**Partes del Data Center**

**Networking Room**: Aquí se conectan los clusters de Jupiter con el resto de Google Cloud a tráves de la red *backbone* de Google.

**Jupiter Network Equipment**: Equipo (software y hardware) desarrollado por Google, para conectar todos los servidores de los *data centers*, para que sean casi uno solo.

**Maglev Load Balancers**: Son Load Balancers Globales. Equilibran la carga a Google Compute Engine, para que así atender un millón de solicitudes por segundo sin *pre*-*warming*.

**Custom Chips**:

* **Titan**: Microcontrolador seguro de bajo consumo diseñado teniendo en cuenta los requisitos y escenarios de seguridad de hardware de Google.
* **Cloud TPUs**: Chip diseñado para acelerar las cargas de trabajo de aprendizaje automático con TensorFlow.

**Water Pipes**: Agua fría que corre desde la planta de enfriamiento hasta el centro de datos, donde se utiliza para extraer calor del interior de las *hot huts*. Luego, el agua tibia se devuelve a la planta de enfriamiento donde se elimina el calor residual y el agua regresa al centro de datos.

**HotH**

**ut**: Sistemas de enfriamiento personalizados para los racks de servidores de Google. Sirven como hogares temporales para el aire caliente que sale de nuestros servidores, aislándolo del resto del piso del centro de datos.

**Cooling Plant**: En los centros de datos de Google, se usa el “enfriamiento gratuito” que proporciona el clima a través de un sistema de agua. Es decir, la planta de enfriamiento recibe agua caliente del centro de datos y agua fría de las torres de enfriamiento, el calor se transfiere del agua caliente al agua fría. El agua enfriada regresa al piso del centro de datos para extraer más calor del equipo allí, y el agua caliente fluye hacia las torres de enfriamiento para ser enfriada.

Eras del computo en la nube

* Eras de las VM
* Era de la infraestructura en la nube
* Era de la nube transformacional
  + Que requiere la industria el dia de hoy
    - Como podeos actuar de manera mucho mas inteligente
    - Como nos transformamos mientras mantenemos la libertad de adaptarnos
    - Como conectamos a las personas de mejor manera
    - Como nos protegemos
  + La nube de datos
    - adopta el ciclo de vida completo de los datos
    - democratiza el acceso a los daos para impulsar los resultados
    - las soluciones de inteligencia artificial lideres ayudan a las empresas a redecir y automatizar
  + La nube abierta
    - Aprovecha la flexibilidad y la innovacion de ser open source
    - Disfruta de la libertad de un entorno multinube para crear y ejecutar aplicaciones desde cualquier lugar
    - aprovecha las soluciones de nuestro ecosistema de socios para ampliar tus opciones tecnologicas
  + La nube colaborativa
    - Entorno de trabajo reinventado
    - Nuevas formas de fortalecer las conexiones humanas
    - Ayuda a las empresas a conectarse con clientes y socios
  + La nube de confianza
    - Una plataforma segura que brinda transparencia y habilita
    - la soberania
    - Una arquitectura probada de Confianza cero
    - Destino compartido, no responsabilidad compartida

La nube transformacional

* La nube mas limpia / Sustentabilidad
* te ahorra dinero
* Facil de usar y se optimiza automaticamente
* Soluciones de industria a la medida

Arquitecturas de Computo en GCP

Arquitecturas de Computo en GCP

Opciones de computo

* Compute Engine
  + Virtual Machines
  + Bear Metal (servidores completos por el tea de licenciamiento especial)
* GKE
  + Kubernetes Engine
  + como orquestrar diferentes tipos de contenedores
* App Engine (Serverless Platform)
  + Para correr aplicaciones web
  + cero administracion de servidores
* Cloud Run
  + Contenedores serverless
* Cloud Function
  + Funcion Serverless
* Firebase
  + PaaS de Front-end y desarrollo movil
  + Se conoce como Back-end as a Service

Computo Serverless

Desarrolla, implementa y escala aplicaciones de forma rapida y segura en un entorno totalmente gestionado

* Auto-escalado
* Completamente administrado
* Speed to Market

La red de Google

Aggressive Global Rollout

* Es una red privada con una dimension y alcance bastante grande
* Como construir cables submarinos
* Aterrizaje de un cable submarino
* Vinculos submarinos para cables
  + son repetidores para la amplificacion de senales opticas
  + es bastante particular y bastante segura
  + esto permite un alcance global

Red de Google

* Red Global
  + Reduce la carga de configuracion
  + Alcance global
* Migracion en vivo
  + Resistencia de la red
  + Alta Disponibilidad
  + Actualizaciones y Mantenimiento administrados
* Escala y Rendimiento
  + Escalado horizontal
  + Mejor rendimiento de las aplicaciones
  + Sin punto de estrangulamiento

Cloud DNS

DNS global de baja latencia

* Se integra con Global Anycast IP Load Balancing
* Gestion de registros sencilla y escalable
* DNSSEC para verificar la integridad del registro DNS

Content Delivery Networks

Una CDN global probada

* Una red de distribucion de contenido creada para llegar a usuarios en todo el mundo
* Soporte de objetos grandes para media y juegos

Network Tiers

* Red premium para llegar a tus usuarios rapidamente
* Red estandar para aplicaciones as sensibles a los costos

VPC Service Controls

* Mitiga los riesgos de filtracion de datos
* Extiende los limites de seguridad en los entornos de la nube
* Enforce context-aware access
* Gestion centralizada de las politicas de seguridad

Cloud Armor

Defensa contra DDoS y los ataques web

* Defensa DDoS construida a escala
* Defensa contra Top 10 OWASP
* Integrado con un rico ecosistema de socios de
* seguridad
* “Absorber los ataques mas grandes requiere el ancho de banda necesario para ver medio millon de videos de Youtube al mismo tiempo, en HD”

Los recursos de Compute Engine se alojan en varias ubicaciones en todo el mundo. *Estas ubicaciones se componen de regiones y zonas*.

* **Una región** es una ubicación geográfica específica donde puedes alojar recursos. Las regiones tienen tres o más zonas. Por ejemplo, la región us-west1 corresponde a una región en la costa oeste de Estados Unidos que tiene tres zonas: us-west1-a, us-west1-b y us-west1-c.
* *Los recursos que se ubican en una zona*, como las instancias de máquina virtual o los discos persistentes zonales, *se denominan recursos zonales*. Otros recursos, como las direcciones IP externas estáticas, son regionales. Cualquier recurso de esa región puede usar los recursos regionales, sin importar la zona, mientras que, en el caso de los recursos zonales, solo los pueden usar otros recursos en la misma zona.
* Ubicar recursos en diferentes zonas de una región reduce el riesgo de interrupciones en la infraestructura que afectan a todos los recursos de forma simultánea. Ubicar recursos en diferentes regiones proporciona un grado aún mayor de independencia de fallas. Esto te pe
* rmite diseñar sistemas sólidos con recursos distribuidos en diferentes dominios con fallas.

Hoy Septiembre 2021, regiones low carbon de Google Cloud:

#### Americas

* Oregon (us-west1)
* Iowa (us-central1)
* Montréal (northamerica-northeast1)
* São Paulo (southamerica-east1)

#### Europa

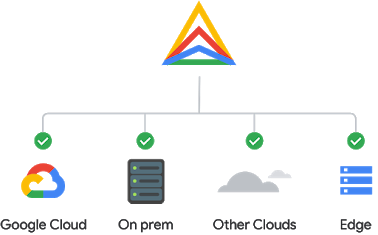
* Zurich (europe-west6)
* Finland(europe-north1)

#### PUE (Power Usage Effectivenes)

Es la effectividad del uso de energía electrica.

**Nube híbrida y multinube**

* Debido a que las cargas de trabajo, la infraestructura y los procesos son exclusivos de cada empresa, cada estrategia híbrida debe adaptarse a necesidades específicas. El resultado es que los términos nube híbrida y múltiples nubes, a veces, se usan de forma inconsistente.
* En el contexto de Google Cloud, el término nube híbrida describe una configuración en la que las cargas de trabajo comunes o interconectadas se implementan en varios entornos de computación, uno basado en la nube pública y, al menos, uno privado.
* El término múltiples nubes describe las configuraciones que combinan al menos dos provee
* dores de servicios en la nube pública.



#### BigQuery: patrones en la nube

Como BigQuery aprovecha la infraestructura de la nube para trabajar de forma paralela y darnos resultados.

1. Mandamos query en SQL.
2. Punto de presencia: entra a la red de Google.
3. Llegar al DataCenter más cercano, viajando por la private fiber network de Google.
4. La query se encamina a un cluster dentro del data center. Podemos tener anchos de banda muy potentes como 1 petabyte por segundo de datos.
5. Un nodo ejecutador convierte nuestra query en un plan ejecutador; es decir, divide nuestra query en pedacitos para procesarlos de manera paralela.
6. Escogen máquinas que ejecutarán nuestros p
7. Pedacitos de query de forma paralela.
8. El resultado se junta y se regresa al usuario.

Beneficios de Google Cloud

1. Inteligente:
   * Convierte los datos en información valiosa en tiempo real usando IA
   * La toma de decisiones ágil
2. Abierta y flexible:
   * Elección y flexibilidad con soluciones de código abierto, hibridas y multinube.
   * Protege a tu negocio del vendedor lock-in
3. Colaboración y productividad
   * Google worspace proporciona toda las herramientas digitales que necesitas para ayudar a que su empresa prospere hoy y mañana
   * Los equipos colaboran, los trabajadores de primera linea se mantienen conectados y las empresas crean nuevas experiencias para los clientes
   * Las soluciones flexibles de Workspace hacen que trabajar desde cualquier lugar sea una realidad
4. Segura
   * Sus datos se almacenan, procesan y protegen en la misma infraestructura que se utiliza para las propias operaciones es de Google
   * Solo Google Cloud cifra los datos en reposo y en tránsito de forma predeterminada
   * Con la red de Google, sus datos no se transfieren a través de redes públicas, lo que aumenta el rendimiento y la seguridad.
5. Sustentable
   * Google Cloud es el único proveedor de nube importante que compra suficiente energía renovable para cubrir todas nuestras operaciones
   * Las emisiones operativas netas de su uso de la nube son cero y la electricidad utilizada se corresponde con un 100% de energía renovable
6. Ahorras costos
   * Google Cloud ayuda aumentar la eficiencia operativa y optimizar el gasto TI
   * La migración de aplicaciones de Google Cloud puede ahorrar hasta un 32% (en comparación con on-prem)
   * La factura con respecto a proyecto proporciona visibilidad del ROI de iniciativas especificas
7. Fácil de usar
   * Google Cloud es fácil de usar y se optimiza automáticamente
   * Diseñada para implementar fácilmente servicios en la nube a gran escala
8. Soluciones de Industria
   * Mejore la eficiencia y la agilidad, reduzca costos y captura nuevas oportunidades de mercado
   * Desde telesalud retail de nueva generación, Google Cloud crea soluciones personalizadas para abordar sus mayores desafíos.
   * Empresas como Netflix, P&G y Target confían en nuestras soluciones, experiencia y red de socios únicas y pioneras en la industria.

Seguridad de Varias Capas

Es una nube construida por desarrolladores para Desarrolladores

* On-Premises
  + Responsabilidad del 100% de la seguridad
* IaaS
  + Responsabilidad del proveedor toda la seguridad del hardware y de su conectividad
* PaaS
  + Responsabilidad del proveedor toda la seguridad de usuarios, accesos, autorizaciones
* SaaS
  + Solo es responsabilidad del usuario las access policies y el contenido

Seguridad de extremo a extremo

* Imágenes Bases Seguridad
* Análisis de Vulnerabilidades (De las dependencias que tenemos en las imágenes)
* Autorización binaria
* Contenedores Escudados
* Sandbox de Contenedores
* Detección de amenazas a contenedores

Estándares, regulaciones y certificaciones

* Identidades seguras criptográficamente
* Identidad del usuario
* Identidad del Dispositivo
* Identidad de la maquina
* Identidad del Servicio
* Identidad del código

Sobre los estándares, regulaciones y certificaciones:

* Los contratos de Google Cloud para instituciones financieras en **México** abordan los requisitos de los marcos de trabajo de la CNBV
* Los contratos de Google Cloud para instituciones financieras en **Argentina** abordan los requisitos del BCRA Comunicación A 6375.

Google Cloud se somete con regularidad a varias auditorías independientes de terceros de los controles de seguridad, privacidad y cumplimiento.

**¿Qué es exactamente el Clickjacking?**  
.  
El *Clickjacking* también llamado UI Redressing, es una técnica maliciosa destinada a persuadir a un usuario de Internet a dar click en enlaces aparentemente seguros; pero que tienen como objetivo brindarle la oportunidad al hacker de robar información o tomar el control del ordenador del usuario.  
.  
En otras palabras, es una forma de piratería informática maliciosa que le da la oportunidad al atacante de tener acceso a datos sensibles; instalar malwares o, en algunos casos, crear PCs “zombies”. En el peor de los casos, el cibercriminal puede obtener el control de servicios vitales de una empresa para lograr beneficios económicos a través de la extorsión.  
.  
Cuando aplican el clickjacking, los atacantes a menudo utiliza marcos ocultos para robar información. Aunque no es una técnica nueva; los hackers se esfuerzan en encontrar medios innovadores para engañar a los usuarios. Por lo que no dudan en utilizar su dominio de la web; sus conocimientos relacionados con el comportamiento de los internautas y las nuevas tecnologías (html5, display none, etc.), para

perfeccionar sus técnicas maliciosas.  
.  
Fuente: [GB Advisors](https://www.gb-advisors.com/es/clickjacking-ui-redressing/#:~:text=El%20Clickjacking%20tambi%C3%A9n%20llamado%20UI,control%20del%20ordenador%20del%20usuario.)

RESUMEN DE ENCRIPTACION DE INFORMACION:

1. Toda la información en el disco duro está cifrada
2. Cada disco duro solo contiene partes de la información de un mensaje y jamás la imagen original completa

Data Encryption keys: llaves generadas para encriptar cada parte individual de un mensaje original

Key encryption Keys: llaves que pueden ser generadas por Google o por el propietario de la información  
(en caso de querer aumentar aun mas la seguridad de manera independiente a google) y que son usadas para encriptar las llaves que encriptan la información

**IMPORTANTE**

Billing accounts son el vehículo de pago para tus gastos en GCP, y tienen dos tipos:

1.- Se puede tener un self-service en el cual paga lo que usas sin necesidad de un contrato  
2.- Se firma un contrato como un servicio tradicional y se generan solicitudes de pago

\_Payment Profile: \_Acá se guarda la tarjeta de crédito y es la que gestiona.

Establecer las *Buenas prácticas:*

1. Establecer los medios de pago en el payment profile
2. Generar una billing account y ligarla a la organización

## La jerarquía de recursos en Google Cloud

* Mapea la estructura organizacional.
* Administra a escala.
* Separación.
* Herencia de políticas.

#### Organización

Es raíz de la jerarquía de recursos. Esta tiene varias cosas asignadas directamente a la organización:

* La Billing Account está asignada a esta.
* Los grupos administradores puede operar en este nodo.
* Los permisos que toda la organización deba tener se pueden asignar aquí, y heredarlos a los nodos que están debajo.

<h5>Cloud Identity</h5>

Si usamos Google Workspace, el SaaS (Software as a Service) de Google, las identidades son una forma de autenticar a los usuarios que pertenecen a tu organización y tienen acceso a tu Google Cloud.

Cloud Identity nos permite generar los usuarios para Google Cloud sin necesidad de tener Google Workspace. Nos da 50 identidades sin costo.

A la organización se le liga un dominio para identificarla.

#### Folders

Modela la estructura organizacional con GCP (ya sean departamentos, equipos, aplicaciones, cargas de trabajo, ciclo de vida, facturación y aislamiento de seguridad).

Los folders pueden contener proyectos y carpetas.

Poder agrupar las estructuras en folders nos permite:

* Limitar el acceso, crear grupos y darles permisos en un espacio específico.
* Discriminar costos, saber cuanto me cuesta un nodo en específico.

#### Proyectos

Contienen los recursos computacionales. Un proyecto es un agrupador de recursos.

Es importante desarrollar un proyecto con una necesidad en mente.  
Ejem:

* Proyecto de CI/CD
* Proyecto de un Micro servicio
* Proyecto para el sitio de marketing

Ventajas de los proyectos pequeños:

* Fácil mantenimiento
* Más seguridad
* Facilidad de Evolución

## Identidad y control de acceso

### ¿Quién es el miembro?

Puede ser

* una **persona**
* un **subsistema** (ejem. Aplicación): esto se le conoce como service account.

**Zero Trust / Confianza Cero**: No confiamos en lo que está dentro de nuestro perímetro de seguridad de forma automática.

* Las comunicaciones dentro del perímetro de seguridad están cifradas y vienen con permisos.
* Establecemos que aplicaciones pueden hablar con que aplicaciones.
* Determinamos el tipo de recursos que las aplicaciones pueden generar.

### ¿Qué puede hacer?

Existe una taxonomía muy grande de recursos relacionados con que puede hacer.

Los recursos tienen ciertos permisos asignados. Además los permisos permiten realizar acciones sobre un recurso:

* Generar uno nuevo
* Modificarlo
* Borrarlo
* Hacerle update

### ¿En cuál recurso?

Las políticas de seguridad se asignan a cada uno de los recursos. En una política podemos establecer el rol de los miembros.

Quién puede hacer qué en cuál recurso.

El quién es persona o aplicación.  
El qué son permisos y se asignan a través de roles.

### Roles

Los roles son una colección de permisos detallados que asignamos a grupos.

Podemos generar nuestros propios roles, pero ya hay varios existentes.

### Asignación de políticas y herencia

Se puede asignar a varios niveles: podemos asignar políticas a nivel org. folder, proyecto y recurso.  
Además de que heredan la política de los nodos superiores.

### Estructura de una política

{

"bindings": [

{

"role": "roles/storage.objectAdmin",

"members": [

"user:alice@acme.com",

"serviceAccount:my-other-app@appspot.gserviceaccount.com",

"group:admins@acme.com",

"domain:acme.com" ]

},

{

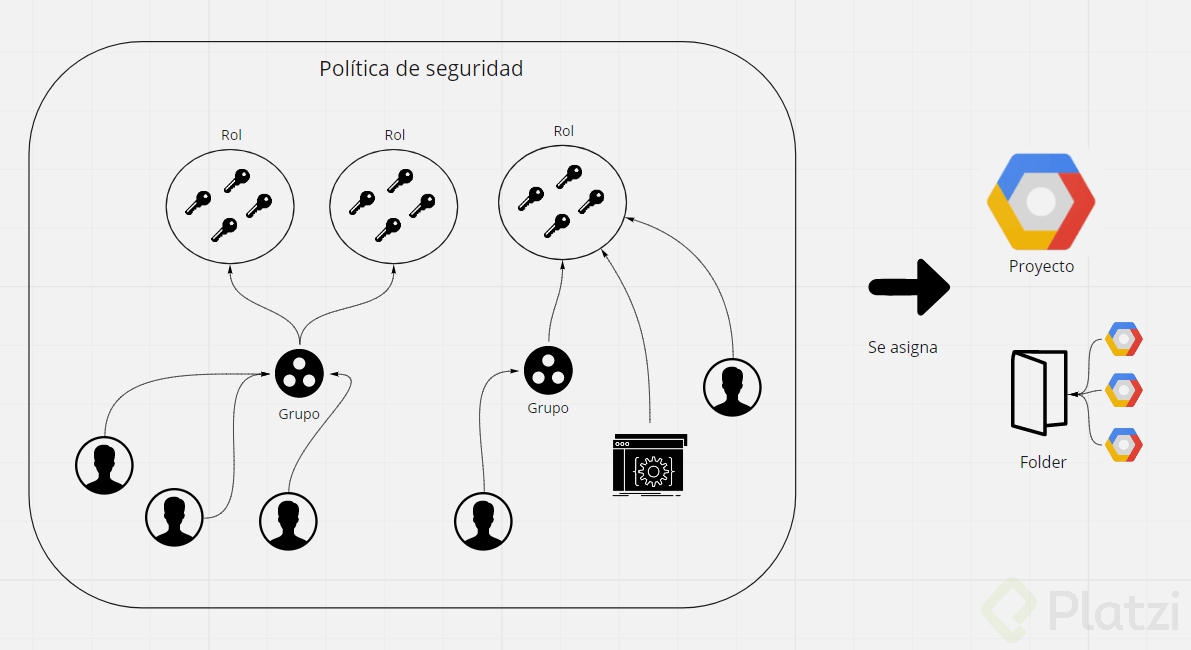
"role": "roles/storage.objectViewer", # rol

"members": ["user:bob@acme.com"] # a los que les asignaremos el rol

}

]

}



Los grupos de devops y developers:

### gcp-devops

Los profesionales de DevOps crean o administran canalizaciones de extremo a extremo que admiten integración y entrega continuas, supervisión y aprovisionamiento de sistemas.

### gcp-developers

Los desarrolladores son los responsables de diseñar, codificar y probar aplicaciones.

Roles de IAM

* User
* Group
  + Role
  + Resource

Grupos a nivel de organización

* Super Administradores
  + igual al super usuario de Linux
  + es un usuario con un montón de poderes
* Org. Admins
  + Define políticas de IAM
  + Determina la estructura de la jerarquía de recursos
  + Crea proyectos hasta que la organización este madura
* Network Admins
  + Crea redes, subredes, dispositivos de red (enrutadores en la nube, VPN en la nube y balanceadores de carga en la nube)
  + Mantiene las reglas del firewall, a menos que las mantenga el administrador de seguridad
* Security Admins
  + Establece políticas y restricciones para toda la organización, carpetas y proyectos
  + Establece roles de IAM para proyectos
  + Mantiene la visibilidad de los logs y los recursos
* Billing Admins
  + Configura una cuenta de facturación
  + Monitorear el uso de los recursos

¿Como interactuar con Google Cloud platform?

* Todo en GCP se interactúa a través de API
* Puedes interactuar con GCP a través de 3 métodos:
  + La web App
  + La aplicación móvil
  + La CLI para la terminal

Cloud Marketplace

¿Qué es el Google Cloud Marketplace?

* Es una AppStore
  + esta especializada en software empresarial
  + Plataforma de compras
* Ventajas de Marketplace
  + Es fácil de instalar
  + Una sola factura de Google
* Como funciona el Marketplace
  + Tiene una gran selección de software
  + Se cotiza a través de precio de lista o de negociaciones privadas (se respeta el precio del cliente y su confidencialidad)