Você pode especificar um ou mais security groups durante a criação de instâncias e adicionar ou modificar regras para permitir o tráfego necessário.

# — Máquinas virtuais – Amazon EC2

## Disco do EC2



O Amazon EC2 oferece opções de armazenamento flexíveis e duráveis para instâncias.



Um disco raiz EBS é adicionado automaticamente durante a criação da instância, com tamanho e tipo sugeridos para a AMI escolhida.



As opções de armazenamento podem ser usadas independentemente ou combinadas conforme necessário.



É importante respeitar as configurações mínimas para evitar problemas de desempenho ou inicialização da instância.

# — Máquinas virtuais – Amazon EC2

## Detalhes avançados

Ao final do processo de criação de uma instância EC2, antes de lançar, ainda é possível selecionar algumas opções, onde podemos destacar:



### Termination protection

Se ativado, a instância não pode ser encerrada até que a proteção contra encerramento seja desativada.



### Detailed Cloudwatch

Diminui de 5 para 1 minuto o intervalo de métricas da instância.



### User Data

Campo que permite serem adicionados comandos ou scripts de comandos para serem executados pela instância logo após o boot.

## — Block Storage – Amazon EBS



Amazon Elastic Block Storage (EBS) oferece volumes de armazenamento em blocos para instâncias EC2.



Os dados nos volumes EBS são persistentes e podem ser movidos entre instâncias EC2 na mesma zona de disponibilidade.



Volumes EBS agem como discos rígidos externos, permitindo flexibilidade no armazenamento de dados.

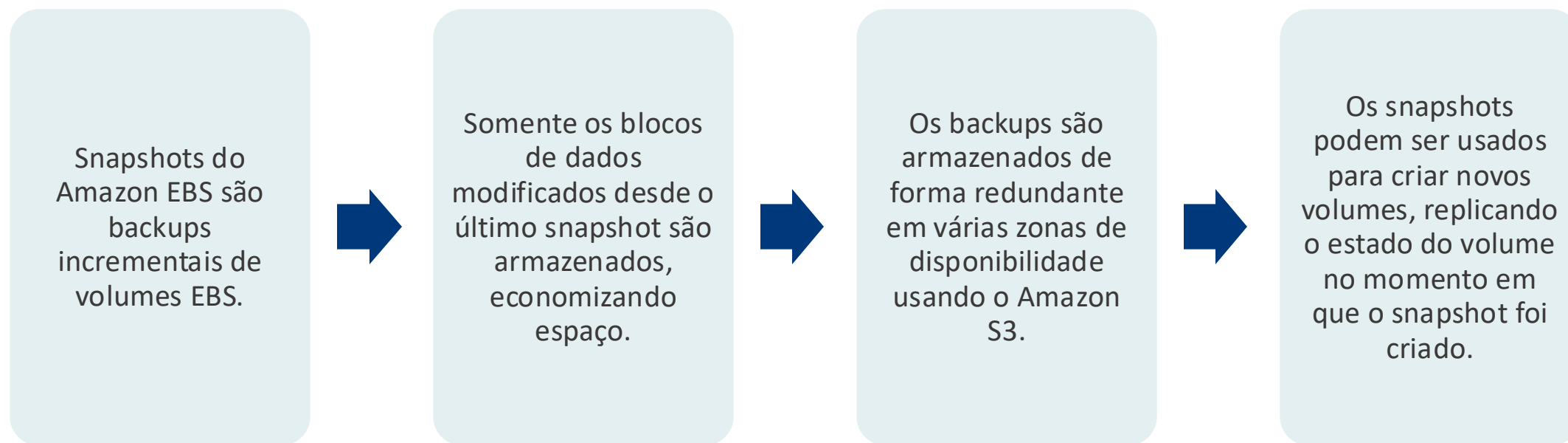


Recentemente, a AWS lançou o recurso multi-attach que permite anexar volumes EBS a várias instâncias EC2 simultaneamente em algumas circunstâncias.



# — Block Storage – Amazon EBS

## Snapshots de EBS



# — Block Storage – Amazon EBS

## Casos de uso do EBS

O Amazon EBS é útil quando você precisa recuperar dados rapidamente e manter os dados por um longo prazo. Os volumes são comumente usados nos seguintes cenários:

**Sistemas operacionais**

**Bancos de dados**

**Aplicativos corporativo**

**Aplicativos com taxa de  
transferência intensiva**

# — Block Storage – Amazon EBS

## Tipos de EBS

Escolha volumes SSD (unidades de estado sólido) como gp3 ou io2 para cargas de trabalho com alto desempenho em E/S aleatórias.



Opte por volumes HDD (unidades de disco rígido) como st1 ou sc1 para cargas de trabalho com E/S sequenciais intensivas.



A seleção depende das necessidades específicas de sua aplicação e do tipo de acesso aos dados.



Cada categoria tem duas opções para atender a diferentes demandas de desempenho.

# — Object storage - Amazon S3



Amazon S3 é uma solução de armazenamento independente, não vinculada à computação, para armazenar e recuperar dados pela web.



Os objetos são armazenados em "buckets" e antes de fazer upload de objetos, é necessário criar um bucket.



Ao criar um bucket, você especifica seu nome e a região da AWS onde deseja que ele resida.

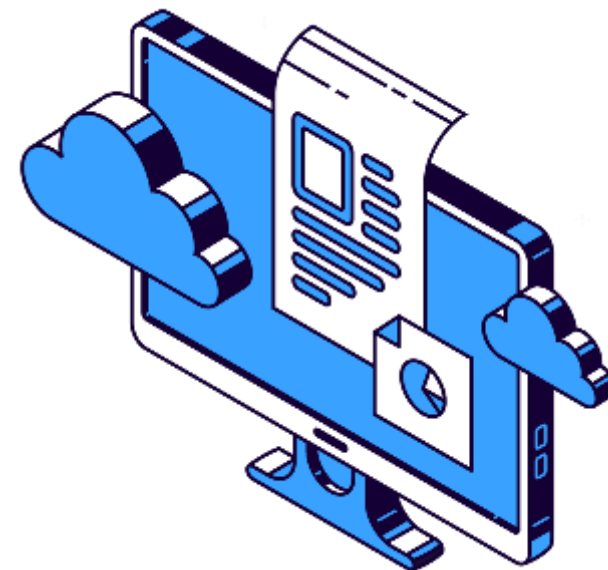


Amazon S3 oferece alta durabilidade e disponibilidade de objetos em um ano.

# — Object storage - Amazon S3

## Versionamento no S3

- O Amazon S3 usa nomes de objetos para identificação. O controle de versão mantém várias versões de objetos no mesmo bucket, evitando substituições.
- A exclusão não remove permanentemente e a substituição cria novas versões acessíveis.



# — Object storage - Amazon S3

## Classes de armazenamento no S3

**S3 Standard:** Alta performance e resiliência para dados frequentemente acessados.

**S3 Standard-IA:** Baixo custo, bom para dados de longo prazo com acesso rápido.

**S3 Glacier Instant Retrieval:** Baixo custo e acesso rápido para dados raramente acessados.

**S3 Glacier Flexible Retrieval:** Baixo custo para dados acessados 1-2 vezes por ano.

**S3 Glacier Deep Archive:** Classe mais acessível para dados preservados a longo prazo.

# — Object storage - Amazon S3

## Casos de uso

O Amazon S3 é amplamente utilizado em diversos casos, incluindo:

- Backup e armazenamento de arquivos.
- Hospedagem de mídia (vídeos, fotos, músicas).
- Data lakes devido à escalabilidade.
- Hospedagem de sites estáticos.



## — File storage – Amazon EFS

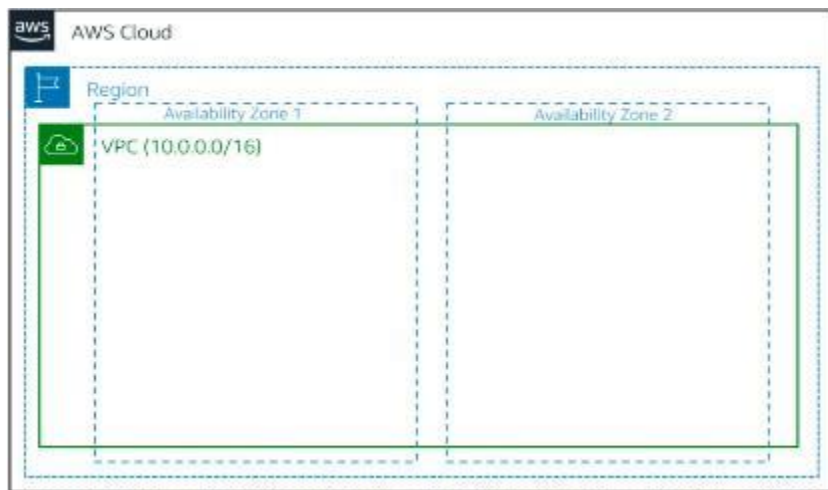


Amazon EFS é um sistema de arquivos escalável para armazenamento de arquivos compartilhados.

- É ideal para cenários em que vários clientes precisam acessar os mesmos dados simultaneamente.
- Ele se expande e contrai automaticamente para dimensionar sob demanda.
- Pode lidar com petabytes de dados sem interrupções.



# — VPC – Virtual Private Cloud



A Amazon Virtual Private Cloud (Amazon VPC) permite criar redes privadas isoladas na AWS.

- Em uma VPC, recursos como instâncias EC2 podem ser organizados em sub-redes.
- Para criar uma VPC, você define seu nome, região e intervalo de IP (CIDR).
- A AWS provisiona uma rede e endereços IP com base nessas configurações.

# — VPC – Virtual Private Cloud

## Alta disponibilidade em VPC



Crie pelo menos duas sub-redes distribuídas em diferentes zonas de disponibilidade (AZs).



Lembre-se de que falhas podem ocorrer a qualquer momento.



Recursos, como instâncias EC2, não são automaticamente altamente disponíveis em várias AZs.



Para alta disponibilidade, provisione várias máquinas virtuais em AZs diferentes e use balanceadores de carga para distribuir o tráfego.

# — VPC – Virtual Private Cloud

## Endereço IP elástico

- Endereço IP elástico é um IPv4 público estático na nuvem.
- Pode ser associado a uma única instância ou interface de rede.
- Mascara falhas de instância ao remapear rapidamente o endereço para outra.
- Taxas associadas quando não estão em uso ou associados a instâncias paradas.



# — VPC – Virtual Private Cloud

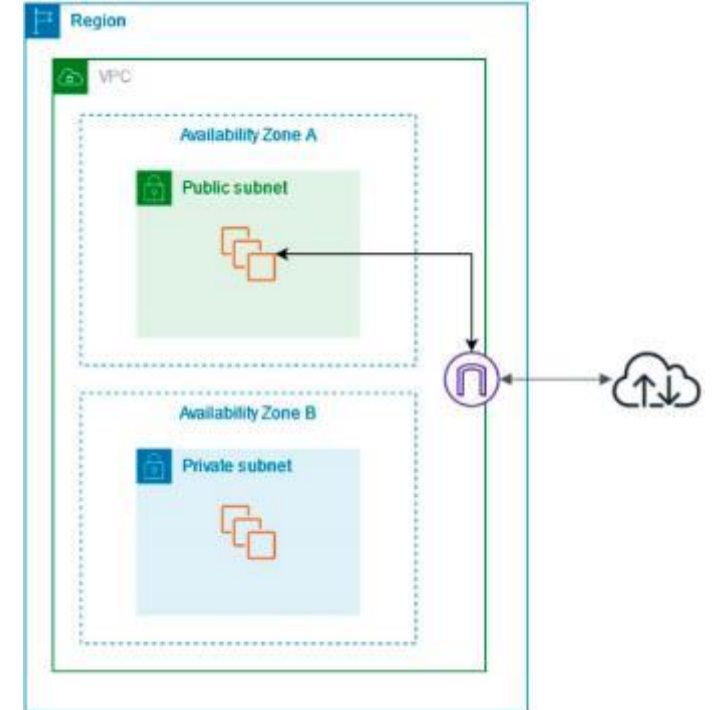
## IPs reservados

- A AWS reserva cinco endereços IP em cada sub-rede da VPC para fins de roteamento, DNS e gerenciamento de rede.
- Esses endereços não podem ser usados para instâncias.

Endereço IP	Propósito
10.0.0.0	Endereço de rede
10.0.0.1	Roteador da VPC
10.0.0.2	Servidor DNS
10.0.0.3	De uso futuro
10.0.0.255	Endereço de broadcast

## — Gateway de internet (internet gateway)

- Gateway de internet é essencial para conectividade da VPC.
- Funciona como um modem, conectando a VPC à internet.
- Altamente disponível e escalável, abrange todas as AZs.
- Deve ser criado e anexado à sua VPC.



# — Gateway de internet (internet gateway)

## Gateway NAT

Ao criar um gateway NAT, você especifica um dos seguintes tipos de conectividade:

### **Pública (padrão)**

Instâncias em sub-redes privadas usam gateway NAT público para se conectar à internet, sem receber conexões não solicitadas.

### **Privada**

Instâncias em sub-redes privadas usam gateway NAT privado para conectividade com outras redes privadas.

## — Tabelas de rota

- Tabelas de rota na AWS determinam o fluxo de tráfego na VPC.
- Destino é o intervalo de endereços IP de destino.
- Alvo é a conexão usada para enviar o tráfego.

Destination ▾	Target ▾	Status ▾	Propagated
0.0.0.0/0	<a href="#">igw-63082</a>	✓ Active	No
172.31.0.0/16	local	✓ Active	No

# — Tabelas de rota

## VPC padrão

- AWS fornece uma VPC padrão em cada região.
- Inclui uma sub-rede pública por AZ, gateway de internet e configuração de DNS.
- Ideal para iniciar instâncias EC2, como blogs ou sites simples.
- VPC padrão tem bloco CIDR /16, sub-redes /20 por AZ, gateway de internet e configurações predefinidas.





## — Aplicação web estática e web dinâmica



A AWS oferece várias arquiteturas para aplicativos web, dependendo de requisitos e características.



Para hospedar um site estático, o Amazon S3 é uma opção econômica e simples, sem custos de execução.

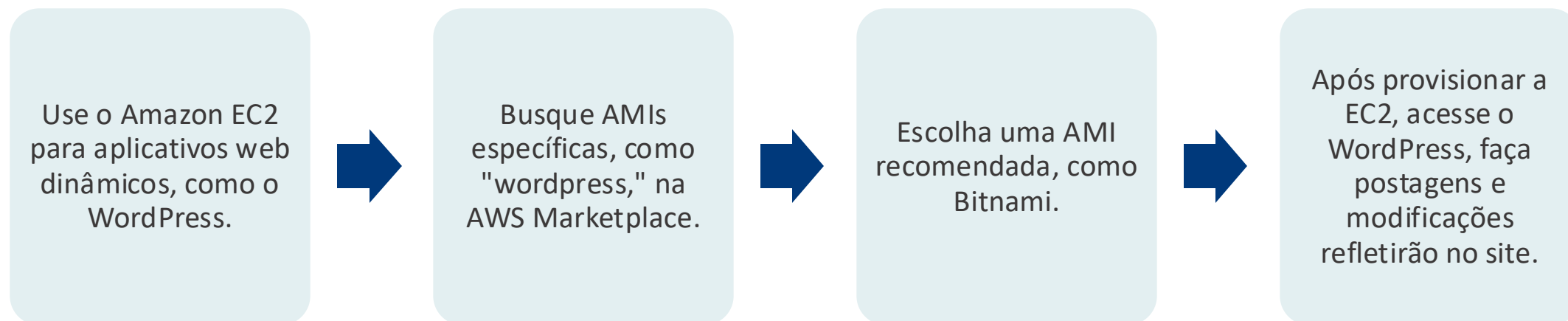


É possível configurar o Amazon S3 para hospedagem estática, permitindo acesso público e ajustando permissões.



Um exemplo de site estático pode ser baixado do GitHub e hospedado no bucket do Amazon S3.

## — Aplicação web dinâmica



# Ambiente de computação em nuvem – Google Cloud



# — Entendendo computação em nuvem



Computação em nuvem elimina a necessidade de infraestrutura local, economizando espaço e recursos.



Permite acesso sob demanda a servidores e recursos, evitando preocupações com hardware, instalações e manutenção.



Recursos são alugados conforme a necessidade, eliminando gastos desnecessários.



Facilita a escalabilidade e flexibilidade dos recursos de TI.

## — Soluções como serviço



A computação em nuvem oferece três modelos de serviços: **IaaS**, **PaaS** e **SaaS**.



IaaS fornece infraestrutura sob demanda, mas não permite escolher hardware.

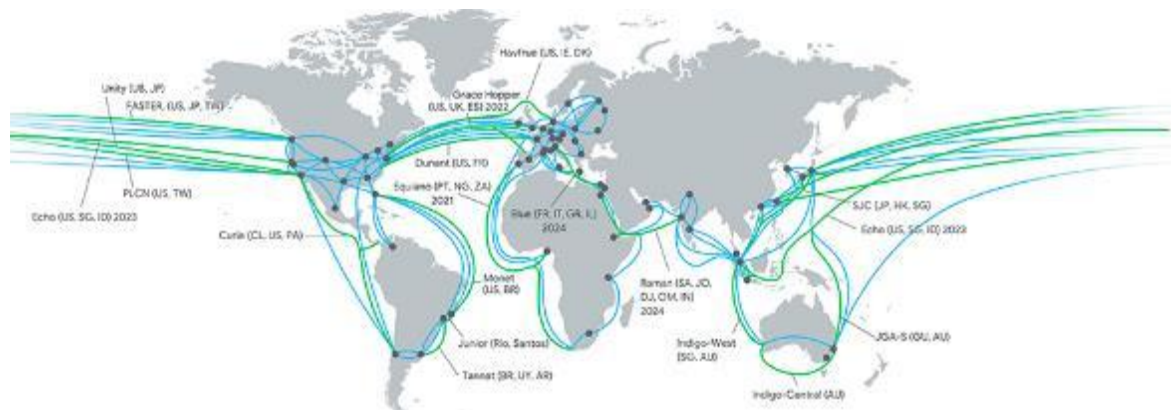


PaaS agrega software de plataforma, limitando a flexibilidade do sistema operacional e bibliotecas.



SaaS é a solução mais abstrata, ideal para aplicativos sem necessidade de personalização de infraestrutura.

# — A computação em nuvem do Google



Google Cloud Platform (GCP) é o serviço de nuvem do Google com datacenters em várias regiões.

- GCP oferece infraestrutura como serviço (IaaS) e tecnologias avançadas.
- O Google possui uma rede própria de cabos submarinos conectando seus datacenters.
- Produtos populares do Google usam a mesma infraestrutura do GCP, garantindo segurança e eficiência.

## — Redes em ambientes Google Cloud



Google cloud utiliza VPC (virtual private cloud) para comunicação em nuvem.



VPC é global e permite alocar sub-redes em várias regiões para otimizar o acesso e a recuperação de desastres.



Isso melhora a latência e disponibilidade para usuários de diferentes locais.



Serve para estratégias de recuperação de desastres e melhora a experiência do usuário.

# — Máquinas virtuais em ambientes Google Cloud



Máquinas virtuais (VMs) no Google Cloud são "emulações" de computadores físicos, oferecendo flexibilidade para executar diferentes sistemas operacionais.



O Google Cloud fornece VMs como parte de sua infraestrutura como serviço (IaaS) chamada Compute Engine, com várias opções para diferentes necessidades de recursos.



Após escolher uma VM, os usuários podem personalizá-la com sistemas operacionais e software.



A responsabilidade de gerenciamento de VMs é compartilhada: o Google cuida da infraestrutura física, enquanto os usuários administram o software e recursos da VM.



## — Aplicações para ambientes de nuvem



Aplicações na nuvem devem ser "cloud native" para otimizar o consumo de recursos.

- Duas arquiteturas principais: "com estado" e "sem estado".
- Arquiteturas "sem estado" suportam implantação "serverless" e escalabilidade elástica.
- Google Cloud oferece soluções como o Cloud Run para aplicações "sem estado" e outras opções para aplicações "com estado".

## — Segurança em Google Cloud

	On-premises	IaaS	PaaS	SaaS
Responsabilidade do usuário/cliente				
Responsabilidade do Google Cloud				
Conteúdo				
Políticas de acesso				
Usabilidade				
Implantação				
Segurança de App Web				
Operações				
Acesso e autenticação				
Segurança de rede				
Sistema Operacional				
Armazenamento				
Boot				
Hardware				

A segurança em Google Cloud segue uma matriz de responsabilidades.

- Normas regulamentadoras, como a LGPD e a ISO/IEC 27001, são seguidas para garantir a proteção de dados e a segurança da infraestrutura.
- O Google Cloud possui protocolos de segurança rigorosos em seus datacenters.

## — Segurança na nuvem

- A computação em nuvem facilita a inovação, mas a segurança ainda é uma preocupação.
- Diversos tipos de ameaças afetam as empresas, impactando seus negócios.
- "Segurança na nuvem" engloba práticas e tecnologias para proteger dados, aplicativos e infraestrutura.
- Inclui gestão de acesso, segurança contra ataques e listas de bloqueio.



# — Segurança na nuvem

## Gestão de acesso e identidade



IAM (Gestão de Identidade e Acesso) controla o acesso a informações e recursos em ambientes na nuvem.



O Google Cloud oferece uma solução integrada de IAM para gerenciar usuários e seus níveis de acesso.



Exemplo: Usuários com níveis de acesso específicos podem visualizar/editar apenas informações relevantes a suas responsabilidades.



A autenticação de vários fatores, como senha e SMS, reforça a identidade do usuário e aumenta a segurança.

# — Segurança na nuvem

## Segurança contra ataques

O Google Cloud oferece o Cloud Armor, que utiliza IA e aprendizado de máquina para mitigar ataques a aplicações e servidores dos clientes.



O Cloud Armor analisa dados para identificar e evitar ameaças, como ataques DDoS que causam indisponibilidade.



O reCAPTCHA, outra tecnologia do Google, distingue acessos humanos de automatizados, protegendo contra bots maliciosos.



Ambas as tecnologias contribuem para reforçar a segurança contra ataques às aplicações.

# — Segurança na nuvem

## Lista de bloqueio

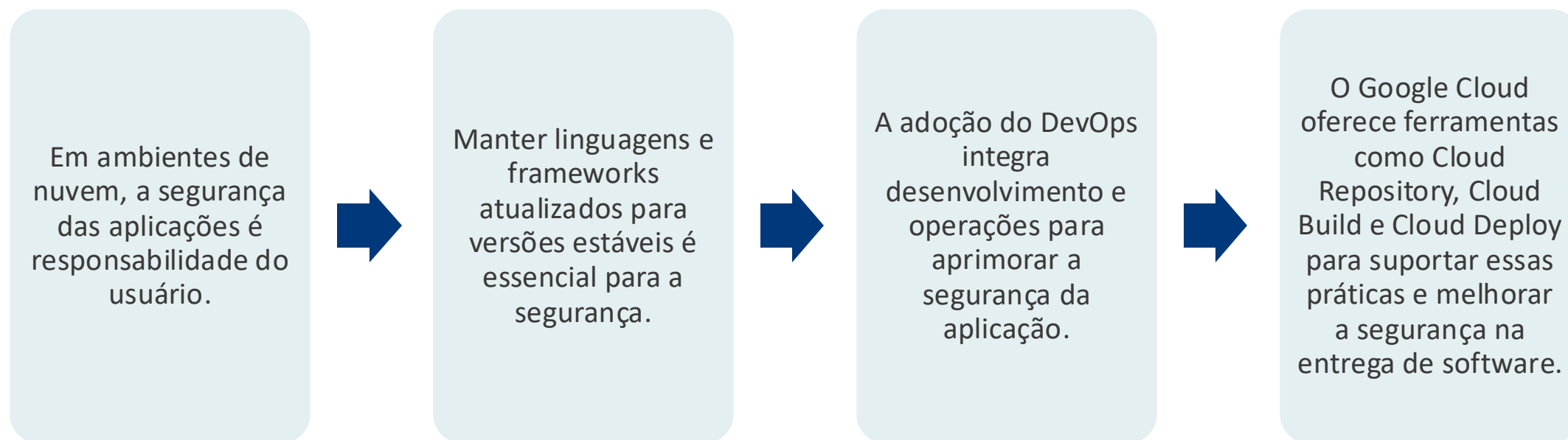
Listas de bloqueio (blocklist) e listas de permitidos (allowlist) são estratégias comuns de controle de acesso.

Elas permitem criar listas de bloqueio ou permissões com base em IPs ou regiões.

Úteis para negar acesso a IPs externos ou bloquear tráfego de países, reduzindo ataques em massa.

Essas listas são ferramentas eficazes para fortalecer a segurança de ambientes online.

## — Segurança nas aplicações



# — Operações em Google Cloud

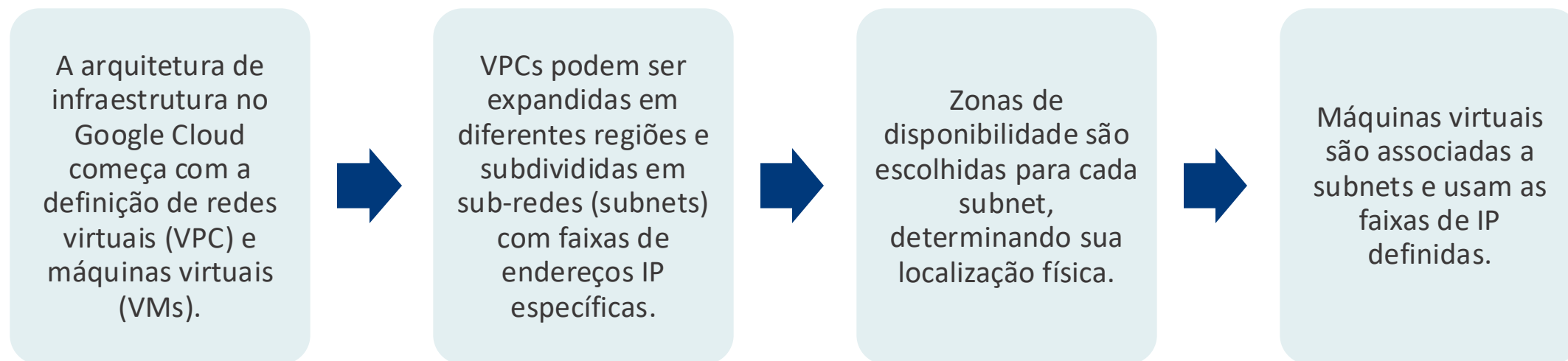


Operações em nuvem envolvem operar e gerenciar infraestrutura para manter desempenho e disponibilidade.

- Monitoramento é fundamental, com LOGS registrando eventos relevantes, ajudando na prevenção e correção.
- O Google Cloud oferece o Cloud Monitoring para coletar dados detalhados de aplicações e infraestrutura.
- Esses dados auxiliam na melhoria contínua, prevenção de problemas e tomada de decisões embasadas em métricas reais.



## — Aplicação da arquitetura de infraestrutura



## — Aplicação da arquitetura de aplicativos

- Para ambientes de nuvem, é ideal adotar a arquitetura nativa de nuvem, que se adapta às tecnologias oferecidas pelo provedor.
- O Google Cloud oferece ferramentas para facilitar o desenvolvimento de aplicativos e melhorar o desempenho do negócio.
- Em um cenário de e-commerce, funções como página do produto e check-out apresentam desafios de desenvolvimento significativos.



# — Aplicação da arquitetura de aplicativos

## Página do produto

A função da página do produto em um site de e-commerce envolve mostrar informações como nome, descrição, preço e estoque.

Para garantir consistência e disponibilidade dessas informações, é essencial utilizar um banco de dados organizado em tabelas.

Em ambientes de nuvem, o Google Cloud oferece o Cloud SQL, um banco de dados SQL gerenciado, altamente disponível e escalável.

Com o Cloud SQL, os desenvolvedores podem se concentrar na aplicação, sem se preocupar com a gestão de infraestrutura do banco de dados.

# — Aplicação da arquitetura de aplicativos

## Finalização de compras e checkout

- Na finalização de compras de e-commerce, dependência de sistemas pode causar atrasos e frustração.
- A "comunicação assíncrona" permite processos independentes sem espera síncrona.
- O Google Cloud oferece o serviço Pub/Sub, gerenciando a comunicação assíncrona entre sistemas, melhorando flexibilidade e disponibilidade.

