Arquitectura del Sistema de Banca por Internet BP

Tabla de contenido

1. Introducción

Se describe la arquitectura para banca por Internet de BP, diseñada como una solución cloud-native robusta y escalable basada en Microsoft Azure. La arquitectura implementa principios modernos de microservicios, Clean Architecture, CQRS y patrones de alta disponibilidad para proporcionar servicios bancarios digitales seguros y eficientes. El sistema está diseñado para cumplir con las regulaciones bancarias y estándares internacionales de seguridad financiera. La solución integra capacidades avanzadas de reconocimiento facial para onboarding digital, sistemas de notificación multicanal obligatorios, y mecanismos de auditoría inmutable que garantizan el cumplimiento normativo. El enfoque arquitectónico prioriza la experiencia del usuario sin comprometer la seguridad.

1.1 Objetivos del Sistema

- Consulta de movimientos históricos y saldos en tiempo real
- Transferencias entre cuentas propias e interbancarias
- Pagos de servicios y obligaciones
- Onboarding digital con verificación biométrica y prueba de vida
- Notificaciones obligatorias por múltiples canales
- Auditoría completa y trazabilidad de transacciones

1.2 Principios Arquitectónicos Fundamentales

- **Clean Architecture:** Implementación de separación clara de responsabilidades organizadas en capas concéntricas donde las dependencias apuntan hacia el núcleo, manteniendo la lógica de negocio completamente independiente de frameworks externos y tecnologías específicas.
- **Microservicios:** Descomposición funcional del sistema en servicios independientes que pueden desarrollarse, desplegarse y escalarse de forma completamente autónoma según las necesidades específicas de cada dominio de negocio.
- **CQRS (Command Query Responsibility Segregation):** Separación arquitectónica completa entre operaciones de escritura (commands) y lectura (queries) para optimizar rendimiento y escalabilidad según patrones de uso específicos.
- **Event Sourcing:** Almacenamiento de todos los cambios del sistema como secuencia ordenada de eventos inmutables que proporcionan trazabilidad completa y capacidad de reconstrucción del estado en cualquier momento histórico.

2. Análisis de Requerimientos

2.1 Requerimientos Funcionales Críticos

Requerimiento	Descripción	Prioridad	Impacto Arquitectónico
Consulta de Movimientos	Acceso histórico con filtros avanzados	Alta	CQRS con optimización de lectura
Transferencias Interbancarias	Procesamiento seguro con ISO 20022	Alta	Saga Pattern para transacciones distribuidas
Autenticación OAuth2.0	Flujo PKCE para aplicaciones públicas	Alta	Azure AD B2C con custom policies
Onboarding Biométrico	Reconocimiento facial con prueba de vida	Alta	Integración con Azure Cognitive Services
Notificaciones Obligatorias	Mínimo 2 canales diferentes	Alta	Orquestador con Azure Communication Services
Auditoría Completa	Registro inmutable de acciones	Alta	Event Sourcing con PostgreSQL

2.2 Requerimientos No Funcionales Detallados

Seguridad y Compliance:

- **Estándares**: Cumplimiento completo PCI DSS, ISO 27001
- **Encryption**: TLS 1.3 para datos en tránsito, AES-256 para datos en reposo.
- **Regulaciones Ecuador**: Ley Orgánica de Protección de Datos , normativas Superintendencia de Bancos.
- **Key Vaults:** Para almacenar datos críticos como contraseñas, claves de API y cadenas de conexión.

3. Decisiones Arquitectónicas Fundamentales

3.1 Stack Tecnológico Principal

Backend Microservicios: .NET Core 8

- Performance excepcional con AOT (Ahead-of-Time) compilation que reduce tiempo de startup en 70% y consumo de memoria, crítico para auto-scaling rápido en contenedores.
- Integración nativa completa con ecosistema Azure que simplifica observabilidad, deployment y gestión de secretos.
- Soporte empresarial robusto de Microsoft con roadmap.
- Ecosistema maduro con librerías especializadas.

Frontend Web: Angular 17 con PWA

- Framework empresarial con arquitectura estructurada que facilita desarrollo por equipos grandes, garantizando mantenibilidad a largo plazo.
- Integración con Azure AD B2C mediante MSAL Angular que simplifica implementación OAuth2.0/OIDC sin dependencias adicionales.
- Progressive Web App, TypeScript nativo para la implementación de principios SOLID.

Aplicación Móvil: Xamarin.Forms/MAUI

- Desarrollo native multiplataforma, código compartido entre iOS/Android manteniendo performance nativo para operaciones biométricas.
- Cohesión tecnológica completa con backend .NET que permite reutilización directa de DTOs, validaciones y lógica de negocio.
- Acceso nativo a APIs biométricas del dispositivo (Touch ID, Face ID, fingerprint) sin wrappers de terceros que comprometan seguridad.
- Capacidades offline robustas con SQLite local para consultas críticas durante conectividad intermitente.

3.2 Plataforma Cloud: Microsoft Azure

- Ecosistema financiero especializado con servicios PaaS diseñados específicamente para instituciones bancarias, incluyendo Azure SQL con encriptación, Key Vaults y Azure Security Center para PCI DSS y regulaciones financieras.
- Cumplimiento regulatorio nativo con certificaciones SOC 2 Type II, ISO 27001, PCI DSS Level 1.
- Capacidades avanzadas de optimización de costos con Instancias Reservadas, computación Spot para cargas de trabajo no-críticas y autoescalado inteligente que reduce los costos operativos hasta un 60% en comparación con la infraestructura tradicional.

3.3 Arquitectura de Datos para Banca

Microsoft SQL Server (Azure SQL Database Managed Instance)

- Capacidades avanzadas de encriptación específicamente diseñadas para datos financieros: Transparent Data Encryption (TDE), Always Encrypted para columnas sensibles, y Dynamic Data Masking.
- Consistencia ACID robusta con niveles de aislamiento configurables que garantizan la consistencia para transacciones financieras críticas y prevent race conditions.

Azure Database for PostgreSQL (Flexible Server)

- Soporte JSONB nativo que permite almacenar eventos de auditoría con estructura flexible manteniendo capacidades de consulta SQL.
- Write-Ahead Logging (WAL) y streaming replication proporcionan durabilidad superior crítica para audit logs que deben ser inmutables.
- Extensions especializadas como pg_audit para automatic audit logging, data queries útiles en estructuras organizacionales bancarias.

Estrategia de Cache:

- Se usa MemoryCache en la aplicación para datos de sesión y configuraciones que requieren una latencia ultra-baja sin sobrecarga de red.
- Se usa Azure Cache for Redis para los datos que se comparten entre múltiples instancias de servicios, como los límites de transacciones y las preferencias de los usuarios.

4. Diagrama de Contexto (C4 Nivel 1)

4.1 Características del Diagrama de Contexto

El Diagrama de Contexto diseñado para stakeholders ejecutivos y de negocio. El diagrama identifica los actores humanos que interactúan con el sistema, sistemas externos críticos para la operación, y las relaciones de comunicación principales con descripción de los protocolos utilizados. El diagrama incluye sistemas de notificación obligatorios para cumplimiento normativo, integraciones biométricas para onboarding digital, y conexiones con la infraestructura bancaria nacional e internacional.

Actores Principales del Sistema:

- **Cliente BP**: Usuario final del sistema. Utiliza tanto aplicaciones web como móviles para acceder a servicios financieros, consultar movimientos históricos, realizar transferencias y gestionar sus finanzas personales.
- **Administrador BP**: Personal especializado interno del banco responsable de supervisar operaciones del sistema, configurar parámetros de negocio como límites de transacciones y tarifas. Requiere interfaces administrativas especializadas.

Sistemas Críticos del Ecosistema:

- **Sistema Banca Internet BP**: Plataforma digital central que constituye el núcleo de la transformación digital bancaria, proporcionando servicios financieros modernos 24/7 a través de arquitectura cloud-native escalable. Implementa microservicios especializados para cada dominio de negocio bancario manteniendo alta disponibilidad y performance bajo demanda variable.
- **Azure Active Directory B2C:** Servicio de identidad empresarial que maneja authentication y authorization de manera segura para millones de usuarios, implementando estándares OAuth2.0/OIDC con capacidades de MFA adaptativo.
- **Plataforma Core Bancaria**: Sistema que mantiene registros oficiales de cuentas, productos bancarios, movimientos y balances. Representa la fuente de verdad para información financiera crítica y debe ser integrado mediante APIs robustas que garanticen consistencia y integridad de datos.
- **Red Interbancaria:** Infraestructura nacional que facilita transferencias entre diferentes instituciones financieras utilizando protocolos estandarizados como ISO 20022 y SWIFT.

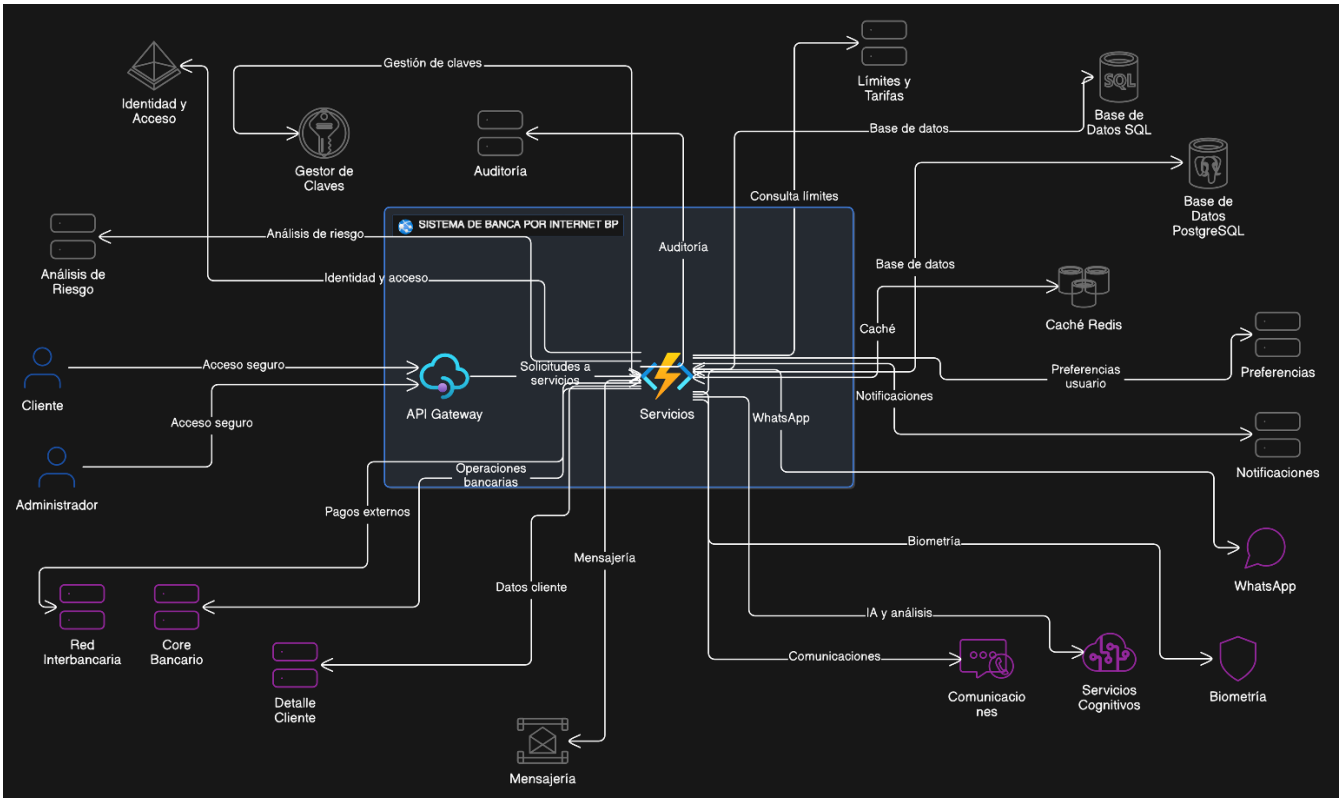

Ilustración 1. Diagrama de contexto

5. Diagrama de Contenedores (C4 Nivel 2)

5.1 Características del Diagrama de Contenedores

Aplicaciones Frontend:

- Aplicación Web SPA: Angular 17 con Progressive Web App y OAuth2.0
- Aplicación Móvil: Xamarin.Forms multiplataforma para iOS/Android
- Portal Administrativo: Interface administrativa

Servicios Microservicios:

- Servicio de Autenticación: OAuth2.0, JWT tokens y integración biométrica
- Servicio de Gestión de Usuarios: CRUD con patrón Cache-Aside
- Servicio de Cuentas: Consultas optimizadas con CQRS
- Servicio de Transferencias: Procesamiento con Saga Pattern

Bases de Datos:

- SQL Server Database: Base de datos relacional principal
- Azure Database for PostgreSQL: Especializada en auditoría
- Azure API Management: Gateway de APIs

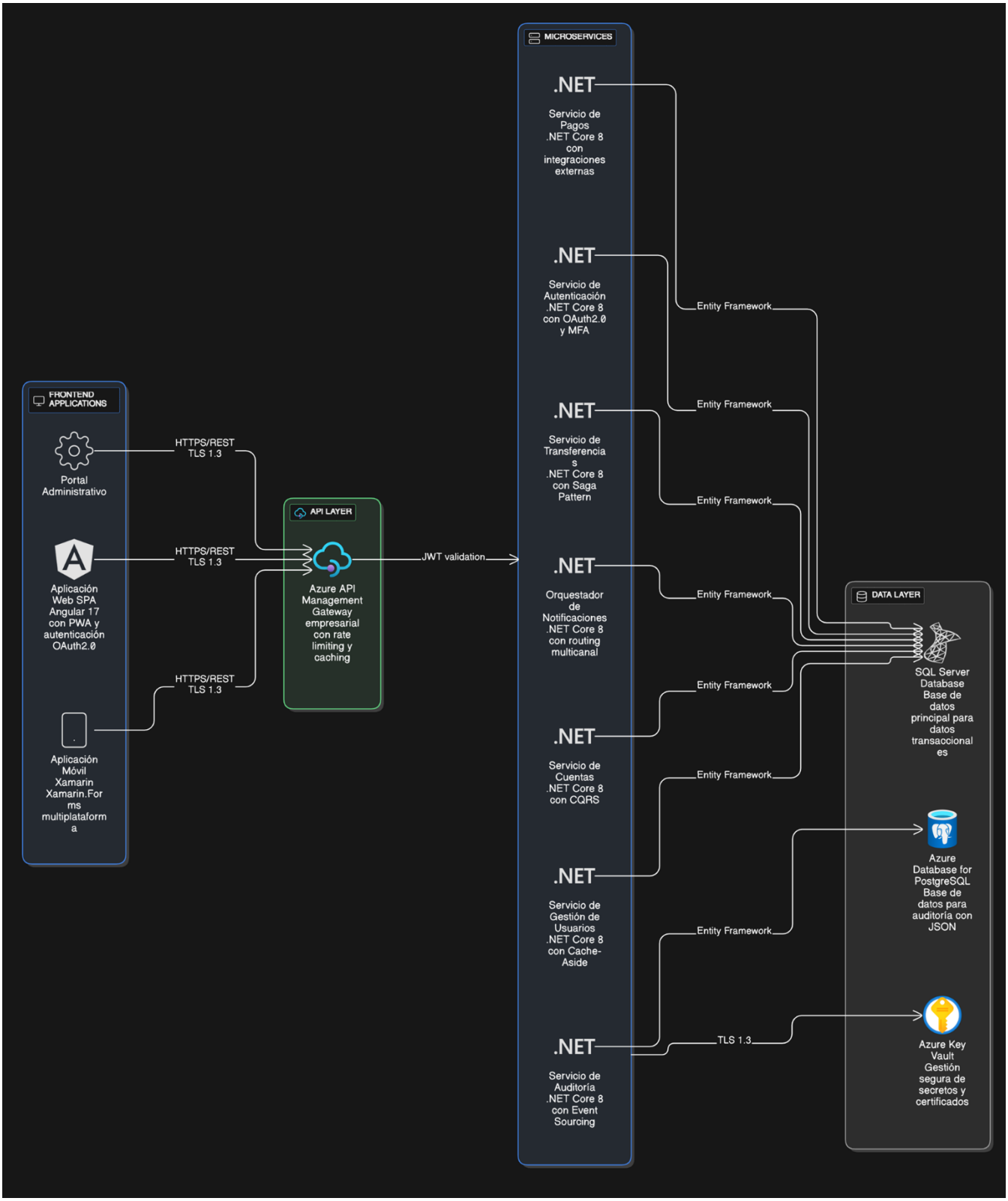

Ilustración 2. Diagrama de Contenedores

6. Diagrama de Componentes (C4 Nivel 3)

6.1 Análisis Detallado del Servicio de Transferencias (Componente Crítico)

El Servicio de Transferencias representa el componente más crítico y complejo del sistema, responsable por el procesamiento de transacciones financieras que involucran múltiples sistemas externos, validación compleja, detección de fraude, y cumplimiento de regulaciones. Este servicio implementa el Saga Pattern para gestionar transacciones distribuidas, asegurando la consistencia eventual mientras provee capacidades de reversión (rollback) cuando las transacciones fallan en cualquier paso del proceso. El componente mantiene un mapeo de estados en cada paso del ciclo de vida de la transacción, desde la iniciación hasta el asentamiento final, con la capacidad de recuperarse de cualquier punto de fallo.

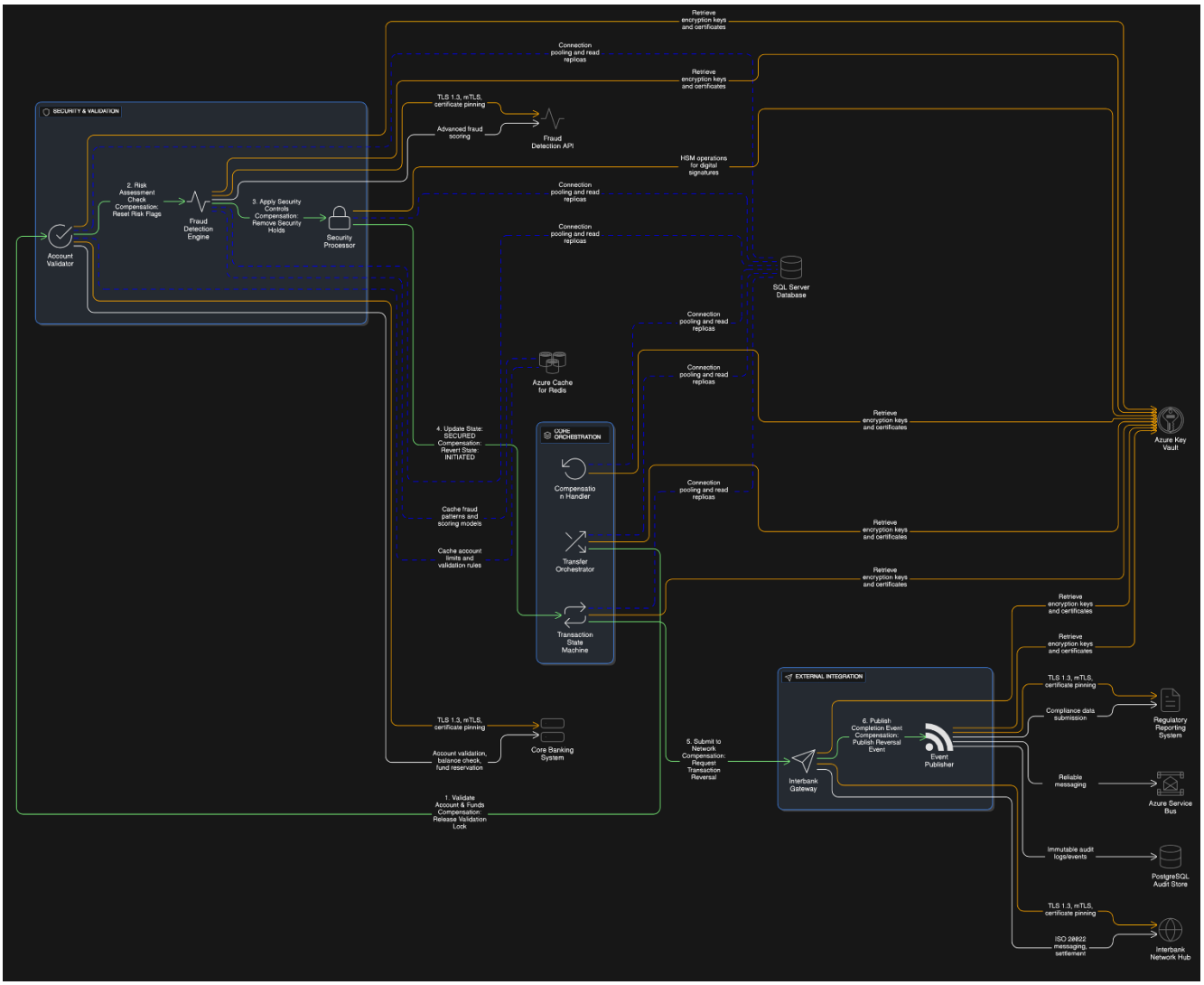

Ilustración 3. Diagrama de Componentes

7. Arquitectura de Autenticación y Autorización

7.1 Implementación OAuth 2.0 con PKCE

La autenticación se basa en **OAuth 2.0 Authorization Code flow** mejorado con **PKCE**, ideal para **SPAs** y **mobile apps** que no pueden almacenar secretos de cliente de forma segura. El sistema gestiona el ciclo de vida completo del **token** para mitigar vulnerabilidades y prevenir daños financieros y de reputación.

- **PKCE** elimina los ataques de interceptación de código, una preocupación crítica en aplicaciones bancarias.
- Cumplimiento con OAuth 2.0 Security Best Current Practice (RFC 8252), un estándar de la industria para datos sensibles.

7.2 Autenticación de Múltiples Factores Adaptativa (MFA)

El sistema usa **MFA** adaptativa, ajustando los requisitos de autenticación según la evaluación de riesgos en tiempo real. Esto equilibra seguridad y experiencia de usuario. La evaluación considera factores como la confianza del dispositivo, ubicación y biometría conductual.

SMS/Email OTP con Azure Communication Services:

- Proporciona garantías de entrega a nivel empresarial, vitales para el cumplimiento normativo.
- Gestión de plantillas que asegura mensajes consistentes y multilingües.
- Seguimiento de entrega para evidencia de auditoría y resolución de disputas.
- Mecanismos de fallback que garantizan la entrega incluso durante fallos.

Notificaciones Push con Aprobación Biométrica:

- Notificaciones enriquecidas proveen contexto detallado para una aprobación informada.
- La confirmación biométrica en el dispositivo ofrece autenticación fuerte sin afectar la experiencia de usuario.
- La criptografía asimétrica asegura la autenticidad y previene ataques de suplantación.
- La entrega en tiempo real permite una respuesta de seguridad inmediata.

8. Arquitectura de Integración y Onboarding

8.1 Flujo Integral de Onboarding Digital con Biometría

El proceso de **onboarding** permite altos estándares de seguridad y cumplimiento. El sistema combina biometría con procesos tradicionales **KYC**. El 95% de las solicitudes se procesan automáticamente en 10 minutos.

- Inicio y Pre-detección: La aplicación móvil Xamarin realiza una evaluación de seguridad inicial del dispositivo y un cuestionario previo. Un motor de evaluación de riesgos identifica las solicitudes de alto riesgo.

- Captura de Documentos y Procesamiento: La integración con la cámara guía a los usuarios para capturar documentos. Azure Cognitive Services realiza el análisis, la extracción de texto y la validación de autenticidad. Los modelos de machine learning detectan manipulaciones.
- Reconocimiento Facial con Anti-Spoofing: El flujo de reconocimiento facial usa múltiples técnicas de detección de liveness para prevenir ataques de presentación (deepfakes, videos, máscaras).
- Verificación de Identidad Avanzada: Un proceso integral combina la comparación facial (selfie vs. documento) con la verificación de dirección y empleo. Una matriz de puntuación de riesgos determina la aprobación, revisión manual o rechazo.

9. Arquitectura de Notificaciones Obligatorias

9.1 Sistema Multicanal de Notificaciones

Se definen dos canales de notificaciones. La arquitectura implementa patrones para mensajería de alta confiabilidad, con manejo integral de errores, reintentos y estrategias de **fallback**.

9.2 Arquitectura del Orquestador de Notificaciones

El **Notification Orchestrator Service** es el núcleo del sistema, responsable de la lógica de enrutamiento, selección de plantillas y coordinación de la entrega. Mantiene una gestión de estado completa. Para las notificaciones se definen dos canales principales:

Canal 1: Azure Communication Services (SMS y Email): Ofrece capacidades de comunicación de grado empresarial con alta fiabilidad y cumplimiento.

Canal 2: WhatsApp Business API: Accede a una base de usuarios masiva y proporciona notificaciones multimedia con cifrado de extremo a extremo.

10. Diseño de Solución de Auditoría

10.1 Arquitectura de Event Sourcing

Se utiliza **Event Sourcing** para auditoría, capturando cada cambio como un evento inmutable, lo que proporciona un **audit trail** completo. Permite la reconstrucción del estado del sistema en cualquier momento, ofreciendo transparencia a los reguladores y capacidades forenses.

Implementación con PostgreSQL:

- JSONB Performance: PostgreSQL tiene una implementación JSONB con capacidades de indexación nativa que permiten consultas complejas sobre millones de eventos sin sacrificar el rendimiento.
- Write-Ahead Logging (WAL): WAL garantiza la durabilidad de los datos, asegurando que no se pierda ningún evento de auditoría, incluso durante fallos del sistema.
- Regulatory Query Capabilities: El soporte de SQL permite realizar las consultas complejas que los reguladores suelen solicitar.

- Atomic Transaction Support: El cumplimiento ACID de PostgreSQL garantiza que los eventos relacionados se escriban de forma atómica.

11. Seguridad y Cumplimiento Normativo

11.1 Normativas Aplicables

Para el cumplimiento normativo se revisa la documentación actual y se definen normativas nacionales e internacionales.

Regulaciones Internacionales - Estándares Globales:

PCI DSS Level 1 - Payment Card Industry Data Security Standard: El PCI DSS Level 1 compliance es obligatorio para cualquier organización que procese más de 6 millones de transacciones de tarjeta de crédito/débito anualmente.

ISO 27001 - Information Security Management System: ISO 27001 provee información para establecer, implementar, mantener y continuamente mejorar el information security management system (ISMS)..

SOX Compliance - Sarbanes-Oxley Act Requirements: El SOX compliance aplica a compañías que cotizan en bolsa y requiere controles específicos sobre los reposrtes financieros, afectando los Sistemas IT que soportan los procesos financiero.

Regulaciones Ecuador - Marco Legal Nacional:

Ley Orgánica de Protección de Datos Personales (LOPD): La ley de protección de datos de Ecuador requiere controles específicos sobre el procesamiento de datos personales, almacenamiento y transferencia, impactando directamente las decisiones de arquitectura del sistema.

11.2 Arquitectura de Defensa en Profundidad

Esta estrategia implementa múltiples capas de seguridad que trabajan en conjunto.

- **Capa de Seguridad de Red**: Azure Firewall (con Advanced Threat Protection), Azure DDoS Protection Standard y Azure Application Gateway con WAF (para proteger contra vulnerabilidades OWASP Top 10).
- **Controles de Seguridad de API**: Autenticación OAuth 2.0/OIDC con validación de JWT, limitación de tasa y validación de entrada.
- **Capa de Seguridad de Datos**: Transparent Data Encryption (TDE) y Always Encrypted para proteger los datos en reposo y en tránsito. Se usa Azure Key Vault con HSM para las claves criptográficas.

12. Monitoreo y Observabilidad

12.1 Telemetría Completa

La observabilidad en sistemas bancarios requiere visibilidad completa desde las interacciones del usuario hasta el estado de la infraestructura. La integración con **Azure Application Insights** proporciona una visibilidad de extremo a extremo y capacidades de correlación para la rápida identificación y resolución de problemas.

12.2 Estrategia de Logging

Se usa **Structured Logging** con **Serilog** para análisis sofisticado, alertas automatizadas y cumplimiento. Esto incluye **correlation IDs** para rastrear los registros a través de diferentes servicios.

13. Gestión de Costos en Azure

13.1 Estrategia de Optimización de Recursos

La gestión de costos equilibra los requisitos de rendimiento, fiabilidad y eficiencia.

- **Instancias Reservadas (RIs):** Ahorros sustanciales para cargas de trabajo predecibles (bases de datos, servicios **Always-On**)..
- **Instancias Spot:** Ahorros de hasta 90% para cargas de trabajo no críticas, como procesamiento por lotes o entornos de desarrollo.
- **Auto-scaling Inteligente:** Usa algoritmos para optimizar la asignación de recursos. Permite un 100% de capacidad en horas pico y una reducción del 40-60% fuera de ellas.

13.2 Análisis de Servicios Gestionados vs. Autogestionados

La decisión de usar servicios gestionados se basa en el **TCO**. Aunque los costos directos pueden ser más altos, eliminan gastos ocultos de gestión operativa y seguridad. Por ejemplo:

- **SQL Server Managed Instance:** Elimina sobrecarga anual de operaciones.
- **Azure Kubernetes Service (AKS):** Elimina el costo de un ingeniero DevOps.

Esto permite que el equipo interno se enfoque en la lógica de negocio en lugar de la infraestructura.