TABLA DE CONTENIDO

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:

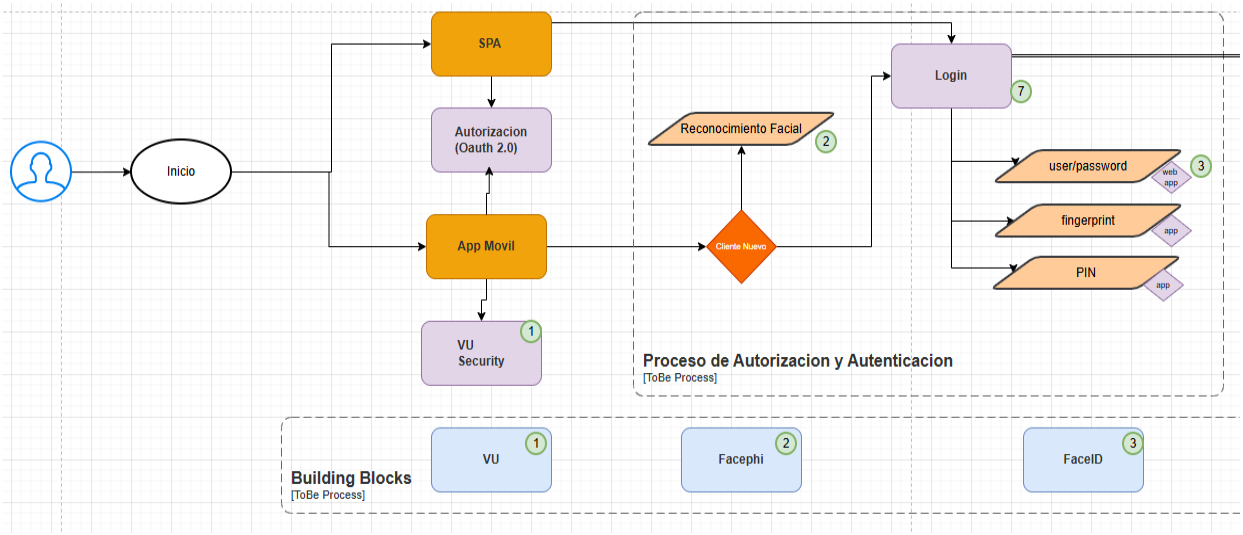
- Core Bancario: datos básicos de cliente, movimientos y productos.
- Sistema Complementario: amplía la información cuando se requieren datos en detalle.

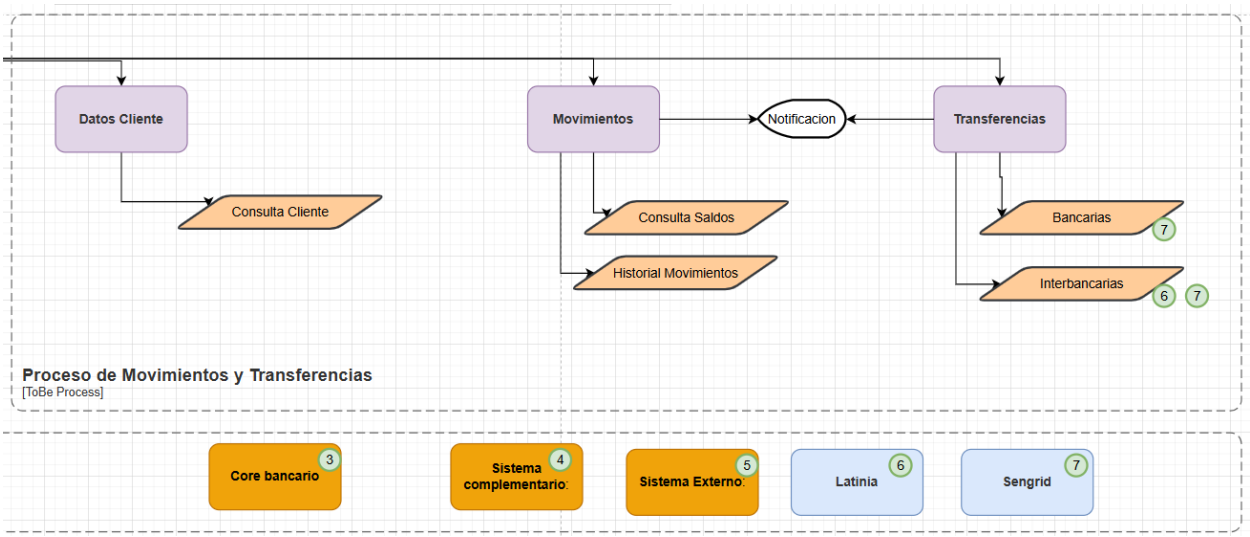
Planteamiento del To-Be

Proceso	Detalle
Acceso	El Front contará con dos aplicaciones: • Una SPA - Restricción: (web) • Una aplicación móvil - Restricción: framework multiplataforma Ambas aplicaciones autenticarán mediante un servicio OAuth 2.0 ya disponible en la compañía (configurable).

Onboarding biométrico	Cliente Nuevo App: usa reconocimiento facial • 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	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: • Consulta de datos básicos • Consulta de movimientos • Transferencias
Restricciones	Por normativa, los usuarios deben: • 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**

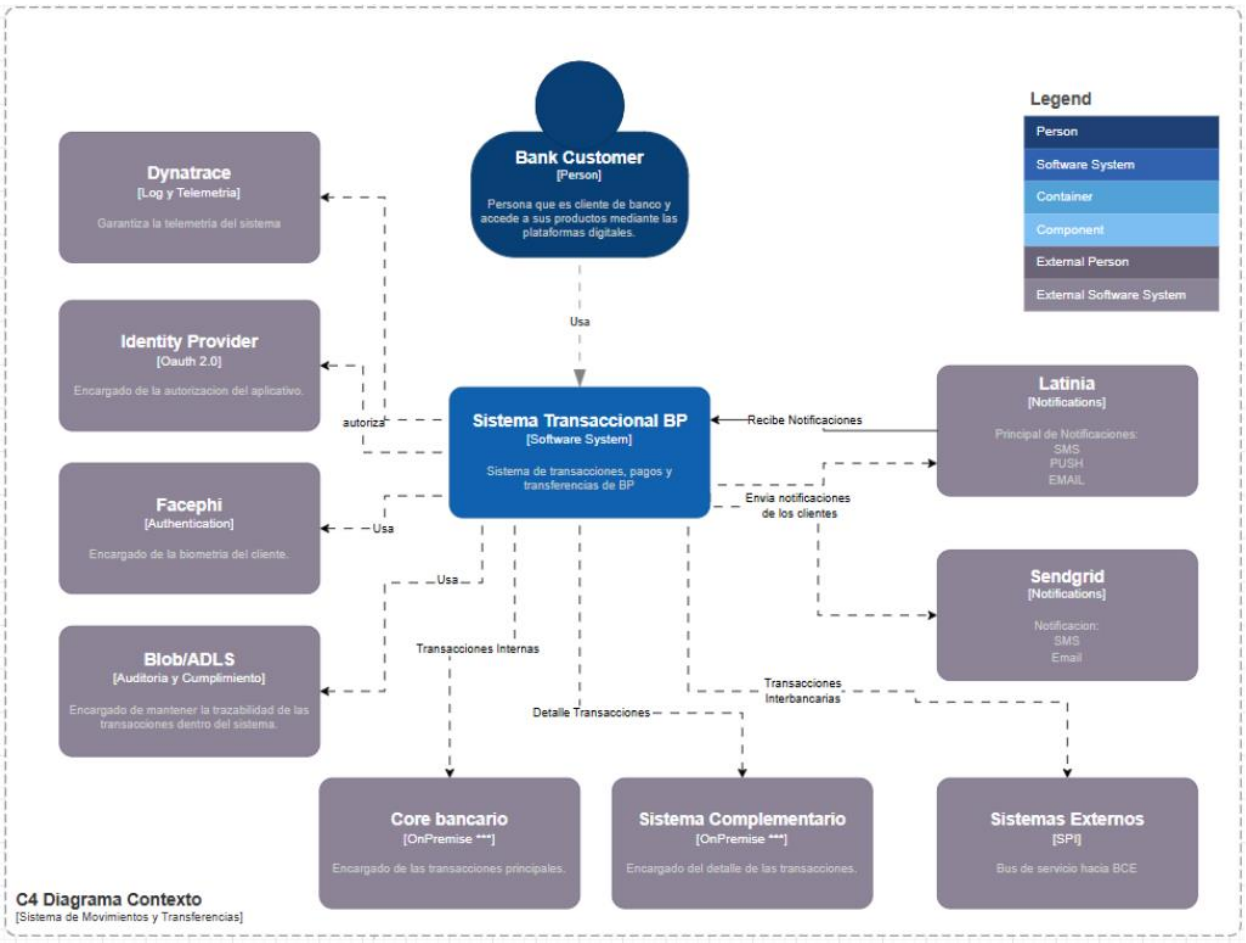
Requisitos No Funcionales

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

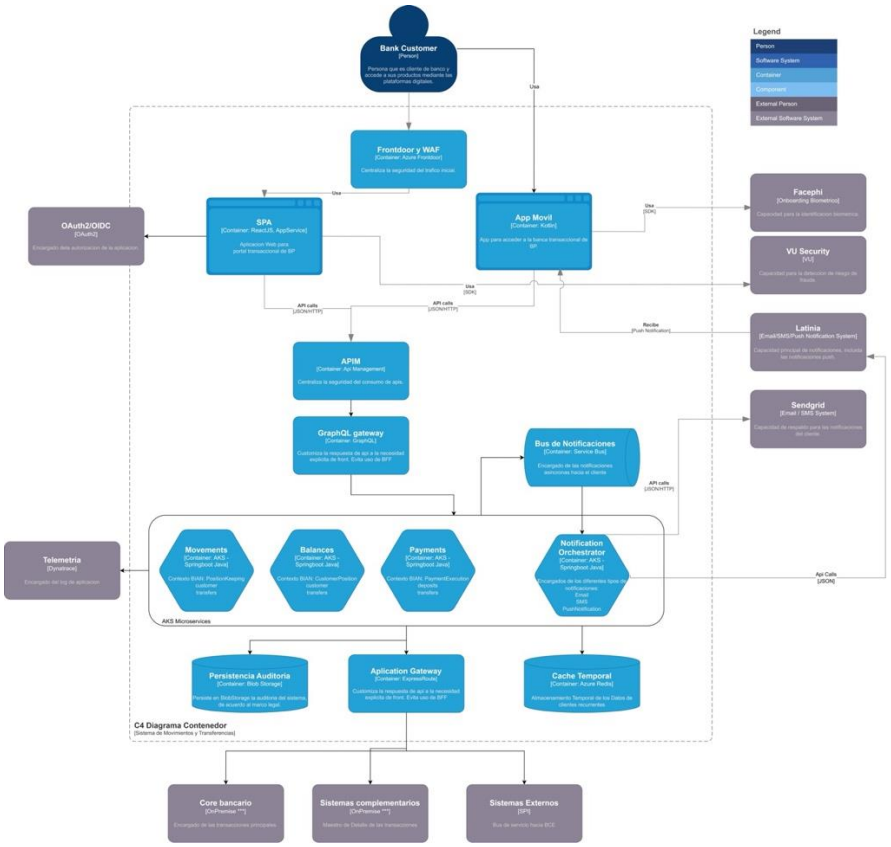
Luego de la contextualización y entendimiento de negocio, se procede con el planteamiento de la arquitectura de solución bajo el modelo C4.

C4 – Context



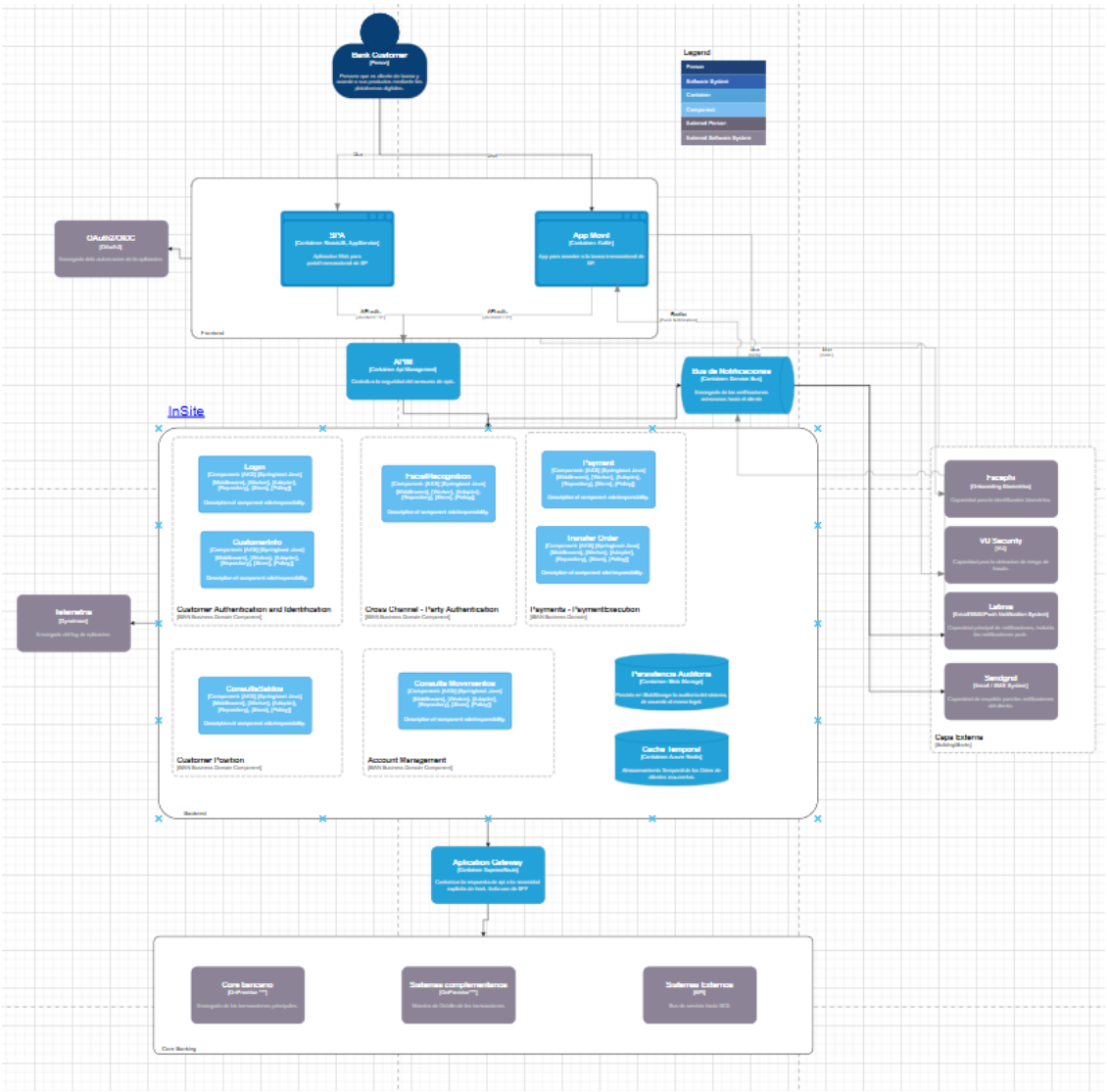
Actores	Detalle	Descripción
Usuarios	Usuarios de Banco	Clientes existentes de banco, con al menos un activo (cuenta de ahorro).
Sistema	SPA	Aplicacion Web Construida en ReactJS, y desplegada en AppService de Azure.
	App	Aplicacion Movil Kotlin, para garantizar el despliegue multiplataforma.
Sistemas 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 → APIM (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)

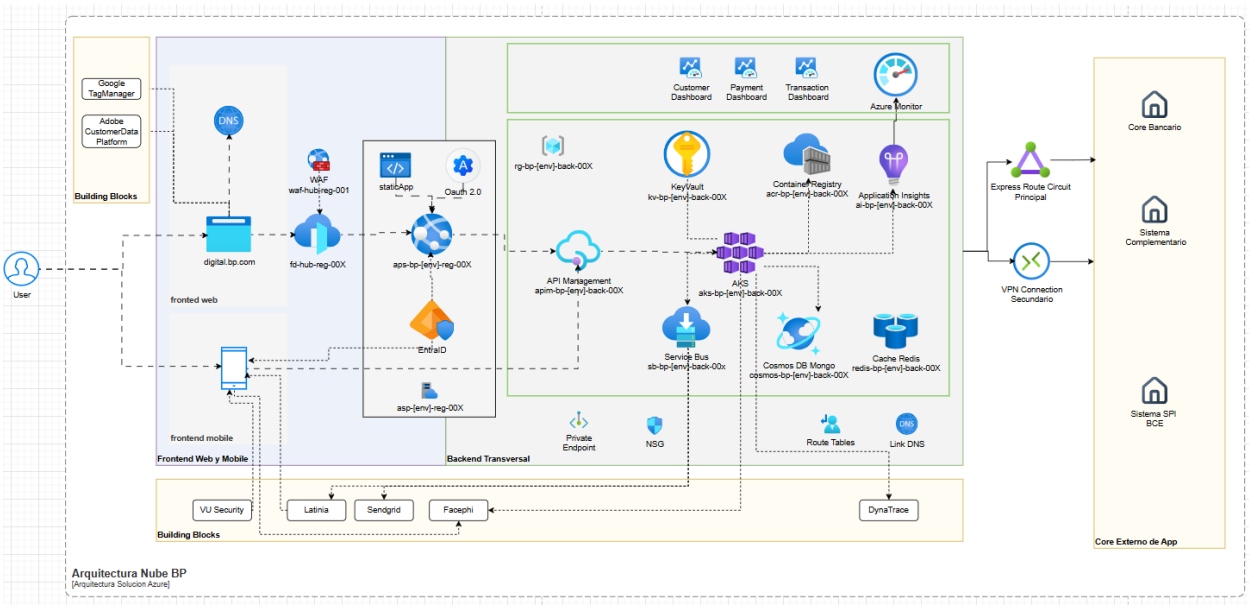
C4 – Componentes



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 (Latinia/SendGrid), DLR Listener, fallback, traza a ADLS

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

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 policies (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 auditoria 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.