En la nube - Práctico

MIGUEL ÁNGEL RODRÍGUEZ RAMOS
SUBDIRECTOR GENERAL DE SISTEMAS Y TECNOLOGÍA
INFORMÁTICA DEL AYUNTAMIENTO DE MADRID

¿Quién soy?

```
{
  "nombre": "Miguel Ángel Rodríguez Ramos",
  "organización": "Informática del Ayuntamiento de Madrid",
  "cargo": "Subdirector General de Sistemas y Tecnología",
  "formación": [
  "Cuerpo TIC AGE 2007", "Ingeniero en Informática",
  "Máster en Gestión pública TIC"
  ]
  "experiencia": ["AGE 2007-2018", "Ayto. Madrid 2018-…"]
  "asociación": [
  "ProtAAPP – Protege las Administraciones Públicas",
  "ASTIC"
  ]
  "aficiones": ["tecnología", "ciberseguridad"]
  "rrss": "https://www.linkedin.com/in/miguelangelrodriguezz"
}
```

En Preparatics anteriores…

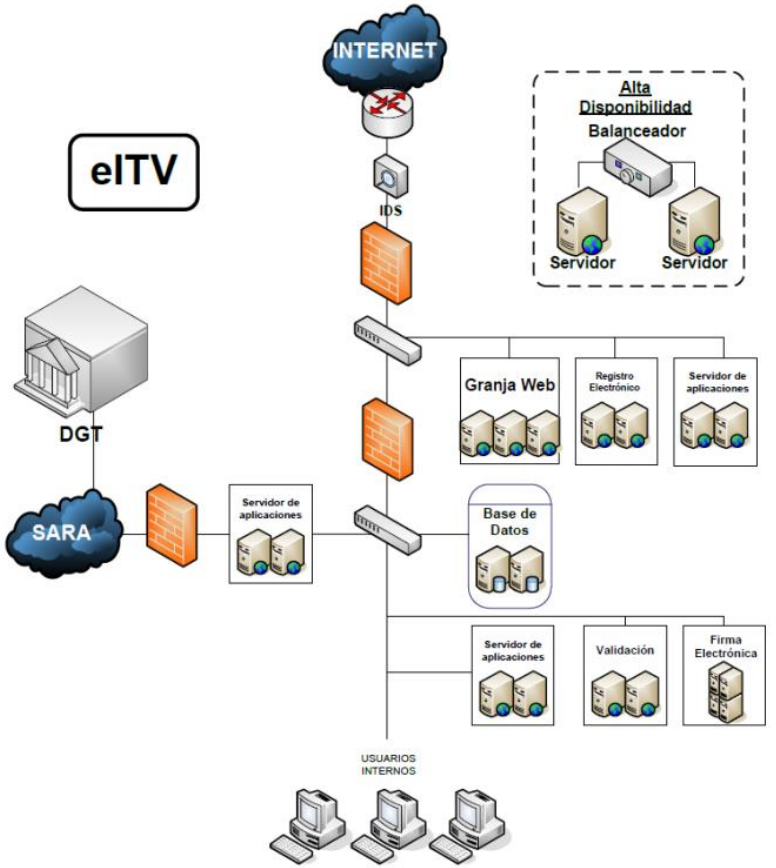
- Preparatic 20 - Inspección Técnica de Vehículos (eITV)
  - Enunciado: https://www.preparatic.org/material/20120414/Caso_Practico_4_Ejercicio_Preparatic_XX.pdf
  - Solución: https://www.preparatic.org/material/20120414/Simulacro_4_Ej_Preparatic_XX_eITV.pdf

- Preparatic 21 - Infraestructuras Comunes de Telecomunicación (ICT)
  - Enunciado: https://www.preparatic.org/material/20140405/EnunciadoSimulacroPreparatic.pdf
  - Solución: https://www.preparatic.org/material/20140405/Presentacion%20Preparatic%20ICT.pdf

- Preparatic 25 – Turespaña - Sesión 8 - Julio de 2018
  - Enunciado: https://www.preparatic.org/material/20180707/Preparatic25-Sesion8-CasoPreparaticTurespa%C3%B1a2018.pdf
  - Solución: https://www.preparatic.org/material/20180707/Preparatic25_sesion8_20180707-Turespa%C3%B1a_Solucion.pdf
  - Sesión en YouTube: https://www.youtube.com/watch?v=dLxjwaRhecs

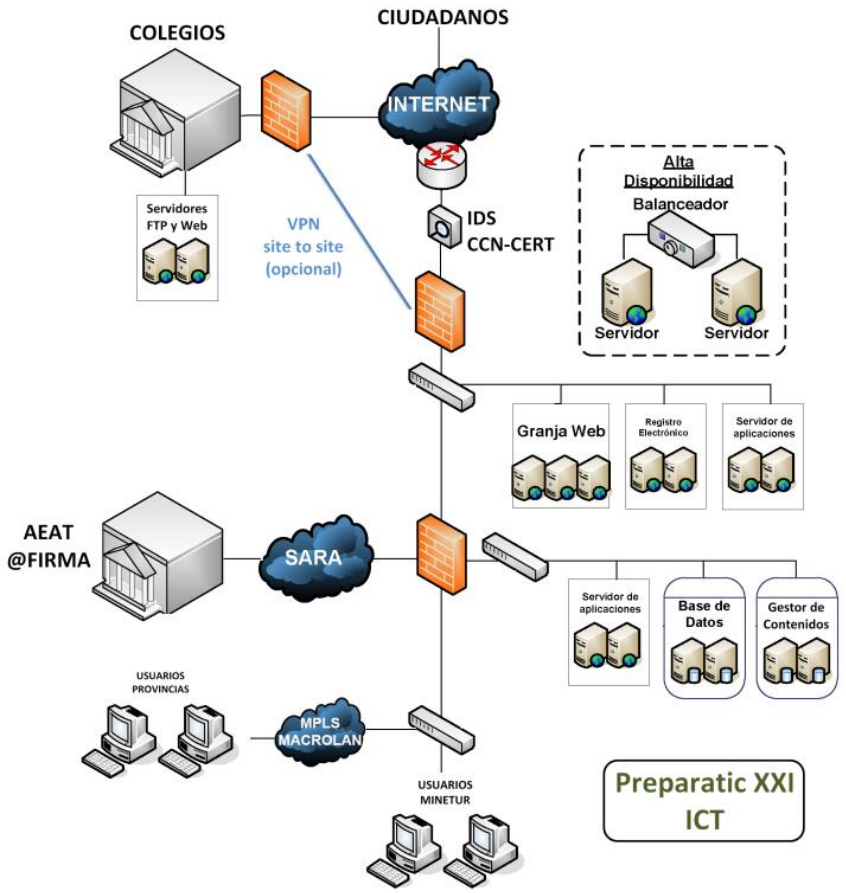
Preparatic 20 - eITV

1. Identificar actores del sistema.
2. Asociar perímetros de interconexión.
   1. Internet.
   2. Red interna.
   3. Red SARA.
3. Desplegar capas de servidores Web, de aplicaciones, bases de datos. En alta disponibilidad.



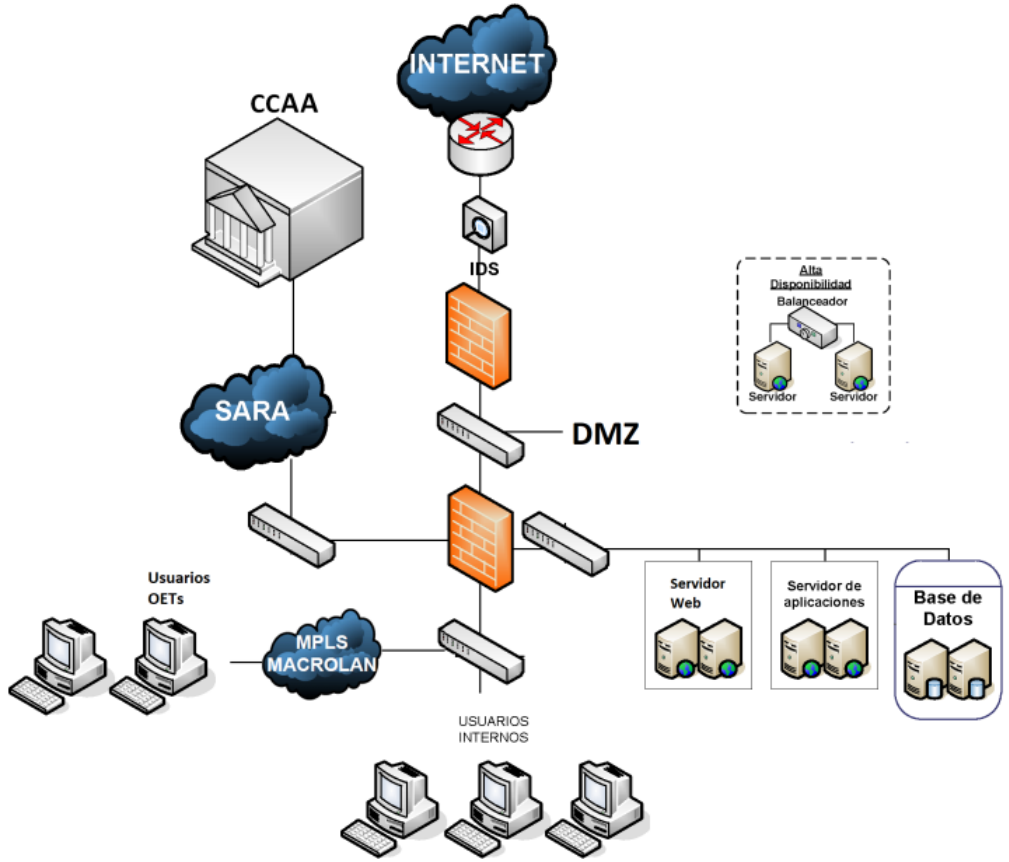
Preparatic 21 - ICT

1. Identificar actores del sistema.
2. Asociar perímetros de interconexión.
   1. Internet.
   2. Red interna.
   3. Red provincial.
   4. Entidad colaboradora – Colegio profesional.
   5. Red SARA.
3. Desplegar capas de servidores Web, de aplicaciones, bases de datos. En alta disponibilidad.



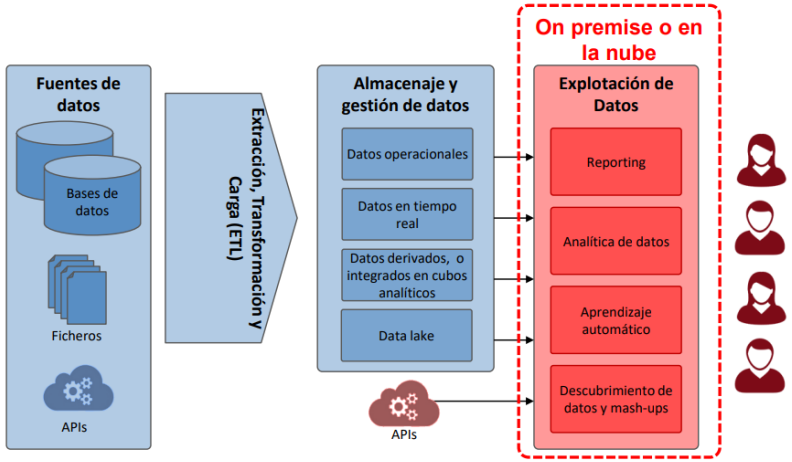
Preparatic 25 - Turespaña

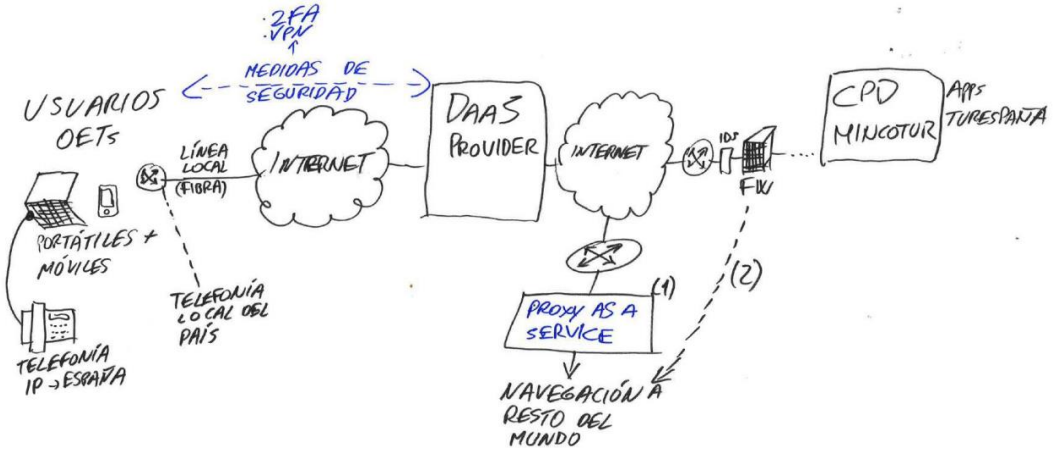
1. Identificar actores del sistema.
2. Asociar perímetros de interconexión.
   1. Internet.
   2. Red interna.
   3. Red internacional.
   4. Entidad colaboradora – Colegio profesional.
   5. Red SARA.
3. Desplegar capas de servidores Web, de aplicaciones, bases de datos. En alta disponibilidad.



Preparatic 25 - Turespaña

- Microservicios y contenedores.
- Red internacional y entorno de escritorio de las oficinas.
- Escritorios virtuales VDI, Desktop as a Service (Cloud).
- CRM para la relación con la ciudadanía.
- Arquitectura de datos de tres capas (Fuentes, Almacén, Explotación).





Consejos generales

- Sentido común.
- La forma sigue a la función. Principio de arquitectura de la escuela de Chicago. Revisar enunciado y adecuarlo a lo que piden.
- Coherencia. Ojo con mezclar microservicios con monolitos. Ejemplo gestor documental.
- El legacy existe y no todo es nube.
- El tribunal es plural y diverso.
- Comodín para interconectar cosas diferentes – Middleware.
- Ojo con la plantilla de servicios compartidos de la AGE con NubeSARA.
- Open + Agnóstico (No vendor lockin) + MultiCloud + Seguro y cumplir el ENS + Ágil + Sostenible y contratable = IMPOSIBLE.

Supuestos cloud friendly

- Tecnologías habilitadoras – Datos + IA – Plataformas de IA inviables on-premise y almacenes de datos DataCloud.
- Conexión con sistemas nativos en nube (Ejemplo el CRM en modo SaaS).
- Maximizar agilidad y time to market. Suponiendo que dispongamos de un servicio de cloud funcionando y capacidad de pago por uso. En otro caso, la contratación lo hace inviable.
- Prototipado rápido – Falla pronto y barato – Escenarios demostradores.
- Arquitecturas ligeras (micro frente a monolitos).
- Bajo acoplamiento o acoplamiento a través de APIs, servicios o tecnologías de integración.

Ecosistema de prestación de servicios públicos

- Las AAPP son prestadores de servicios a ciudadanos.
  - Administrativos (Sede, Registro, Archivo…).
  - Consumo finalista (deportes, cultura, …).
  - Información (transparencia, datos, …).
  - Salud y Educación (hospitales, centros de salud, centros educativos…).
- Las AAPP gestionan infraestructuras y “cosas”.
  - Ciudad – SmartCity.
  - Territorio – Visión geográfica de todos los servicios.
  - Cosas – Farolas, luminarias, semáforos…
- Las AAPP tienen empleados.
  - Empleado público de oficina – Productividad y colaboración.
  - Empleado público en calle – Policías, agentes de movilidad, bomberos.
  - Empresas colaboradoras – Personal externo.

Ecosistema público complejo y diverso

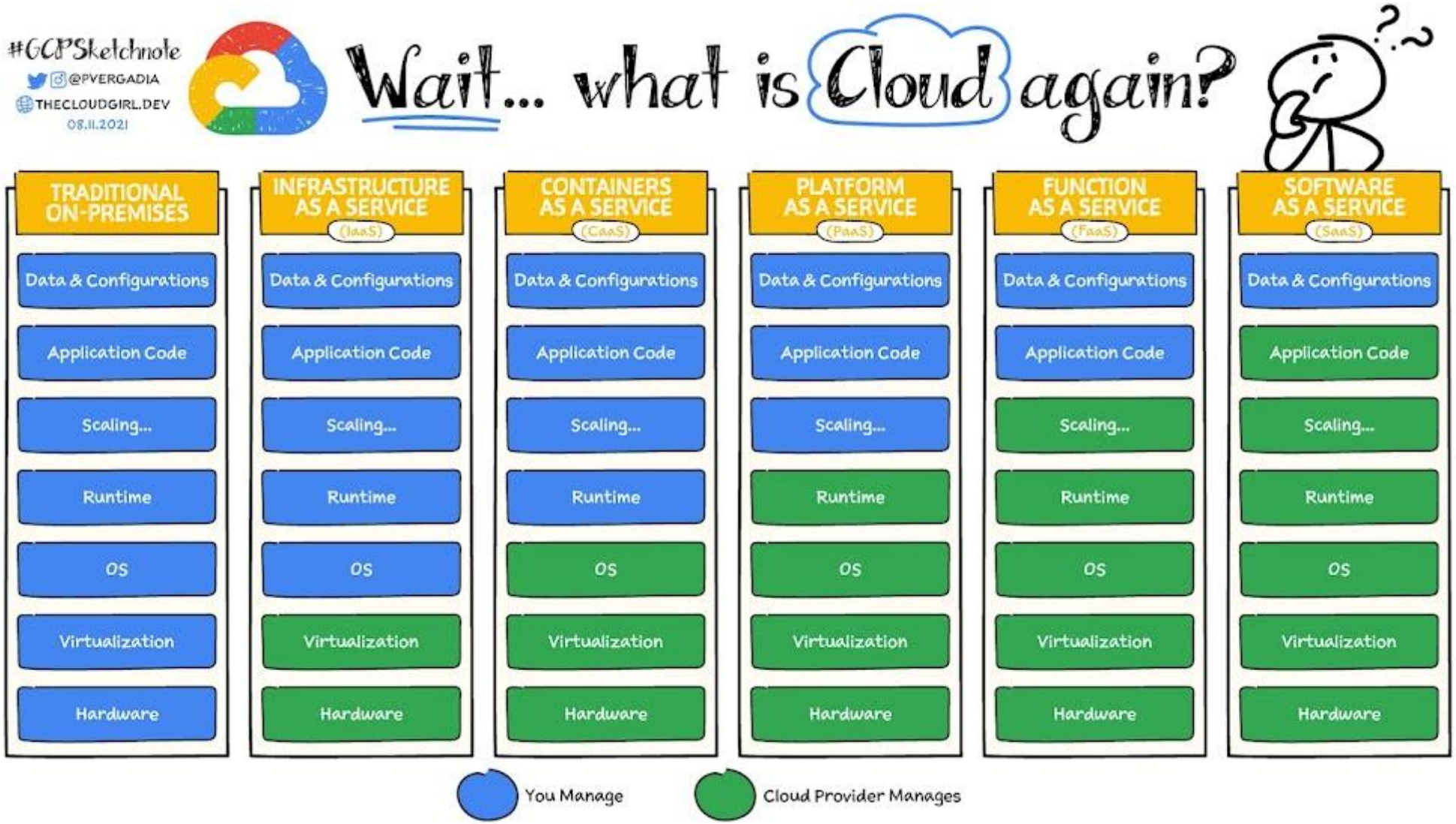
- Servicios a ciudadanos.
  - Multicanal.
  - Mobile first.
  - Proactivo.
  - Inteligente.
  - Resiliente, escalable, seguro, eficiente.
- Infraestructuras y “cosas”.
  - Eficiente, normalizado, seguro.
  - Sostenible.
  - Inteligente.
  - Conectado – Cosas conectadas y empresas prestadoras.
- Empleados.
  - Ubicuo, remoto, teletrabajo.
  - Multidispositivo.

- **Tecnologías**
- Portales.
- CRM.
- Desarrollos a medida.
- Productos y soluciones de negocio.
- Fabricantes SW y HW.
- B2B: APIs, Datasets.
- GIS.
- IoT, Industrial, SCADA, 5G.
- Proveedores cloud.
- GIS 2D, 3D. Gemelo Digital.
- Aparatos médicos.
- Datawarehouse, Datalake.
- Inteligencia Artificial Generativa.
- RPA.
- Legacy.

La nube – Conceptos

- Outsourcing: terciarización o externalización de un servicio.
- Servicio gestionado: prestación de un servicio extremo a extremo con características establecidas y acuerdos de nivel de servicio.
- La nube: cuando una infraestructura o servidor es de otro o está lejos.
- **Outsourcing ≠ Servicio gestionado ≠ En la nube.**
- **Máquinas propias en un housing ≠ Nube pública**
- Nube pública: comparte recursos y ofrece servicios al público a través de Internet.
- Nube privada: que no se comparte y ofrece servicios a través de una red interna privada, normalmente hospedada en el entorno local.
- Nube híbrida: comparte servicios entre nubes públicas y privadas.

La nube – Responsabilidad compartida

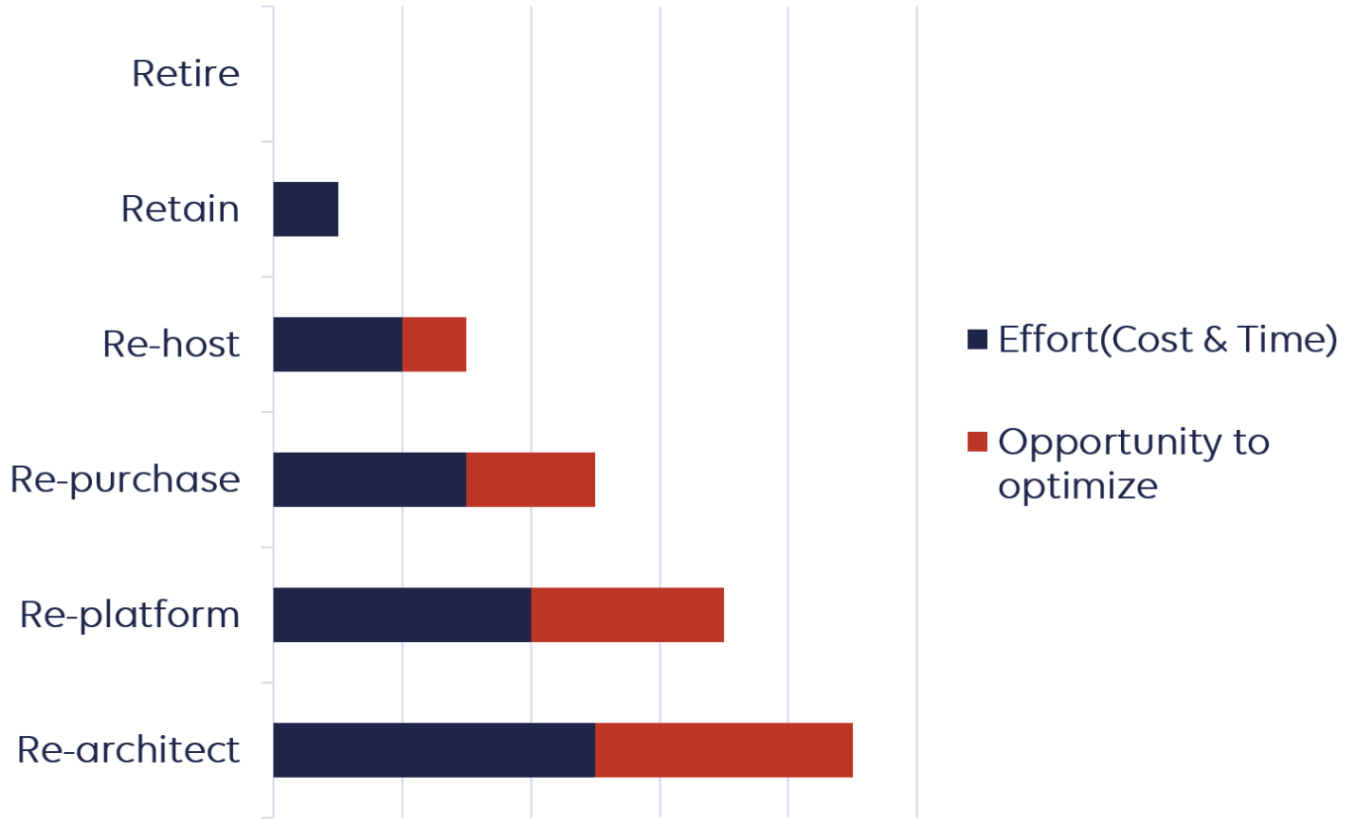


Centro de Excelencia Cloud

- Servicio horizontal de la organización de TI.
- Reskilling del personal.
- Metodología y buenas prácticas para otros.
- Comunidad de personas que usan la cloud.
- Landing zones de los hiperescalars.
- Finops – optimización y control de costes.
- Seguridad, identidad, monitorización y observabilidad comunes a todos.

El camino hacia la nube – 7Rs

- Retire – Retirar la aplicación.
- Retain – Mantenerla on-premise.
- Re-Locate – Subir a nube a nivel de IaaS. Vmware on cloud.
- Re-Host – Lift&Sift – Subirla a la nube directamente.
- Re-Purchase – Dejar de usar un producto y comprar otro cloud.
- Re-Platform – Parecido a Re-Host pero con pequeñas reformas. Ejemplo, pasar BBDD a Bases de datos gestionadas.
- ReArchitect / Refactor / ReBuild / ReDesign – Rehacer en cloud.



Landing zone

- Conectividad privada de baja latencia
  - Azure ExpressRoute.
  - AWS Direct Connect.
  - Google Cloud Interconnect (GCI).
- Conectividad privada a través de Internet (VPN Gateway).
- Direccionamiento IP privado – Extensión del datacenter – NubeSARA como nodo de conectividad MultiCloud.
- Seguridad, identidad y red en cada landing de cada proveedor de cloud.
- Documentación y ejemplos:
  - Azure: https://learn.microsoft.com/es-es/azure/cloud-adoption-framework/ready/landing-zone/
  - AWS: https://docs.aws.amazon.com/es_es/prescriptive-guidance/latest/migration-aws-environment/understanding-landing-zones.html
  - GCP: https://cloud.google.com/architecture/landing-zones?hl=es-419

La nube como un Lego – Cajas de piezas

UX - FRONT

DevOps

GESTIÓN

MONTITORIZACIÓN

OBSERVABILIDAD

APLICACIONES

SERV. APPS

PERSISTENCIA EN BBDD OPERACIONALES Y ALMACÉN OBJ. (S3)

INTEGRACIÓN

DATA

ANALÍTICA

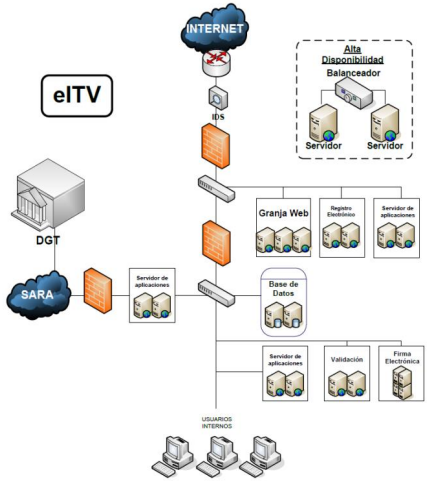
IA - ML

IA GEN

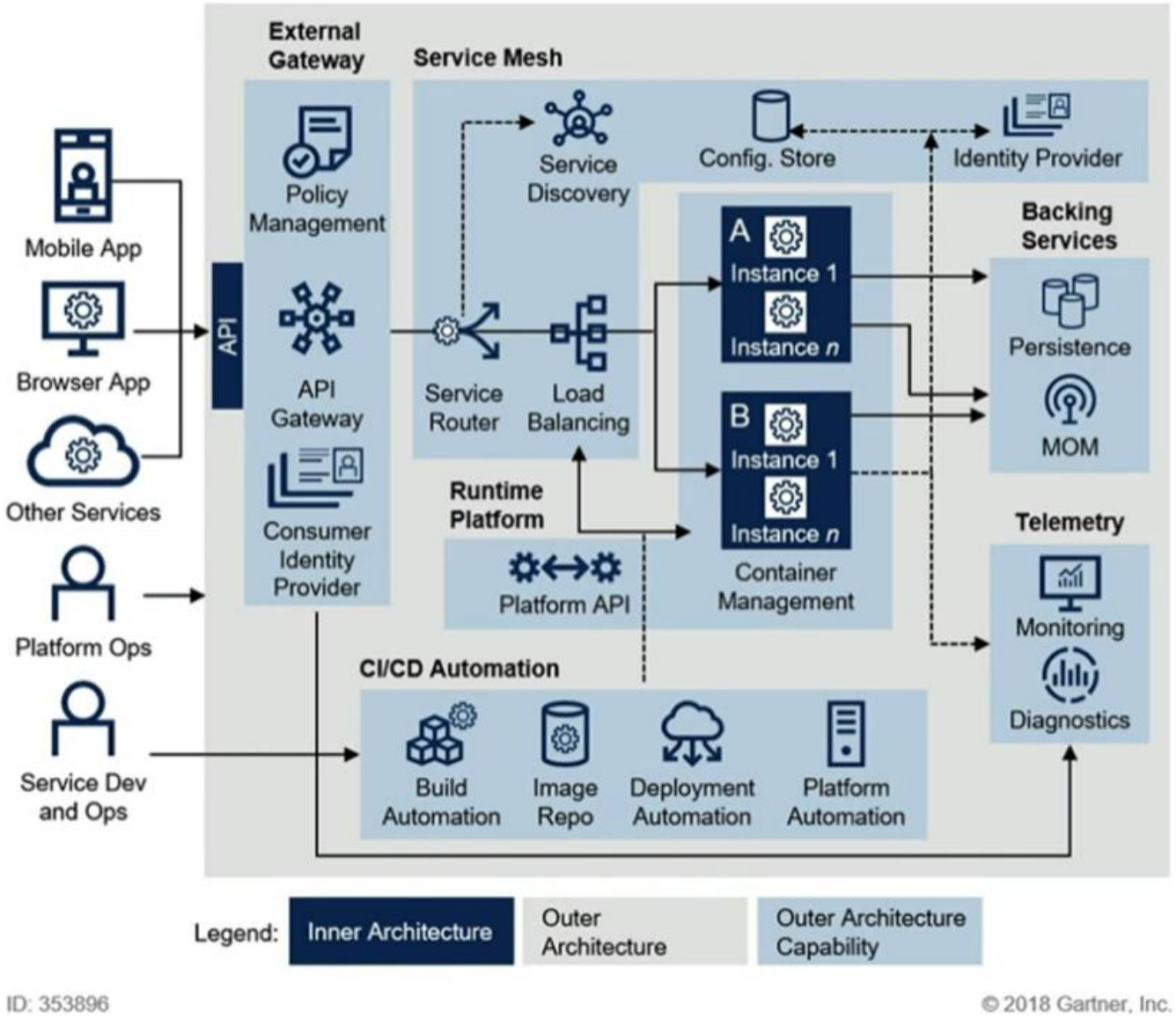
NO → IaaS – CÓMPUTO, ALMACENAMIENTO, BACKUP

SEGURIDAD, IDENTIDAD, RED

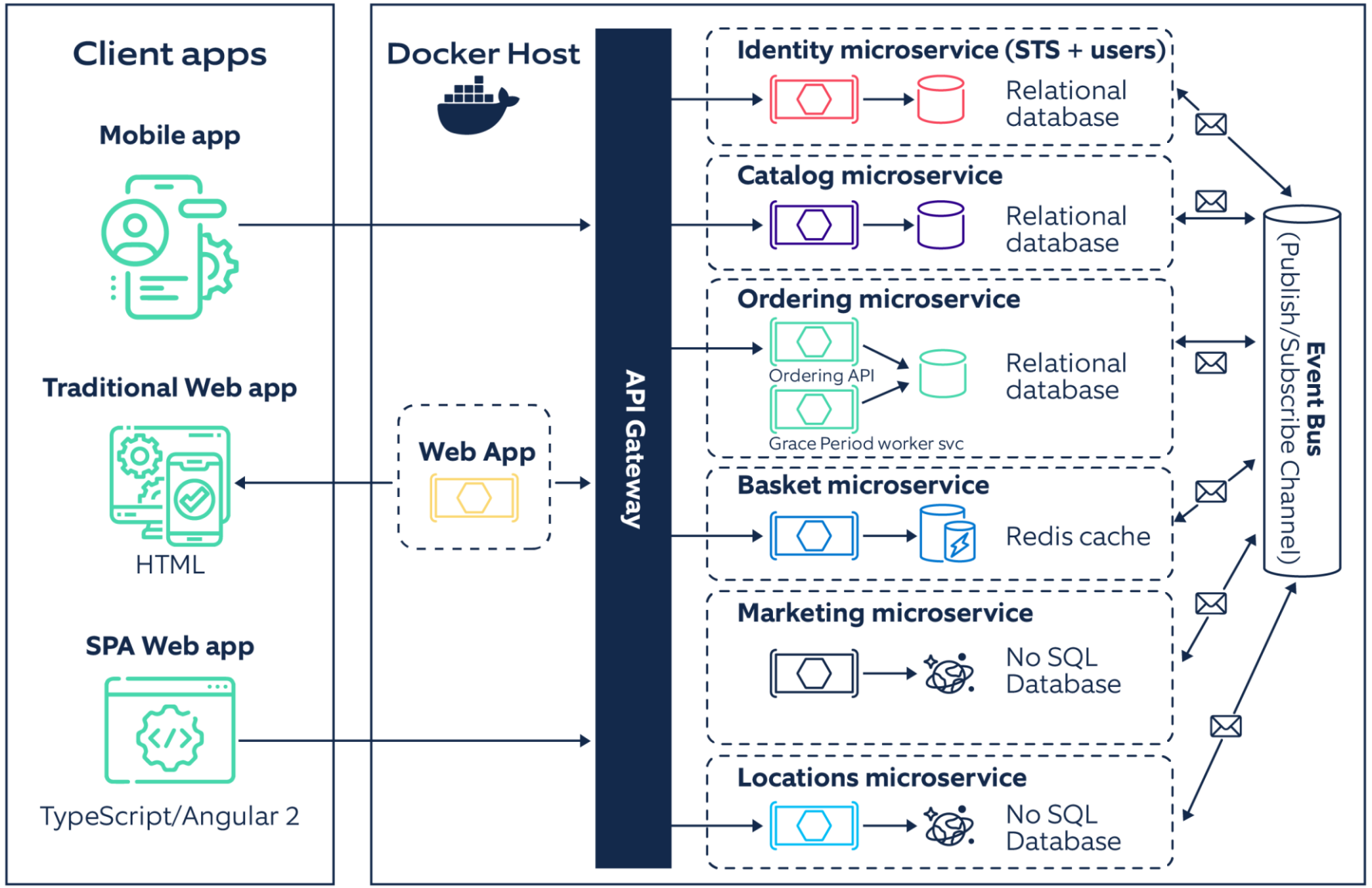
IOT



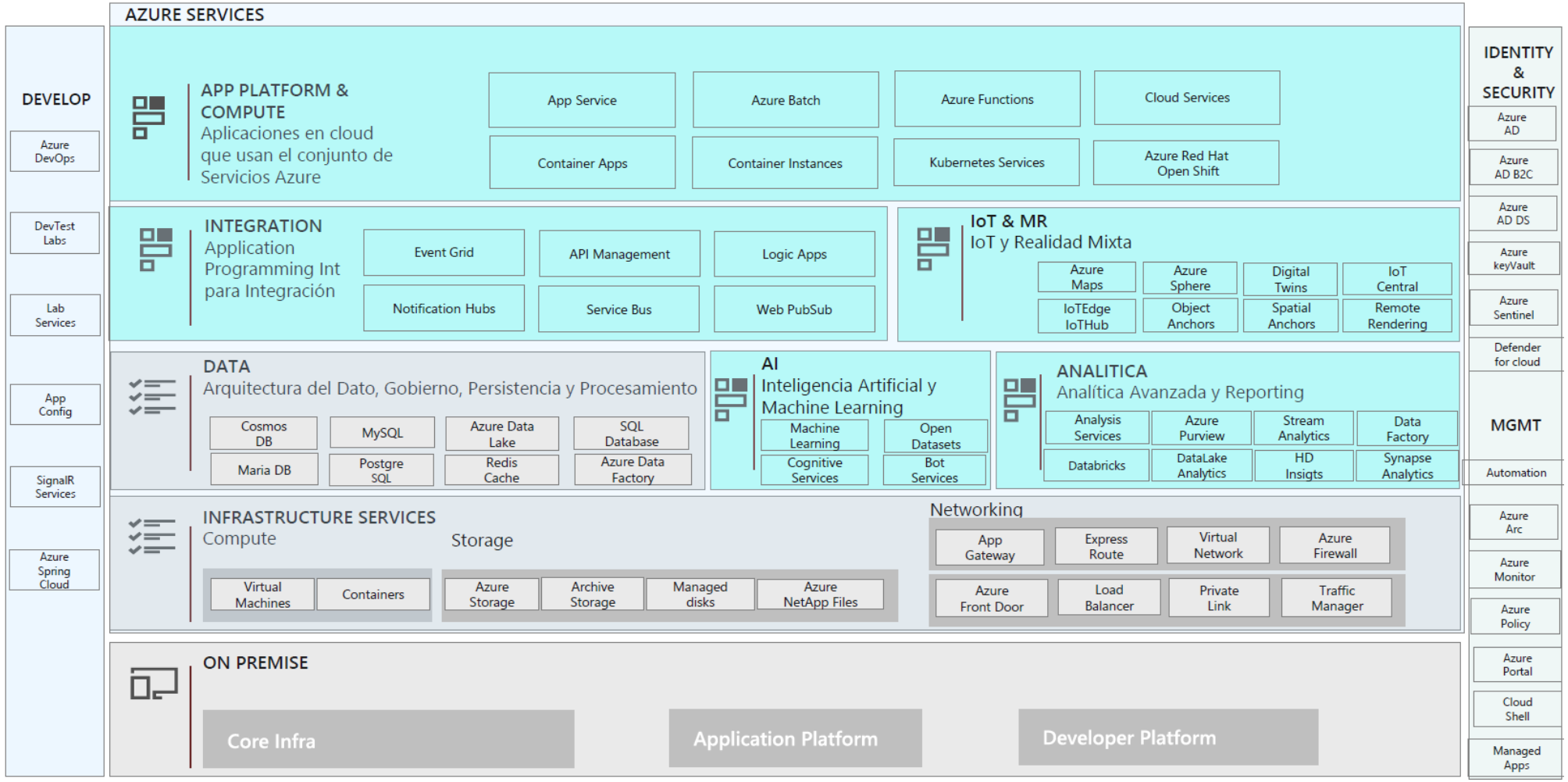
Ejemplo 1


External Gateway
Service Mesh
Policy Management
Service Discovery
Config. Store
Identity Provider
Mobile App
Browser App
Other Services
API
API Gateway
Service Router
Load Balancing
A
Instance 1
Instance n
B
Instance 1
Instance n
Backing Services
Persistence
MOM
Runtime Platform
Platform API
Container Management
Telemetry
Monitoring
Diagnostics
Consumer Identity Provider
Platform Ops
Service Dev and Ops
CI/CD Automation
Build Automation
Image Repo
Deployment Automation
Platform Automation
Legend:
Inner Architecture
Outer Architecture
Outer Architecture Capability
ID: 353896
© 2018 Gartner, Inc.

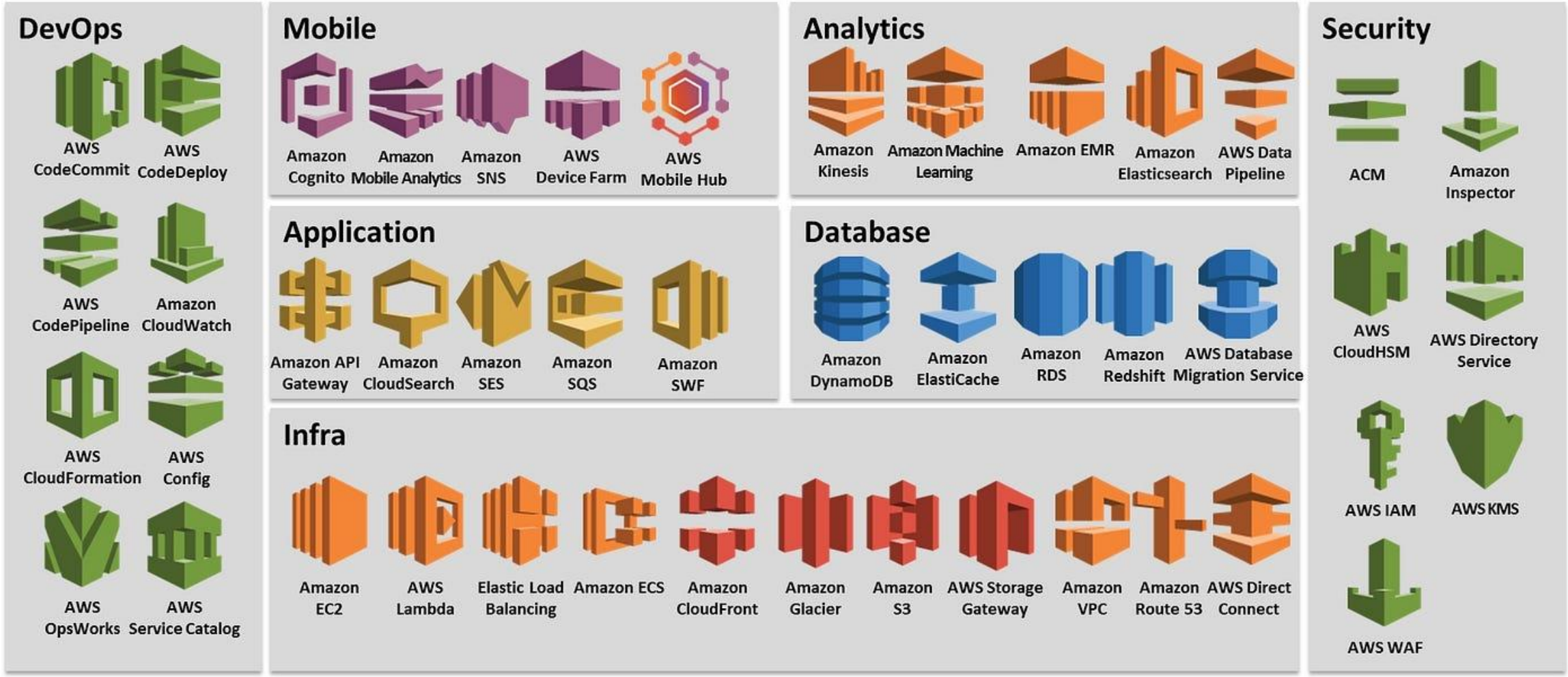
Ejemplo 2


Client apps
Mobile app
Traditional Web app
HTML
SPA Web app
TypeScript/Angular 2
Docker Host
Web App
API Gateway
Identity microservice (STS + users)
Relational database
Catalog microservice
Relational database
Ordering microservice
Ordering API
Grace Period worker svc
Relational database
Basket microservice
Redis cache
Marketing microservice
No SQL Database
Locations microservice
No SQL Database
Event Bus
(Publish/Subscribe Channel)

La nube como un Lego – Azure o equivalente

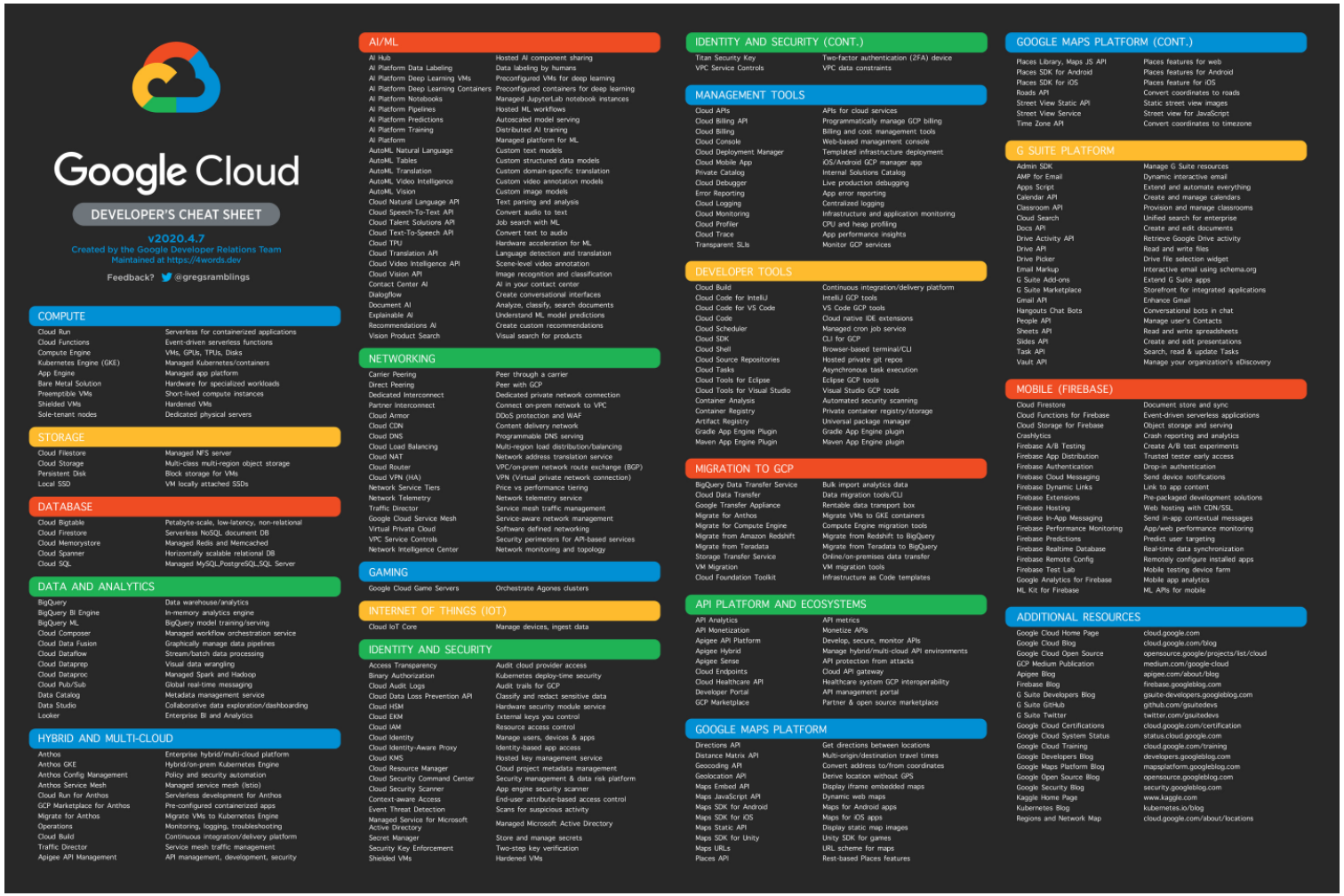


La nube como un Lego – AWS o equivalente



La nube como un Lego – GCP o equivalente

- Ejemplo de catálogo de servicios en GCP
- https://media.codingcat.dev/image/upload/c_limit,w_3840/f_auto/q_auto/v1/ccd-cloudinary/9b45cb61e60e9c6c7ca6dcfaf2fff458ca26bcc2-5400x3600-1?_a=BAVFB+DW0



Frontend

- React
- Angular
- Vue
- React Native – Móvil.
- Flutter – Móvil.
- Elegir en función de la agilidad en el desarrollo, mantenibilidad y ciclo de versiones, número de desarrolladores en el mercado, etc…

UX - FRONTEND

Gestión, desarrollo, monitorización

- IDE – Visual Studio Code.
- Gestión código fuente – GITlab, GitHub.
- Calidad/Seguridad – Sonarqube + OWASP –
- CI/CD – Jenkins – Tekton – GitHub actions.
- Artefactos: Nexus – Artifactory.
- Cada nube tiene el suyo – Microsoft es el más extendido con Github.
- GITops, Infraestructura por código y framework de automatización – Ansible, Terraform, AWX, Airflow.
- Monitorización: Nagios, Checkmk, Zabbix – Monitorización de cada cloud.
- Observabilidad, logging y APM: Elastic ELK, Graylog.

DevOps

GESTIÓN

MONTITORIZACIÓN

OBSERVABILIDAD

Aplicaciones y persistencia

- Capa de aplicación.
  - Servidor de aplicaciones – IaaS.
  - Contenedores en orquestador Kubernetes – CaaS (AKS, EKS, GKS, OpenShift).
  - Azure Appservice, AWS Elastic Beanstalk, Google App Engine – PaaS.
  - Batch – Cada proveedor de cloud tiene su planificador de batch.
- Bases de datos relacionales.
  - Servidores de BBDD sobre IaaS – Mayor carga de gestión.
  - Bases de datos gestionadas – Azure PostgreSQL, AWS PostgreSQL, Cloud SQL for PostgreSQL
  - Bases de datos nativas cloud – Propias de cada nube
- Bases de datos NoSQL.
- Almacenamiento de objetos.
  - Azure Blob Storage.
  - AWS S3.
  - Google Cloud Storage.

APLICACIONES

SERV. APPS

PERSISTENCIA EN BBDD OPERACIONALES Y ALMACÉN OBJ. (S3)

Integración

- API Gateway + API Manager + Seguridad en APIs vs WAF.
  - Azure API Management.
  - Amazon API Gateway.
  - Google Apigee.
  - Kong.
- Kafka – RabbitMQ – Los de los proveedores de cloud.
  - Colas de mensajería, eventos, pub-sub
  - Data Streams y CDC – Apoyo a la arquitectura de datos.
- Referencias de apps + integración.
  - https://learn.microsoft.com/es-es/azure/architecture/
  - https://learn.microsoft.com/es-es/azure/architecture/guide/
  - https://learn.microsoft.com/es-es/azure/architecture/guide/architecture-styles/
  - https://learn.microsoft.com/es-es/azure/architecture/web-apps/

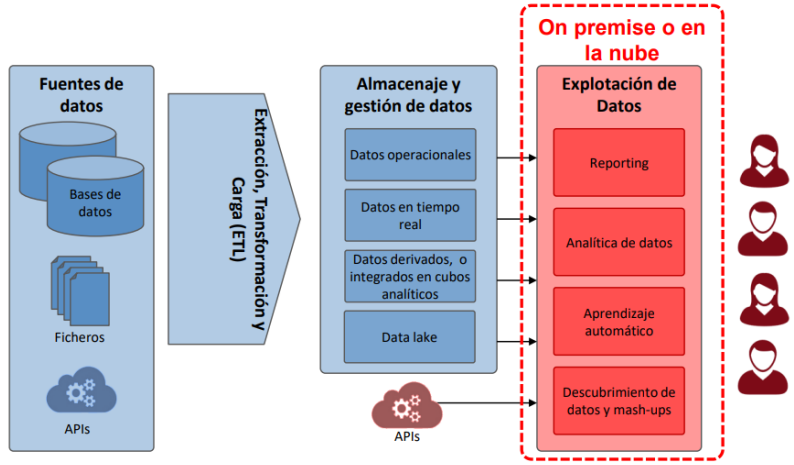
INTEGRACIÓN

Data - Analítica

- Fuentes de datos.
  - Bases de datos.
  - IoT – IoT hub.
  - URLs (Scraping) / APIs.
  - Ficheros – FTPs – Sharepoints.
- Ingesta (Airflow, Azure data factory, Python, Kafka, Debezium).
  - ETLs / ELTs.
  - Batch.
  - Real Time / Data Streams / CDC.
- Almacén / Lakehouse / DataCloud / DataLake – DataCatalog
  - Google Big Query, Snowflake, Databricks – DataCloud MultiNube.
- Consumo.
  - Power BI, Google Looker, Tableau, Visores GIS, SAS.

DATA

ANALÍTICA



IA ML – IA Generativa

- Muy cercano al Data, los pipelines de ingesta de datos y el catálogo de datos.
- GPU on-premise vs servicios cloud – Agilidad frente al mercado de nvidia.
- Modelos fundacionales – Huggingface (ML / IA Gen).
- LLMs grandes frente a pequeños que resuelvan problemas concretos.

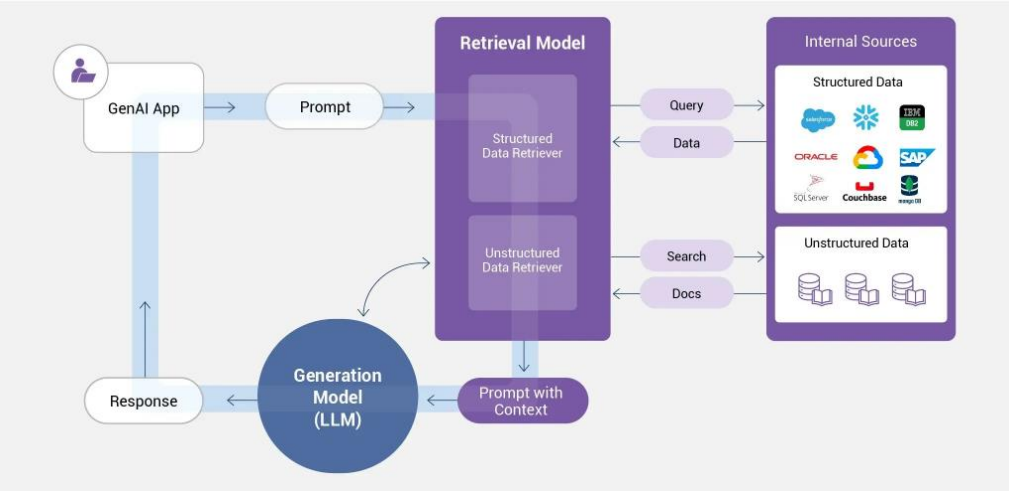
IA - ML

IA GEN

- RAG - La generación mejorada por recuperación usando base de conocimientos autorizada fuera de los orígenes de datos de entrenamiento
- LLM Gateway: https://www.tensorops.ai/post/llm-gateways-in-production-centralized-access-security-and-monitoring
- Almacenamiento de datos en vectores con pesos (Embeddings).
  - https://gustavo-espindola.medium.com/qu%C3%A9-son-los-embeddings-y-c%C3%B3mo-se-utilizan-en-la-inteligencia-artificial-con-python-45b751ed86a5
  - Extensión vectorial para PostgreSQL – pgvector / Almacenar los embeddings en PaaS de cloud.

IA ML – IA Generativa

- RAG mediante GKE: https://cloud.google.com/architecture/rag-capable-gen-ai-app-using-gke?hl=es-419
- RAG mediante Vertex AI: https://cloud.google.com/architecture/rag-capable-gen-ai-app-using-vertex-ai?hl=es-419
- Prompt tuning: https://www.k2view.com/blog/rag-prompt-engineering/#Grounding-LLMs-with-rag-prompt-engineering

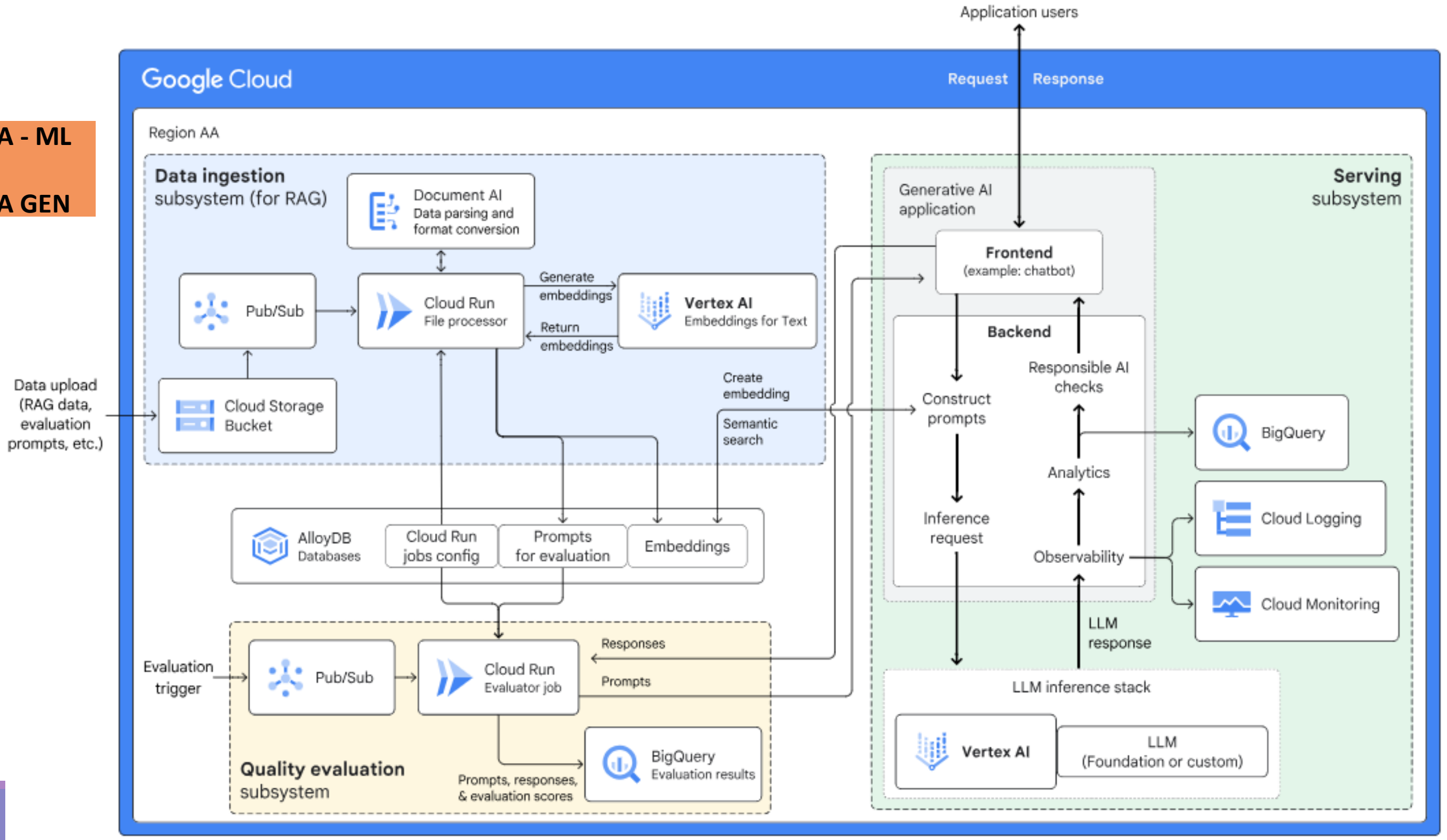


IA - ML

IA GEN

IA - ML

IA GEN


Application users
Google Cloud
Request
Response
Region AA
Data ingestion
subsystem (for RAG)
Document AI
Data parsing and
format conversion
Pub/Sub
Cloud Run
File processor
Generate
embeddings
Return
embeddings
Vertex AI
Embeddings for Text
Data upload
(RAG data,
evaluation
prompts, etc.)
Cloud Storage
Bucket
Create
embedding
Semantic
search
AlloyDB
Databases
Cloud Run
jobs config
Prompts
for evaluation
Embeddings
Evaluation
trigger
Pub/Sub
Cloud Run
Evaluator job
Responses
Prompts
Quality evaluation
subsystem
Prompts, responses,
& evaluation scores
BigQuery
Evaluation results
Generative AI
application
Serving
subsystem
Frontend
(example: chatbot)
Backend
Construct
prompts
Responsible AI
checks
Inference
request
Analytics
Observability
BigQuery
Cloud Logging
Cloud Monitoring
LLM
response
LLM inference stack
Vertex AI
LLM
(Foundation or custom)

IoT - Cosas conectadas

- Sensores de ciudad – Smart Sports Center - IoTMADLAB https://iotmadlab.es/documentos/
- Relación con 5G - https://www.madrid.es/UnidadesDescentralizadas/OficinaDigital/Nav_OfDigital/ficheros/20240315-III-FORO-5G.pdf
- Gestión + Ingesta de IoT hacia el mundo IT – Similar a la ingesta del data con las particularidades de IoT.
  - Azure IoThub: https://azure.microsoft.com/es-es/products/iot-hub
  - AWS IoT: https://aws.amazon.com/es/iot/
  - GCP IoT: https://cloud.google.com/architecture/connected-devices/iot-platform-product-architecture?hl=es-419

IOT

Seguridad en cloud

SEGURIDAD, IDENTIDAD, RED

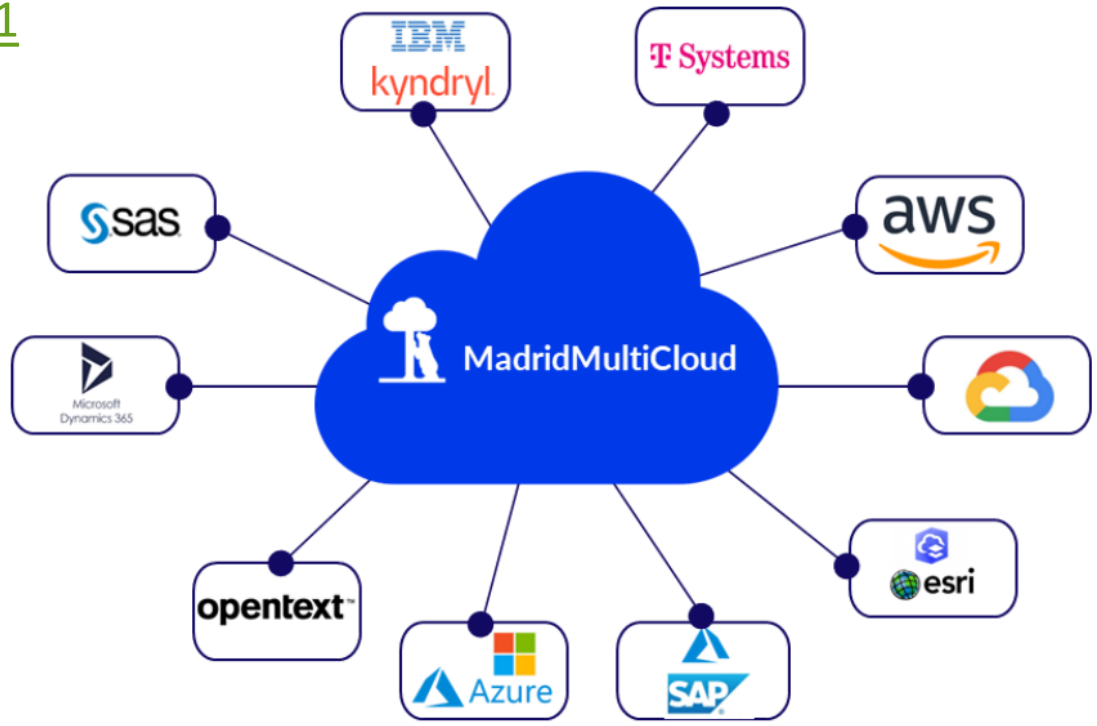
- Pocos cortafuegos (uno hacia Internet y otro en la landing zone hacia dentro).
- Protección de identidades y APIs (API Manager con gestión de apikeys + WAF de APIs).
- Cloud-Native Application Protection Platform (CNAPP)
  - Servicios SaaS y PaaS – no EDR.
  - Proteger la cadena de suministro DevSecOps y cadena de dependencias de librerías software.
  - Protección de contenedores y registro (Container Registry).
  - Segmentación en suscripciones o proyectos – no requieres cortafuegos.
- Cloud security posture management (CSPM). Visibilidad, monitorización y cumplimiento normativo.
- Zero Trust – Todo en Internet, 2FA, Autenticación máquina-máquina.
- CASB para acceso a servicios SaaS: https://www.zscaler.com/es/resources/security-terms-glossary/what-is-cloud-access-security-broker
- ZTNA – Seguridad de los puestos de usuario que transforma el modelo de VPN tradicional.

Contratación

- Contratación centralizada – NO permiten pago por uso de proveedores cloud.
  - SDA 24 - 24/2022 EQUIPOS DE COMUNICACIONES, SERVIDORES Y SISTEMAS DE ALMACENAMIENTO.
  - 25/2022 SUMINISTRO DE SOFTWARE DE SISTEMA, DESARROLLO Y APLICACIÓN (SDA 25/2022).
- Acuerdos Marco.
  - Acuerdo marco de servicios y suministros de nube de innovación para soportar la transformación digital de la Comunidad de Madrid (2 lotes).
- Contrato abierto.
  - Contrato mixto de suministros y servicios para la provisión de infraestructuras en nube pública destinada a la estrategia de transformación digital del Ayuntamiento de Madrid.
  - Madrid MultiCloud – varios hiperescalares.
  - Pago por uso.
  - Centro de excelencia cloud.

Material de consulta

- Madrid Talento – Oposiciones Ayuntamiento de Madrid. https://www.madrid.es/portales/munimadrid/es/Inicio/Educacion-y-empleo/Empleo/Oposiciones/Madrid-Talento/?vgnextfmt=default&vgnextchannel=e6ef82106d081810VgnVCM2000001f4a900aRCRD
- Madrid MultiCloud (Enlace al itinerario Madrid MultiCloud).
- Cloud Native Computing Foundation - https://landscape.cncf.io/



Muchas gracias

MIGUEL ÁNGEL RODRÍGUEZ RAMOS
SUBDIRECTOR GENERAL DE SISTEMAS Y TECNOLOGÍA
INFORMÁTICA DEL AYUNTAMIENTO DE MADRID