

# Google Cloud Fundamentos

**Carlos Barbero**

Cloud Architect na SantoDigital, trabalho com Google Cloud desde 2011.

**@carlosrgomes**



# Objetivo Geral

O objetivo do curso é apresentar os fundamentos iniciais ao se trabalhar com Google Cloud, abordaremos questões referentes a domínio, acessos, políticas de organizações, gestão de identidade, recursos, controle de custos entre outros assuntos pertinentes a todos que necessitam iniciar a utilização de forma segura e prática.

# Percurso

**Etapa 1**

**Pontos importantes na adoção da nuvem**

**Etapa 2**

**Gestão de Identidade**

**Etapa 3**

**Gestão de recursos**

# Percorso

**Etapa 4**

**Gestão de acesso (IAM)**

**Etapa 5**

**Rede**

**Etapa 6**

**Monitoramento e Registro**

# Percorso

**Etapa 7**

**Gestão de dados**

**Etapa 8**

**Controle de custos**

**Etapa 9**

**Introdução a Infraestrutura com código**

# Percorso

**Etapa 10** CI/CD

**Etapa 11** Arquitetura resiliente

**Etapa 12** Gestão de incidentes

# Pré-requisitos

- Esse curso possui o pré-requisito ter participado do curso sobre Introdução ao Google Cloud e dedicação pessoal para aperfeiçoar o conhecimento abordado.

## Etapa 1

# Pontos Importantes na adoção da nuvem

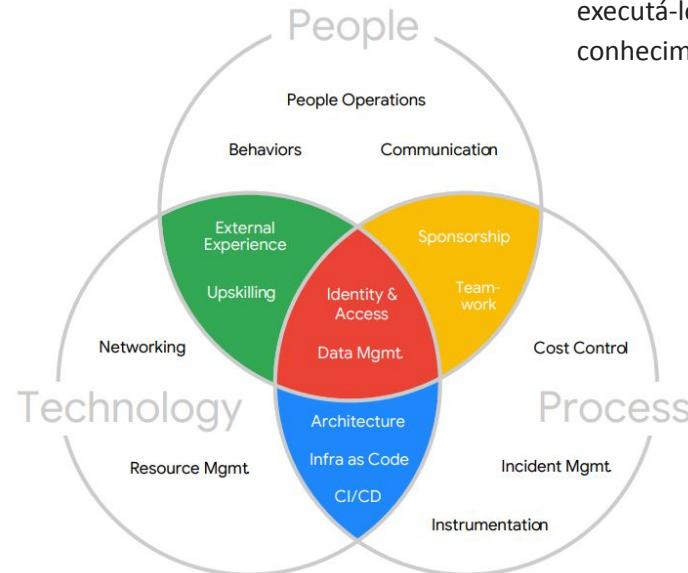
# Pontos importantes na adoção da nuvem

## Aprender Continuamente

Utilize sempre as melhores práticas

## ESCALAR eficientemente

Codificar atividades e políticas em código, tornando-as escalonáveis e auditáveis.



## LIDERAR com efetividade

Definir claramente os objetivos e executá-los com precisão e conhecimento.

## Proteger de forma abrangente

Defender profundamente para que atende aos objetivos certos\*, reduzindo a ocorrência de erros humanos \*, e acompanhar novas ameaças constantemente\*

[https://services.google.com/fh/files/misc/google\\_cloud\\_adoption\\_framework\\_whitepaper.pdf](https://services.google.com/fh/files/misc/google_cloud_adoption_framework_whitepaper.pdf)

Etapa 2

# Gestão de Identidade

# Percorso

**Etapa 1**

**Pontos importantes na adoção da nuvem**

**Etapa 2**

**Gestão de Identidade**

**Etapa 3**

**Gestão de recursos**

# Objetivo

- Autenticação confiável e segura da identidade dos usuários ou serviços
- Proteção contra perda de credenciais e tentativas de falsificação de identidade

# Casos de Uso

## Como sysadmin

Desejo sincronizar contas de usuário do Active Directory ou Azure AD com o Google Cloud, então tenho uma única fonte de informações e de processo de entrada/saída.

Quero que os usuários se autentiquem usando **single sign-on (SSO)**, para que os funcionários não precisem gerenciar e lembrar de outra senha (ou reutilizar a mesma senha).

# Casos de Uso

## Como empresa

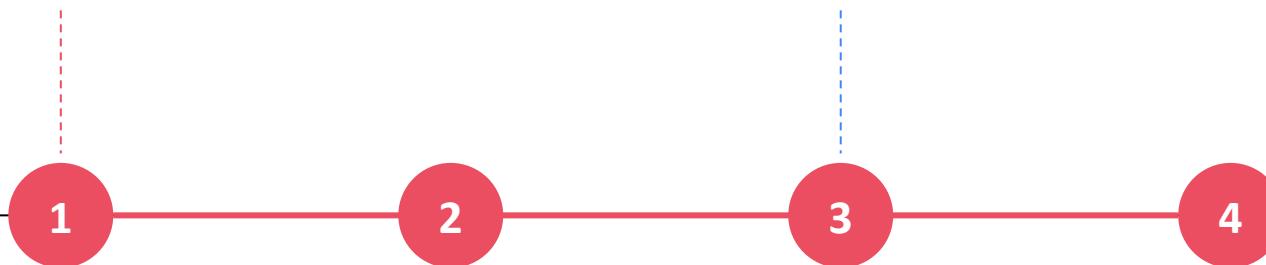
Quero segregar grupos de **administradores com funções específicas**, para que possa conceder as permissões de administrador adequadas de maneira fácil e consistente (incluindo Organização, Segurança, Rede, Finanças).

Desejo criar **várias organizações do Google Cloud** para conseguir a separação de interesses entre unidades de negócios e ambientes independentes

# Itens que abordaremos

Cloud identity

Provisionamento de usuários



1

2

3

4

Opções de  
autenticação

Auditoria

# Cloud Identity

## Autenticação



Cloud Identity

## Autorização



Cloud IAM

## Auditoria



Cloud Operations Audit Logging  
& Reports API

# O que é Cloud Identity?



- Cloud Identity é uma solução de Identidade como Serviço (IDaaS) que **permite que você gerencie de maneira centralizada usuários e grupos** que podem acessar os recursos de nuvem do [Google Cloud](#) and [Google Workspace](#)
- É o mesmo serviço de identidade que alimenta o Workspace e também pode ser usado como IdP para aplicativos de terceiros (compatível com aplicativos SAML e LDAP)

<https://cloud.google.com/identity/docs/overview>

# O que o Cloud Identity nos fornece?



## Recursos unificados



Gestão do ciclo de vida dos usuários



Segurança de conta



Single sign-on



Cloud Directory



Gestão de dispositivos



Relatórios e análises

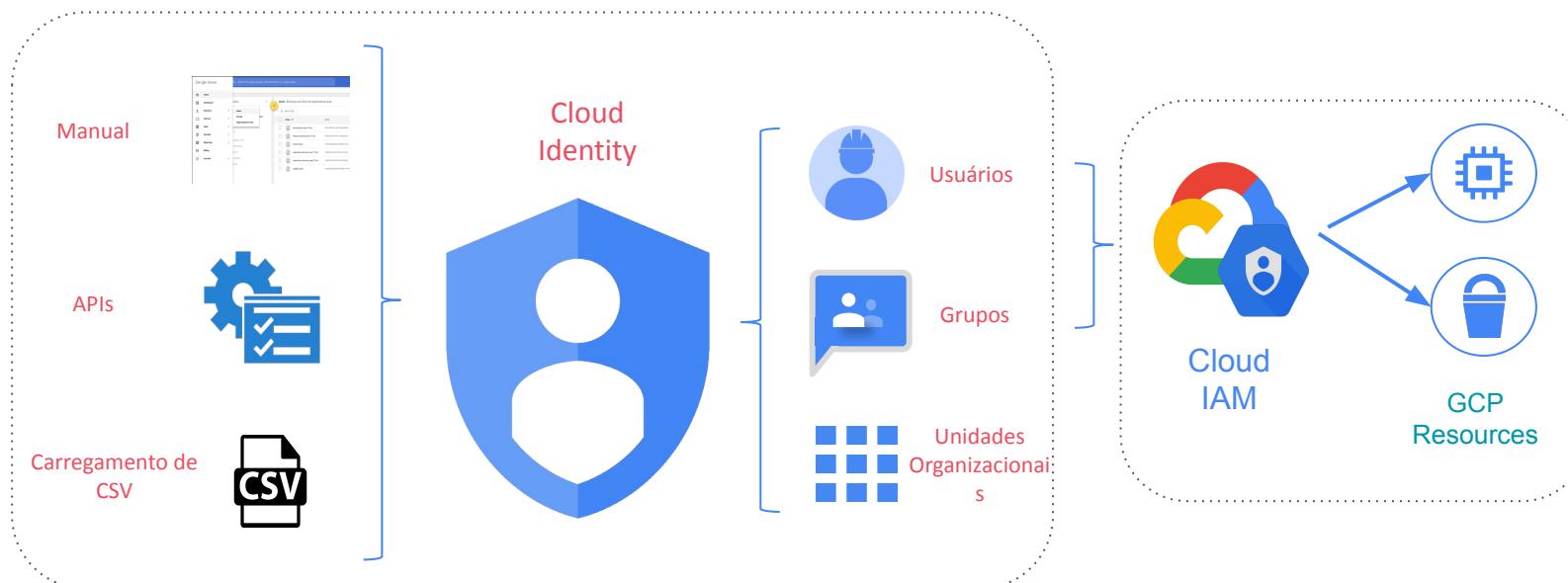


Gerenciamento de App



Extensível por meio de APIs

# Usuários e Grupos

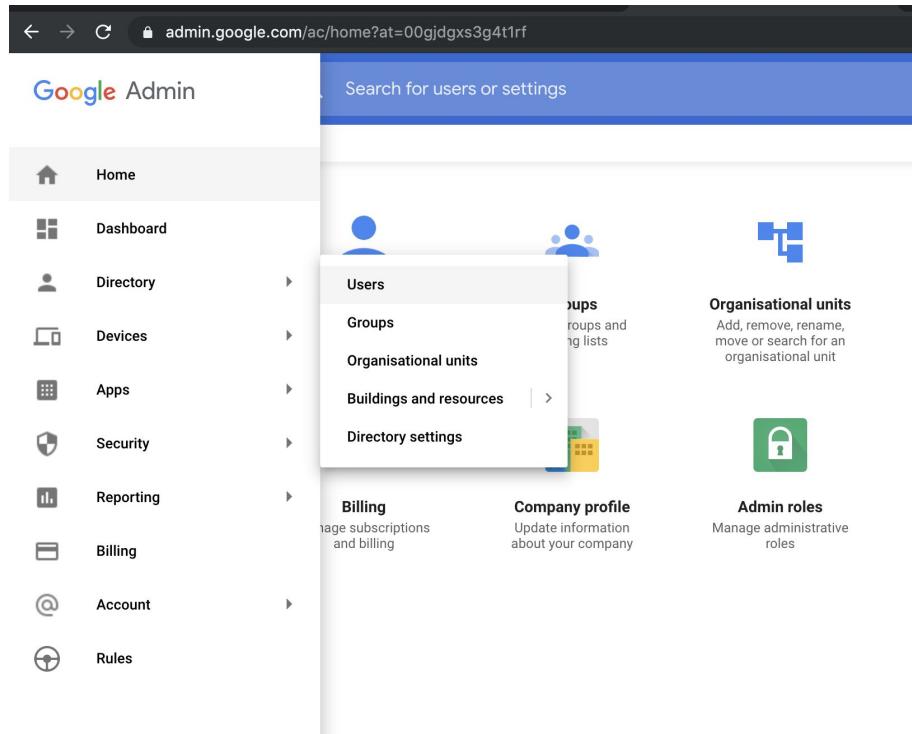


# Usuários e Grupos

Usuários e grupos criados no Cloud Identity são as **identidades do Google** onde podem ser atribuídos **papéis IAM** no console do GCP.

Os **papéis do Cloud Identity** gerenciam apenas aspectos do Cloud Identity, como gerenciamento de usuário / grupo, e **são diferentes dos papéis do GCP** que gerenciam permissões para recursos da nuvem

# Consoles



## Cloud Identity (admin.google.com)

- *Gerenciando usuários,*
- *Grupos e configurações de Autenticação*

# Consoles

The screenshot shows the Google Cloud Platform dashboard at [console.cloud.google.com/home/dashboard?folder=&organizationId=&project=sso-server-200417](https://console.cloud.google.com/home/dashboard?folder=&organizationId=&project=sso-server-200417). The left sidebar lists various services: Home, Compute Engine, BigQuery, Marketplace, Billing, APIs & Services, Support, IAM & admin, Getting started, and Security. The 'IAM & admin' section is expanded, showing the 'IAM' menu with options: Identity & Organisation, Organisation policies, Quotas, Service accounts, Labels, Settings, Privacy & Security, Cryptographic keys, Identity-Aware Proxy, Roles, Audit Logs, and Manage resources. The main content area displays a chart titled 'Compute Engine' showing CPU utilization over time, with a legend indicating 'instance/cpu/utilization: 1.7e-3'. A link 'Go to Compute Engine' is present below the chart.

Google Cloud  
([console.cloud.google.com](https://console.cloud.google.com))

Papéis e Autorizações para o  
Google Cloud

# Administração e Gestão

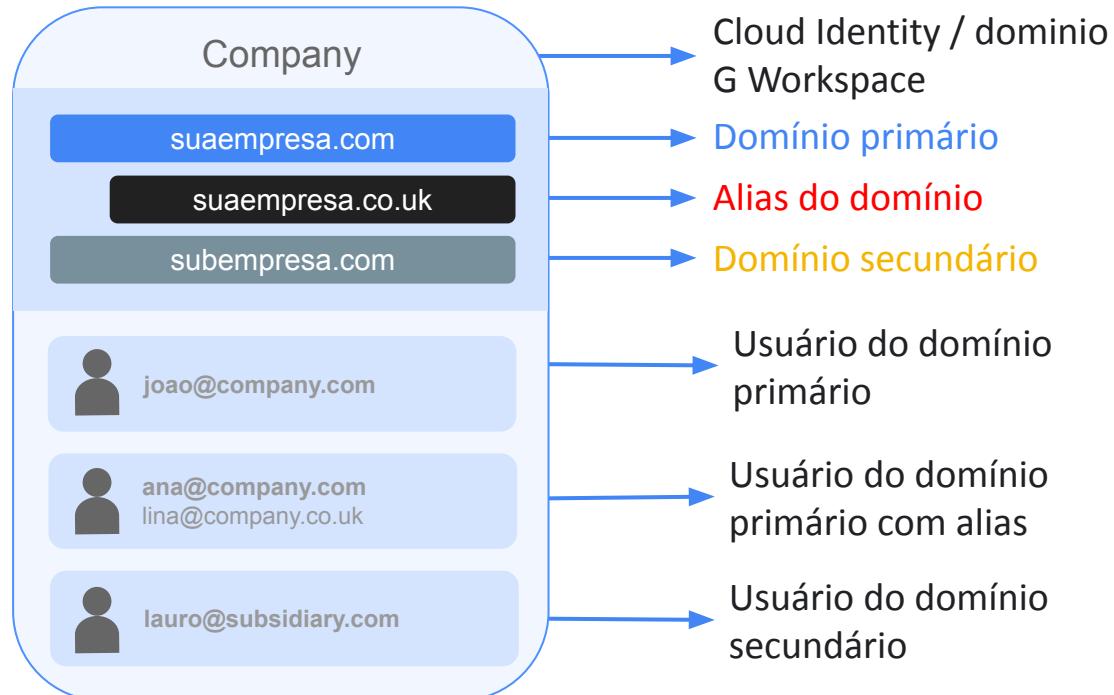
## Cloud Identity Admin console, Admin SDK

- Criação e gerenciamento de contas de usuário
- Criação e gerenciamento de grupos
- Atribuição de papéis de acesso e administração de identidade para usuários
- Impõe opções de autenticação para usuários

## GCP Console, gcloud CLI, API

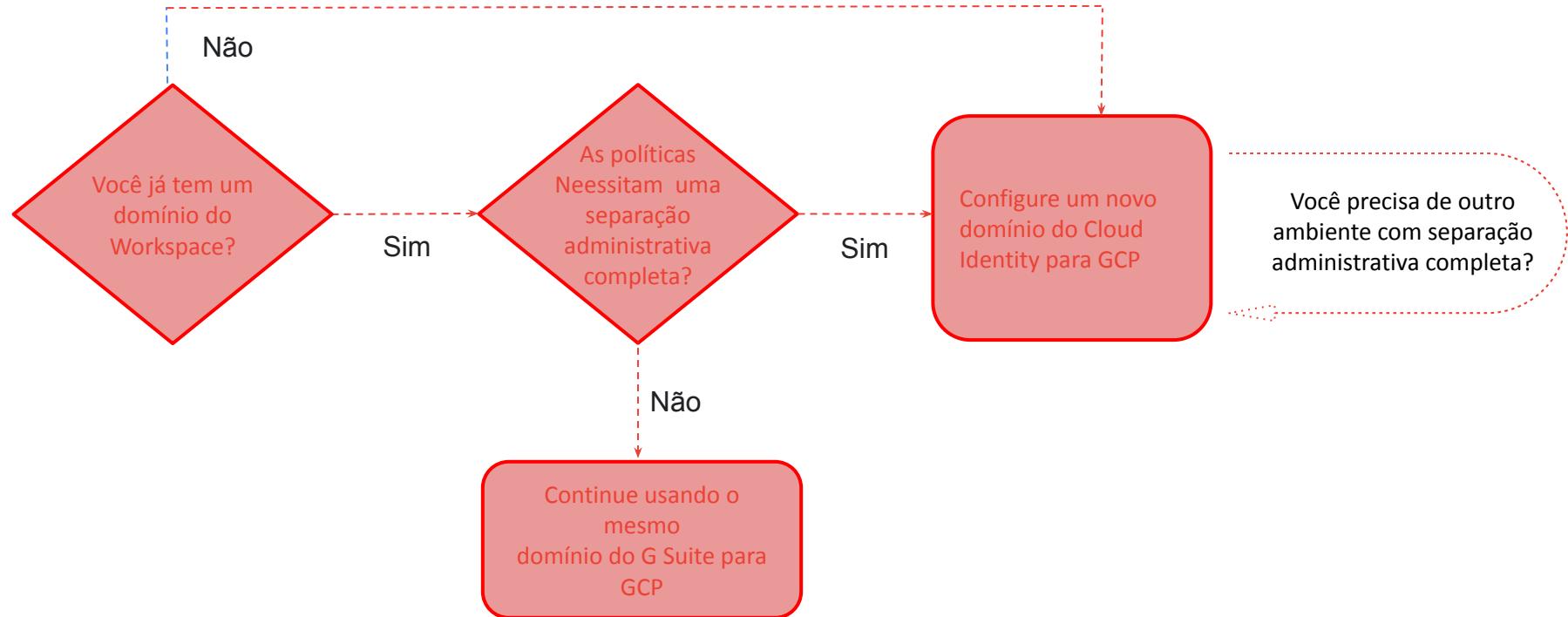
- Provisionamento de recursos do Cloud Platform
- Atribuição de papéis de acesso e gerenciamento de identidade para recursos do Cloud Platform a usuários e grupos definidos no Cloud Identity
- Configuração da rede e a integração local

# Palavras chave



# Cloud Identity: Configuração

## Mapa decisão



# Cloud Identity: free vs Premium

	Cloud Identity Free	Cloud Identity Premium
Gerenciamento básico de dispositivos móveis	✓	✓
Aplicação básica da senha (dispositivo móvel)	✓	✓
Apagamento remoto da conta (dispositivo móvel)	✓	✓
Gerenciamento fundamental para computadores	✓	✓
Computadores da empresa	✓	✓
Desconexão remota (computadores)	✓	✓
Verificação de endpoints	✓	✓

[Link](#)

# Responsabilidade dos Administradores



(Cloud Identity) Super  
Admin



(Cloud IAM) Organization  
Admin

# Boas práticas segurança



Workspace

GCP

# Exemplo Prático

## Provisionando Usuários

### Cloud Identity



Etapa 3

# Gestão de Recursos

# Percorso

**Etapa 1**

**Pontos importantes na adoção da nuvem**

**Etapa 2**

**Gestão de Identidade**

**Etapa 3**

**Gestão de recursos**

# Objetivos

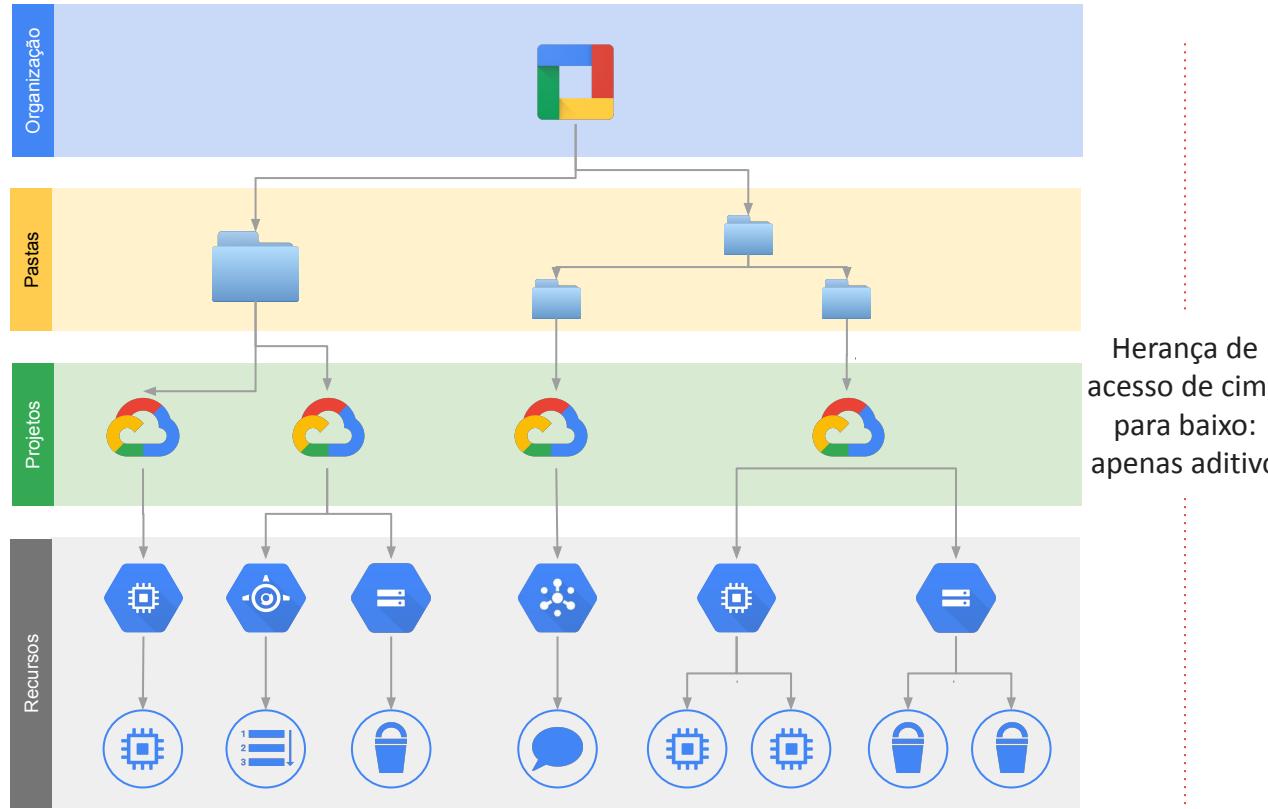
- Organizar nomes e recursos na nuvem
- Garantir processos e projetos estruturados

# Motivações de uso

- Desejo ter uma hierarquia de recursos para poder controlar e descobrir quem é o responsável.
- Desejo ter controle e restrições dos recursos.
- Desejo ter meus projetos de forma organizada e segura com informações claras.
- Desejo automatizar processos para evitar erros humanos e criar padrões programáveis via código.



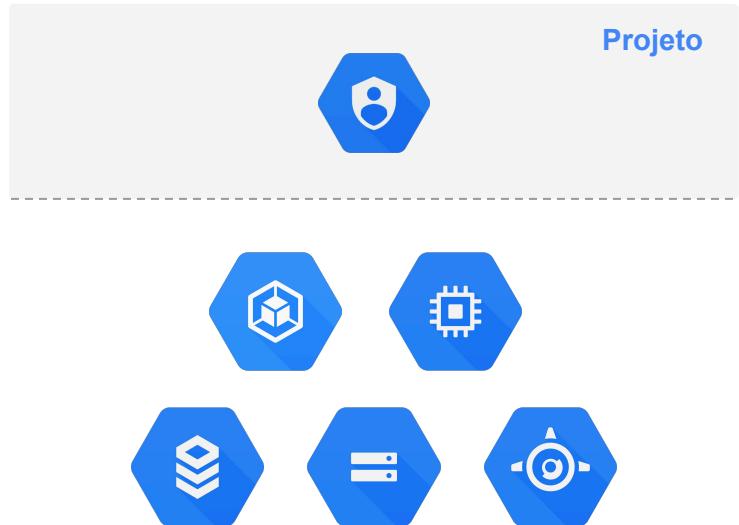
# Hierarquia da Organização



A política efetiva para um recurso é a união da política definida neste recurso e a política herdada de seu pai.

# Projetos

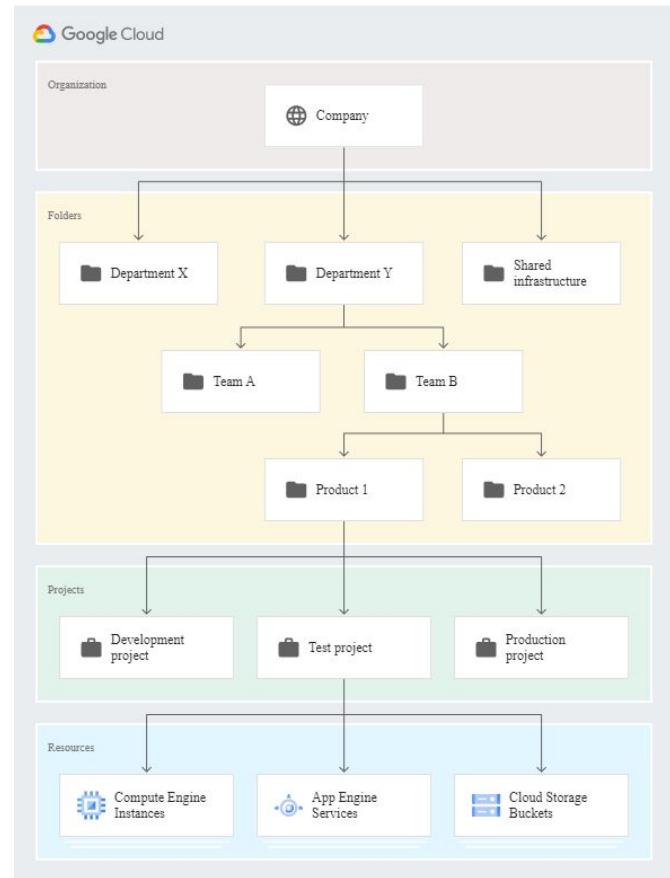
- Onde estão nossos workloads e produtos que estamos utilizando Ex: Compute Engine, Storage etc..
- Projetos são completamente isolados uns dos outros
- Utilizamos para agrupamentos de workloads divididos por uma lógica de negócio ex: financeira, jurídica, inovação.
- Os projetos podem fazer parte de uma organização
- O provisionamento é simples e gratuito



# Pastas / Folder

As pastas são nodes no [Cloud Platform Resource Hierarchy](#). Uma pasta pode conter projetos, outras pastas ou uma combinação de ambos. As organizações podem usar pastas para agrupar projetos no nó da organização em uma hierarquia. Por exemplo, sua organização pode conter vários departamentos, cada um com seu próprio conjunto de recursos do Google Cloud. Com as pastas, você pode agrupar esses recursos por departamento ou agrupar recursos que compartilham políticas comuns do IAM. Cada pasta pode conter várias pastas ou recursos. No entanto, uma determinada pasta ou recurso pode ter somente um pai.

<https://cloud.google.com/resource-manager/docs/creating-managing-folders>

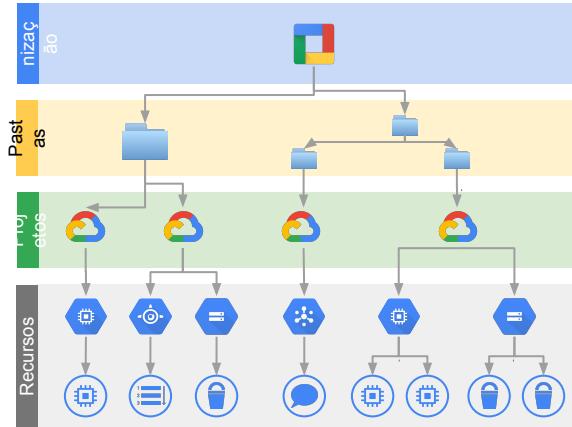


# Organização

O recurso Organização representa uma organização e é o nó **raiz na hierarquia de recursos do Google Cloud**. Ele é o ancestral hierárquico dos recursos de projeto e de pastas. O recurso **Organização** está **intimamente associado a uma conta do Google Workspace ou do Cloud Identity**. Quando um usuário com uma conta do Google Workspace ou do Cloud Identity cria um projeto do Google Cloud, um recurso Organização é provisionado automaticamente para ele.

Quando um usuário gerenciado cria um projeto, o requisito é que ele esteja em alguma organização. Se um usuário especificar uma organização e tiver as permissões corretas, o projeto será atribuído a ela.

<https://cloud.google.com/resource-manager/docs/cloud-platform-resource-hierarchy#organizations>

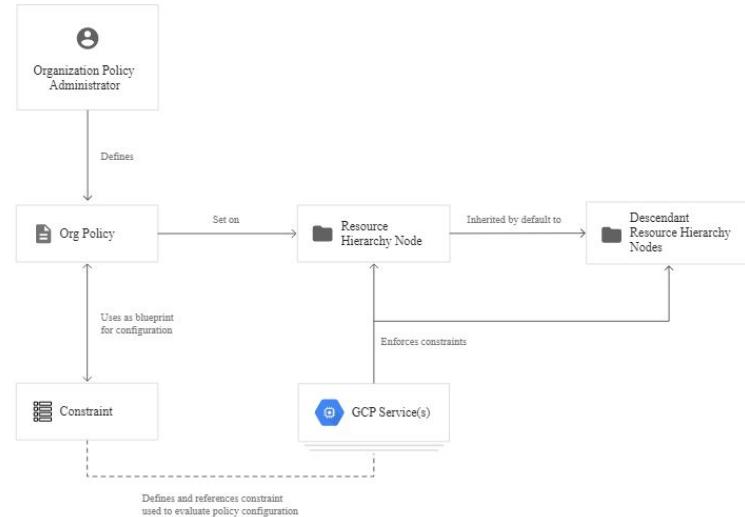


# Políticas de Organização

O Serviço de políticas da organização oferece controle centralizado e programático sobre os recursos da nuvem da sua organização. Como [administrador de políticas da organização](#), você tem permissão para configurar restrições em toda a [hierarquia de recursos](#).

## Benefícios

- Centralizar o controle para configurar limitações sobre como os recursos da sua organização podem ser usados.
- Definir e estabelecer proteções para que suas equipes de desenvolvimento permaneçam dentro dos limites de conformidade.
- Ajudar os proprietários de projetos e suas equipes a se movimentarem rapidamente sem a preocupação de violar a conformidade.



# Políticas de Organização

## Conceitos

### Restrições

Uma restrição é um tipo específico de limitação quanto a um serviço ou uma lista de serviços do Google Cloud. Pense na restrição como um esquema que define quais comportamentos são controlados. O serviço do Google Cloud mapeado para essa restrição e associado ao nó da hierarquia de recursos aplicará as limitações configuradas na política da organização.

### Herança

Ao definir uma política da organização em um nó da hierarquia de recursos, todos os descendentes desse nó herdam a política por padrão. Um usuário com o papel de administrador de políticas da organização pode definir nós descendentes da hierarquia de recursos com outra política que substitua a herança ou os mescle com base nas regras de avaliação de hierarquia. Para saber mais sobre a avaliação da hierarquia, consulte a página Noções básicas sobre a hierarquia.

# Políticas de Organização

## Conceitos

### Violações

Uma violação ocorre quando a execução ou o estado de um serviço do Google Cloud contraria a configuração de restrições da política da organização dentro do escopo da hierarquia de recursos. Se uma restrição de política da organização for aplicada retroativamente, ela será rotulada como tal na [página Restrições da Política da Organização](#).



# Políticas da Organização Recomendadas

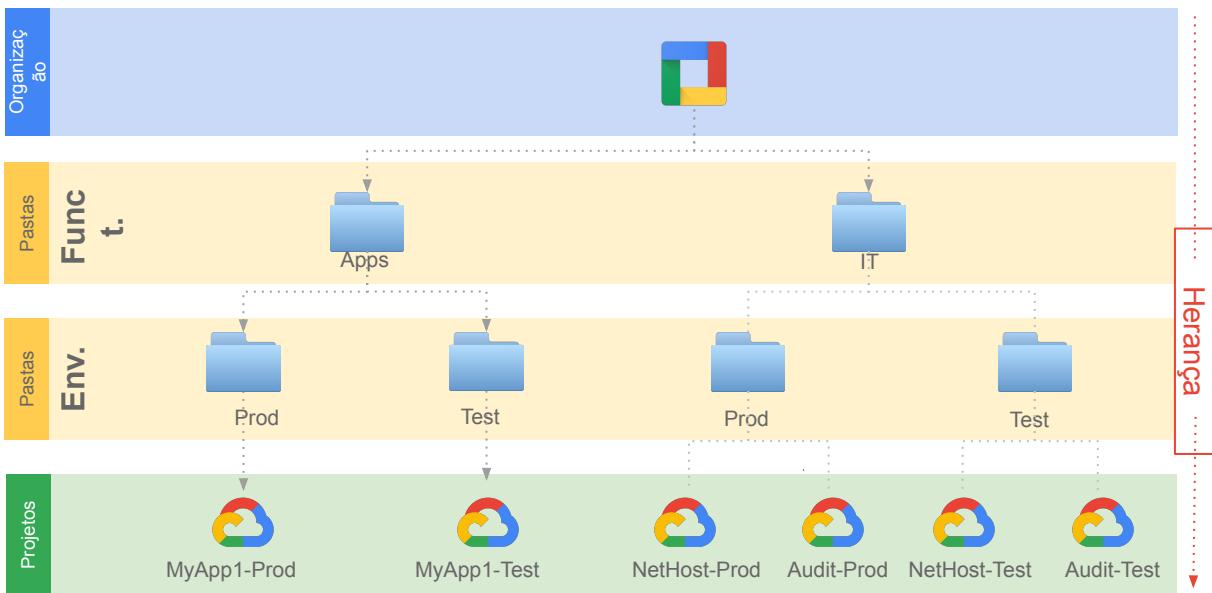
<https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints>

Serviços	Restrições	Descrição	Util para
Google Compute Engine	IPs externos para instâncias de VM	Define um conjunto de instâncias de VM com permissão para usar endereços de IP externos	Garantir uma superfície <b>externa mínima</b> . Normalmente, as VMs devem possuir apenas IPs internos.
	Pular criação de rede padrão	Ignora a criação da rede padrão e recursos relacionados durante a criação do projeto.	Aplicar o uso de redes VPC protegidas e gerenciadas de forma centralizada
	Exigir login para o OS	Ativa o login do SO em todos os projetos recém-criados.	Garantir que o acesso por SSH às VMs é <b>gerenciado de forma centralizada pelo IAM</b> , e não por chaves SSH armazenadas como metadados de projeto/VM.
Cloud IAM	Compartilhamento restrito por domínio (Beta)	Define o conjunto de membros (domínios) que podem ser adicionados às políticas do Cloud IAM.	Se proteger contra atos <b>maliciosos e erros humanos</b> , garantindo o acesso apenas aos usuários em <b>domínios permitidos</b> .
Google Cloud	Restrição de localização dos recursos (Beta)	Define o conjunto de locais onde os recursos do Google Cloud baseados em localização podem ser criados	Estar em <b>conformidade com regulamentos</b> que restringem a localização de recursos (por exemplo: GDPR)
Cloud Storage	Aplicar apenas políticas no bucket	Requer buckets para usar apenas a política de Bucket	As <b>políticas de acesso no nível do objeto</b> ignoram a política no nível do bucket. Eles são difíceis de serem enxergadas e podem se tornar um <b>risco à segurança</b> .

# Design da Organização

	Poucos projetos	Muitos projetos
Complexidade do projeto	Baixa	Alta
Complexidade do IAM	Alta	Baixa
Tráfego de rede entre projetos	Menos frequente – N/A	Mais frequente – VPN/shared VPC
Menor privilégio	Mais difícil	Menos difícil

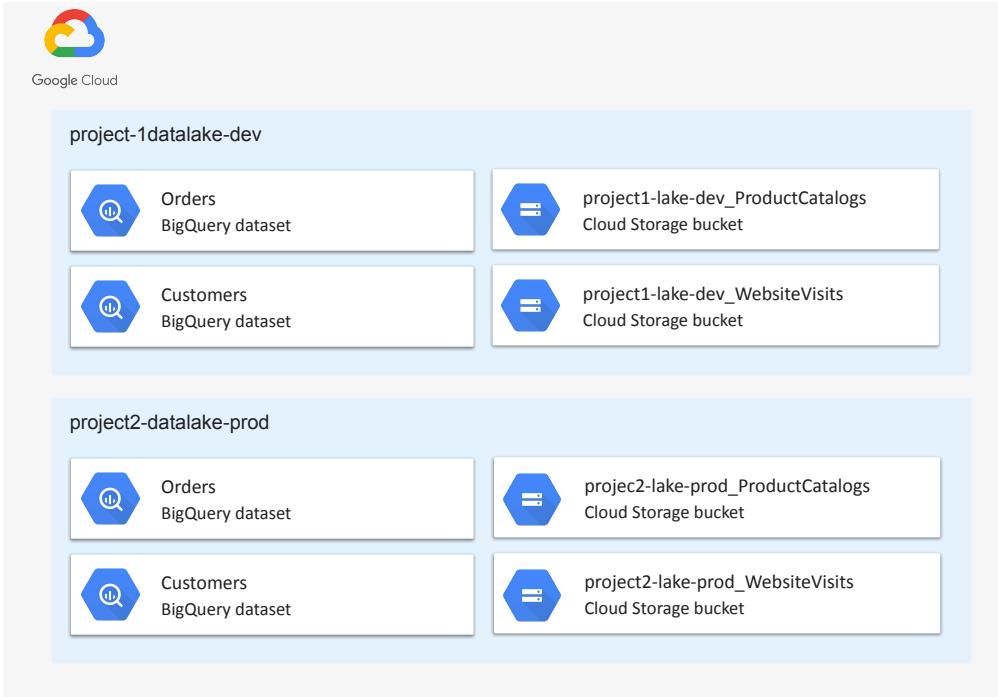
# Hierarquia Baseada em Funções



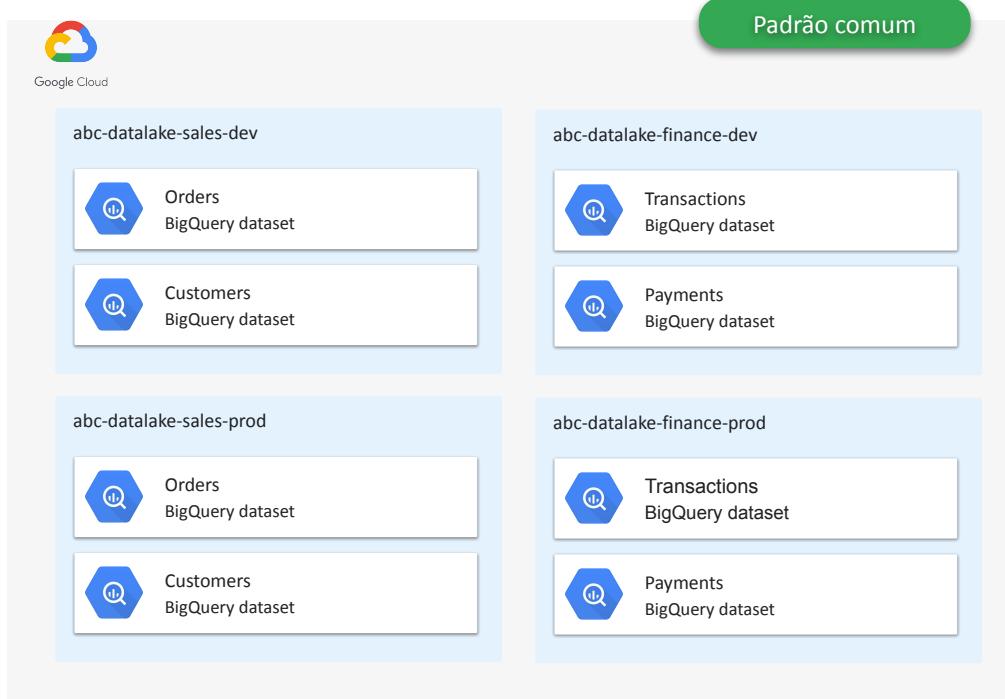
Prós	Contras
Permite separação para serviços compartilhados	Estrutura complexa e automação usando IaC
Preserva a separação por função e ambiente	Não separa o acesso por unidade de negócio

# Um projeto para cada ambiente

Anti-pattern



# Um projeto para cada aplicação e Ambiente



# Design: Nome do Projeto

	Nome do projeto	Número do projeto	ID do projeto
Atribuído	Pelo usuário	Automaticamente	Pelo usuário
Único globalmente	Não	Sim	Sim
Mútavel	Sim	Não	Não
Considerações de design	Nenhuma	Nenhuma	<p><b>Prefixo com o nome da empresa</b> para ajudar a garantir exclusividade global</p> <p><b>Não inclua atributos que podem mudar</b> no futuro, por exemplo: nome da equipe, tecnologia usada</p>

# Organização do Projeto

- Um projeto por aplicativo ou serviço para cada ambiente
- Possível atributos adicionais: classificação de dados
- Esquema de nomenclatura de ID de projeto consistente para todos os projetos da empresa

Projeto por aplicação  
ou serviço  
  
“empresa-departamento-  
produto-dev”

Dev

Projeto por aplicação  
ou serviço  
  
“empresa-departamento-  
produto-test”

Test

Projeto por aplicação  
ou serviço  
  
“empresa-departamento-  
produto-prod”

Prod

# Estrutura de pastas

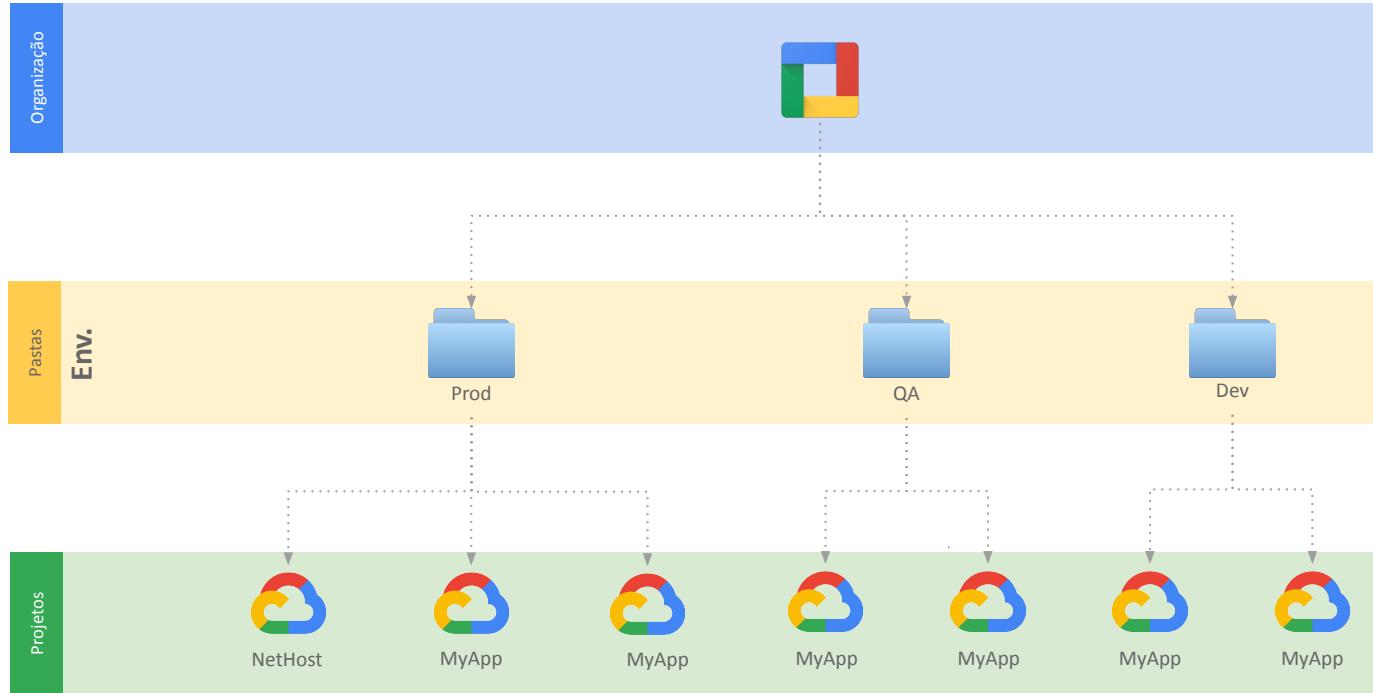
## Níveis

Na maior parte dos casos, três ou quatro níveis de pasta são suficientes

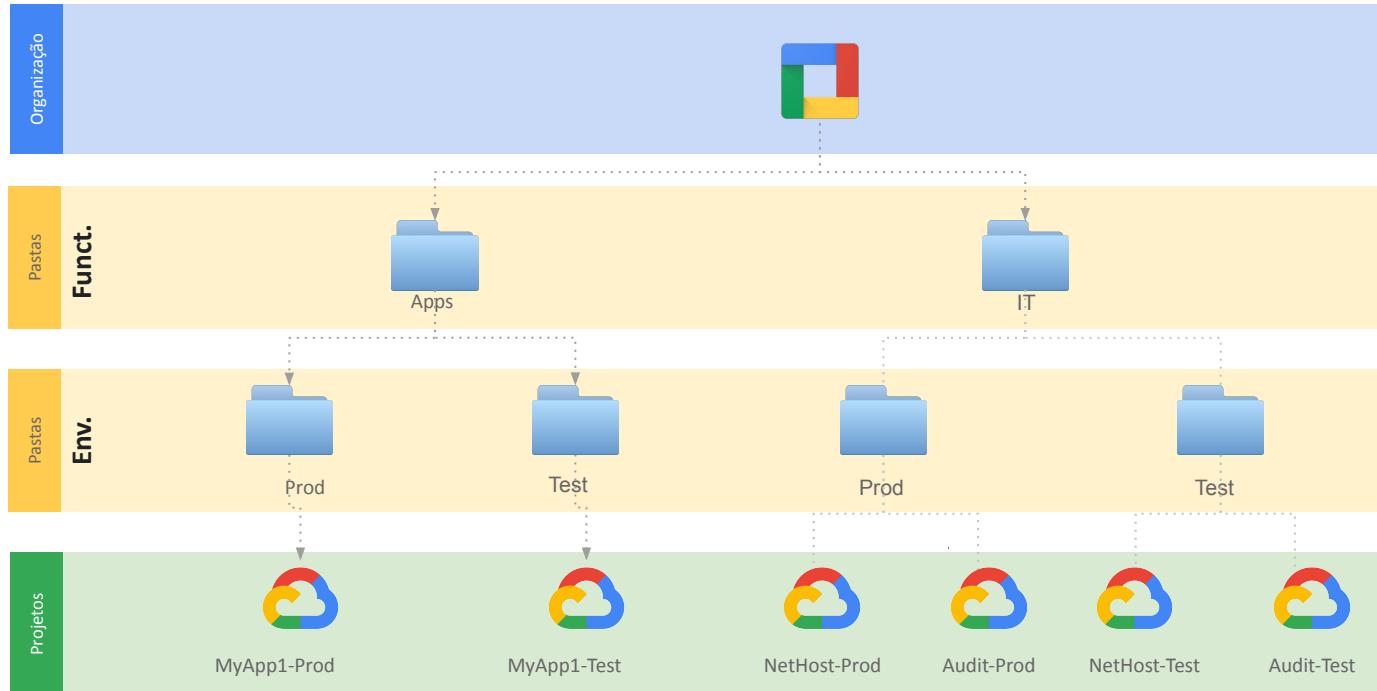
## Extensível

A estrutura de pasta é flexível e facilmente extensível. Você pode **começar de forma simples**, e adicionar mais níveis quando necessário

# Hierarquia Baseada em Ambientes



# Hierarquia Baseada em Funções



# Modelos Operacionais

- Centralizado: time operacional
- Descentralizado: engenheiros/ dev + time operacional
- Criação de Projetos: automatizado
- Cotas de Recursos
- Monitoramento de cotas: Cloud Operations

# Exemplo Prático

## Organizando nossos projetos



## Etapa 4

# Gestão de Acessos

# Percorso

**Etapa 1**

**Pontos importantes na adoção da nem**

**Etapa 2**

**Gestão de Identidade**

**Etapa 3**

**Gestão de recursos**

# Percorso

**Etapa 4**

**Gestão de acesso (IAM)**

**Etapa 6**

**Rede**

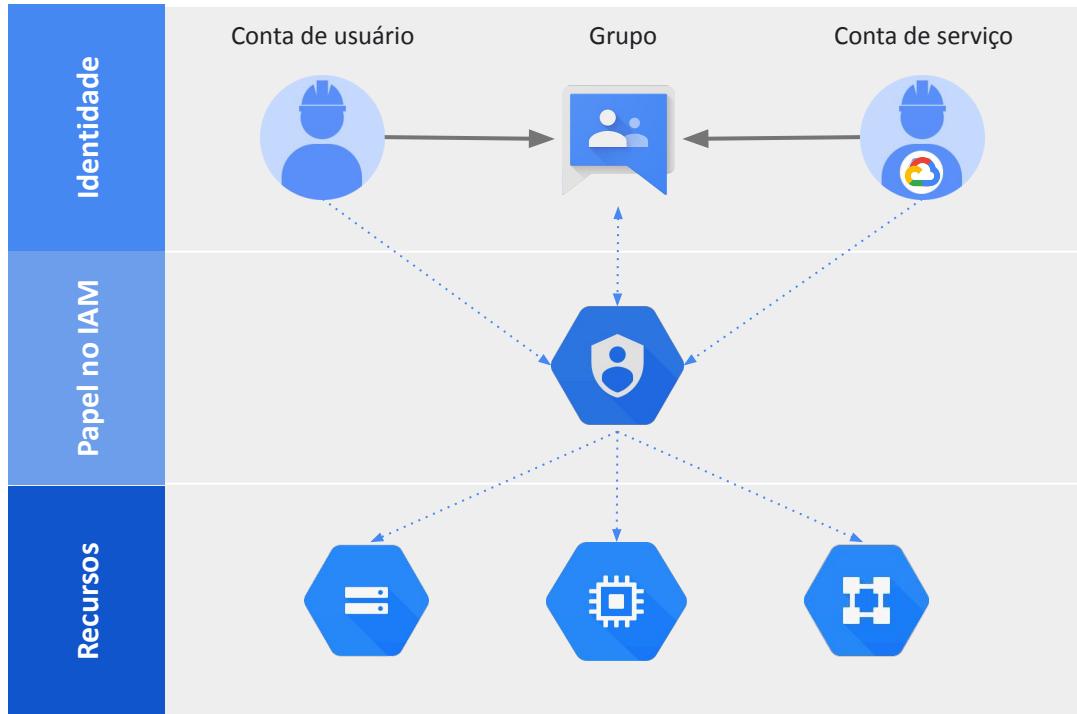
**Etapa 6**

**Monitoramento e Registro**

# Objetivo

- Garantir que apenas as pessoas e serviços certos estejam autorizados a executar as ações certas com os recursos certos.
- Atingir isso de maneira sustentável e gerenciável.

# Políticas do Cloud IAM



O IAM permite que você adote o princípio de segurança de privilégio mínimo, para conceder apenas o acesso necessário aos recursos.

As políticas do IAM podem ser aplicadas nos níveis de Organização, Pasta e Projeto. Para determinadas soluções do Google Cloud, elas também podem ser aplicadas no nível do recurso.

# Cloud IAM

- Papéis do Cloud IAM: **Papéis** são um conjunto de **permissões** que podem ser atribuídas a **usuários, grupos e contas de serviço**.
- IAM para organização
- Papéis Organizacionais.
- IAM para pastas
- IAM para Projetos
- Papéis Personalizados

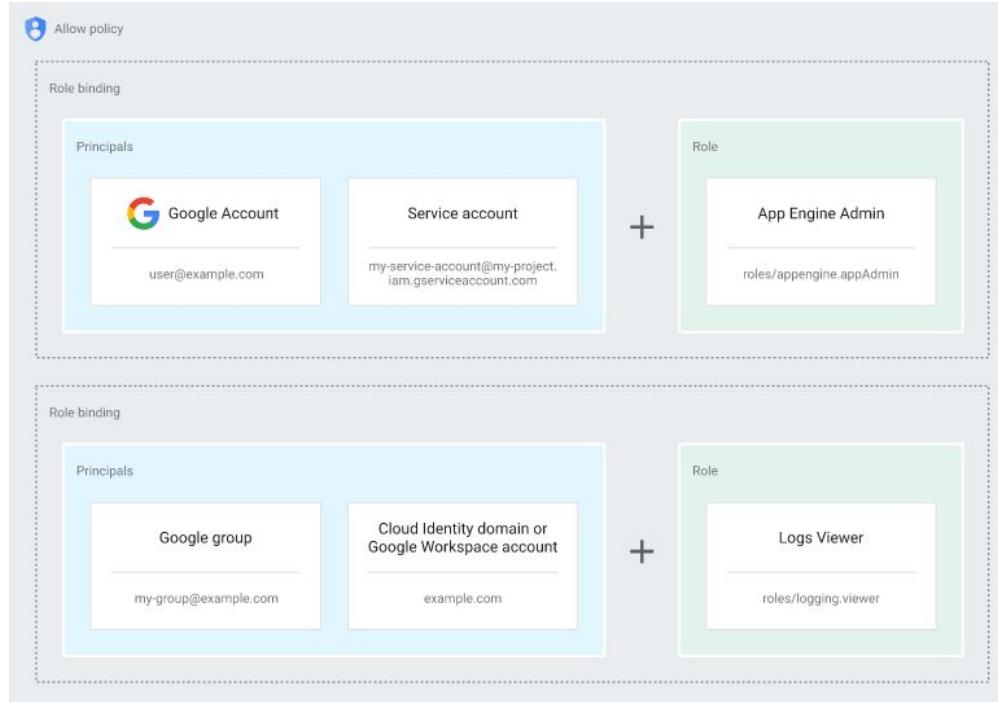
# Como o Cloud IAM Funciona?

Com o IAM, você gerencia o controle de acesso definindo *quem* (identidade) tem *qual acesso* (papel) a *que recurso*. As instâncias de máquina virtual do Compute Engine, os clusters do Google Kubernetes Engine (GKE) e os buckets do Cloud Storage são todos recursos do Google Cloud. As organizações, pastas e projetos que você usa para organizar seus recursos também são recursos.

No IAM, a permissão para acessar um recurso não é concedida *diretamente* ao usuário final. Em vez disso, as permissões são agrupadas em *papéis*, que são concedidos a *principais* autenticados. No passado, o IAM muitas vezes se referia aos principais como *membros*. Algumas APIs ainda usam esse termo.

Uma *política de permissão*, também conhecida como *política do IAM*, define e aplica os papéis concedidos aos principais. Cada política de permissão é anexada a um recurso. Quando um principal autenticado tenta acessar um recurso, o IAM verifica a política do recurso para determinar se a ação é permitida.

# Como o Cloud IAM Funciona?



# Condições Cloud IAM



Quem ?



pode fazer o  
que

Google Cloud Platform



em qual recurso



sob quais  
condições

# O que são Contas de Serviço?

- Usado por **aplicativos** que precisam fazer uso de **APIs do Google Cloud**.
- Autenticação baseada em **pares de chaves**
- Gerenciado por projeto no **Cloud Console**, mas pode ser adicionado a grupos no **Admin Console**.
- Nova Conta de Serviço
- Conta de Serviço default.

# Práticas recomendadas para proteger contas de serviço

[LINK](#)

# Cloud Security Command Center



O [Security Command Center](#) é o serviço centralizado de vulnerabilidade e relatórios de ameaças do Google Cloud. O Security Command Center ajuda a fortalecer a postura de segurança ao avaliar a superfície de segurança e ataque de dados, fornecer inventário e descoberta de ativos e identificar configurações incorretas, vulnerabilidades e ameaças, além de ajudar você a mitigar e corrigir riscos.

# Políticas de Organização

O serviço de política da organização restringe as configurações de recursos permitidas. As políticas podem ser aplicadas à organização, pastas e projetos. Requer função IAM: política da organização / administrador da política da organização. [LINK](#)

[Policy Intelligence](#) : O Policy Intelligence utiliza os recursos de ML e IA do Google para ajudar as empresas compreender e gerenciar suas políticas de IAM para reduzir o risco

## Etapa 5

# Rede

# Percurso

**Etapa 1**

**Pontos importantes na adoção da nem**

**Etapa 2**

**Gestão de Identidade**

**Etapa 3**

**Gestão de recursos**

# Percorso

**Etapa 4**

~~Gestão de acesso (IAM)~~

**Etapa 5**

**Rede**

**Etapa 6**

**Monitoramento e Registro**

# Objetivo

Conectar e proteger serviços e o fluxo de dados entre eles por meio de limites lógicos, independentemente da identidade ou das permissões de um serviço.

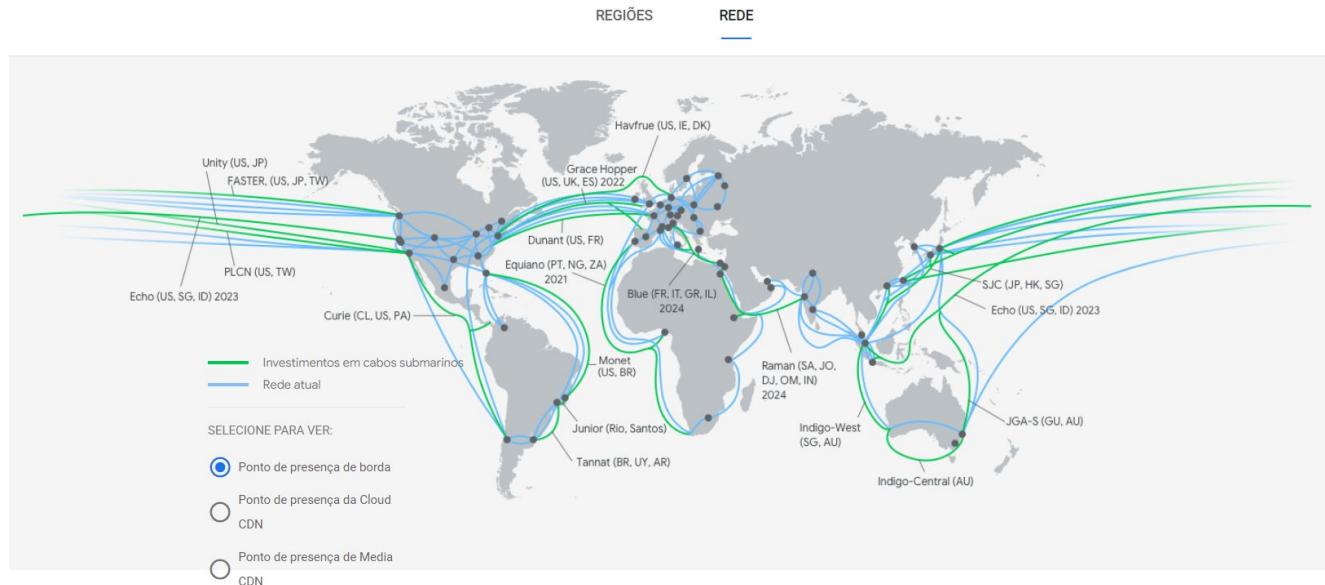
# Redes VPC

Uma rede de nuvem privada virtual (VPC) é uma versão virtual de uma rede física, implementada dentro da rede de produção do Google, usando [Andromeda](#). Uma rede VPC fornece o seguinte:

- Fornece conectividade para suas [instâncias de máquina virtual \(VM\) do Compute Engine](#), incluindo [clusters do Google Kubernetes Engine \(GKE\)](#), [ambiente flexível do App Engine](#) e outros produtos do Google Cloud baseados em VMs do Compute Engine.
- Oferece balanceamento de carga TCP/UDP interno nativo e sistemas de proxy para balanceamento de carga de HTTP(S) internos.
- Conecta-se a redes locais usando túneis do Cloud VPN e anexos do Cloud Interconnect.
- Distribui o tráfego dos平衡adores de carga externos do Google Cloud para back-ends.

Os projetos podem conter várias redes VPC. A menos que você crie uma política organizacional que proíba isso, os novos projetos começam com uma rede padrão (uma rede VPC de modo automático) que tem uma sub-rede (sub-rede) em cada região.

# Infraestrutura de Rede Global



<https://cloud.google.com/about/locations#network>

# Camada de Rede

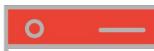
Premium

Standard

<https://gweb-network-tier-demo-archive.firebaseio.com/>

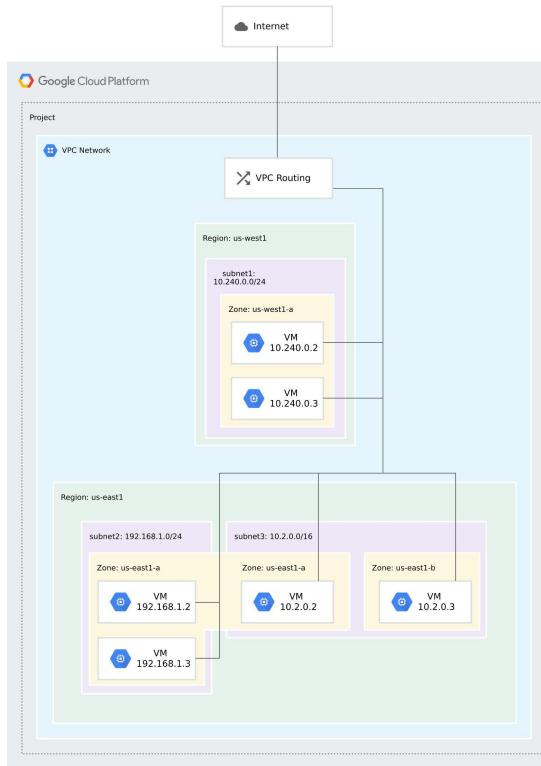
# Proteção e Criptografia

 Primary focus  
of this document

Application		Google Cloud Platform services
Platform		<b>Database and file storage:</b> protected by AES256 or AES128 encryption
Infrastructure		<b>Distributed file system:</b> data chunks in storage systems protected by AES256 encryption with integrity
		Block storage
Hardware		<b>Storage devices:</b> protected by AES256 or AES128 encryption

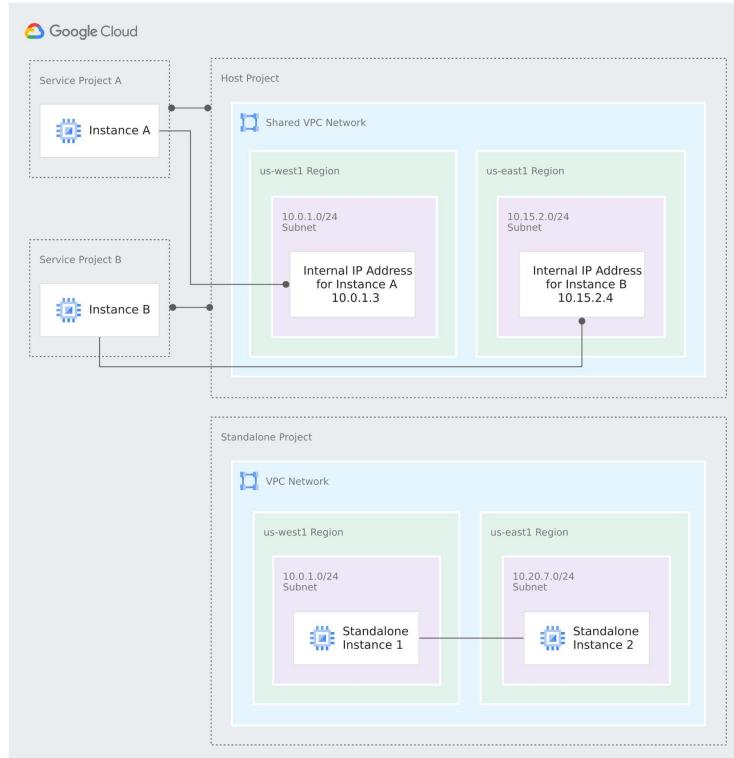
<https://cloud.google.com/docs/security/encryption/default-encryption?hl=pt-br>  
<https://cloud.google.com/docs/security/encryption-in-transit>

# Conceitos VPC



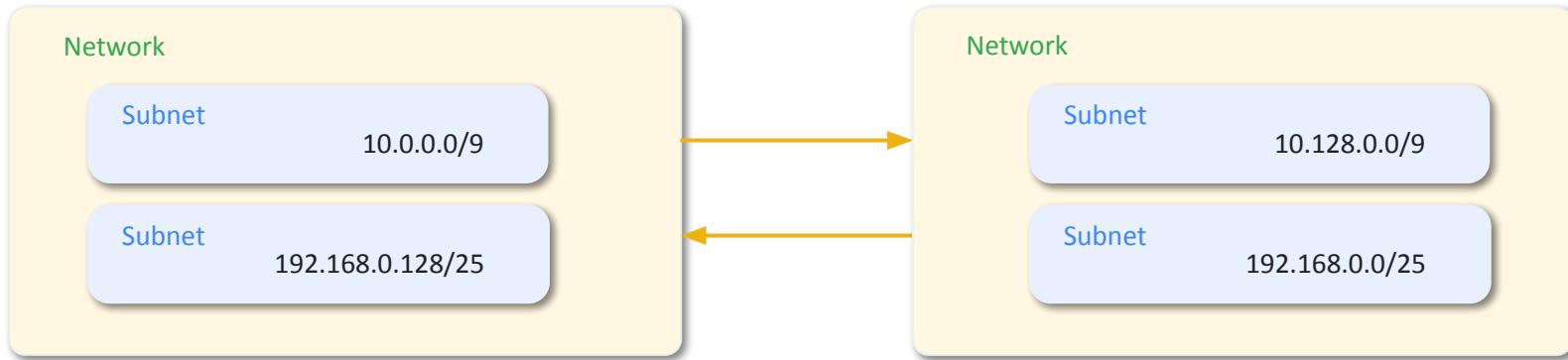
<https://cloud.google.com/vpc/docs/vpc?hl=pt-br>

# Conceitos Shared VPC



[https://cloud.google.com/vpc/docs/shared-vpc#use\\_cases](https://cloud.google.com/vpc/docs/shared-vpc#use_cases)

# Peering Rede VPC

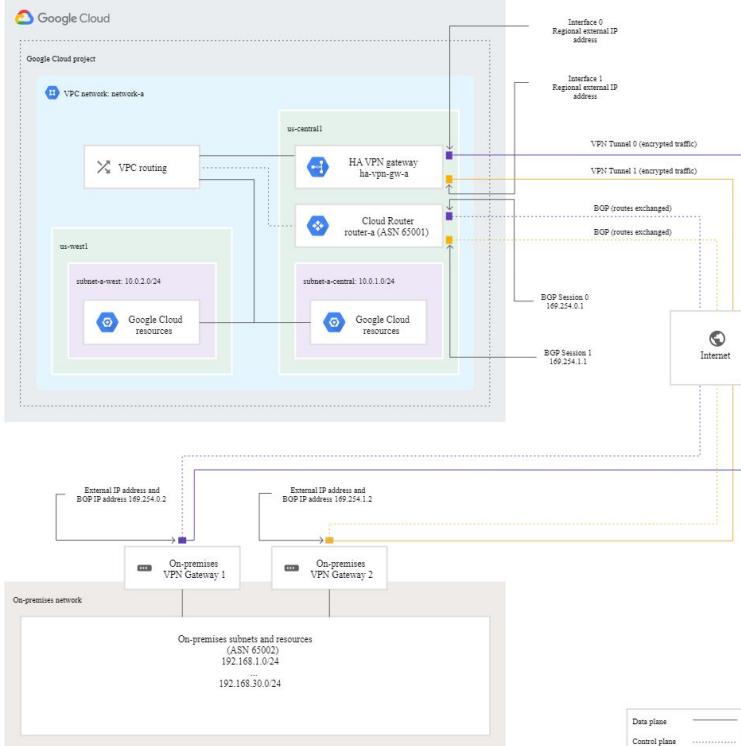


O peering de rede VPC do Google Cloud permite conectividade de endereço IP interno em duas redes de nuvem privada virtual (VPC), pertencentes ou não ao mesmo projeto ou à mesma organização.

O peering de rede VPC permite conectar redes VPC para que as cargas de trabalho em diferentes redes VPC possam se comunicar internamente. O tráfego fica restrito à rede do Google e não passa pela Internet pública.

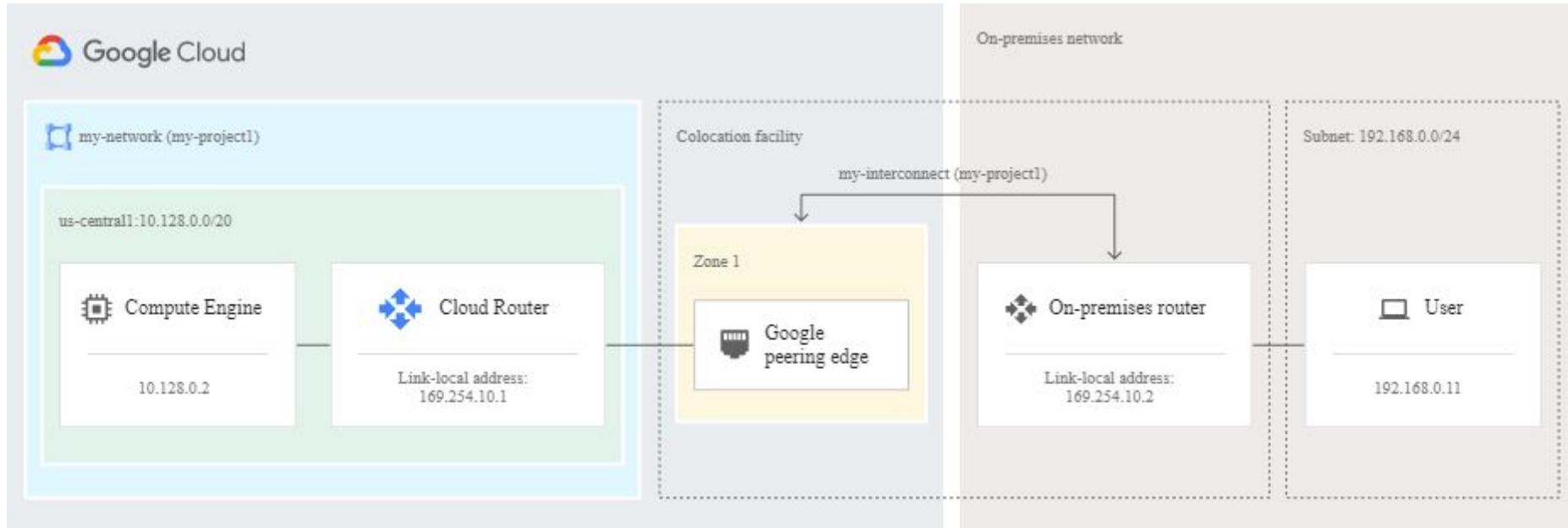
[https://cloud.google.com/vpc/docs/vpc-peering#overlapping\\_subnets\\_at\\_time\\_of\\_peering](https://cloud.google.com/vpc/docs/vpc-peering#overlapping_subnets_at_time_of_peering)

# Google Cloud VPN



<https://cloud.google.com/network-connectivity/docs/vpn/concepts/overview>

# Google Cloud Interconnect



<https://cloud.google.com/network-connectivity/docs/interconnect/concepts/dedicated-overview#how-it-works-dedicated>

## Etapa 6

# Monitoramento e Registro

# Percorso

**Etapa 1**

**Pontos importantes na adoção da nem**

**Etapa 2**

**Gestão de Identidade**

**Etapa 3**

**Gestão de recursos**

# Percorso

**Etapa 4**

~~Gestão de acesso (IAM)~~

**Etapa 6**

**Rede**

**Etapa 6**

**Monitoramento e Registro**

# Objetivo

Examinar o comportamento de um sistema sob qualquer circunstância para que os objetivos de nível de serviço possam ser quantificados.

Verificar os registros de atividades e identificar quem executa determinadas ações.

# Google Cloud Operations



<https://cloud.google.com/stackdriver/docs>

# Activity

The screenshot shows the Google Cloud Activity page for the project 'barbero-devops-iac'. The left sidebar lists various services: FIXADAS (APIs e serviços, IAM e administração, Marketplace, Compute Engine, Kubernetes Engine, Cloud Storage, BigQuery, Rede VPC), and others like Visão geral do Cl... and Ver todos os produtos. The main area has tabs for PAINEL, ATIVIDADE (selected), and RECOMENDAÇÕES. A search bar at the top right contains the text 'Pesquisa regis'. Below the tabs, a date selector shows '07/07/2022'. The activity log table lists 14 entries from 14:44, all showing the execution of 'google.longrunning.Operations.GetOperation' by 'carlos@carlosbarbero.com.br'.

Time	Action	User
14:44	google.longrunning.Operations.GetOperation	carlos@carlosbarbero.com.br executou google.longrunning.Operations.Get...
14:44	Concluída:google.api.serviceusage.v1.ServiceUs...	carlos@carlosbarbero.com.br executou google.api.serviceusage.v1.Servic...
14:44	google.longrunning.Operations.GetOperation	carlos@carlosbarbero.com.br executou google.longrunning.Operations.Get...
14:44	google.longrunning.Operations.GetOperation	carlos@carlosbarbero.com.br executou google.longrunning.Operations.Get...
14:44	google.longrunning.Operations.GetOperation	carlos@carlosbarbero.com.br executou google.longrunning.Operations.Get...
14:44	google.longrunning.Operations.GetOperation	carlos@carlosbarbero.com.br executou google.longrunning.Operations.Get...
14:44	google.longrunning.Operations.GetOperation	carlos@carlosbarbero.com.br executou google.longrunning.Operations.Get...
14:44	google.longrunning.Operations.GetOperation	carlos@carlosbarbero.com.br executou google.longrunning.Operations.Get...
14:44	google.longrunning.Operations.GetOperation	carlos@carlosbarbero.com.br executou google.longrunning.Operations.Get...
14:44	google.longrunning.Operations.GetOperation	carlos@carlosbarbero.com.br executou google.longrunning.Operations.Get...
14:44	google.longrunning.Operations.GetOperation	carlos@carlosbarbero.com.br executou google.longrunning.Operations.Get...
14:44	google.longrunning.Operations.GetOperation	carlos@carlosbarbero.com.br executou google.longrunning.Operations.Get...
14:44	google.longrunning.Operations.GetOperation	carlos@carlosbarbero.com.br executou google.longrunning.Operations.Get...
14:44	google.longrunning.Operations.GetOperation	carlos@carlosbarbero.com.br executou google.longrunning.Operations.Get...

<https://cloud.google.com/identity-platform/docs/activity-logging>

<https://console.cloud.google.com/home/activity?project=barbero-devops-iac>

# Google Cloud Logging

The screenshot shows the Google Cloud Logging interface. On the left, there's a sidebar with navigation links: Operations, Registros, Buscador de registros, Painel de registros, Métricas baseadas em regis..., Roteador de registros, and Armazenamento de registros. The main area has a header with 'Google Cloud' and 'barbero-devops-iac'. It includes a search bar ('Pesquisa'), a login button, and various icons for notifications and help. Below the header, there are buttons for 'REFINAR ESCOPO' and 'Projeto', and a 'COMPARA LINK' button. The main content area is titled 'Buscador de registros' and has tabs for 'Consulta' (which is selected), 'Recente (0)', 'Salvo (0)', 'Sugeridos (0)', 'Biblioteca', 'Limpar consulta', 'Salvar', and a filter icon. There are also filters for 'Últimos 1 hora', 'Pesquisar todos os campos', 'Recurso', 'Nome do registro', and 'Gravidade'. A toggle switch 'Exibir consulta' is turned on. Below this is a histogram titled 'Histograma' showing a single data point at '13 de jul, 16:08'. At the bottom, there are buttons for 'Resultados da consulta', 'Correlacionar por', and filters for 'GRAVIDADE', 'CARIMBO DE DATA/HORA', 'RRT', 'RESUMO', and 'FILTRAR'.

<https://cloud.google.com/logging/docs/how-to?hl=pt-br>

## Etapa 7

# Gestão de Dados

# Percorso

**Etapa 7**

**Gestão de dados**

**Etapa 8**

**Controle de custos**

**Etapa 9**

**Introdução a Infraestrutura com código**

# Objetivo

Desejo armazenar dados com segurança, descobrir o quanto sensível eles são e gerenciar quem pode acessá-los, com o objetivo de manter os dados seguros cumprindo as regulamentações exigidas em meu país.

# Google Cloud KMS

Key Management Service (KMS) hospedado na nuvem Permite que você gerencie a criptografia para seus serviços em Cloud da mesma maneira que você faz on-premises.

Sua empresa pode gerar, usar, rotacionar e destruir chaves de criptografia AES256. O Cloud KMS está integrado ao IAM e ao Cloud Audit Logging para que você possa gerenciar permissões em chaves individuais e monitorar como elas são usadas.

## Funcionalidades

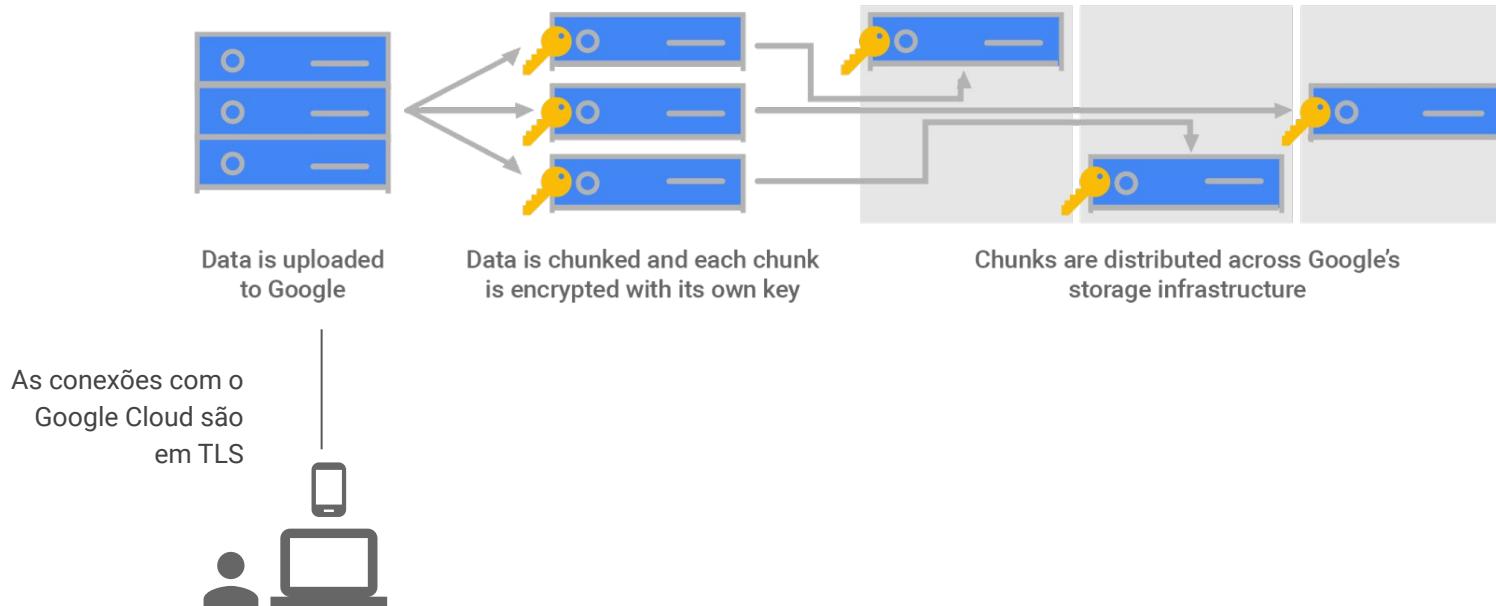
- AES256 key
- Criptografar e descriptografar via API
- Rotação de chave automatizada e à vontade
- Atraso para destruição de chave
- Alta disponibilidade global
- Suporta criptografia de software e hardware

## Hardware encryption

- Serviço baseado em nuvem de Hardware Security Module (HSM)
- [FIPS 140-2 Level 3](#) certified
- Chaves de criptografia de hosts
- Executa operações criptográficas

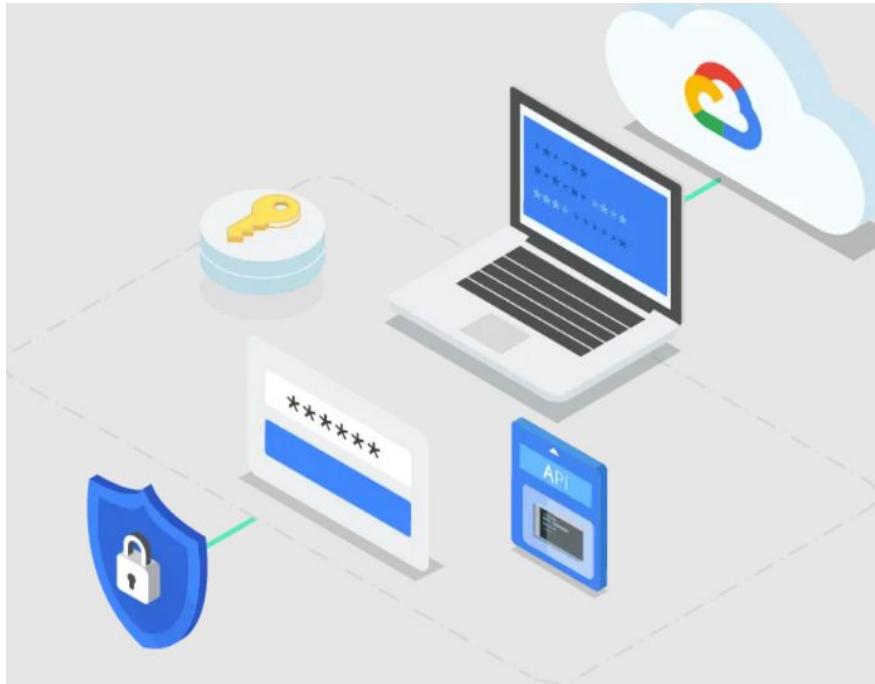
<https://cloud.google.com/security-key-management?hl=pt-br#section-5>

# Criptografia Default



<https://cloud.google.com/docs/security/encryption/default-encryption#:~:text=Google%20uses%20the%20Advanced%20Encryption,to%202015%20that%20use%20AES128.>

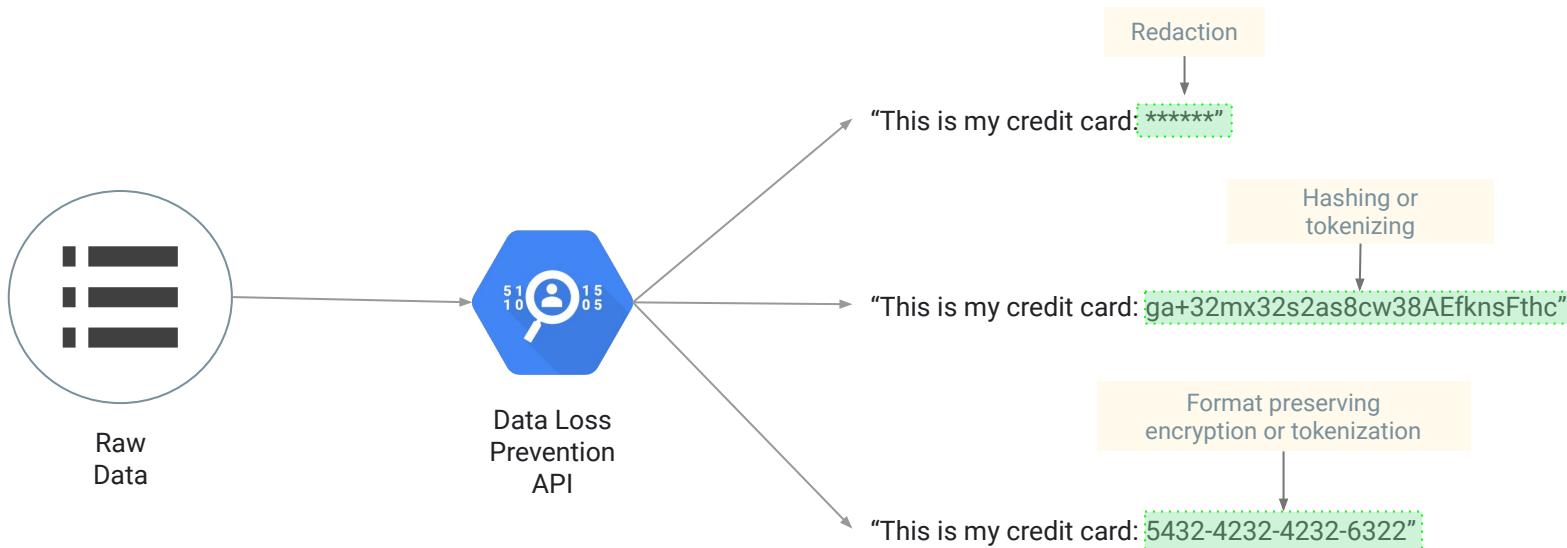
# Secret Manager



<https://cloud.google.com/secret-manager>

# Google Cloud DLP

Fornece uma API programática para detecção de dados PII



# Google Cloud DLP

ID	Job Title	Phone	Comments
359740	Senior Engineer	307-964-0673	Please email them at jane@imadethisup.com
981587	VP, Engineer	713-910-6787	none
394091	Lawyer	692-398-4146	Updated phone to: 692-398-4146
986941	Senior Ops Manager	294-967-5508	none
490456	Junior Ops Manager	791-954-3281	Tried to verify account with their SSN 222-44-5555

<https://cloud.google.com/dlp#section-1>

# Google Cloud Storage



Armazenamento de objetos para empresas de todos os tamanhos. Armazene qualquer quantidade de dados. Recupere-os quantas vezes quiser.

<https://cloud.google.com/storage>

Etapa 8

# Controle de Custos

# Percorso

**Etapa 7**

**Gestão de dados**

**Etapa 8**

**Controle de custos**

**Etapa 9**

**Introdução a Infraestrutura com código**

# Objetivo

Fazer o controle de custos de forma eficiente e gerenciável, bem como conscientizar da importância de controle de custos.

# Controle de Custos

# FinOps

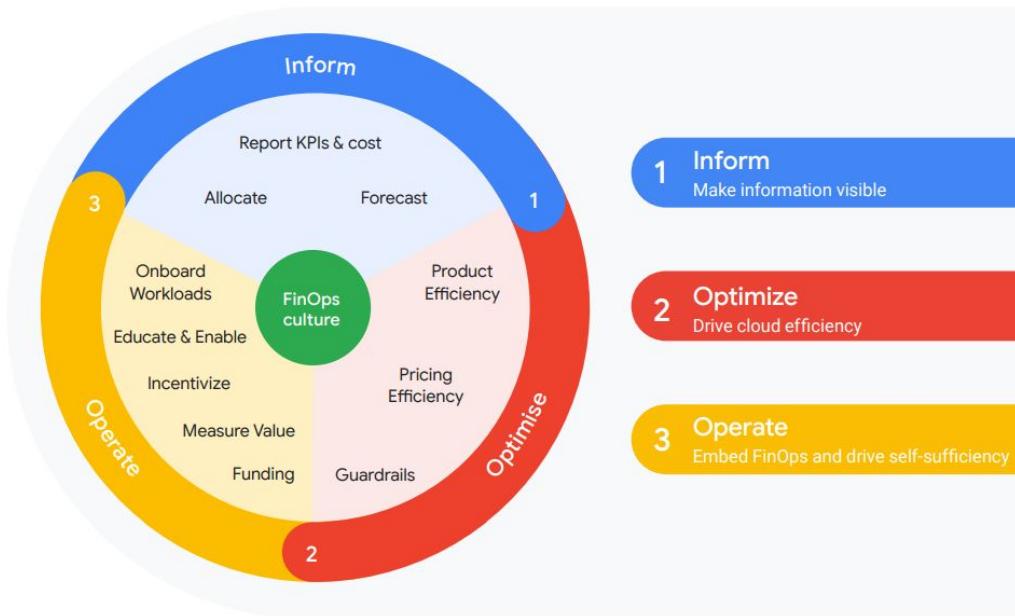


FinOps é uma prática cultural e disciplina de gerenciamento financeiro em nuvem em evolução que permite que as organizações obtenham o máximo valor comercial, ajudando as equipes de engenharia, finanças, tecnologia e negócios a colaborar em decisões de gastos orientadas por dados.

*(Definition Updated: November 2021 by the FinOps Foundation  
Technical Advisory Council*

<https://cloud.google.com/resources/cloud-finops-getting-started-whitepaper>  
<https://cloud.google.com/learn/what-is-finops#section-7>  
<https://www.finops.org/introduction/what-is-finops/>

# FinOps



**1 Inform**  
Make information visible

**2 Optimize**  
Drive cloud efficiency

**3 Operate**  
Embed FinOps and drive self-sufficiency

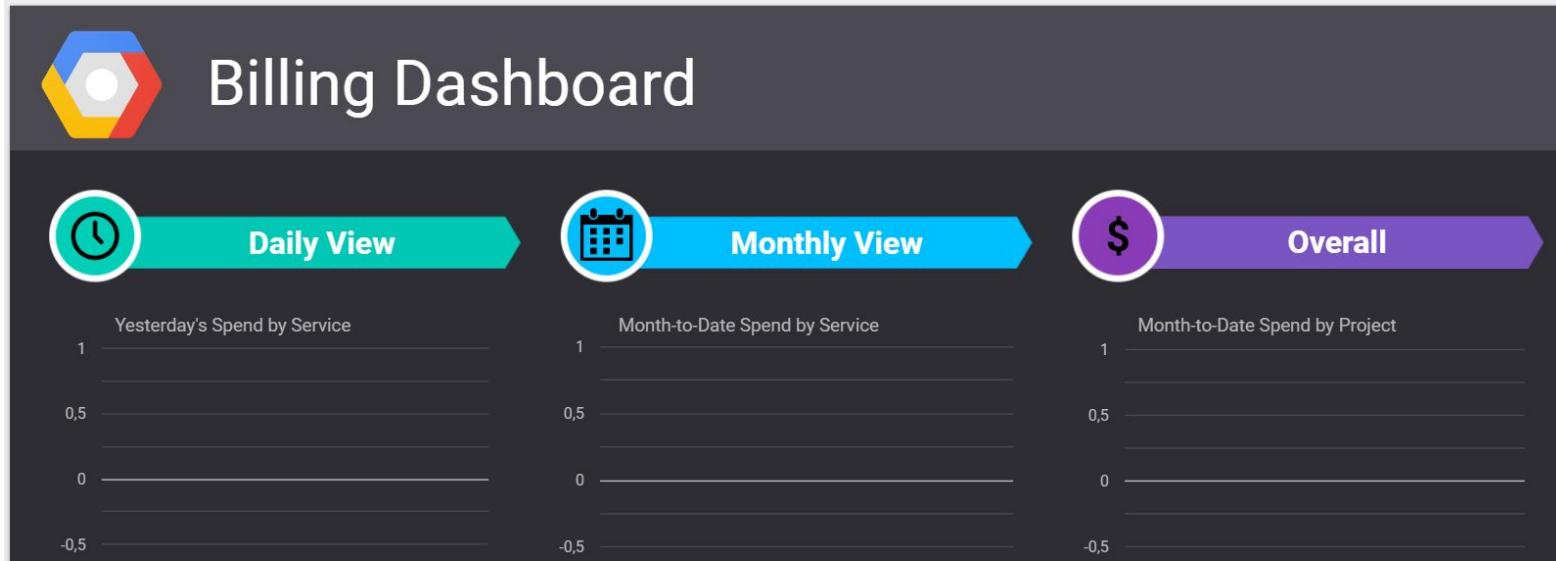
# Billing Account

A Billing Account possui uma relação entre um projeto do GCP e uma conta de faturamento é de muitos para um, o que significa que vários projetos do GCP são anexados a uma conta de faturamento para toda a organização.

## Melhor prática

Use uma única conta de faturamento para simplificar. Desenvolva mecanismos internos de estorno para alocar custos entre departamentos.

# Relatório DataStudio



<https://datastudio.google.com/u/0/reporting/0B7GT7ZlyzUmCZHfNDIKVE>

[NHYmc/page/dizD](#)

## Etapa 9

# Infraestrutura como Código

# Percorso

**Etapa 7**

**Gestão de dados**

**Etapa 8**

**Controle de custos**

**Etapa 9**

**Introdução a Infraestrutura com código**

# Objetivo

Automatizar por meio de código a configuração e o provisionamento de recursos gcp, evitando erros humanos, economizando tempo.

# IAC

## Ferramentas

Iac é uma ferramenta de automação de processos, voltada para provisionamento de recursos.

## Gestão

Para fazer alterações na infraestrutura, os engenheiros de automação devem fazer uma solicitação no sistema para implantar na produção.

## Controle de versão de código

Toda o código é configurado e armazenado em ferramentas de controles de versão como por exemplo git

## Processo de implantação

Através de *pipelines*

# Benefícios

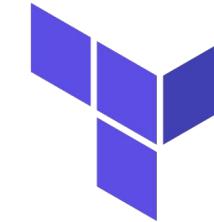
- Controlado pelos commits no git.
- Declarativo
- Infraestrutura diferencial entre o estado desejado e o estado atual.
- Módulos reutilizáveis em uma organização

# Produtos



Google  
Cloud Deployment  
Manager

<https://cloud.google.com/deployment-manager/docs>



HashiCorp  
**Terraform**

<https://cloud.google.com/docs/terraform>

## Etapa 10

# Integração e entrega contínua (CI/CD)

# Percorso

**Etapa 10** CI/CD

**Etapa 11** Arquitetura resiliente

**Etapa 12** Gestão de incidentes

# Objetivo

Automatização no processos de implantação de sistemas por meio de um pipeline de processo de CI / CD, com propósito de que todas mudanças possam ser testadas, auditadas e implantadas com o mínimo de interrupção.

# O que significa?

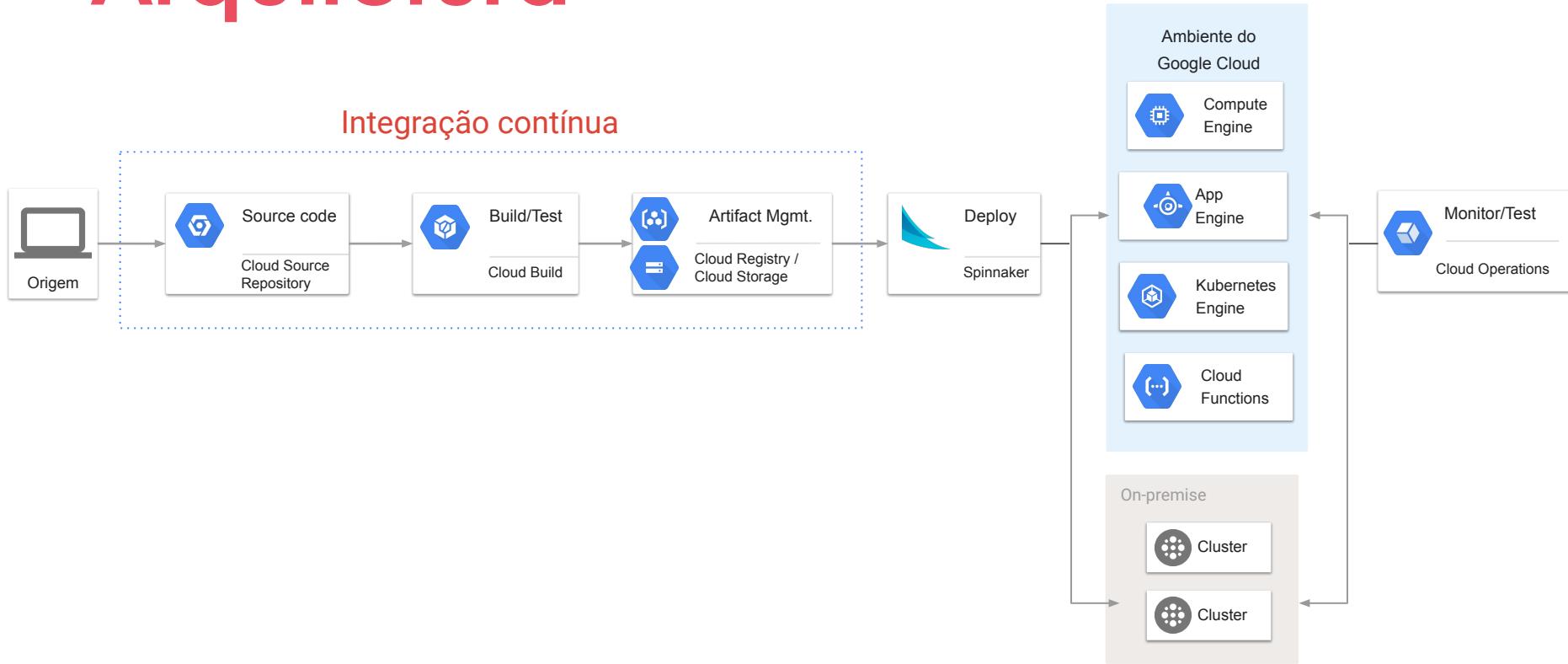
**Integração Contínua (CI)** É uma prática recomendada ágil e de DevOps para integrar, como parte da rotina, alterações de código na ramificação principal de um repositório e testar as alterações com o máximo de antecedência e frequência possível.

**Entrega Contínua(CD)** É a capacidade de obter alterações de todos os tipos – incluindo novos recursos, alterações de configuração, correções de bugs e experimentos – em produção ou nas mãos dos usuários, com segurança e rapidez de maneira sustentável.

**Implantação Contínua** é a estratégia para lançamentos de software em que qualquer confirmação de código que passa no CI é automaticamente liberado no ambiente de produção.

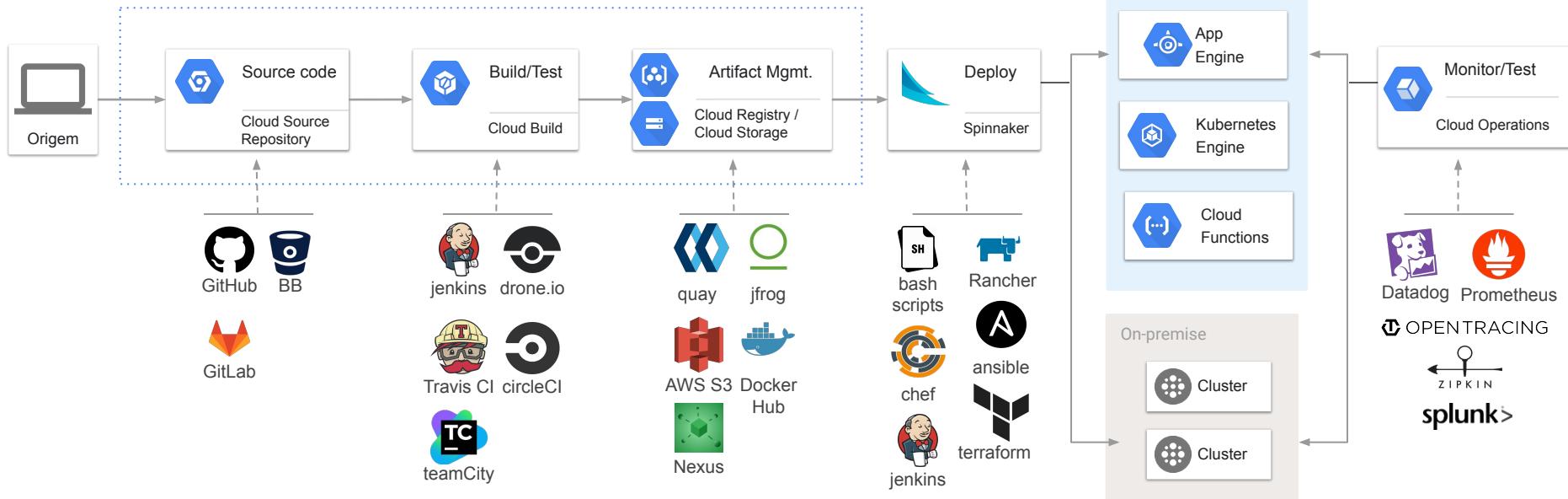
# Arquitetura

## Integração contínua

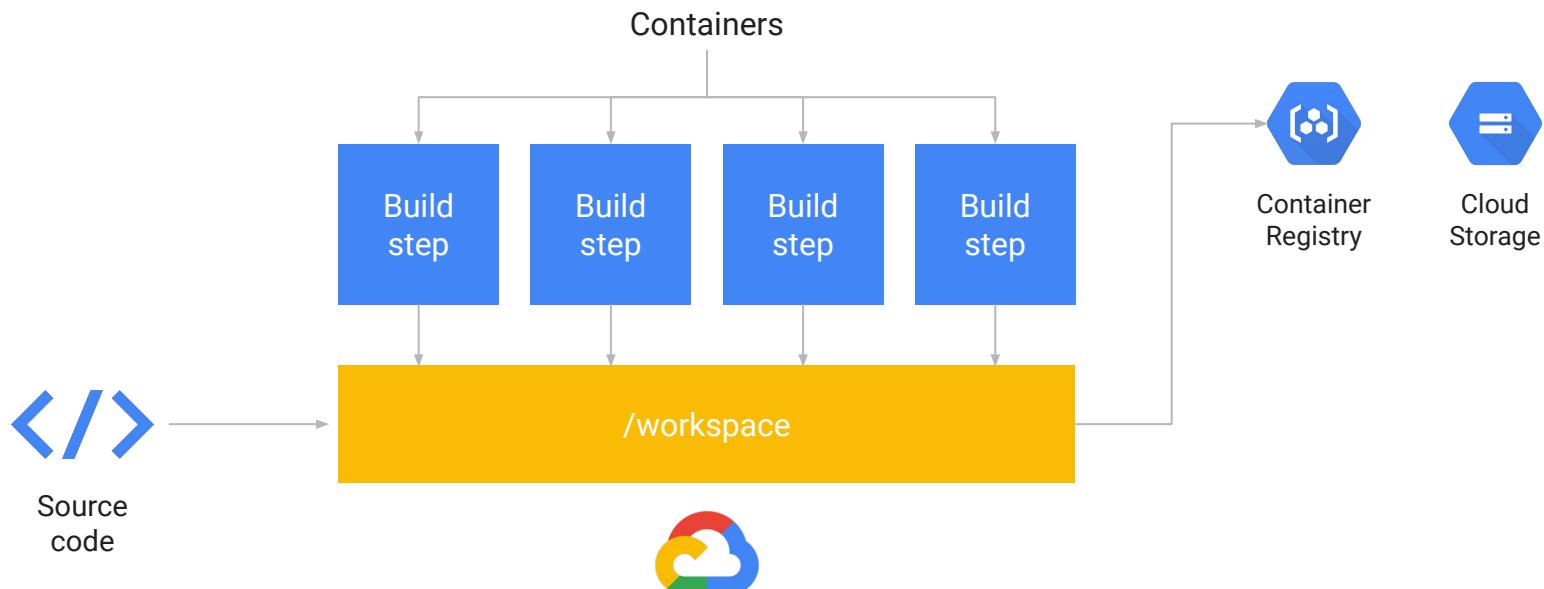


# Ferramentas

## Integração contínua



# Google Cloud Build



Etapa 11

# Arquiteturas Resilientes

# Percurso

Etapa 10



Etapa 11

Arquitetura resiliente

Etapa 12

Gestão de incidentes

# Objetivo

Projetar arquitetura que seja tolerante a falhas e altamente disponível com baixa indisponibilidade dos meus sistemas.

# Disponibilidade

Tempo em que serviço ou aplicação ficaram indisponíveis em um período de tempo especificado. O tempo de inatividade planejado ainda é o tempo de inatividade.

# Nível de Serviço

## SLI

### Indicador

Quantidade mensurável que representa o que é importante para os usuários.

Frequentemente relacionado a confiabilidade ou desempenho.

### Exemplo:

- Taxa de erro do Load balancer

## SLO

### Objetivo

O alvo que você deseja que seu SLI alcance

### Exemplo:

- Taxa de erro do Load balancer <0.01%

## SLA

### Acordo

Consequências quando o SLO não é atendido. Aplicável apenas para serviços GA.

Freqüentemente, um Crédito Financeiro: porcentagem da fatura mensal que será creditada em futuras faturas mensais.

Vinculado à definição de tempo de inatividade e período mínimo de interrupção que é considerado tempo de inatividade.

### Exemplo:

- 99,0% a <99,99%: 10% de crédito
- 95,0 a <99,0%: 25% de crédito
- Tempo de inatividade mínimo = 60s

# Arquiteturas Resilientes

1. Redundância geográfica
2. Serviços gerenciados
3. Alta disponibilidade
4. Automatizado

Etapa 12

# Gestão de Incidentes

# Percurso

Etapa 10

 CD

Etapa 11

~~Arquitetura resiliente~~

Etapa 12

Gestão de incidentes

# Objetivo

Meus projetos ou recursos não estão funcionando como deveria, preciso abrir um chamado no gcp.

# Planos de Suporte

Supor te Básico	Supor te Padrão	Supor te avançado	Supor te Premium
<p>Supor te de faturamento e pagamentos. Disponível em várias regiões e idiomas.</p> <p><a href="#">Saiba mais</a></p>	<p>Inicie sua jornada para a nuvem com acesso ilimitado ao suporte técnico que ajuda você a resolver problemas, fazer testes e explorar recursos.</p> <p><a href="#">Saiba mais</a></p>	<p>Otimize sua experiência na nuvem com um suporte robusto e de alta qualidade. Tempos de resposta rápidos e serviços adicionais para executar sua nuvem, além de aumentar a produtividade e a eficiência. <a href="#">Saiba mais</a></p>	<p>Supor te para cargas de trabalho críticas com o reconhecimento do cliente e um TAM nomeado. O Supor te Premium oferece engajamento proativo e melhoria nas eficiências operacionais.</p> <p><a href="#">Saiba mais</a></p>
<p><b>RECURSOS</b></p> <ul style="list-style-type: none"><li>✓ Incluído na sua assinatura do Google Cloud</li><li>✓ Supor te a faturamento de vários canais</li><li>✓ API Active Assist Recommendations</li></ul>	<p><b>RECURSOS</b></p> <ul style="list-style-type: none"><li>✓ US\$ 29/mês + 3% de cobranças mensais</li><li>✓ Acesso ilimitado ao suporte</li><li>✓ Casos P2: tempo de resposta inicial de quatro horas</li><li>✓ Supor te a faturamento de vários canais</li><li>✓ Supor te técnico de vários canais</li></ul>	<p><b>RECURSOS</b></p> <ul style="list-style-type: none"><li>✓ US\$ 500/mês + 3% de cobranças mensais</li><li>✓ Acesso ilimitado ao suporte</li><li>✓ Casos P1: tempo de resposta inicial de uma hora</li><li>✓ Supor te a faturamento de vários canais</li><li>✓ Supor te técnico de vários canais</li></ul>	<p><b>RECURSOS</b></p> <ul style="list-style-type: none"><li>✓ US\$ 12.500/mês + 4% de cobranças mensais <a href="#">Faça uma estimativa dos custos</a> ou <a href="#">fale com a equipe de vendas</a>.</li><li>✓ Acesso ilimitado ao suporte</li><li>✓ Casos P1: tempo de resposta inicial de 15 minutos</li><li>✓ Supor te a faturamento de vários canais</li></ul>
<p><b>COMECE AGORA</b></p> <p><a href="#">Receba Supor te Básico</a></p>			

<https://cloud.google.com/support>

# O que devo informar?

- Recurso
- Nome
- Região
- Localização
- Logs
- Links
- Resumo do que está acontecendo.
- Escolher a Prioridade