

TABLA DE CONTENIDO

Objetivo	2
Necesidad de negocio	2
Identificación del As-Is	2
Planteamiento del To-Be.....	2
Requisitos Funcionales y No Funcionales del sistema	4
Planteamiento de Arquitectura	5
Diagrama Infraestructura de Solución Azure	9
Decisiones de Arquitectura	10

Objetivo

Disponibilizar un sistema de banca en línea que permita a los clientes acceder a su historial de movimientos, sus transacciones, transferencias y pagos.

Necesidad de negocio

Luego de las comunicaciones con stakeholders y la profundización de la necesidad planteada se llega al siguiente planteamiento:

Diseñar un sistema de banca por internet. En este sistema los usuarios podrán:

1. Acceder al historial de sus movimientos.
2. Hacer transferencias y pagos a:
 - Cuentas propias.
 - Interbancarias.

Identificación del As-Is

La información del cliente proviene de dos sistemas:

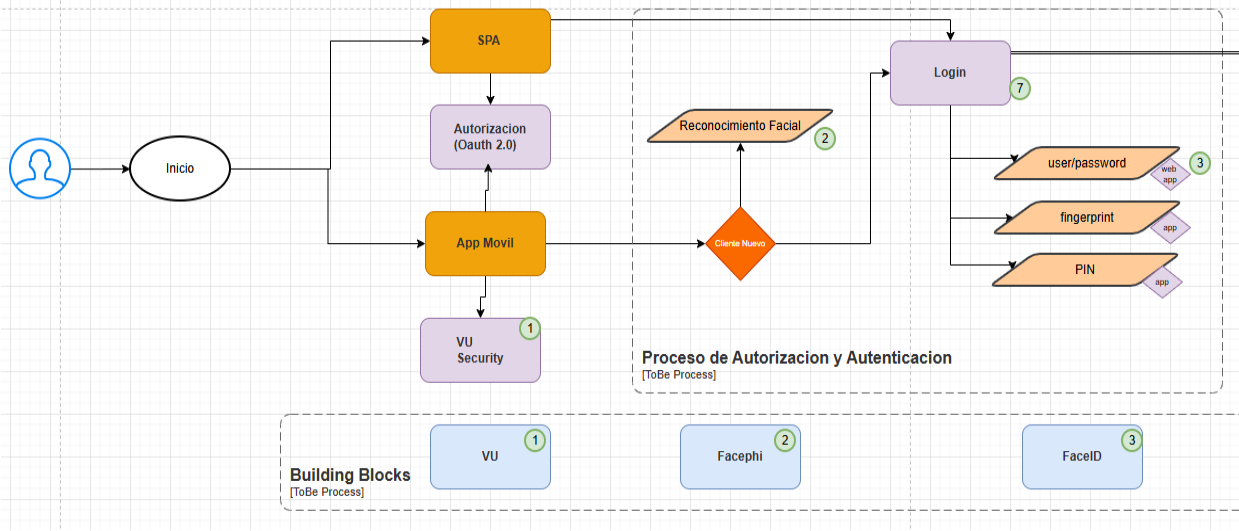
- Core Bancario: datos básicos de cliente, movimientos y productos.
- Sistema Complementario: amplía la información cuando se requieren datos en detalle.

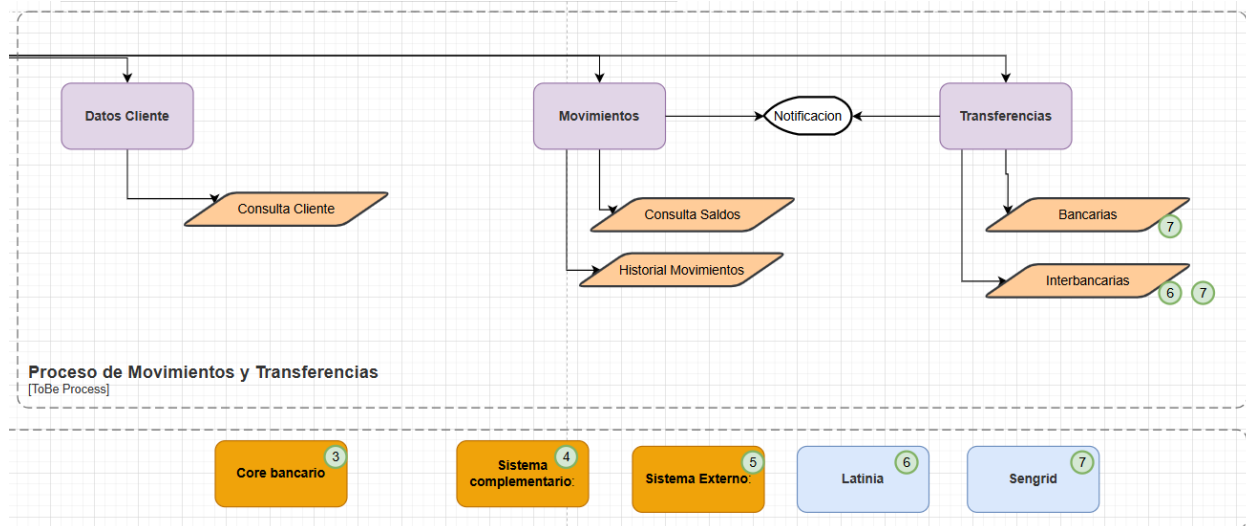
Planteamiento del To-Be

Proceso	Detalle
Acceso	<p>El Front contará con dos aplicaciones:</p> <ul style="list-style-type: none">• Una SPA - Restricción: (web)• Una aplicación móvil - Restricción: framework multiplataforma <p>Ambas aplicaciones autenticarán mediante un servicio OAuth 2.0 ya disponible en la compañía (configurable).</p>

Onboarding biométrico	<p>Cliente Nuevo App: usa reconocimiento facial</p> <ul style="list-style-type: none">La arquitectura debe considerarlo como parte del flujo de autorización y autenticación. Tras el onboarding, el usuario podrá ingresar con usuario/clave, huella u otro método.
Consultas saldos y movimientos	<p>Para obtener datos del cliente, el sistema pasa por una capa de integración compuesta por un API Gateway y consume servicios según el tipo de transacción. Inicialmente existen tres servicios principales:</p> <ul style="list-style-type: none">Consulta de datos básicosConsulta de movimientosTransferencias
Restricciones	<p>Por normativa, los usuarios deben:</p> <ul style="list-style-type: none">Ser notificados de sus movimientos.Usar al menos dos sistemas de notificaciones (externos o propios).

Diagrama To-Be





Requisitos Funcionales y No Funcionales del sistema

Requisitos Funcionales

Requisito	Descripción	Prioridad
Autenticación	Se necesita contar con mecanismos de autorización e identificación que sean seguros de acuerdo con los estándares bancarios. OIDC (Auth Code + PKCE) con Entra ID	Alta
Onboarding biométrico	Se necesita validar a los usuarios mediante la tecnología de reconocimiento facial de Facephi, junto con VU Security	Alta
Consultas saldos y movimientos	Se necesita visualizar los saldos y movimientos del cliente	Alta
Transferencias propias e interbancarias	Se necesita realizar pagos y transferencias a cuentas propias de forma bancaria o interbancaria	Alta
Notificaciones push/SMS/email	Se necesita enviar notificaciones al usuario además de mensajes y correos electrónicos	Alta

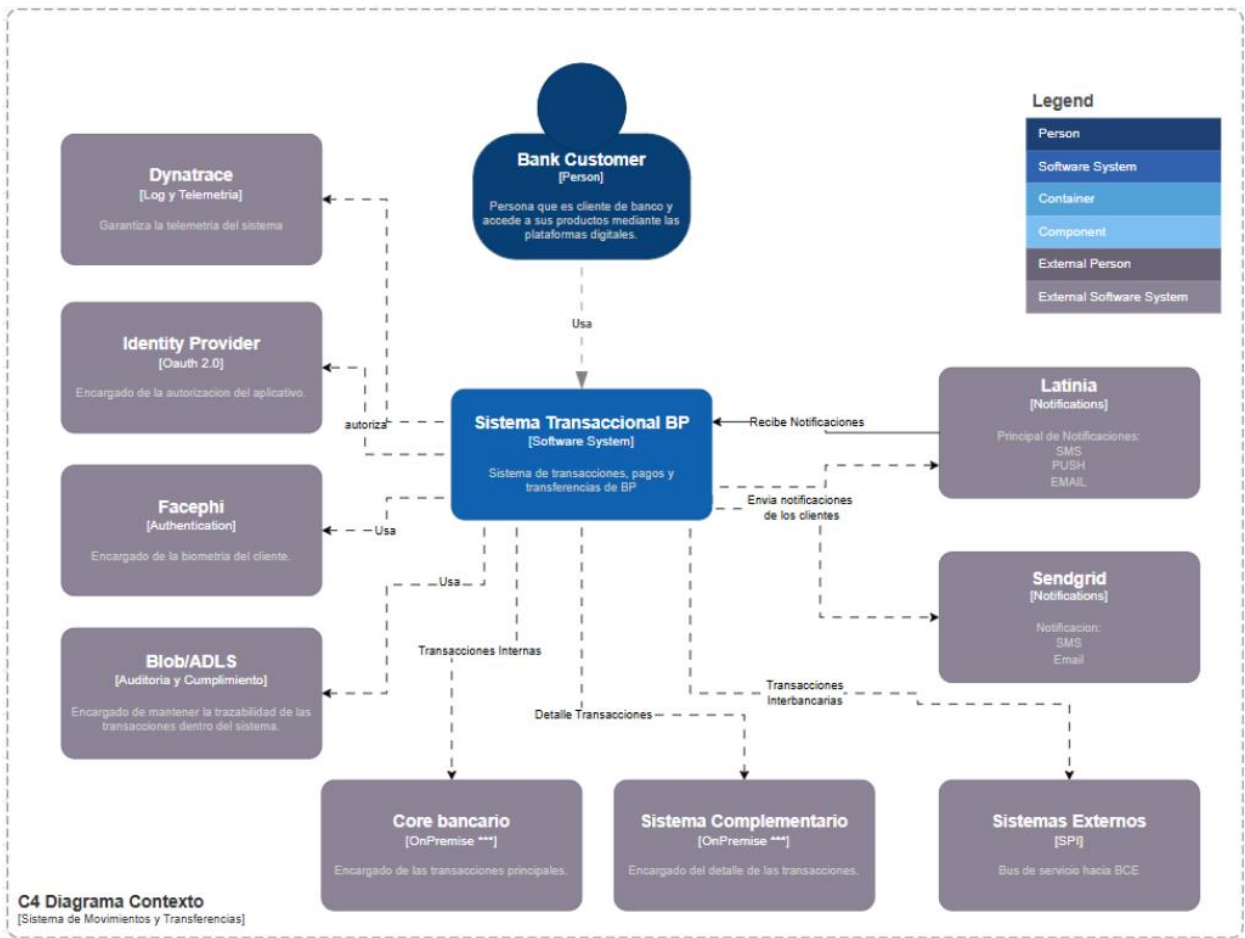
Requisitos No Funcionales

Categoría	Meta	Control
Disponibilidad	≥99%	SLO en Azure Monitor
Latencia	p95 < 300 ms · p99 < 800 ms	App Insights
Seguridad	APIM WAF, mTLS a SPI, CMK	Defender + Policies
Privacidad	PII masking, RBAC/ABAC	DLP/Logs
Auditoría	WORM 7 años	ADLS Gen2
Escala	Autoscale RU/s, HPA AKS	Pruebas de carga

Planteamiento de Arquitectura

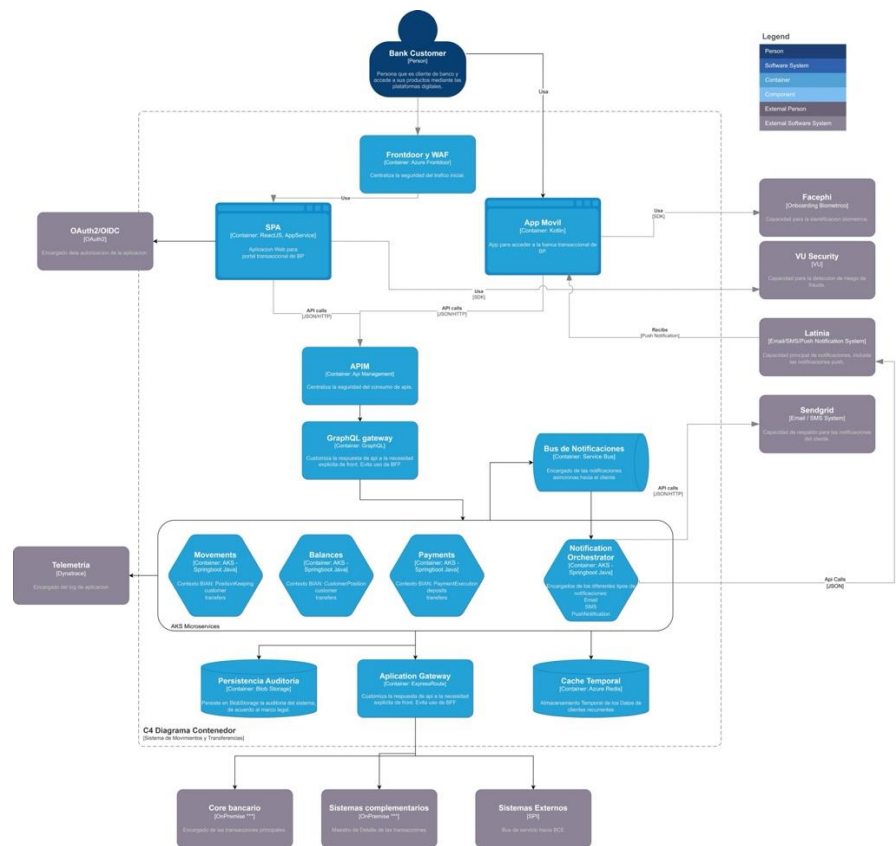
Luego de la contextualización y entendimiento de negocio, se procede con el planteamiento de la arquitectura de solución bajo el modelo C4.

C4 – Context



Actores	Detalle	Descripción
Usuarios	Usuarios de Banco	Clientes existentes de banco, con al menos un activo (cuenta de ahorro).
Sistema	SPA	Aplicacion Web Construida en ReactJS, y desplegada en AppService de Azure.
	App	Aplicacion Movil Kotlin, para garantizar el despliegue multiplataforma.
Sistemas Externos	Facephi	Proveedor de biometría.
	VU Security	Proveedor de Seguridad y Autenticación de dispositivos.
	Latinia	Proveedor de notificaciones principal (push/SMS/email).
	Sendgrid	Proveedor de notificaciones secundario (SMS/email).
	SPI/BCE	Proveedor Banco Central para transferencias interbancarias.
	Core	Sistema interno para datos cliente, historial de pagos y transferencias.
	Core Complementario	Sistema complementario para detalle de transacciones.

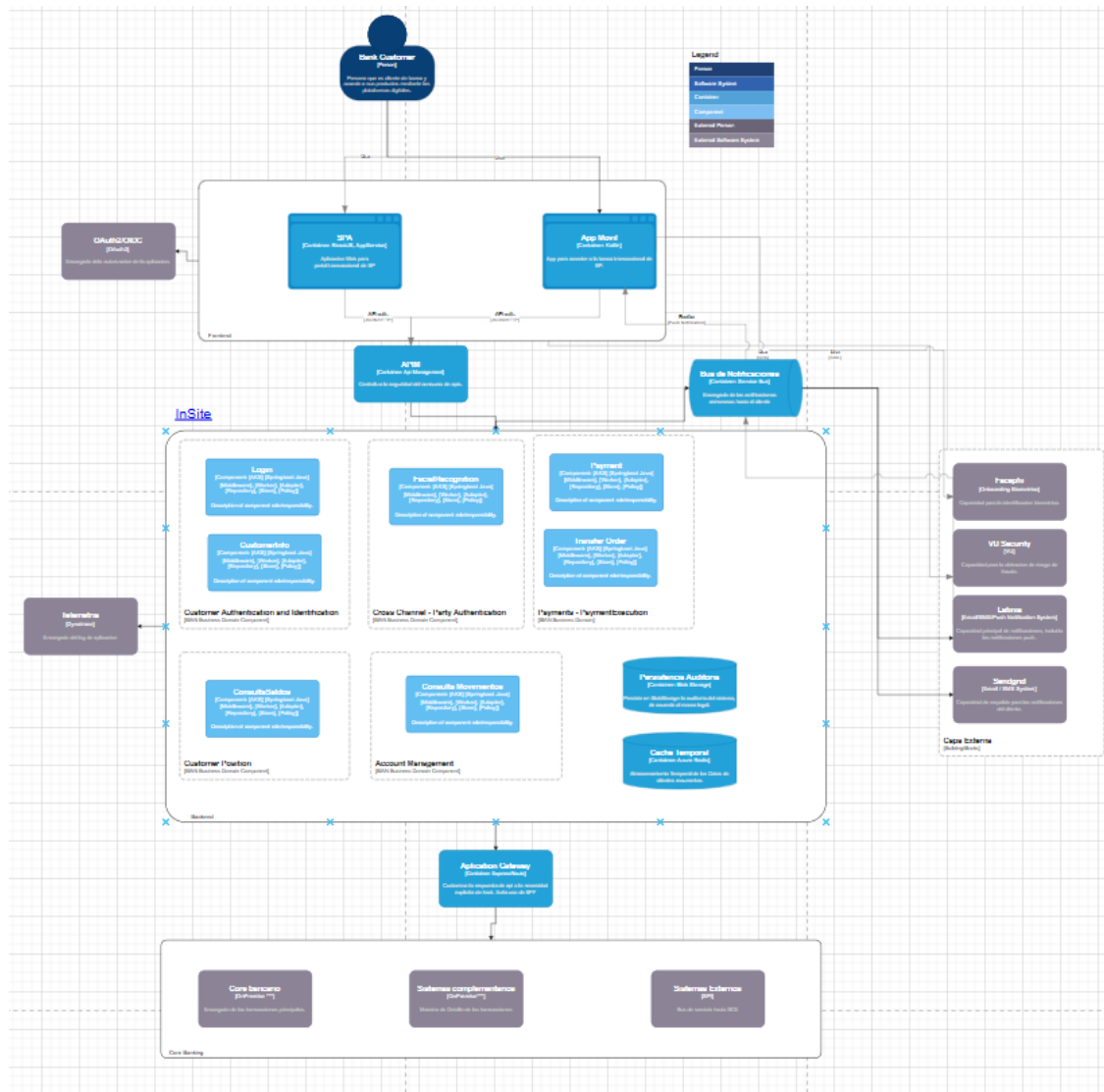
C4 – Contenedores



Actores	Descripción
Edge	Front Door + WAF → APIIM (Internal + Private Link)
Servicios (AKS)	Movements, Balances, Payments, Notification Orchestrator, Interbank Gateway (SPI Adapter)
Plataforma	Service Bus Premium, Cosmos DB (Mongo), Redis, Key Vault/Managed HSM, ADLS Gen2 (WORM)
Observabilidad:	Azure Monitor + App Insights (+Dynatrace)

C4 – Componentes

Componente: Back Domain



Actores	Descripción
Payments	Idempotency Filter, Orchestrator, Outbox Publisher → SB, Saga Coordinator, SPI Client (retry/timeout/circuit-breaker)
Interbank Gateway	transform ISO20022/XSD, firma + mTLS (HSM), Ack Parser, Reconciliación, DLQ Handle
Notifications	ChannelSelector, TemplateEngine, Senders (Latina/SendGrid), DLR Listener, fallback, traza a ADLS

Componente: Front Solution

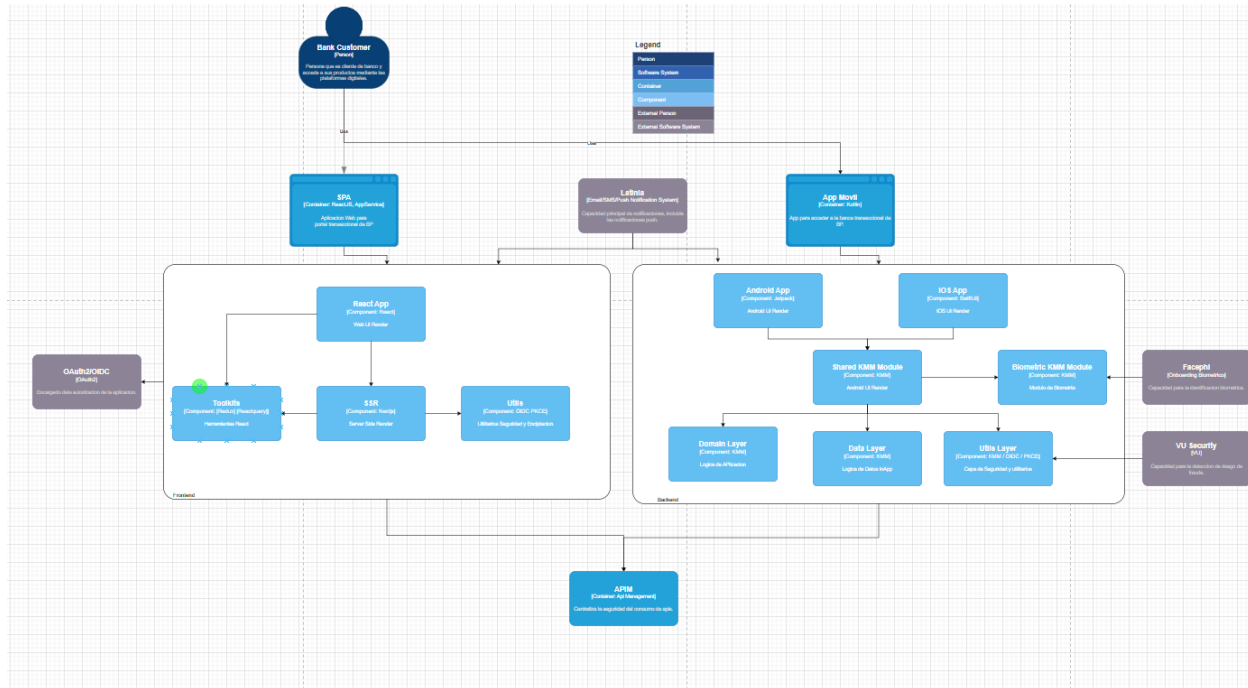
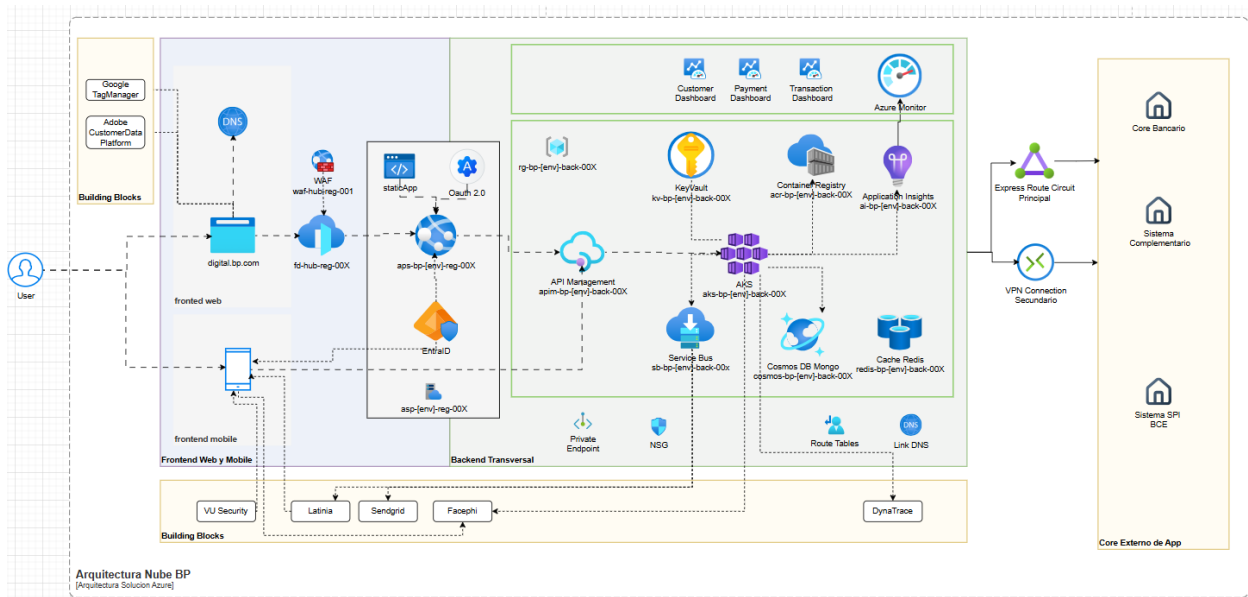


Diagrama Infraestructura de Solución Azure

A continuación, se detalla un diagrama de solución para la implementación en la infraestructura de Azure.



Criterio	Descripción
Seguridad	vNet privada; APIM Internal con Front Door Premium + WAF por Private Link Azure Firewall/NAT, NSG y UDR
Microservicios	AKS private cluster (node pools zonales)
Datos	Cosmos DB multi-región (CMK, autoscale), Service Bus Premium (ZRS + geo-recovery), Redis Premium/Enterprise (geo-replica)
Conectividad	Private Endpoints + Private DNS (Cosmos/SB/Redis/KV/ACR/App Insights) ExpressRoute dual a banca + VPN de respaldo
Observabilidad	Log Analytics → App Insights/Dynatrace; Workbooks y alertas KQL

Decisiones de Arquitectura

Marco Regulatorio de Referencia:

Regulacion	Detalle	Link Referencia
ISO 27001	Estandar Internacional de proteccion de datos.	ISO/IEC 27001:2022 - Information security management systems
BCE	Politica de Tratamiento de datos personales	Política para el tratamiento de datos personales - Banco Central del Ecuador

Elección del Stack Tecnológico:

Canal	Decisión	Alternativas	Justificación (técnica y de riesgo)
WEB	React	Angular, Vue	Integracion con Next.js: SSR/ISR Librerias maduras UI, npm, i18n Alto grado de profesionales con conocimiento de react
MOBILE	KMM (Kotlin Multiplatform + SwiftUI)	Flutter (Dart), React Native (TS),	Integracion nativa a Facephi, Play Integrity , cifrado hardware (Android Keystore), rendimiento nativo, SDKs bancarios sin bridges.

Decisiones de Infraestructura:

ID	Decisión	Alternativas	Justificación (técnica y de riesgo)
----	----------	--------------	-------------------------------------

ADR-001	Azure como nube objetivo	AWS/GCP	Sinergia con stack y skills; ExpressRoute con banca; catálogo PaaS maduro para integración y seguridad.
ADR-002	APIM modo Internal + Front Door/WAF + Private Link	APIM público	Minimiza superficie pública (Zero-Trust), centraliza políticas (JWT, schema, rate-limit, idempotency) y protege contra DDoS/bots.
ADR-003	AKS para microservicios de dominio	App Service, Functions	Requiere (mTLS/OTel), control de red con mayor precisión. AKS ofrece mayor control y portabilidad.
ADR-004	Cosmos DB (Mongo API)	SQL/PG	Latencia baja global, multi-región nativa, autoscale RU/s; modelo documento encaja para auditoría legal 7 años.
ADR-005	Service Bus Premium + Outbox/Saga	Storage Queues, sync	Garantías de entrega (DLQ, sessions), ordenación y aislamiento; patrones de resiliencia para pagos e interbancario.
ADR-006	Redis Premium/Enterprise para caché	Sin caché, Memcached	Reduce latencia en lecturas (datos cliente), y geo-replica para continuidad.
ADR-007	Interbank Gateway (SPI Adapter) en AKS	Llamadas directas desde Payments	Aísla contratos ISO20022/XSD, firma/mTLS ; desacopla cambios hacia la capa Core y facilita pruebas/fallback.
ADR-008	Doble proveedor de notificaciones (Latinia/Sendgrid)	Proveedor único	Cumplir con normativa legal y reducir riesgo operativo.
ADR-009	ADLS Gen2 con WORM/Legal Hold para auditoría	Logs en BD	Evidencia inmutable para el área de auditoría y cumplimiento
ADR-010	Entra ID (OIDC, Auth Code + PKCE)	IdP propio	Estándar, política MFA/CA , device binding; reduce brecha de seguridad.
ADR-011	Managed Identity + Key Vault/Managed HSM	Secrets en config	Elimina secretos estáticos; HSM para certificados SPI y rotaciones automáticas a 360 días no críticas y 30 días críticas.
ADR-012	Observabilidad Azure Monitor + App Insights (+Dynatrace)	Solo logs básicos	Trazas distribuidas en Azure Monitor, KQL; Dynatrace como canal de reportes desacoplado de la infraestructura.

Partida Presupuestaria:

Microsoft Azure
Estimate
Su presupuesto

Service category	Service type	Region	Description	Estimated
Compute	Azure Kubernetes Service (AKS)	West US	Premium; Administración de clústeres para 0 clústeres; 1 D2 v3 (2 vCPU, 8 GB de RAM) x 730 Horas (Pago por uso), Linux; 0 discos de sistema operativo administrados – S4	\$85.41
Web	API Management	East US	API Management v2 Service, Standard Tier, 1 Base unit(s) x 730 Horas, 0 Scale out unit(s) x 730 Horas, 0 API requests per month, 0 Self-hosted Gateways x 730 Horas	\$700.00
Redes	Application Gateway	East US	nivel de Estándar V2, 730 puerta de enlace fija Horas, 1 unidades de proceso y 1000 conexiones persistentes con rendimiento 1 de MB/s, transferencia de datos 5 GB	\$151.84
Integración	Service Bus	East US	Nivel Premium: 1 unidades de mensajes al día x 1 particiones x 730 Horas	\$677.08

Bases de datos	Azure Cosmos DB	East US	Azure Cosmos DB for NoSQL (anteriormente Core), Procesamiento aprovisionado estándar (manual), Cantidad siempre gratis deshabilitada, Pago por uso, Business Critical, Per Partition Automatic Failover- Este de EE. UU. (región de escritura), 1000 RU/s x 730 Horas, 0 GB de almacenamiento transaccional, Almacenamiento analítico deshabilitado, 2 copias de almacenamiento de copias de seguridad periódicas, Puerta de enlace dedicada no habilitada	\$116.80
----------------	-----------------	---------	--	----------

DevOps	Azure Monitor	East US	Log Analytics: Log Data Ingestion: 0 GB Daily Auxiliary Logs without processing, 0 GB Daily Auxiliary Logs with processing, 0 GB Daily Basic logs, 0 GB Daily Analytics logs ingested, 1 months of Interactive Retention, 0 months of Retention, 0 GB data restored for 0 days, 0 queries per day with 0 GB data scanned per query, 0 GB of Log Data Exported per day, Platform Log Data Processed per day: 0 GB with Destination to Storage or Event Hub and 0 GB with Destination to Marketplace Partners, 0 Search job Queries per day with 0 GB data scanned per query; 0 Puntos de conexión de MI de SCOM; Prometheus administrado: uso del método de estimación de recopilación predeterminado (con un clúster de 0 nodos de Linux, 0 nodos de Windows, 0 contenedores y 0 pods), 0 Promedio diario de usuarios de paneles, 7 paneles, 50000 ejemplos de datos consultados por panel, 25 reglas de alertas de promql, 25 reglas de grabación de promql; Application Insights: 0 GB de registros de análisis diarios ingeridos, 3 meses de retención de los datos, 0 pruebas web Estándar, 5 minutos frecuencia de ejecución, Ejecutar durante 730 horas; 20 recursos supervisados X 1 serie temporal métrica supervisada por recurso, 5 minutos Frecuencia de señal de registro con 50 señales de registro series temporales y 1 supervisadas por señal, 0 eventos adicionales (en miles), 0 correos electrónicos adicionales (en 100 000), 0 notificaciones push adicionales (en 100 000), 0 webhooks adicionales (en millones)	\$84.50
Bases de datos	Azure Cache for Redis	West US	Nivel Premium; 1 partición por instancia, 0 réplicas adicionales por partición, 1 instancia P1, 730 Horas, Pago por uso	\$404.42

Redes	Azure Front Door		Azure Front Door prémium - Instancia base incluida, 5 GB transferencia de datos de salida al cliente, 5 GB Transferencia de datos de entrada al origen, 0 x 10 0000 solicitudes	\$330.51
Seguridad	Key Vault	East US	Almacén: 1.000.000 operaciones, 0 operaciones avanzadas, 50 renovaciones, 50 claves protegidas, 0 claves protegidas avanzadas; grupos de HSM administrados: 0 grupo(s) de HSM B1 estándar x 730 Horas	\$203.00
Redes	Azure ExpressRoute		ExpressRoute, Zona 1, Premium, Medido; 1 circuito de 50 Mbps , 0 GB en la transferencia de datos de salida adicional; Complemento de Global Reach: Deshabilitado	\$130.00
Support		Support		\$0.00
		Licensing Program	Microsoft Customer Agreement (MCA)	
		Billing Account		
		Billing Profile		
		Total		\$2,883.55

Disclaimer

All prices shown are in United States – Dollar (\$) USD. This is a summary estimate, not a quote. For up to date pricing information please visit <https://azure.microsoft.com/pricing/calculator/>

This estimate was created at 11/17/2025 12:30:56 PM UTC.