

ARQUITECTURA TÉCNICA

Migración a Google Cloud Platform

Plataforma Industrial Edge-First

Presentación Técnica para CTO, CIO y Arquitectos

Fecha: 2025-11-01 | Versión: 1.0

AGENDA TÉCNICA

ARQUITECTURA

1. Contexto Técnico Actual
2. Arquitectura Global Edge-First
3. Topología Kafka (Hub-and-Spoke)
4. Arquitectura de Red
5. Arquitectura de Datos (Medallion)

IMPLEMENTACIÓN

6. Stack Tecnológico Completo
7. Sizing y Dimensionamiento
8. DevSecOps y GitOps
9. Estrategia de Migración Técnica
10. Decisiones Críticas y Supuestos

Objetivo: Validar decisiones de arquitectura y obtener aprobación técnica del diseño

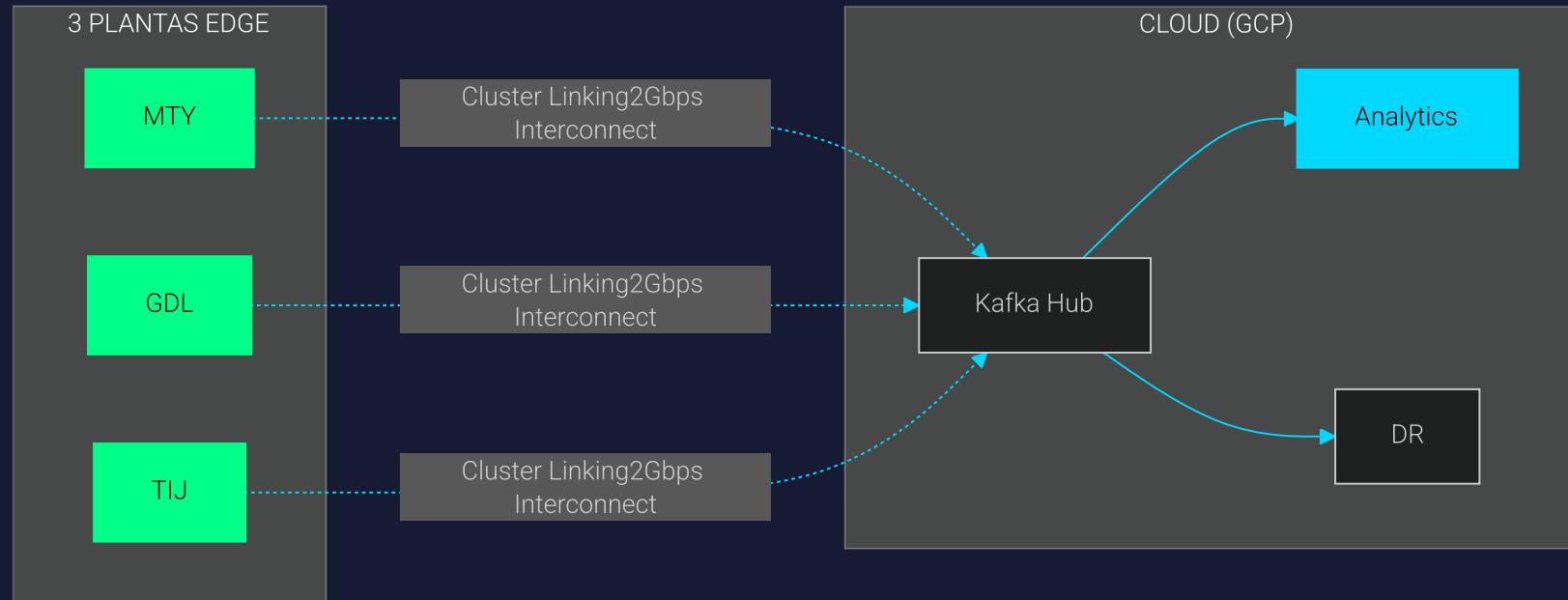
CONTEXTO TÉCNICO ACTUAL

INVENTARIO DE SISTEMAS

CATEGORÍA	CANTIDAD	ESTADO	CRITICIDAD
SQL Server 2008/2012	100	EOL	RPO/RTO=0
SQL Server 2019	210	SOPORTADO	Mixta
SCADA Legacy	40	ANTIGUO	RPO/RTO=0
SCADA Modernos	30	OK	Alta
Apps IIS/.NET	60	SOPORTADO	Media
Stored Procedures + .exe	200+	DEUDA TÉCNICA	Alta

Desafío Técnico Principal: 160 sistemas misión crítica (RPO/RTO=0) + Deuda técnica masiva (200+ stored procedures con .exe) + Infraestructura EOL

ARQUITECTURA GLOBAL: MODELO EDGE-FIRST



Cada Planta: GDC Edge + GKE + Kafka local • 100% Autónoma (7+ días offline) • RPO/RTO=0 local

Cloud: Kafka Hub (us-central1) + DR (us-west1) • Analítica multi-planta • BigQuery DWH

TOPOLOGÍA KAFKA: HUB-AND-SPOKE

CLUSTER ID	UBICACIÓN	PLATAFORMA	ROL	RF	RETENCIÓN
kafka-edge-mty	Monterrey (Edge)	CONFLUENT PLATFORM ON GKE EDGE	Spoke	3	7d
kafka-edge-gdl	Guadalajara (Edge)	CONFLUENT PLATFORM ON GKE EDGE	Spoke	3	7d
kafka-edge-tij	Tijuana (Edge)	CONFLUENT PLATFORM ON GKE EDGE	Spoke	3	7d
kafka-hub-central1	GCP us-central1	CONFLUENT CLOUD	Hub Primario	3 (multi-AZ)	30d hot + ∞ cold
kafka-dr-west1	GCP us-west1	CONFLUENT CLOUD	Hub DR	3 (multi-AZ)	30d hot + ∞ cold

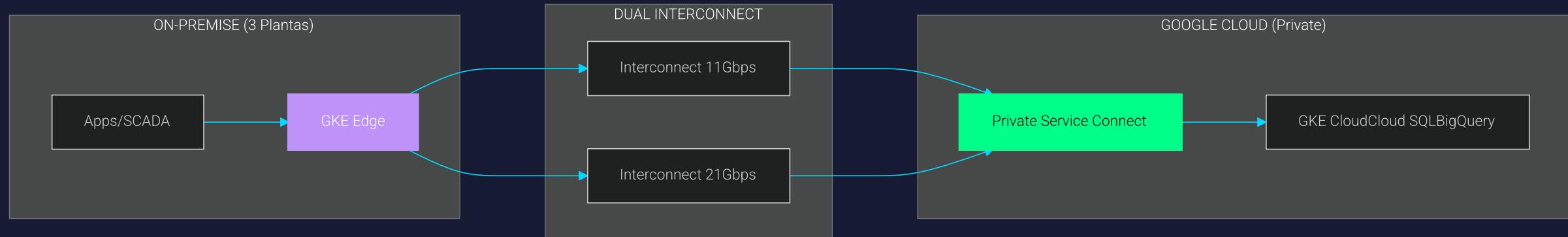
CLUSTER LINKING

- Replicación async edge → cloud
- Latencia: **<50ms** + geo ~35ms
- Exactly-once semantics

TIERED STORAGE

- Cloud: 30d hot + ∞ cold (GCS)
- Edge: 7d local buffer
- Ahorro: 50-70% vs hot-only

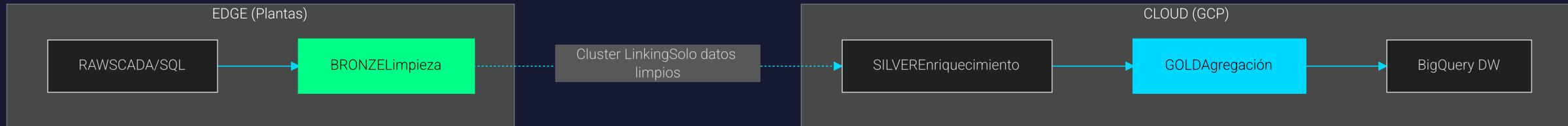
ARQUITECTURA DE RED: CONECTIVIDAD PRIVADA



CAPA	TECNOLOGÍA	PROPÓSITO	ESTADO
L3 - Conectividad	Dual Interconnect 2x1Gbps	Redundancia + throughput 50-150 Mbps/planta	REQ UPGRADE
L4 - Service Mesh	Private Service Connect (PSC)	Comunicación privada sin IPs públicas	NATIVO GCP
L7 - mTLS	Anthos Service Mesh (Istio)	Cifrado end-to-end, zero-trust	NATIVO GCP
Identity	Identity-Aware Proxy (IAP)	Acceso sin VPN tradicional	NATIVO GCP

Supuesto Crítico AP-3: Upgrade a Dual Interconnect 2x1Gbps requiere aprobación CFO/CIO. Costo: \$72K/año. Sin esto, replicación edge → cloud limitada.

ARQUITECTURA DE DATOS: MEDALLION DISTRIBUIDA



CAPA	UBICACIÓN	PROCESAMIENTO	BENEFICIO
RAW	Edge (GDC)	Ingesta SCADA/SQL vía Kafka Connect	Baja latencia, operación local
BRONZE	Edge (GDC)	Spark: Validación, limpieza, dedup	Reduce tráfico WAN 60-70%
SILVER	Cloud (GCP)	Spark: Join multi-planta, normalización	Analítica consolidada
GOLD	Cloud (GCP)	Spark: Agregaciones negocio, KPIs	BI/ML ready

Ventaja Clave: Procesar BRONZE en edge reduce tráfico Interconnect 60-70%. Solo datos limpios se envían a cloud.

STACK TECNOLÓGICO COMPLETO

EDGE (ON-PREMISE)

COMPUTE

GDC Edge - GKE local, operación autónoma

EVENTOS

Confluent Platform on K8s - Kafka + KSQL + Connect

PROCESAMIENTO

Dataproc on GKE - Spark capa BRONZE

STORAGE

Local SSD NVMe - 7d retención Kafka

GESTIÓN Y GOBIERNO

PLANO DE CONTROL

Anthos - Gestión unificada edge + cloud

GITOPS

Anthos Config Mgmt - Everything-as-Code

CLOUD (GCP)

COMPUTE

GKE Autopilot - Serverless K8s

EVENTOS

Confluent Cloud - Kafka managed, Tiered Storage

PROCESAMIENTO

Dataproc Serverless - Spark SILVER/GOLD

STORAGE/ANALYTICS

BigQuery + GCS - DW + Lakehouse

SEGURIDAD Y POLÍTICAS

POLÍTICAS

OPA - Validación pipeline + runtime

CI/CD

Harness - Deployment automation con OPA

SIZING Y DIMENSIONAMIENTO

COMPONENTE	NODOS	TIPO	vCPU	RAM	STORAGE
Compute	4-6	n2-standard-16	16	64GB	-
Control Plane	2	n2-standard-4	4	16GB	-
Storage (Kafka)	-	Local SSD	-	-	3-5 TB NVMe

Total por planta: 64-96 vCPU + 256-384GB RAM + 3-5TB SSD

CONFLUENT PLATFORM

- 3 Kafka brokers (RF=3)
- 2 KSQL servers
- Kafka Connect cluster

APPS INDUSTRIALES

- ~30 apps IIS containerizadas
- Ejecutables .exe legacy
- Microservicios nuevos

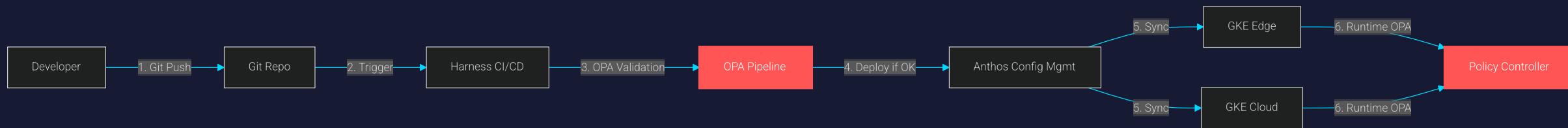
PROCESAMIENTO

- Dataproc (Spark BRONZE)
- Jobs ETL locales
- Validación/limpieza datos

Supuesto AP-6: Sizing 4-6 nodos requiere validación en PoC. Right-sizing post-migración puede ajustar ±30%.

DEVSECOPS: GITOPS CON OPA

FLUJO GITOPS COMPLETO



VALIDACIÓN DUAL OPA

FASE	HERRAMIENTA	POLÍTICAS VALIDADAS	ACCIÓN SI FALLA
Pipeline (CI/CD)	Harness + OPA	Etiquetas obligatorias (cost-center, env, owner), Imágenes permitidas, Límites recursos	Bloqueo deploy
Runtime (Cluster)	Anthos Policy Controller	No privileged pods, Network policies, Service mesh enforcement	Rechazo admisión

Everything-as-Code: Toda configuración (apps, infra, políticas) vive en Git. Cambios auditables, rollback automático, compliance garantizado.

ESTRATEGIA DE MIGRACIÓN TÉCNICA

ONDA	DURACIÓN	SISTEMAS	ESTRATEGIA TÉCNICA	GO/NO-GO
Onda 1 (30%)	Meses 1-6	100 SQL 2008/2012 EOL	CDC Debezium (<5% impacto) Migración a Cloud SQL	PoC Debezium OK
Onda 2 (60%)	Meses 7-12	90 SQL 2019 + 60 IIS	Containerización .NET (Docker + GKE) Refactor IIS a microservicios	10 apps IIS en prod OK
Onda 3 (10%)	Meses 13-18	120 SQL críticas + 40 SCADA	Cutover planificado (ventanas dominicales) Rollback <2h	100% Onda 1+2 estable

CHANGE DATA CAPTURE (CDC)

- **Debezium** para SQL Server
- Captura binlog → Kafka topic
- Migración sin downtime
- PoC crítico: validar <5% CPU/IO

CONTAINERIZACIÓN LEGACY

- **Windows Container** para .exe
- Docker + GKE Windows nodes
- API wrapper para stored procs
- Kafka event-driven orchestration

DECISIONES DE ARQUITECTURA CONSENSUADAS

1. RPO/RTO=0 INTERPRETACIÓN

RPO/RTO=0 = **operación local** (planta). DR negocio: RPO=segundos OK (Cluster Linking).

2. MEDALLION 4 CAPAS

BRONZE en edge (reduce tráfico WAN 60-70%). SILVER/GOLD en cloud (analítica multi-planta).

3. CONFLUENT CLOUD VS SELF-MANAGED

Cloud en GCP (hub/dr). Platform self-managed en Edge (autonomía). Cluster Linking conecta.

4. DUAL INTERCONNECT 2X1GBPS

Requisito indispensable para throughput 50-150 Mbps/planta + redundancia.

SUPUESTOS CRÍTICOS A VALIDAR (30 DÍAS)

TOP 8 SUPUESTOS DE RIESGO ALTO

ID	SUPUESTO	VALOR	IMPACTO SI INCORRECTO	VALIDAR CON
AP-1	GDC Edge disponible en México	Sí	CRÍTICO Arquitectura inviable sin GDC Edge	Google Account Team
AP-2	Confluent Platform en GKE Edge funcional	Sí	CRÍTICO Requiere validación en PoC	Confluent SA
AP-3	Dual Interconnect 2x1Gbps aprobado	\$72K/año	CRÍTICO Sin esto, replicación limitada	CFO, CIO
AP-6	Sizing GKE Edge: 4-6 nodos	16 vCPU/nodo	CRÍTICO Afecta CAPEX y performance	Google GKE Team (PoC)
AP-10	Cluster Linking latencia <50ms	<50ms	CRÍTICO Impacta RPO real edge → cloud	Confluent SA (PoC)
AP-13	Throughput edge → cloud 50-150 Mbps/planta	50-150 Mbps	CRÍTICO Diseño Interconnect depende de esto	Data Engineer (PoC)
AP-17	GKE Edge 100% offline-capable	7+ días	CRÍTICO Autonomía planta en riesgo	Google GDC Team (PoC)
AP-18	Kafka Connect para SCADA legacy	Disponible	CRÍTICO Ingesta SCADA inviable	Admin Legados (PoC)

ACCIÓN REQUERIDA: Validar estos 8 supuestos en próximos 30 días mediante PoC y confirmación con vendors (Google, Confluent).

PLAN DE IMPLEMENTACIÓN TÉCNICO

PRÓXIMOS 90 DÍAS - HITOS TÉCNICOS

DÍA	HITO TÉCNICO	RESPONSABLE	ENTREGABLE
7	Contactar Google GDC Edge Team	Arquitecto Cloud	Confirmación disponibilidad México + cronograma
20	Cotización GDC Edge hardware	Arquitecto Cloud	Cotización formal 3 plantas + pricing
20	Validar Confluent Cloud pricing	FinOps Lead	Pricing via GCP Marketplace + Cluster Linking
30	Diseño detallado de red (Interconnect)	Experto Redes	Topología física + VLAN + QoS config
45	PoC Debezium en SQL Server test	Data Engineer	Validación <5% CPU/IO impact + replicación OK
60	Despliegue Dual Interconnect	Experto Redes	2x1Gbps activo, latencia <10ms validada
75	Despliegue Anthos en proyectos GCP	DevSecOps	3 GKE clusters registrados en Anthos Fleet
90	Primera app IIS containerizada en prod	Legacy Systems Team	1 app .NET corriendo en GKE Edge

Criterio de Éxito (Día 90): PoC Debezium exitoso + Interconnect activo + Anthos desplegado + Primera app containerizada en producción.

PRÓXIMOS PASOS Y APROBACIONES

1. ✓ **Arquitectura:** Validar diseño Edge-First con GDC Edge + Confluent Kafka
2. ✓ **Stack Tecnológico:** GCP nativo (Anthos, GKE, Dataproc, BigQuery)
3. ✓ **Estrategia Migración:** 3 ondas, CDC Debezium, containerización
4. ⚠ **Upgrade Interconnect:** Dual 2x1Gbps (\$72K/año) - Requiere CFO/CIO

POCS REQUERIDOS (30D)

- Debezium CDC SQL Server (<5% impacto)
- Confluent Platform en GKE Edge
- Cluster Linking latencia edge → cloud
- GDC Edge autonomía offline 7+ días

CONFIRMACIONES VENDOR (30D)

- Google: GDC Edge disponibilidad MX
- Google: Pricing GDC Edge hardware
- Confluent: Pricing Cloud + Linking
- Google: Cronograma entrega GDC

Meta: Iniciar Onda 1 en 90 días con validaciones completadas

¿PREGUNTAS?

Discusión Técnica

Documentación Técnica:

Arquitectura Plataforma (arquitectura-plataforma.md)

Arquitectura Redes (arquitectura-redes.md)

Arquitectura Datos (arquitectura-datos.md)

DevSecOps y Gobierno (devsecops-gobierno.md)

Migración Legados (migracion-legados.md)

Decisiones Consensuadas (decisiones-consensuadas.md)