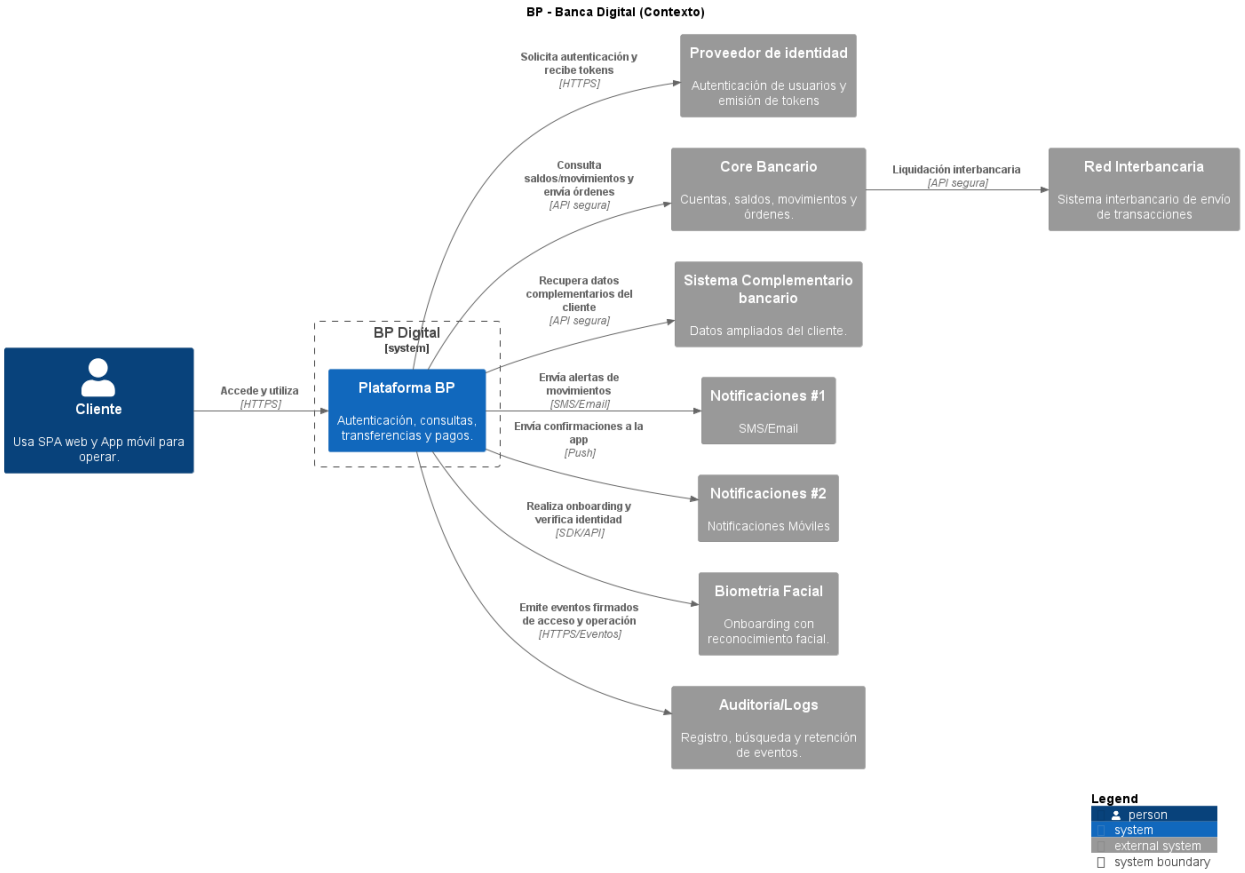
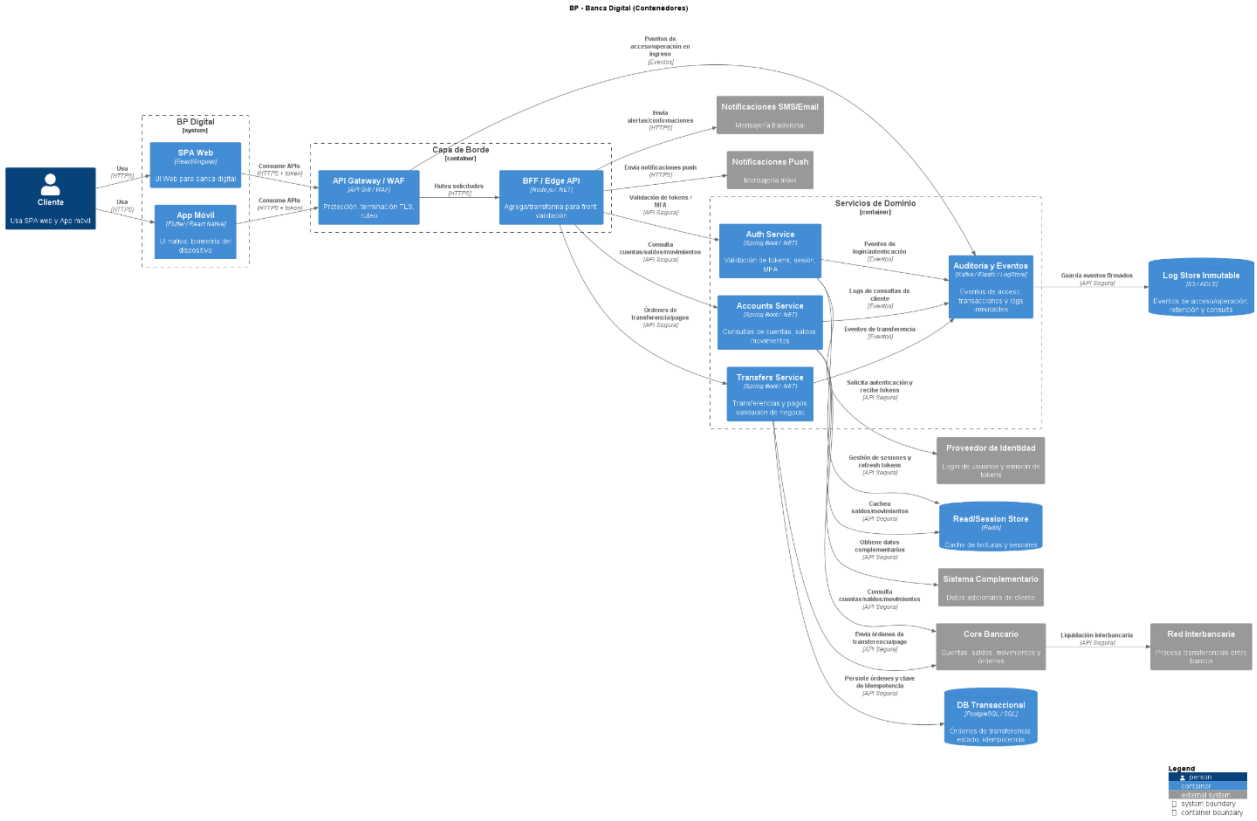
BP Digital

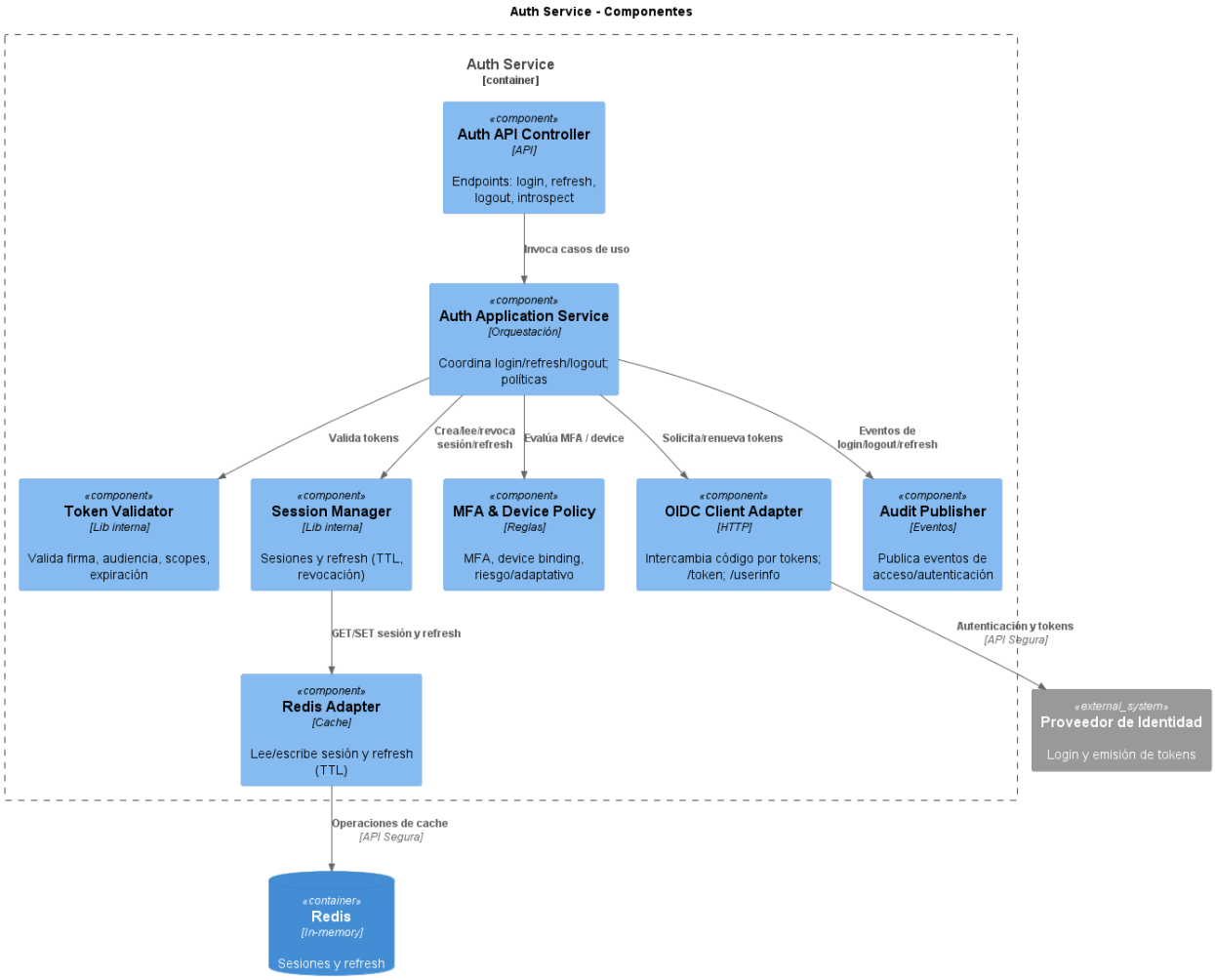
1. Diagrama De contexto



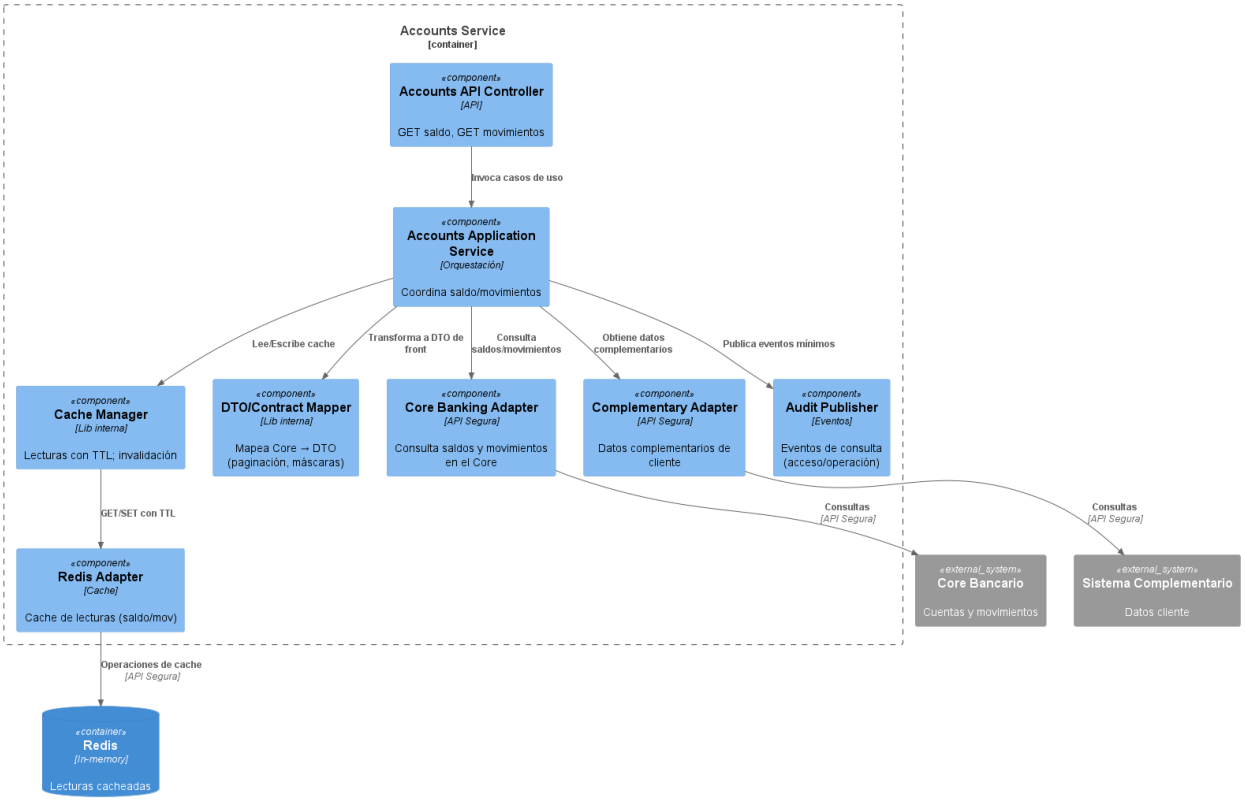
2. Diagrama De contenedores



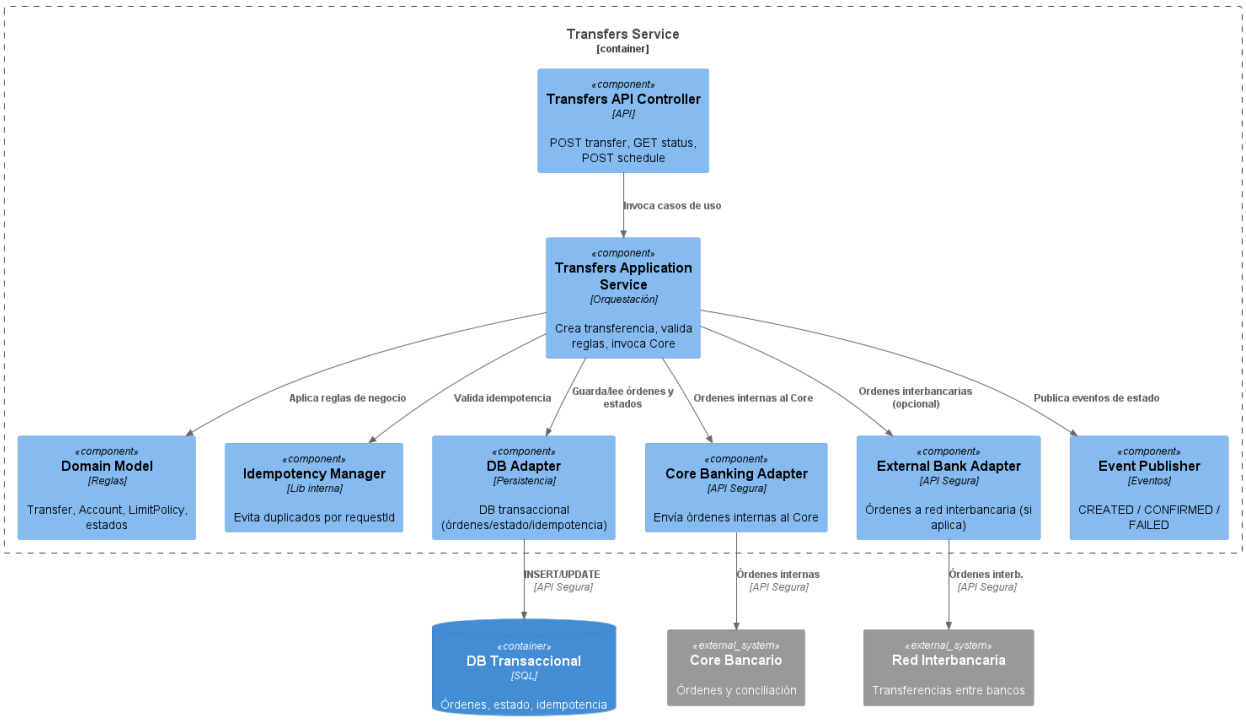
3. Diagramas de Componentes



Accounts Service - Componentes



Transfers Service - Componentes



4. Resumen de la Arquitectura

La plataforma BP Digital permite a los clientes del banco acceder mediante una SPA Web y una App Móvil.

El flujo pasa por una capa de borde (API Gateway + BFF), que protege, valida y enruta solicitudes hacia los servicios de dominio:

- Auth Service → autenticación de tokens, gestión de sesiones, MFA.
- Accounts Service → consultas de saldos y movimientos.
- Transfers Service → órdenes de transferencia y pagos, con validación de negocio e idempotencia.
- Auditoría y Eventos → almacén inmutable para accesos y transacciones.

Se integra con sistemas externos:

- Core Bancario (cuentas, saldos, órdenes).
- Proveedor de Identidad (IdP) (login y tokens).
- Sistema Complementario (datos de cliente).
- Notificaciones (SMS/Email, Push).
- Red Interbancaria (transferencias entre bancos).

Los datos se persisten en:

- Cache (Redis) para sesiones y lecturas rápidas.
- DB Transaccional (PostgreSQL/SQL) para transferencias e idempotencia.
- Log Store inmutable (S3/ADLS) para eventos de auditoría.

5. Requisitos No Funcionales

Alta Disponibilidad (HA)

- Servicios stateless desplegados en clústeres con autoescalado horizontal.
- Multi-AZ en base de datos y cache (Redis).
- API Gateway/WAF gestionados con capacidad de escalado automático.

Tolerancia a Fallos (FT)

- Uso de circuit breakers, timeouts y reintentos hacia Core y sistemas externos.

- Idempotencia en Transfers Service para evitar duplicados en reintentos.
- Eventos asincrónicos desacoplan auditoría y notificaciones del procesamiento principal.

Recuperación ante Desastres (DR)

- Definición de RPO ≤ 5 minutos y RTO ≤ 1 hora.
- Replicación de datos cross-region en DB y Log Store (Aurora Global / Azure Geo-Replication, S3/ADLS replicado).
- Backups automáticos con pruebas de restauración periódicas.
- Infraestructura definida en IaC (Terraform/Bicep/CloudFormation) para reconstrucción rápida.

Seguridad

- Perímetro: WAF, TLS, rate limiting, reglas OWASP.
- Identidad: OAuth2.1 / OIDC con IdP corporativo, MFA para usuarios.
- Datos: cifrado en tránsito (TLS) y en reposo (KMS/Key Vault).
- Secreto: gestión de credenciales en Secrets Manager / Key Vault.
- Auditoría inmutable: logs de accesos y transacciones con retención y protección contra borrado.
- Principio de mínimo privilegio en roles, accesos y segmentación de red.

6. Infraestructura en la Nube

Ejemplo en AWS

- Capa de borde: API Gateway + AWS WAF.
- Servicios de dominio: contenedores en EKS/ECS Fargate.
- Cache: ElastiCache (Redis).
- DB Transaccional: Aurora PostgreSQL (Multi-AZ).
- Log Store: S3 con Object Lock y ciclo de vida (Glacier).
- Eventos: MSK (Kafka) o Kinesis.

- IdP: AWS Cognito o IdP corporativo federado.

Ejemplo en Azure

- Capa de borde: Azure Front Door + WAF.
- Servicios de dominio: AKS o App Service.
- Cache: Azure Cache for Redis.
- DB Transaccional: Azure SQL Database o Flexible Server (PostgreSQL).
- Log Store: Azure Data Lake Storage (ADLS Gen2) con política inmutable.
- Eventos: Event Hubs o Kafka en AKS.
- IdP: Microsoft Entra ID (Azure AD).

7. Conclusiones

El diseño asegura que la plataforma BP Digital sea resiliente, segura y preparada para crecimiento.

- Los diagramas C4 describen las capas de contexto, contenedores y componentes.
- Este documento complementario describe cómo se cumplen los atributos de calidad exigidos: HA, FT, DR y seguridad, además de mapear los contenedores a infraestructura en la nube.