Documento de Arquitectura para Sistema de Banca por Internet BP

Versión 1.0 | Marzo 2025

Contenido

Introducción al Problema

En un mundo donde la tecnología evoluciona a un ritmo acelerado, las instituciones financieras deben adaptarse continuamente para ofrecer soluciones innovadoras y eficientes a sus clientes. El auge de la transformación digital ha cambiado las expectativas de los usuarios, quienes buscan acceder a servicios bancarios de manera rápida, segura y conveniente desde cualquier lugar.

Conscientes de este desafío, la **Financiera BP** ha decidido realizar un cambio en el ecosistema de su producto Banca Personas misma que consiste en una aplicación móvil (Android e IOs) y portal web transaccional, que no solo optimice la experiencia del usuario, sino que también garantice altos estándares de seguridad, escalabilidad y rendimiento. La visión la **Financiera BP** es ofrecer una plataforma moderna y flexible, capaz de integrar nuevas tecnologías y adaptarse a las demandas del mercado, manteniendo siempre el compromiso de brindar un servicio confiable y de calidad.

El presente documento describe la arquitectura de software diseñada para este ecosistema destacando los principios clave que guiarán su desarrollo, la seguridad desde el diseño, la integración con sistemas existentes y la capacidad de escalar a futuro. A través de esta solución, la **Financiera BP** reafirma su compromiso con la innovación, proporcionando una experiencia bancaria digital de primer nivel para sus clientes.

2. Planteamiento del Problema

2.1. Consideraciones

Basado en la descripción del ejercicio se asume que el planteamiento se lo aplica para un ecosistema de Banca Personas con las siguientes consideraciones:

- Consultar el histórico de sus movimientos.
- El usuario podrá realizar transferencias propias (misma entidad)
- El usuario podrá realizar transferencias interbancarias SPI de Banco Central del Ecuador y Pago Directo de Banred

2.1 Requisitos Clave

Categoría	Detalle
Funcionales	Consulta de saldos, transferencias interbancarias, historial de movimientos, notificaciones en tiempo real
No Funcionales	Latencia <500ms, uptime 99.96%, encriptación datos sensibles, auditoría trazable
Regulatorios	Cumplimiento de Circular SUIF 2023-007 (Superintendencia de Bancos de Ecuador), Ley Orgánica de Protección de Datos Personales SSEPS: RESOLUCIÓN Nro. SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-009 - NORMA DE CONTROL DE SEGURIDADES EN EL USO DE CANALES ELECTRÓNICOS PARA LAS ENTIDADES FINANCIERAS CONTROLADAS POR LA SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA
Transaccionales	ISO 22002 Usado para el esquema de consulta, pago y reverso de transacciones.

2.2 Alcance

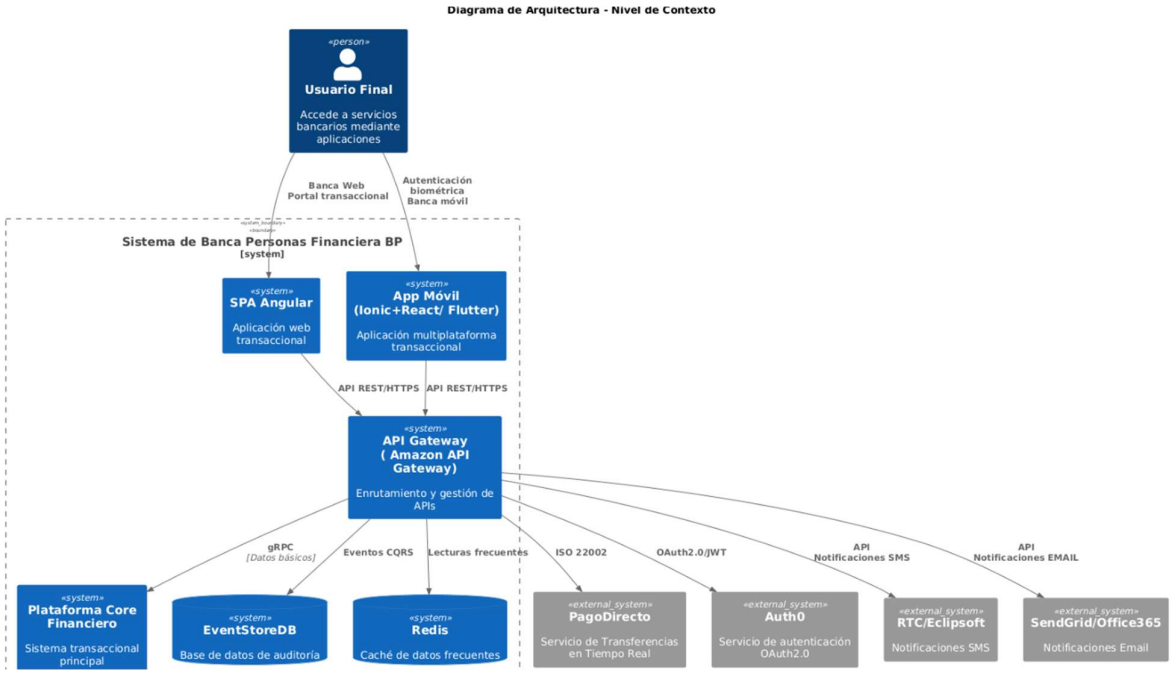
- **Incluye**: Desarrollo frontend/backend, integración con proveedores biométricos, diseño de flujos antifraude.

- **Excluye**: Migración de datos históricos, desarrollo del Core bancario existente.

3. Desarrollo del Proyecto

3.1 Arquitectura Técnica

3.1.1 Diagrama C4 Nivel Contexto



3.1.2 Stack Tecnológico

Aplicaciones Frontend

- **SPA (Angular)**: Desarrollo en Angular por su capacidad para construir aplicaciones empresariales complejas con inyección de dependencias y gestión de estado robusta.
- **Aplicación Móvil (Flutter)**: Flutter es una excelente opción para aplicaciones financieras gracias a su capacidad de ofrecer una única base de código para iOS y Android. Contamos con su alto rendimiento y que garantiza una experiencia fluida y rápida, esencial en entornos financieros.

Capa de Integración

- **API Gateway (Amazon Api Gateway)**: Enruta solicitudes a microservicios, autenticación JWT y transformación de protocolos. Se selecciona este proveedor ya que se busca un ecosistema de nube publica, escalabilidad horizontal, monitoreo y seguridad.
- **Servicios Principales**:
    - **Consulta de Datos Básicos**: Obtiene información de la Plataforma Core.
    - **Consulta de Movimientos**: Combina datos del Core y el Sistema de Detalle.
    - **Transferencias**: Coordina transacciones interbancarias mediante APIs Rest/XML estandarizadas por la ISO 20022 en el caso de PagoDirecto de Banred.
    - **Notificaciones**: Publica eventos a múltiples canales SMS (Eclipsoft) y correo electrónico Office365.

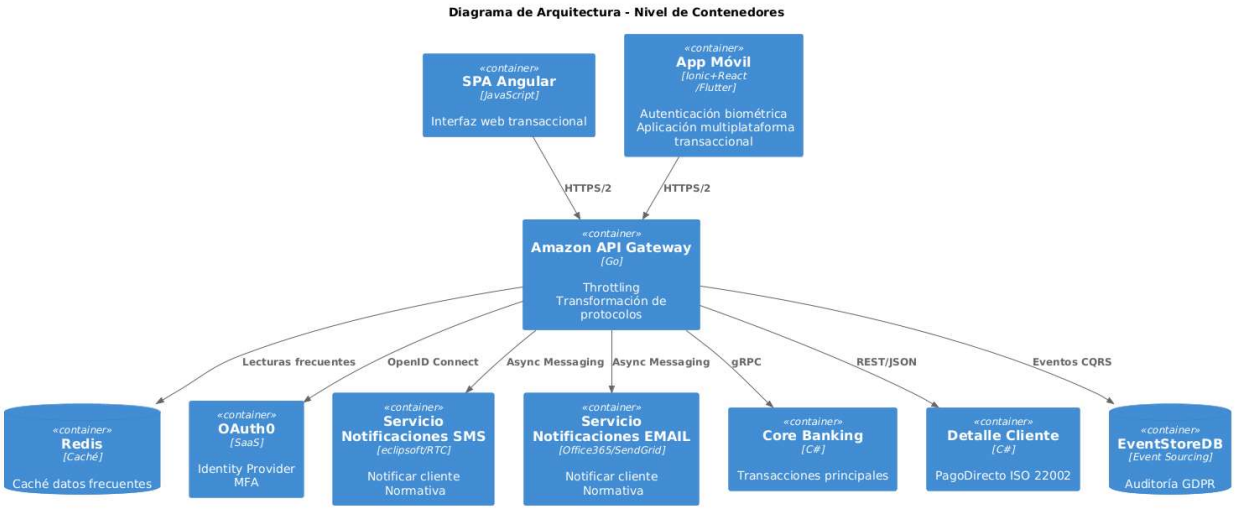
Autenticación y Autorización

- **OAuth0 como Identity Provider**: Implementa el flujo **Authorization Code with PKCE** para aplicaciones móviles, asegurando protección contra ataques MITM. Para el onboarding con reconocimiento facial, Auth0 integra módulos de biometrics mediante WebAuthn o SDKs específicos.

Persistencia y Auditoría

- **Base de Datos Transaccional (Amazon Aurora)**: Almacena datos críticos con replicación Multi-AZ y backups automáticos.
- **Base de Auditoría (EventStoreDB)**: Implementa el patrón **Event Sourcing** para registrar cada acción como un evento inmutable, facilitando trazabilidad y cumplimiento de regulaciones. Esto es una recomendación ya que los eventos de auditoria se pueden almacenar directamente en la base de datos del Core Financiero.
- **Caché (Redis)**: Aplica el patrón **Cache-Aside** para clientes frecuentes, reduciendo latencia en consultas recurrentes.

Capa	Tecnologías
Frontend	(SPA) Angular (Móvil), Flutter
Backend	.NET 8 (Core Banking) ó NodeJS Api Gatewway
Seguridad	OAuth2.0 (MFA)
Infraestructura	AWS EC2 (Auto Scaling), RDS Aurora DB (Auditoria), Redis (Cache) VPN – Site to Site Banred



3.2 Módulos Principales

3.2.1 Autenticación Biométrica

Módulo de Autenticación

- **Biometric Engine**: Componente encargado de validar huellas dactilares y rostros mediante algoritmos de matching (ej. FaceNet). Se integra con **Android KeyStore** y **iOS Secure Enclave** para almacenar claves privadas
- **MFA Authentication**: Evalúa el contexto de acceso (ubicación, dispositivo) para exigir autenticación multifactor (MFA) en casos anómalos, usando reglas configuradas en Auth0.

3.2.2 Transacciones y Servicio de Transferencias

- **Orchestrador de Transacciones**: Coordina los pasos para ejecutar una transferencia:
    - Verificación de fondos (consulta al Core).
    - Enviar SMS/Mail con OTP para validación de transacciones
    - Ejecución de transferencias interbancarias (ISO 20022) para Banred.
    - Actualización de saldos y generación de comprobantes.
- **Compensación (Saga Pattern)**: Si falla un paso, ejecuta transacciones compensatorias para revertir cambios, garantizando consistencia eventual.

3.2.3 Sistema de Notificaciones

- **Priority Queue (RabbitMQ)**: Clasifica notificaciones por urgencia o prioridad.
- **Fallback Channel Manager**: Si un proveedor falla (ej. Eclipsoft /Office365no responde), redirige

4. Consideraciones Normativas de Ecuador

4.1 Leyes Aplicables

Normativa	Impacto en la Arquitectura
LOPDP (Ley Orgánica de Protección de Datos Personales)	- Cifrado de datos en tránsito (TLS 1.3) y reposo (AES-256) - Consentimiento explícito para uso biométrico
Circular SUIF 2023-007	- Doble factor de autenticación para transacciones - Registro de IP y geolocalización en auditorías - Trazabilidad para las transacciones a través de canales electrónicos.

4.2 Protección de Datos

- **GDPR/RGPD**: Encriptación AES-256 de datos personales en tránsito (TLS 1.3) y reposo (AWS KMS). Derecho al olvido implementado mediante borrado lógico en EventStoreDB

4.3 Seguridad Operacional

- **Pentesting Automatizado**: Escaneo continuo con OWASP ZAP y SonarQube para identificar vulnerabilidades.

5. Infraestructura en AWS

5.1 Alta Disponibilidad

- **Regiones Multi-AWS**: Despliegue en us-east-1 y us-west-2 con Amazon Route 53 para balanceo geográfico.

5.2 Recuperación ante Desastres

- **Backups Multi-Región**: Snapshots diarios de RDS y S3 replicados.
- **Conmutación Automática**: AWS CloudFormation templates para recrear infraestructura crítica en menos de 15 minutos RTO.