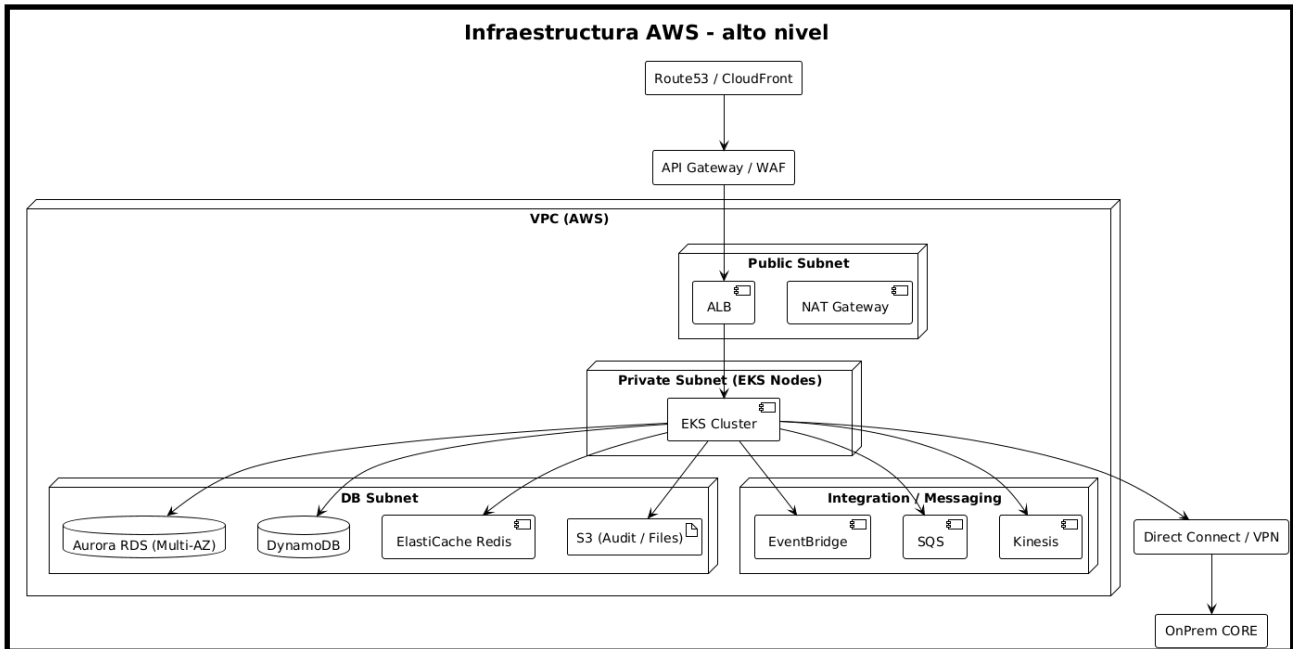


DESARROLLO DEL EJERCICIO

Desarrollado por: Luis Campoverde

- Diagrama de infraestructura.

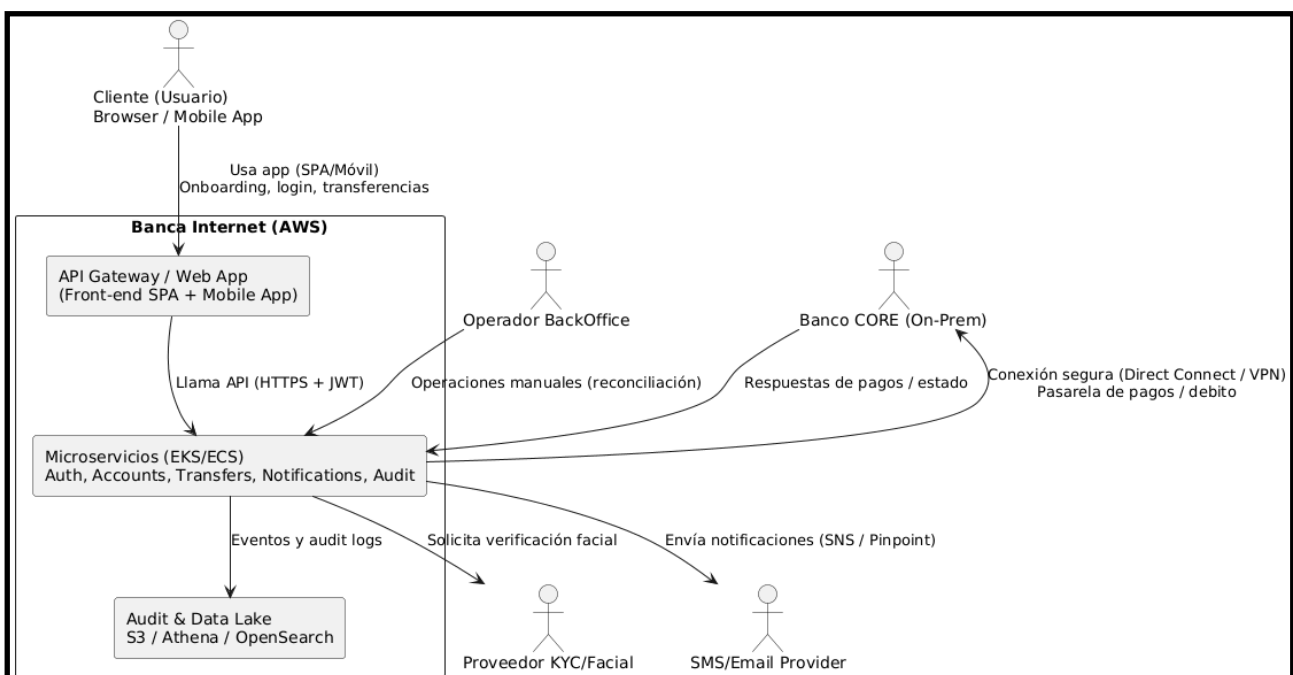
El siguiente diagrama describe como es el acceso desde internet y el Ali Gateway con conectividad y acceso a los diferentes servicios de BD y servicios adicionales.



- DIAGRAMAS:

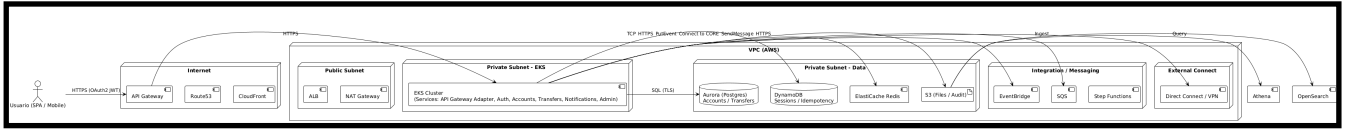
- Diagrama contexto.

El siguiente diagrama nos permite ver la fase de interacción entre el cliente y el sistema para realizar un ingreso de onboarding con autenticación y por medio de una API GATEWAY acceder a los servicios.



- **Diagrama de Contenedores.**

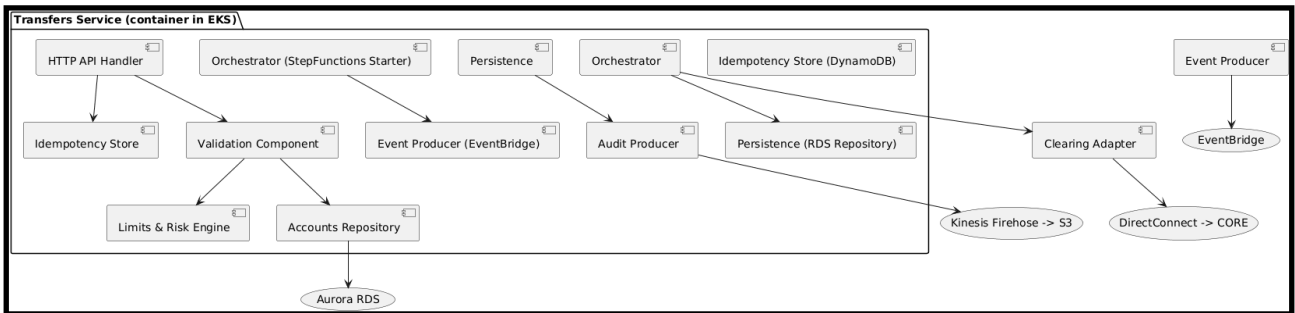
Para este diagrama se tiene un panorama de conectividad entre los servicios y la forma de acceder a cada uno de los componentes hacia el core y us notificaciones.



- Decisiones arquitectónicas (comparativas)

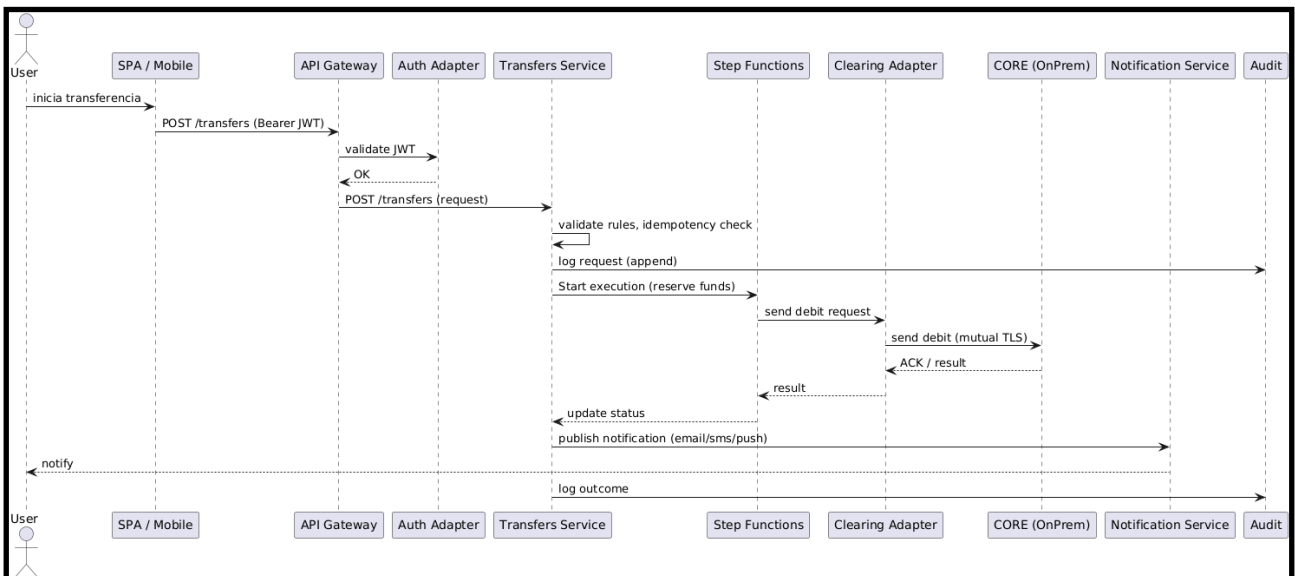
- EKS vs ECS/Fargate: EKS elegido por control y portabilidad; ECS/Fargate alternativa por reducción operativa.
- Aurora vs DynamoDB: Aurora para transaccionalidad fuerte; DynamoDB para key-value de alta concurrencia.
- EventBridge + Step Functions vs Kafka/MSK: EventBridge + Step Functions por integración AWS y simplicidad; MSK si necesidad de throughput masivo o retención stream compleja.
- Rekognition vs Onfido/Veriff: proveedor especializado elegido para KYC por certificación y anti-spoofing.
- KMS vs CloudHSM: KMS por la mayoría de casos; CloudHSM para claves no exportables o requisitos regulatorios.

- **Diagrama de componentes.**



En este diagrama de componentes se puede observar cada uno de los servicios que se va implementar en la solución y a su vez su interacción .

- **Diagrama de secuencia.**



El siguiente diagrama nos permite ver el flujo para el desarrollo e interacción entre los microservicios, la petición enviada y la respuesta necesaria, a su vez podemos ver la escritura de los logs.

A. API Gateway / Edge

- Responsabilidad: enrutamiento, validación JWT, throttling(mecanismo que limita el número de solicitudes (requests)) y autenticación.
- Tecnologías: Amazon API Gateway (HTTP APIs) para endpoints públicos; ALB interno.
- SLA: p95 < 200ms para routing; alta disponibilidad multi-AZ.
- Escalado: gestionado (API Gateway) + EKS Horizontal Pod Autoscaler (HPA).

B. Auth & Session Adapter

- Responsabilidad: delegación a IdP, validación de tokens, refresh, device binding.
- Persistencia: DynamoDB o ElastiCache para metadatos de sesión.
- Notas: usar IRSA (IAM Roles for Service Accounts) para permisos mínimos.

C. User Onboarding & Identity

- Responsabilidad: flujo KYC, verificación facial, firmado de consentimientos.
- Integración: proveedores KYC (Onfido/Veriff) o Amazon Rekognition (si no hay requisitos regulatorios fuertes).
- Datos: PII cifrado con KMS CMK. Guardar solo hashes cuando sea posible.

D. Accounts Service

- Responsabilidad: saldo, movimientos, consultas históricas (resumen y detalle).
- Persistencia: Aurora RDS (transaccional). Lecturas pesadas a replicas y caches (Redis).
- Modelo: usar CQRS; writes -> RDS, reads -> materialized views/replicas or read model in DynamoDB.

E. Transfers & Payments Orchestrator

- Responsabilidad: orquestación de transferencias (validación, reserva, debit core, reconciliation).
- Tecnologías: Step Functions para flujos stateful; EventBridge + SQS para eventos/colas.
- Persistencia: RDS + events persisted to S3 for audit.

F. Clearing Adapter / Switch

- Responsabilidad: conectividad con CORE y sistemas externos (ACH, SWIFT).
- Seguridad: mTLS, network restrictions, idempotency via DynamoDB.

G. Beneficiaries / Standing Orders

- Responsabilidad: CRUD beneficiarios, plantillas de pago programado.
- Persistencia: DynamoDB para lectura rápida y TTL, RDS si se requieren relaciones complejas.

H. Limits & Risk Engine

- Responsabilidad: reglas en tiempo real para límites, fraude y AML callouts.
- Integración: ML services as a microservice or external provider.
- SLA: alta disponibilidad, baja latencia (< 100ms lookups).

I. Notifications Service

- Responsabilidad: enviar email, SMS y push (Pinpoint/SES/SNS).
- Persistencia: log de envíos en S3 + estado en DynamoDB.

J. Audit & Compliance Service

- Responsabilidad: append-only audit logs; signing with KMS; query via Athena/OpenSearch.
- Pipeline: services -> Kinesis Firehose -> S3 (partitioned) -> Glue/Athena + OpenSearch for fast search.

K. Reporting & Analytics

- Responsabilidad: BI, queries históricas.

- Tecnologías: Redshift spectrum or Athena over S3; ETL via Glue.

L. Batch Processor / File Processor

- Responsabilidad: procesar cargas masivas (pagos por archivo).
- Tecnologías: AWS Batch or EKS Jobs; use S3 for file staging.

- **Estimación de costos mensuales (rango aproximado)**

La estimación es indicativa y depende del tráfico, almacenamiento y retención. Valores en USD / mes.

- EKS control plane + worker nodes (3 x m6i.large) : 3 x \$140 = \$420 (nodes) + EKS control plane ~\$0 (ajustar) -> estimate \$500 - \$1500
- RDS Aurora (db.r6g.large primary + 1 read replica) : \$800 - \$3000 (depende de size/IO)
- DynamoDB (sessions/idempotency): \$50 - \$500
- ElastiCache (redis small cluster): \$100 - \$800
- API Gateway (high throughput): \$200 - \$2000
- S3 + Kinesis Firehose + Athena (audit pipeline): \$50 - \$500
- OpenSearch (hot cluster): \$300 - \$2000
- Direct Connect (port + data transfer) or VPN: \$200 - \$1500
- SES / Pinpoint (email/sms): \$20 - \$500 (depends on volume)
- CloudWatch logs/metrics/traces: \$100 - \$1000
- Misc (ECR, NAT GW, LB, WAF, Backup): \$200 - \$2000

Rango total estimado: USD 2,000 — 12,000 / mes (para una instalación de tamaño medio).

- **Plan de pruebas operacionales y KPIs**

- Tests: carga (k6/JMeter), chaos (simulate AZ loss), DR runbooks, pen tests, SCA.
- KPIs: latency p95, availability, transfer success rate, MTTR, RTO/RPO.

- **Conclusiones y próximos pasos**

- Validar requisitos regulatorios y SLAs con negocio.
- Implementar POC mínimo (EKS cluster + API Gateway + Transfers service minimal) y test end-to-end.
- Iterar con pruebas de carga y ajustar sizing y costs.