

Google Cloud Certified Cloud Digital Leader

Domínios, pesos oficiales y habilidades clave del temario de Cloud Digital Leader, para repasar antes del examen.

Nivel: Beginner Duración: 90 min Fuente: guía de estudio oficial de Microsoft Learn

1. Digital Transformation with Google Cloud

17–17%

Why Cloud Technology is Transforming Business

- La computación en la nube es el acceso bajo demanda a recursos informáticos como servicios por internet, pagando solo lo que se usa. La transformación digital usa esas tecnologías para cambiar procesos, cultura y experiencia de cliente. Cloud native describe cómo se crean las aplicaciones (microservicios, contenedores, CI/CD), no dónde se ejecutan y reduciendo la burocracia y los estándares de hardware para poder experimentar y evolucionar, y espera meses para ampliar capacidad, aunque mantiene el control total. En la nube el proveedor gestiona la infraestructura, los recursos se crean o retiran en segundos y se paga por uso. A cambio, el acceso depende de la conexión de red y el cliente depende de la seguridad.
- El cliente depende de la seguridad de la infraestructura física, probar ideas sin esperar a compras de hardware y pagar solo por lo que se usa, con FinOps para maximizar el valor del gasto. Puede reforzar la seguridad gracias a las funciones y expertos del proveedor, y aporta valor estratégico: acceso a las últimas innovaciones y personalización.
- El cliente depende de la seguridad de la infraestructura física, probar ideas sin esperar a compras de hardware y pagar solo por lo que se usa, con FinOps para maximizar el valor del gasto. Puede reforzar la seguridad gracias a las funciones y expertos del proveedor, y aporta valor estratégico: acceso a las últimas innovaciones y personalización.
- El cliente depende de la seguridad de la infraestructura física, probar ideas sin esperar a compras de hardware y pagar solo por lo que se usa, con FinOps para maximizar el valor del gasto. Puede reforzar la seguridad gracias a las funciones y expertos del proveedor, y aporta valor estratégico: acceso a las últimas innovaciones y personalización.
- El cliente depende de la seguridad de la infraestructura física, probar ideas sin esperar a compras de hardware y pagar solo por lo que se usa, con FinOps para maximizar el valor del gasto. Puede reforzar la seguridad gracias a las funciones y expertos del proveedor, y aporta valor estratégico: acceso a las últimas innovaciones y personalización.
- El cliente depende de la seguridad de la infraestructura física, probar ideas sin esperar a compras de hardware y pagar solo por lo que se usa, con FinOps para maximizar el valor del gasto. Puede reforzar la seguridad gracias a las funciones y expertos del proveedor, y aporta valor estratégico: acceso a las últimas innovaciones y personalización.
- El cliente depende de la seguridad de la infraestructura física, probar ideas sin esperar a compras de hardware y pagar solo por lo que se usa, con FinOps para maximizar el valor del gasto. Puede reforzar la seguridad gracias a las funciones y expertos del proveedor, y aporta valor estratégico: acceso a las últimas innovaciones y personalización.
- El cliente depende de la seguridad de la infraestructura física, probar ideas sin esperar a compras de hardware y pagar solo por lo que se usa, con FinOps para maximizar el valor del gasto. Puede reforzar la seguridad gracias a las funciones y expertos del proveedor, y aporta valor estratégico: acceso a las últimas innovaciones y personalización.
- El cliente depende de la seguridad de la infraestructura física, probar ideas sin esperar a compras de hardware y pagar solo por lo que se usa, con FinOps para maximizar el valor del gasto. Puede reforzar la seguridad gracias a las funciones y expertos del proveedor, y aporta valor estratégico: acceso a las últimas innovaciones y personalización.
- El cliente depende de la seguridad de la infraestructura física, probar ideas sin esperar a compras de hardware y pagar solo por lo que se usa, con FinOps para maximizar el valor del gasto. Puede reforzar la seguridad gracias a las funciones y expertos del proveedor, y aporta valor estratégico: acceso a las últimas innovaciones y personalización.

Fundamental Cloud Concepts

- En la nube los recursos se crean o retiran en segundos (agilidad), crecen con el negocio (escalabilidad) y se amplían y reducen con los picos de demanda (elasticidad). Las copias de seguridad y la recuperación ante desastres mejoran la fiabilidad. El coste total de propiedad baja sobre todo porque ya no hay que comprar ni mantener capacidad para el pico que se usa.
- El cliente depende de la seguridad de la infraestructura física, probar ideas sin esperar a compras de hardware y pagar solo por lo que se usa, con FinOps para maximizar el valor del gasto. Puede reforzar la seguridad gracias a las funciones y expertos del proveedor, y aporta valor estratégico: acceso a las últimas innovaciones y personalización.
- El cliente depende de la seguridad de la infraestructura física, probar ideas sin esperar a compras de hardware y pagar solo por lo que se usa, con FinOps para maximizar el valor del gasto. Puede reforzar la seguridad gracias a las funciones y expertos del proveedor, y aporta valor estratégico: acceso a las últimas innovaciones y personalización.
- El cliente depende de la seguridad de la infraestructura física, probar ideas sin esperar a compras de hardware y pagar solo por lo que se usa, con FinOps para maximizar el valor del gasto. Puede reforzar la seguridad gracias a las funciones y expertos del proveedor, y aporta valor estratégico: acceso a las últimas innovaciones y personalización.
- El cliente depende de la seguridad de la infraestructura física, probar ideas sin esperar a compras de hardware y pagar solo por lo que se usa, con FinOps para maximizar el valor del gasto. Puede reforzar la seguridad gracias a las funciones y expertos del proveedor, y aporta valor estratégico: acceso a las últimas innovaciones y personalización.
- El cliente depende de la seguridad de la infraestructura física, probar ideas sin esperar a compras de hardware y pagar solo por lo que se usa, con FinOps para maximizar el valor del gasto. Puede reforzar la seguridad gracias a las funciones y expertos del proveedor, y aporta valor estratégico: acceso a las últimas innovaciones y personalización.
- El cliente depende de la seguridad de la infraestructura física, probar ideas sin esperar a compras de hardware y pagar solo por lo que se usa, con FinOps para maximizar el valor del gasto. Puede reforzar la seguridad gracias a las funciones y expertos del proveedor, y aporta valor estratégico: acceso a las últimas innovaciones y personalización.
- El cliente depende de la seguridad de la infraestructura física, probar ideas sin esperar a compras de hardware y pagar solo por lo que se usa, con FinOps para maximizar el valor del gasto. Puede reforzar la seguridad gracias a las funciones y expertos del proveedor, y aporta valor estratégico: acceso a las últimas innovaciones y personalización.
- El cliente depende de la seguridad de la infraestructura física, probar ideas sin esperar a compras de hardware y pagar solo por lo que se usa, con FinOps para maximizar el valor del gasto. Puede reforzar la seguridad gracias a las funciones y expertos del proveedor, y aporta valor estratégico: acceso a las últimas innovaciones y personalización.
- El cliente depende de la seguridad de la infraestructura física, probar ideas sin esperar a compras de hardware y pagar solo por lo que se usa, con FinOps para maximizar el valor del gasto. Puede reforzar la seguridad gracias a las funciones y expertos del proveedor, y aporta valor estratégico: acceso a las últimas innovaciones y personalización.

Cloud Computing Models and Shared Responsibility

- La IaaS ofrece computación, almacenamiento y redes bajo demanda; el cliente gestiona el sistema operativo, el middleware, las aplicaciones y los datos (por ejemplo, Compute Engine). La PaaS proporciona un entorno gestionado donde el cliente solo aporta código y datos (App Engine, Cloud Run). El SaaS entrega una aplicación completa gestionada por el proveedor, como el correo y el navegador (Google Workspace).
- El cliente depende de la seguridad de la infraestructura física, probar ideas sin esperar a compras de hardware y pagar solo por lo que se usa, con FinOps para maximizar el valor del gasto. Puede reforzar la seguridad gracias a las funciones y expertos del proveedor, y aporta valor estratégico: acceso a las últimas innovaciones y personalización.
- El cliente depende de la seguridad de la infraestructura física, probar ideas sin esperar a compras de hardware y pagar solo por lo que se usa, con FinOps para maximizar el valor del gasto. Puede reforzar la seguridad gracias a las funciones y expertos del proveedor, y aporta valor estratégico: acceso a las últimas innovaciones y personalización.
- El cliente depende de la seguridad de la infraestructura física, probar ideas sin esperar a compras de hardware y pagar solo por lo que se usa, con FinOps para maximizar el valor del gasto. Puede reforzar la seguridad gracias a las funciones y expertos del proveedor, y aporta valor estratégico: acceso a las últimas innovaciones y personalización.
- El cliente depende de la seguridad de la infraestructura física, probar ideas sin esperar a compras de hardware y pagar solo por lo que se usa, con FinOps para maximizar el valor del gasto. Puede reforzar la seguridad gracias a las funciones y expertos del proveedor, y aporta valor estratégico: acceso a las últimas innovaciones y personalización.
- El cliente depende de la seguridad de la infraestructura física, probar ideas sin esperar a compras de hardware y pagar solo por lo que se usa, con FinOps para maximizar el valor del gasto. Puede reforzar la seguridad gracias a las funciones y expertos del proveedor, y aporta valor estratégico: acceso a las últimas innovaciones y personalización.
- El cliente depende de la seguridad de la infraestructura física, probar ideas sin esperar a compras de hardware y pagar solo por lo que se usa, con FinOps para maximizar el valor del gasto. Puede reforzar la seguridad gracias a las funciones y expertos del proveedor, y aporta valor estratégico: acceso a las últimas innovaciones y personalización.
- El cliente depende de la seguridad de la infraestructura física, probar ideas sin esperar a compras de hardware y pagar solo por lo que se usa, con FinOps para maximizar el valor del gasto. Puede reforzar la seguridad gracias a las funciones y expertos del proveedor, y aporta valor estratégico: acceso a las últimas innovaciones y personalización.
- El cliente depende de la seguridad de la infraestructura física, probar ideas sin esperar a compras de hardware y pagar solo por lo que se usa, con FinOps para maximizar el valor del gasto. Puede reforzar la seguridad gracias a las funciones y expertos del proveedor, y aporta valor estratégico: acceso a las últimas innovaciones y personalización.
- El cliente depende de la seguridad de la infraestructura física, probar ideas sin esperar a compras de hardware y pagar solo por lo que se usa, con FinOps para maximizar el valor del gasto. Puede reforzar la seguridad gracias a las funciones y expertos del proveedor, y aporta valor estratégico: acceso a las últimas innovaciones y personalización.

2. Exploring Data Transformation with Google Cloud

16–16%

The Value of Data

- Los datos generan valor cuando se analizan para tomar decisiones. Una base de datos almacena y recupera datos para aplicaciones; las relacionales usan tablas y transacciones ACID. Un almacén de datos, como BigQuery, consolida datos actuales e históricos de muchas fuentes para informes y análisis. Un lago de datos guarda datos estructurados y no estructurados en su formato nativo, sin esquema previo, para exploración e IA.
- Las organizaciones crean valor de tres formas: analizando los datos que ya tienen (por ejemplo, con BigQuery ML para predecir con SQL), recopilando datos nuevos (sensores IoT, eventos de apps) y obteniendo datos externos. Los conjuntos de datos públicos de BigQuery los aloja Google y solo se pagan las consultas; BigQuery sharing permite compartir y descubrir datos de terceros entre organizaciones sin copiarlos.
- Los datos estructurados siguen un esquema fijo en tablas; los semiestructurados, como JSON, tienen etiquetas sin esquema rígido; los no estructurados (texto libre, audio, imágenes, vídeo) son la mayoría de los datos empresariales. La nube permite guardarlos a escala de petabytes en Cloud Storage y lagos de datos, y extraer valor de ellos con IA como Gemini, convirtiéndolos en información estructurada.
- La cadena de valor de los datos va de la ingesta al almacenamiento, el procesamiento, el análisis y la activación. Pub/Sub ingiere eventos de forma asíncrona; Dataflow procesa datos en streaming y por lotes con un único modelo, por ejemplo en flujos ETL (extraer, transformar, cargar) o ELT; BigQuery analiza grandes volúmenes con SQL, y Looker ofrece paneles y métricas gobernadas a los usuarios de negocio.
- La gobernanza de datos abarca todo lo que garantiza que los datos sean seguros, privados, exactos, disponibles y utilizables durante su ciclo de vida. Suele asignar la responsabilidad a los data stewards y vigila la calidad en seis dimensiones: exactitud, integridad, coherencia, actualidad, validez y unicidad. Sin ella, la IA sufre silos, datos de mala calidad, accesos indebidos y fallos de cumplimiento.

Google Cloud Data Management Solutions

- Una base de datos relacional organiza datos estructurados en tablas enlazadas por claves principales y externas, se consulta con SQL y admite transacciones ACID. Las bases de datos NoSQL (documentos, clave-valor, columnas anchas, grafos) usan esquemas flexibles y escalan horizontalmente. El almacenamiento de objetos guarda datos no estructurados como objetos con metadatos e identificador único en un espacio plano.
- BigQuery es un almacén de datos sin servidor y totalmente gestionado que separa almacenamiento y computación, por lo que no hay que aprovisionar ni escalar recursos; con BigQuery Omni consulta datos de Amazon S3 o Azure Blob Storage sin moverlos. Cloud Storage ofrece Standard para datos activos, Nearline para acceso mensual, Coldline para trimestral y Archive, la más barata, para menos de una vez al año.
- Una organización puede trasladar su base de datos tal cual (rehost), llevarla a un servicio gestionado como Cloud SQL o AlloyDB, o modernizarla cambiando de motor. Database Migration Service hace migraciones homogéneas y heterogéneas con instantánea inicial y replicación continua para minimizar la inactividad, y convierte esquema y código con ayuda de Gemini. Bare Metal Solution permite ejecutar Oracle como en local.

Making Data Useful and Accessible

- Looker democratiza los datos con una capa semántica: los analistas definen métricas y relaciones una sola vez en LookML y los usuarios de negocio exploran eligiendo dimensiones, medidas y filtros sin escribir SQL. Conversational Analytics, con Gemini, responde preguntas en lenguaje natural, y Connected Sheets lleva los datos gobernados a Google Sheets, siempre con una única fuente de verdad.
- Looker sobre BigQuery genera SQL que se ejecuta en el propio almacén, así que paneles e informes reflejan los datos actuales a gran escala sin copias aparte. Los datos se integran en los flujos de trabajo con el programador (correo, webhook, Amazon S3, SFTP), con alertas en los mosaicos de los paneles cuando se cumple una condición y con integraciones de terceros a través de un action hub.
- La analítica de streaming procesa y analiza los registros de forma continua a medida que se generan, en lugar de por lotes, cuyos datos pueden quedar obsoletos. Así los datos son útiles desde el primer instante: precios y promociones en tiempo real a partir de los clics, alertas de seguridad ante actividad anómala o avisos cuando una red eléctrica supera un umbral.
- Pub/Sub es un servicio de mensajería asíncrono y escalable que desacopla a quienes producen eventos de quienes los procesan y se usa para ingerir datos de aplicaciones y dispositivos IoT. Dataflow es un servicio totalmente gestionado de procesamiento unificado en streaming y por lotes, basado en Apache Beam, que escala automáticamente y transforma los datos antes de llevarlos a BigQuery.

3. Innovating with Google Cloud Artificial Intelligence

16-16%

AI and ML Fundamentals

- La inteligencia artificial es el campo amplio de crear máquinas que imitan funciones cognitivas humanas; el aprendizaje automático es un subconjunto de la IA que aprende de los datos sin programación explícita para una tarea concreta. La analítica de datos y la BI describen lo ocurrido con informes y paneles, mientras que el ML aprende patrones de datos históricos para predecir resultados nuevos.
- El ML resuelve problemas distintos según los datos: el aprendizaje supervisado usa datos etiquetados para clasificar o predecir valores (sentimiento, spam, previsiones); el no supervisado busca patrones en datos sin etiquetar (segmentación, anomalías); el semisupervisado combina pocos datos etiquetados con muchos sin etiquetar, y el de refuerzo aprende por prueba y error. Usos típicos: fraude, recomendaciones y bajas.
- El ML crea valor de negocio porque analiza conjuntos de datos enormes que superan el análisis manual y mejora cuantos más datos consume; permite escalar decisiones aplicando patrones aprendidos de forma coherente y con menos error humano, y desbloquea datos no estructurados como documentos, imágenes y audio, por ejemplo con Document AI para extraer datos estructurados.
- Un modelo de ML solo es tan bueno como sus datos: si son sesgados, los resultados también lo serán. Los datos de entrenamiento deben representar a toda la población, evitar la fuga de datos y la desviación entre entrenamiento y servicio, y cumplir dimensiones de calidad como validez, integridad y actualidad. En producción, se validan antes de reentrenar y se detiene el pipeline ante anomalías de esquema.
- La IA explicable reúne herramientas que muestran cómo llega un modelo a sus resultados: aumenta la confianza de quienes deciden, facilita depurar modelos y ayuda a detectar sesgos, y debe aplicarse en todo el ciclo, desde los datos hasta el servicio. La IA responsable se apoya en principios de equidad, transparencia, responsabilidad, privacidad y seguridad, y genera la confianza que los clientes exigen.

Google Cloud's AI and ML solutions

- Al elegir una solución de IA hay que sopesar rapidez, esfuerzo, diferenciación y experiencia necesaria. Las API preentrenadas son lo más rápido y no exigen expertos; AutoML entrena con datos propios sin código pero con objetivos predefinidos; el entrenamiento personalizado da control total y más diferenciación a cambio de más tiempo y conocimientos de ciencia de datos.
- Google Cloud ofrece tres caminos: API preentrenadas (Vision, Natural Language, Translation, Speech-to-Text, Text-to-Speech) para tareas comunes sin datos propios; AutoML para entrenar sin código un modelo con los datos y etiquetas de la organización; y entrenamiento personalizado cuando hace falta control total sobre el algoritmo, el framework y la escala del entrenamiento.

Building and using Google Cloud AI and ML solutions

- BigQuery ML permite crear, evaluar y ejecutar modelos de aprendizaje automático con consultas SQL dentro de BigQuery, donde se guardan como las tablas. Lleva el aprendizaje automático a los datos, así que no hay que exportarlos a otros frameworks, y pone el ML al alcance de los analistas que ya conocen SQL, con modelos como regresión, K-means o series temporales.
- Las API preentrenadas resuelven tareas comunes sin entrenar modelos: Natural Language analiza texto (sentimiento, entidades, clasificación); Vision analiza imágenes (etiquetas, OCR, caras, contenido explícito); Translation traduce texto; Speech-to-Text transcribe audio a texto; y Text-to-Speech genera voz natural a partir de texto. Se pueden combinar, por ejemplo transcribir y luego traducir.
- AutoML permite a una organización entrenar, sin código y con poco esfuerzo técnico, modelos propios a partir de sus datos etiquetados: imágenes con sus categorías o tablas con una columna objetivo para clasificar, hacer regresiones o prever. Así obtiene predicciones adaptadas a su negocio, siempre que los datos sean representativos y las categorías sean reconocibles para una persona.
- Vertex AI, cuyos servicios forman parte ahora de Gemini Enterprise Agent Platform, permite crear modelos personalizados optimizados para el resultado propio de cada empresa, con cualquier framework, algoritmo y métrica, y con ajuste de hiperparámetros. Al ser un servicio gestionado, los equipos no administran servidores y se centran en el modelo que los diferencia de la competencia.
- TensorFlow es una biblioteca de aprendizaje automático gratuita y de código abierto, creada por Google, que forma un ecosistema integral para crear, entrenar y desplegar modelos en la nube, en equipos propios o en móviles. Las Cloud TPU son circuitos ASIC diseñados por Google para acelerar el ML, ideales para modelos grandes dominados por cálculos con matrices.

4. Modernize Infrastructure and Applications with Google Cloud

17-17%

Cloud modernization and migration

- Modernizar la infraestructura con Google Cloud evita los ciclos de renovación de hardware y los costes iniciales, y pasa el gasto de capital a gasto operativo. Modernizar las aplicaciones aporta agilidad para lanzar funciones antes, escalabilidad, seguridad y acceso a análisis e IA; se puede avanzar poco a poco con contenedores en GKE o Cloud Run, o con API gestionadas con Apigee.
- Una carga de trabajo es una aplicación, servicio o conjunto de datos que consume recursos como cómputo o almacenamiento. Para cada una se decide: retirar (dar de baja), conservar (dejarla donde está), realojar (lift and shift, casi sin cambios), cambiar de plataforma (optimizarla al moverla, por ejemplo con una base de datos gestionada), refactorizar (cambiar el código hacia lo nativo de la nube) o reimaginar (rediseñar y reescribir).

Computing in the cloud

- Una VM es un ordenador basado en software con su propio sistema operativo; un contenedor empaqueta código y dependencias y comparte el kernel del anfitrión. Los microservicios dividen una aplicación en servicios independientes, y Kubernetes orquesta contenedores. El autoescalado añade o quita VM según la carga, el balanceo de carga reparte el tráfico y las VM interrumpibles son más baratas, pero Compute Engine puede detenerlas.
- Ejecutar cómputo en la nube permite aumentar o reducir la capacidad según la demanda sin comprar servidores, con un modelo de pago por uso. Las VM se duplican en minutos para crear entornos idénticos, la carga se reparte entre muchos servidores para que otro tome el relevo si uno falla, y las regiones cercanas a los usuarios reducen la latencia.
- Compute Engine da control total del sistema operativo y acceso root; GKE admite aplicaciones con estado y control detallado; Cloud Run ejecuta contenedores sin estado sin gestionar infraestructura, pero limita la personalización. Las plataformas que escalan a cero pueden sufrir arranques en frío, y en Cloud Run el disco local es efímero, así que los archivos deben ir a Cloud Storage.
- Compute Engine crea y ejecuta VM en la infraestructura de Google sin inversión inicial. Aporta valor con tipos de máquina personalizados que evitan pagar capacidad sobrante, migración en vivo durante el mantenimiento del host, grupos de instancias que escalan y se reparan solos, Spot VMs para lotes tolerantes a fallos y descuentos por compromiso de uso para cargas estables.
- El realojamiento (lift and shift) traslada cargas con pocos o ningún cambio: es el enfoque más rápido, reutiliza herramientas y conocimientos, y es obligado cuando una aplicación no se puede modificar ni retirar. Su contrapartida es que la carga aún no aprovecha funciones de la nube. Migrate to Virtual Machines lleva VM a Compute Engine, y VMware Engine mantiene herramientas VMware.

Serverless computing

- En la computación sin servidor el proveedor aprovisiona, gestiona y escala la infraestructura, y se paga por el uso real, sin coste por capacidad inactiva. El escalado no exige ajustar reglas y puede llegar a cero, y los desarrolladores se centran en el código con sus lenguajes habituales. Sus límites son los arranques en frío, la menor visibilidad y la dependencia del proveedor.
- Cloud Run ejecuta contenedores o código fuente sin gestionar clústeres, escala a cero y divide el tráfico entre revisiones para lanzamientos graduales. Cloud Run functions ejecuta código de un solo propósito ante eventos y solo cobra el tiempo de ejecución. App Engine es una plataforma web totalmente gestionada, aunque Google recomienda Cloud Run a los usuarios nuevos.

Containers in the cloud

- Una VM virtualiza el hardware y ejecuta su propio sistema operativo invitado, por lo que puede alojar sistemas distintos; un contenedor virtualiza solo el sistema operativo y comparte el kernel, así que es más ligero y arranca en segundos. La misma imagen funciona igual en desarrollo, pruebas y producción, lo que agiliza el CI/CD y separa responsabilidades entre desarrollo y operaciones.
- Los microservicios permiten escalar cada servicio por separado y aíslan los fallos, de modo que un servicio caído no tiene por qué tumbar toda la aplicación; la comunicación por eventos, por ejemplo con Pub/Sub, reduce el acoplamiento. Los contenedores empaquetan cada servicio con sus dependencias y se ejecutan en local y en la nube, lo que facilita la nube híbrida.
- GKE es Kubernetes gestionado: Google gestiona el plano de control y, en modo Autopilot, también nodos, escalado y seguridad; encaja con microservicios complejos y aplicaciones con estado. Cloud Run ejecuta contenedores sin estado sin clústeres y con pago por uso. Ambos usan imágenes de contenedor estándar, así que las cargas pueden moverse entre ellos.

The value of APIs

- Una API es un software que permite que dos aplicaciones se comuniquen: define puntos de entrada estables a la lógica y los datos para que otros desarrolladores los reutilicen. Implica un contrato que evoluciona de forma predecible, de modo que el backend puede cambiar sin romper a los consumidores, y sirve de capa de abstracción para conectar sistemas heredados con productos nuevos.
- Exponer datos y servicios valiosos como API públicas abre nuevos canales de negocio: socios y desarrolladores crean productos sobre ellas y la organización puede cobrar por su uso. En Apigee, las API se agrupan en productos de API con planes de tarifas que definen cuotas y cargos, con facturación prepago o pospago e incluso reparto de ingresos con los desarrolladores.
- Apigee es la plataforma nativa de Google Cloud para crear, gestionar y proteger API. Sus proxies separan a los consumidores del backend y sus políticas añaden seguridad, cuotas y limitación de tráfico sin cambiar el código; además ofrece portales para desarrolladores, análisis, monetización y Apigee hybrid para procesar el tráfico en el propio clúster de Kubernetes.

Hybrid and multi-cloud

- La nube híbrida combina instalaciones propias o nube privada con nube pública: permite cumplir normativas, mantener sistemas difíciles de migrar, modernizar al propio ritmo y ejecutar aplicaciones en el edge con baja latencia. La multinube usa varios proveedores públicos para aprovechar lo mejor de cada uno, evitar la dependencia de un proveedor y reducir puntos únicos de fallo.
- Anthos, cuyas capacidades multiclúster forman ahora parte de GKE, ofrece un único punto de gestión para clústeres en Google Cloud, otras nubes e instalaciones propias. Las flotas agrupan los clústeres para aplicar la misma configuración y políticas y verlos desde la consola; GKE Multi-Cloud crea clústeres en AWS y Azure, y los clústeres adjuntos incorporan los ya existentes.

5. Trust and Security with Google Cloud

17-17%

Trust and security in the cloud

- Las amenazas principales incluyen el ransomware, hoy convertido en extorsión multifacética con motivación económica, el phishing, el malware, los ataques DDoS, las amenazas internas y las configuraciones incorrectas, una de las primeras causas de filtraciones en la nube. Frente al entorno local, la nube reparte la responsabilidad con el proveedor y exige controlar identidades y cargas de trabajo dinámicas.
- Un modelo de seguridad en la nube protege la confidencialidad (solo acceden personas autorizadas), la integridad (nada se altera sin autorización) y la disponibilidad (los servicios siguen accesibles, también frente a DDoS). El control y el cumplimiento se apoyan en claves gestionadas por el cliente en Cloud KMS, en Access Transparency para auditar el acceso del personal de Google y en controles auditables.
- Términos clave: zero trust elimina la confianza implícita y verifica cada acceso según identidad y contexto; el mínimo privilegio concede solo el acceso necesario; DLP descubre, clasifica y desidentifica datos regulados; SIEM analiza registros para detectar amenazas. El cifrado simétrico usa una sola clave y el asimétrico, una pública y otra privada.

Google's trusted infrastructure

- Google diseña sus propios centros de datos, servidores, red y chips de seguridad como Titan, que autentica el hardware y su arranque. Los servidores a medida eliminan componentes innecesarios que podrían introducir vulnerabilidades, la seguridad física se refuerza por capas y la protección se construye en capas sucesivas, del hardware a las operaciones: defensa en profundidad.
- El cifrado protege los datos en tres estados: en reposo (Google Cloud los cifra por defecto y CMEK da control de las claves), en tránsito (TLS hacia Google Front End) y en uso (Confidential Computing). La autenticación verifica la identidad, la autorización con IAM decide quién puede hacer qué sobre qué recursos y la auditoría con Cloud Audit Logs registra quién hizo qué, dónde y cuándo.
- La verificación en dos pasos (2SV) evita que una contraseña robada baste para entrar y mitiga el phishing; Google recomienda llaves de seguridad FIDO, sobre todo para superadministradores. IAM controla quién puede hacer qué sobre qué recursos: se conceden roles (conjuntos de permisos) a entidades principales sobre recursos, preferiblemente roles predefinidos y no básicos.
- Cloud Armor protege aplicaciones frente a ataques DDoS y ataques web como la inyección SQL o el XSS, en Google Cloud, entornos híbridos o multinube. Ofrece protección siempre activa contra DDoS volumétricos de capa 3 y 4, reglas WAF preconfiguradas contra el OWASP Top 10 y Adaptive Protection, que usa aprendizaje automático para detectar ataques de capa 7 y sugerir reglas.
- Las operaciones de seguridad (SecOps) consisten en detectar, investigar y responder a las amenazas. Google Security Operations es una plataforma nativa de la nube que une SIEM, SOAR e inteligencia de amenazas, ingiere telemetría de entornos locales, otras nubes y SaaS, ofrece detecciones mantenidas por Google y guías que automatizan la respuesta para reducir el tiempo de reacción.

Google Cloud's trust principles and compliance

- Los principios de confianza de Google Cloud dicen que los datos son del cliente, que Google no los vende ni los usa para publicidad, que se cifran por defecto y que ningún gobierno tiene puertas traseras. La seguridad es una responsabilidad compartida: Google protege la infraestructura y el cliente sus datos y accesos; con el destino compartido, Google además aporta guías y plantillas seguras.
- Google genera confianza con transparencia: sus informes de transparencia publican datos sobre cómo gobiernos y empresas afectan a la privacidad y explican cómo responde a las solicitudes de gobiernos, y Access Transparency registra cada acceso de su personal a los datos del cliente. Además, auditores externos independientes verifican sus controles y emiten certificaciones y atestaciones.
- Las leyes de donde opera la empresa, las de donde están sus clientes y la normativa del sector pueden exigir que los datos residan en un lugar concreto o queden fuera del alcance del proveedor. Google Cloud permite elegir dónde se crean los recursos con políticas de organización, aplicar regímenes con Assured Workloads, gestionar claves fuera de la nube y usar Google Distributed Cloud en local o aislado.
- El centro de recursos de cumplimiento reúne las certificaciones, atestaciones y guías de Google Cloud organizadas por región y sector, y explica que para leyes como HIPAA Google ofrece documentos y correspondencias, no certifica al cliente. Compliance Reports Manager permite descargar bajo demanda y sin coste adicional los certificados ISO/IEC, informes SOC y autoevaluaciones.

6. Scaling with Google Cloud Operations

17-17%

Financial governance and managing cloud costs

- La gobernanza financiera en la nube (FinOps) une tecnología, finanzas y negocio para que cada equipo responda de su gasto. Google Cloud recomienda alinear el gasto con el valor de negocio, fomentar la conciencia de costes, usar solo lo necesario y optimizar de forma continua; los presupuestos de Cloud Billing avisan al superar umbrales reales o previstos y pueden automatizar respuestas con Pub/Sub.
- En la nube la mayoría de los costes son gasto operativo (OpEx) que se genera al consumir, frente al gasto de capital (CapEx) del hardware propio. Los descuentos por compromiso de uso rebajan el precio a cambio de comprometer uso o gasto durante un plazo; las Spot VMs usan capacidad sobrante, más barata pero interrumpible; y la economía unitaria mide el coste por unidad de negocio.
- La jerarquía de recursos va de la organización a las carpetas (opcionales) y los proyectos, que contienen los recursos. Con la organización, los proyectos son de la empresa y se gestionan de forma centralizada; las carpetas representan departamentos y delegan la administración; y los roles concedidos en un nivel superior se heredan, porque la política efectiva es la unión de la propia y la de los ancestros.
- Los presupuestos de Cloud Billing comparan el gasto real o previsto con un importe planificado y, mediante reglas de umbral, avisan por correo o por Pub/Sub para automatizar respuestas; por sí solos no detienen el gasto. Las cuotas, en cambio, limitan cuánto puede consumir un proyecto de un recurso o API y bloquean el exceso.
- Los informes de Cloud Billing muestran en la consola un gráfico de costes de la cuenta de facturación que se puede filtrar por intervalo de tiempo y agrupar por proyecto, servicio, SKU, ubicación o clave de etiqueta. Para el mes en curso incluyen el coste real acumulado y una previsión basada en la tendencia, y los datos pueden descargarse en CSV.

Operational excellence and reliability at scale

- Modernizar las operaciones en Google Cloud significa apoyarse en servicios gestionados con escalado automático, automatizar las tareas repetitivas para eliminar el toil y entregar software con CI/CD y despliegues progresivos. Google Cloud Observability recoge registros, métricas y trazas de forma automática para detectar y resolver problemas antes.
- La observabilidad consiste en recoger y analizar telemetría para entender el estado de las aplicaciones: métricas (medidas numéricas periódicas), registros (eventos con marca de tiempo) y trazas (recorrido de una solicitud). Un dominio de fallo es un recurso que puede fallar de forma independiente, como una VM o una zona, y la degradación controlada mantiene el servicio con funciones reducidas ante sobrecarga.
- La recuperación ante desastres parte del RTO (tiempo máximo sin servicio) y del RPO (periodo máximo de pérdida de datos); cuanto menores sean, más cuesta, y se elige un patrón frío, templado o caliente. Para alta disponibilidad, Google Cloud recomienda replicar los componentes críticos entre zonas y regiones con conmutación automática y escalar horizontalmente.
- Un SLI mide el comportamiento del servicio, un SLO fija el objetivo interno y un SLA es la promesa al cliente con penalización; el presupuesto de errores (1 menos el SLO) guía cuándo publicar o priorizar la fiabilidad. DORA mide la entrega con frecuencia de despliegue y tiempo de espera (velocidad) y tasa de fallos y tiempo de restauración (estabilidad); los postmortems son sin culpas.
- Todos los clientes tienen Basic Support (documentación, foros, ayuda con la facturación y Active Assist). Standard Support se orienta a cargas en desarrollo, Enhanced Support a producción y Premium Support a cargas críticas, con Technical Account Manager, Customer Aware Support, Operational Health Reviews y Event Management Service para picos planificados.

Sustainability with Google Cloud

- Google ya compensa en cómputo anual su consumo eléctrico con compras de energía eólica y solar, y su objetivo es la energía libre de carbono 24/7: cubrir cada hora y en cada región su consumo con energía libre de carbono. Publica el Google CFE% y la intensidad de carbono de la red de cada región para que los clientes tengan en cuenta el carbono al elegir ubicación.
- Carbon Footprint estima las emisiones del uso de Google Cloud por proyecto, región y producto, con cifras basadas en la ubicación y en el mercado y exportación a BigQuery. Region Picker ayuda a elegir región según carbono, precio y latencia, y el recomendador de proyectos desatendidos de Active Assist propone cerrar proyectos olvidados para reducir coste, riesgo y emisiones.