Diagrama de Contexto

El presente diagrama de contexto del sistema ofrece una visión macro de la arquitectura de integración propuesta para la modernización de los sistemas bancarios. Este nivel proporciona un entendimiento general de cómo la plataforma bancaria integrada interactúa con diversos actores, incluyendo usuarios internos y externos, así como sistemas y servicios de terceros. Esta perspectiva es crucial para identificar las principales interacciones y flujos de información, estableciendo las bases para el diseño detallado en niveles posteriores.

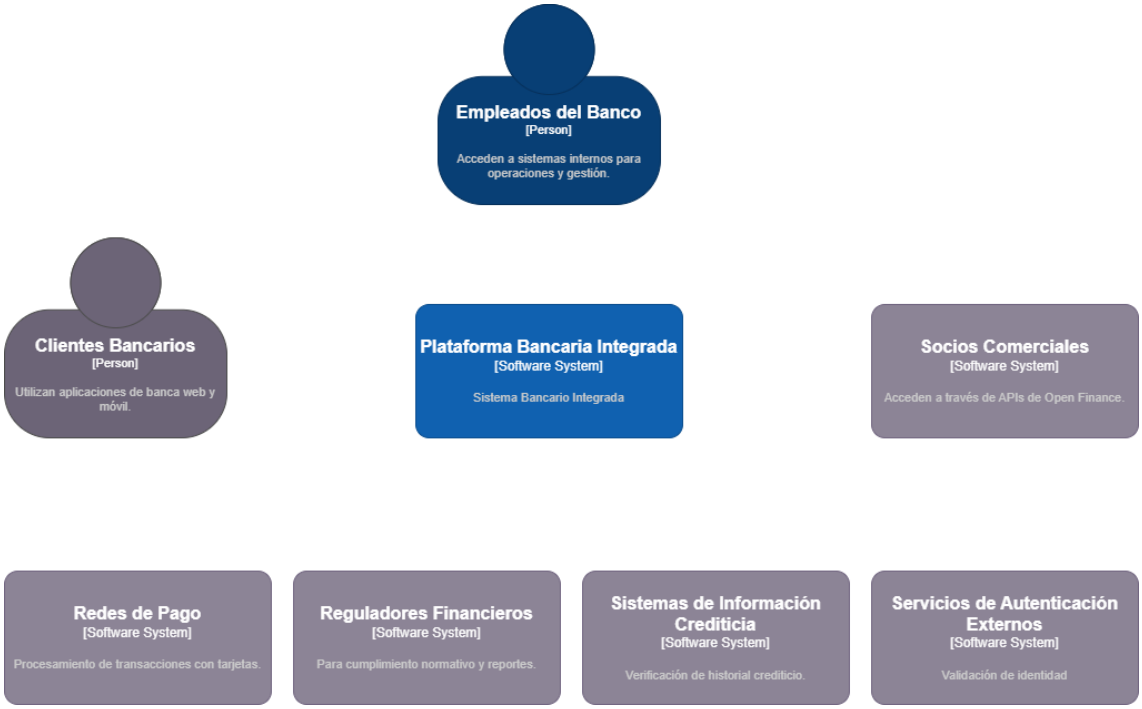

Ilustración 1. Diagrama de contexto.

Descripción Principal: Plataforma Bancaria Integrada

La **Plataforma Bancaria Integrada** es el núcleo de nuestra arquitectura propuesta. Esta plataforma unifica el core bancario tradicional con el nuevo core bancario digital, permitiendo una transición fluida hacia servicios modernos y eficientes. Actúa como el punto central de interacción para todos los usuarios y facilita la comunicación con sistemas externos críticos para las operaciones bancarias.

Usuarios del Sistema

1. **Clientes Bancarios**

Los clientes son el eje central de las operaciones bancarias. A través de las aplicaciones de banca web y móvil, los clientes pueden acceder a una variedad de servicios, como:

- Consultar saldos y movimientos.
- Realizar transferencias y pagos.
- Solicitar productos financieros.
- Recibir notificaciones y alertas.

La experiencia del cliente se optimiza mediante interfaces intuitivas y personalizadas, garantizando al mismo tiempo la seguridad y privacidad de sus datos.

2. **Empleados del Banco**

Los empleados acceden a sistemas internos para:

- Gestionar cuentas y operaciones.
- Brindar atención y soporte al cliente.
- Realizar análisis y reportes internos.

Se implementan estrictas políticas de gestión de identidad y acceso para asegurar que solo el personal autorizado tenga acceso a información sensible.

3. **Socios Comerciales**

A través de las **APIs de Open Finance**, terceros pueden:

- Ofrecer servicios financieros complementarios.
- Integrar soluciones innovadoras que enriquecen la oferta del banco.
- Acceder a información autorizada por los clientes para brindar servicios personalizados.

Este ecosistema abierto promueve la innovación y amplía las oportunidades de negocio.

Sistemas Externos

- **Redes de Pago**

La plataforma se integra con redes de pago para procesar transacciones con tarjetas y otros medios electrónicos, asegurando la eficiencia y seguridad en las operaciones.

- **Reguladores Financieros**

Cumpliendo con las regulaciones vigentes, el sistema reporta periódicamente información a los organismos supervisores, garantizando transparencia y cumplimiento normativo.

- **Sistemas de Información Crediticia**

Para evaluar la solvencia y riesgo de los clientes, se consultan sistemas de información crediticia, facilitando la toma de decisiones en la otorgación de créditos y otros productos financieros.

- **Servicios de Autenticación Externos**

Se incorporan servicios avanzados de autenticación, como biometría y autenticación de dos factores, fortaleciendo la seguridad en el acceso y uso de los servicios bancarios.

Interacciones y Flujos de Información

El diagrama ilustra las principales interacciones entre los usuarios, el sistema principal y los sistemas externos.

- Cuando un **cliente bancario** inicia sesión en la aplicación móvil, el sistema verifica su identidad a través de servicios de autenticación externos y permite el acceso a su información personal y transaccional.

- Un **empleado del banco** puede acceder al sistema para actualizar la información de un cliente, proceso que está sujeto a controles de seguridad y auditoría.
- Un **tercero** puede solicitar, con el consentimiento del cliente, información necesaria para ofrecer un servicio financiero personalizado, a través de las APIs seguras proporcionadas por la plataforma.

Consideraciones de Seguridad y Cumplimiento Normativo

La plataforma está diseñada con una sólida infraestructura de seguridad que incluye:

- **Cifrado de Datos**: Tanto en tránsito como en reposo, utilizando protocolos como SSL/TLS.
- **Autenticación y Autorización**: Implementación de OAuth 2.0 y gestión de permisos basada en roles.
- **Monitoreo y Auditoría**: Registro detallado de actividades para detectar y prevenir actividades fraudulentas.
- **Cumplimiento Normativo**: Alineación con la ley orgánica de protección de datos personales y otras regulaciones aplicables.

Diagrama de Contenedores

El diagrama de contenedores ofrece una visión detallada de la arquitectura del sistema, mostrando cómo las aplicaciones, servicios y bases de datos se organizan y comunican. Este nivel es esencial para comprender la estructura general, las tecnologías empleadas y cómo se logra la integración en la modernización del sistema bancario.

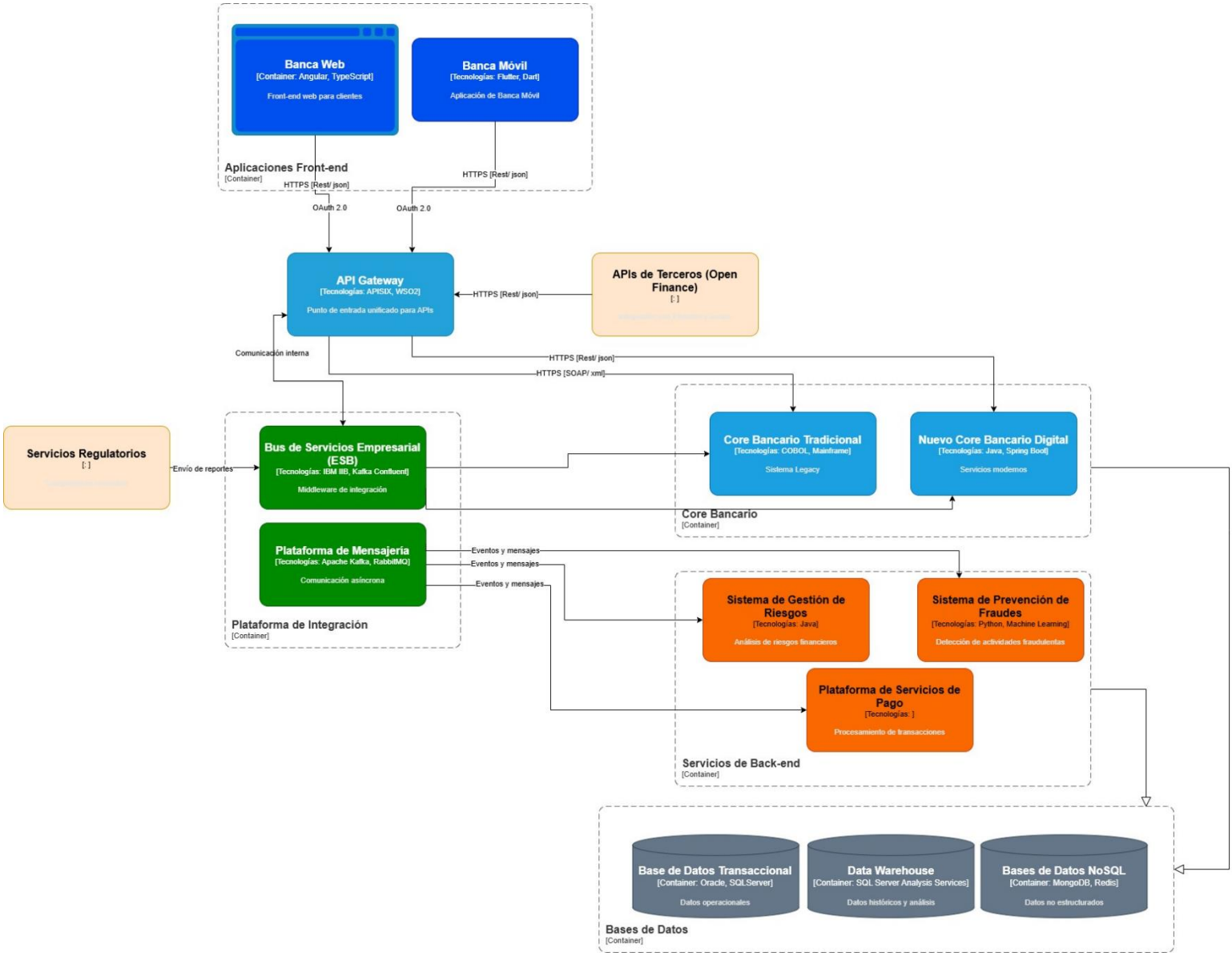

Ilustración 2. Diagrama de Contenedores

Descripción de los Contenedores Principales

Aplicaciones Front-end

Banca Web

La aplicación de banca web permite a los clientes acceder a servicios bancarios desde cualquier navegador. Desarrollada con **Angular** y **TypeScript**, ofrece una interfaz intuitiva y responsiva. Se comunica con el sistema a través del **API Gateway**, asegurando una comunicación segura y eficiente.

Banca Móvil

La aplicación de banca móvil proporciona acceso desde dispositivos iOS y Android, desarrollada con **Flutter** respectivamente. Ofrece funcionalidades similares a la banca web, optimizadas para dispositivos móviles.

Core Bancario

Core Bancario Tradicional

Sistema legacy que maneja operaciones bancarias fundamentales. Se han desarrollado adaptadores para permitir su integración con el nuevo ecosistema, asegurando que las funcionalidades existentes continúen operativas.

Nuevo Core Bancario Digital

Diseñado para soportar servicios digitales modernos, desarrollado con **Java** y **Spring Boot**. Es modular y escalable, permitiendo incorporar nuevas funcionalidades de manera ágil.

Plataforma de Integración

Bus de Servicios Empresarial (ESB)

Implementado con **IBM IIB**, actúa como canal central de comunicación, facilitando la transformación y enrutamiento de mensajes.

API Gateway

Utilizando **APISIX**, centraliza el acceso a todas las APIs, aplicando políticas de seguridad y permitiendo el monitoreo del tráfico.

Plataforma de Mensajería

Apache Kafka gestiona la comunicación asíncrona y basada en eventos, mejorando la escalabilidad y resiliencia.

Servicios de Back-end

Sistema de Gestión de Riesgos

Analiza transacciones y perfiles para identificar riesgos, desarrollado en **Java** con motores de reglas.

Sistema de Prevención de Fraudes

Detecta patrones sospechosos utilizando **Python** y **Machine Learning**, procesando eventos en tiempo real.

Bases de Datos

Base de Datos Transaccional

Utiliza **Oracle, SQLServer** para almacenar operaciones transaccionales, con replicación y clustering para alta disponibilidad.

Data Warehouse

Implementado con **SQL Server Analysis Services**, almacena datos para análisis y reportes.

Bases de Datos NoSQL

MongoDB almacena datos no estructurados, **Redis** mejora el rendimiento como caché.

Sistemas Externos

APIs de Terceros (Open Finance)

Expuestas a través del **API Gateway**, permiten a terceros autorizados interactuar con servicios bancarios, utilizando **OAuth 2.0** para seguridad.

Servicios Regulatorios

Comunicación con organismos reguladores para envío de reportes y cumplimiento normativo.

Diagrama de Componentes

Nuevo Core Bancario Digital

En esta sección, se presenta el Nivel 3 del modelo C4, enfocado en el diagrama de componentes del Nuevo Core Bancario Digital. Este nivel proporciona una visión detallada de la arquitectura interna, mostrando cómo los diferentes módulos interactúan para ofrecer funcionalidades bancarias modernas y seguras.

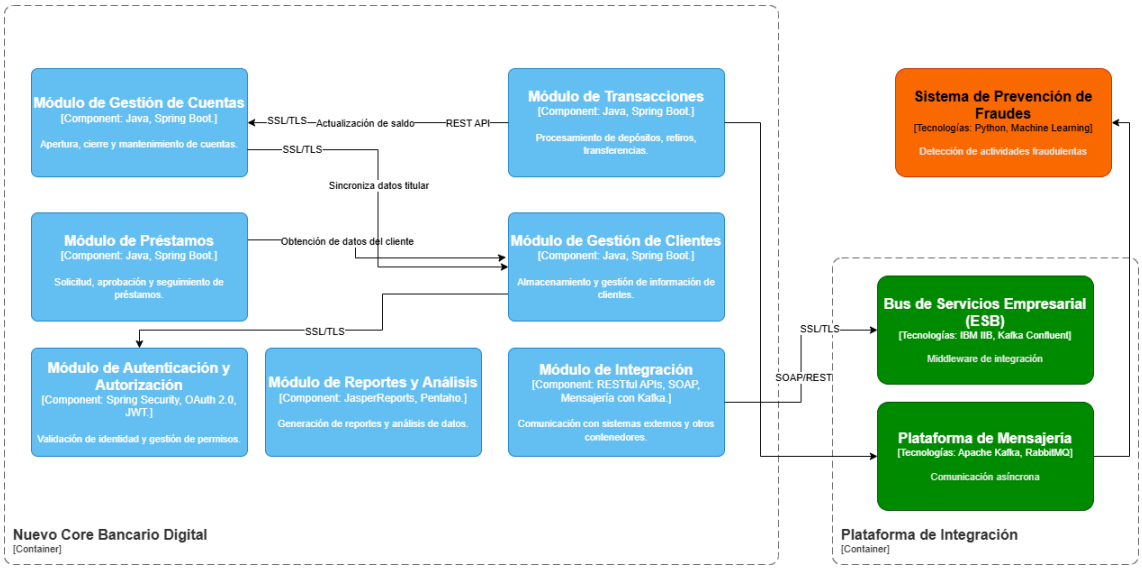

Ilustración 3. Diagrama de componentes Nuevo Core Bancario

El diagrama de componentes (ver Ilustración 3) indica los módulos principales y sus interacciones. El **Módulo de Gestión de Cuentas** se encarga de la apertura, cierre y mantenimiento de cuentas bancarias, gestionando distintos tipos de cuentas como ahorros, corrientes e inversiones. Actualiza información de cuentas y balances, y está desarrollado en Java con Spring Boot, utilizando una base de datos Oracle. Este módulo interactúa con el **Módulo de Transacciones** para validar y actualizar saldos, se comunica con el **Módulo de Gestión de Clientes**

para asociar cuentas a clientes y proporciona datos al **Módulo de Reportes y Análisis** para la generación de informes financieros.

El **Módulo de Gestión de Clientes** almacena y gestiona la información personal y financiera de los clientes, verificando identidades y actualizando datos. También desarrollado en Java con Spring Boot y Oracle, interactúa con el **Módulo de Autenticación y Autorización** para gestionar credenciales y accesos, colabora con el **Módulo de Gestión de Cuentas** en la asociación de cuentas a clientes y proporciona datos al **Módulo de Préstamos** para evaluaciones crediticias.

El **Módulo de Autenticación y Autorización** es esencial para controlar el acceso a todos los demás módulos, implementando protocolos como OAuth 2.0 y utilizando tokens JWT para garantizar que solo usuarios autenticados y autorizados puedan acceder a las funcionalidades del sistema. Soporta autenticación multifactor y se integra con servicios de autenticación externos para mayor seguridad.

El **Módulo de Transacciones** procesa depósitos, retiros y transferencias, validando fondos y límites, y registrando transacciones. Utiliza Apache Kafka para publicar eventos de transacciones que son consumidos por el **Sistema de Prevención de Fraudes**, permitiendo el análisis en tiempo real y la detección de actividades fraudulentas.

El **Módulo de Préstamos** gestiona solicitudes y aprobaciones de préstamos, evaluando el riesgo crediticio en colaboración con el **Sistema de Gestión de Riesgos**. Gestiona desembolsos y cobros a través del **Módulo de Gestión de Cuentas** y proporciona información al **Módulo de Reportes y Análisis** sobre la cartera de préstamos.

El **Módulo de Reportes y Análisis** genera informes operativos, financieros y regulatorios, recopilando datos de todos los módulos internos. Utiliza herramientas como JasperReports y Pentaho, y se integra con sistemas de Business Intelligence para apoyar la toma de decisiones estratégicas.

El **Módulo de Integración** gestiona la comunicación con sistemas externos y legados, exponiendo APIs para terceros y socios comerciales. Utiliza RESTful APIs, SOAP y mensajería con Apache Kafka, facilitando la integración con el Bus de Servicios Empresarial (ESB) y permitiendo a fintechs y partners acceder a servicios del banco.

Estrategia para garantizar alta disponibilidad y recuperación ante desastres

Se implementa una arquitectura de microservicios desplegada en una infraestructura distribuida y redundante. Los servicios se ejecutan en contenedores Docker, orquestados mediante Kubernetes, lo que permite distribuir las cargas de trabajo en múltiples nodos dentro de un clúster. Esta configuración elimina puntos únicos de falla, ya que si un nodo o servicio falla, Kubernetes reasigna automáticamente las cargas a otros nodos disponibles, manteniendo el servicio en funcionamiento.

Para mitigar riesgos asociados a desastres naturales o fallos de infraestructura en una ubicación específica, se realiza un despliegue geográficamente distribuido en múltiples zonas de disponibilidad y regiones. Esto implica que los servicios y datos críticos se replican en diferentes centros de datos físicamente separados.

Se utilizan balanceadores de carga a nivel de red y aplicación para distribuir el tráfico entre las diferentes instancias de los servicios. Esto no solo optimiza el rendimiento, sino que también facilita el failover automático. Si una instancia de servicio deja de responder, el balanceador de carga detecta la falla mediante verificaciones de salud y redirige el tráfico a las instancias operativas restantes, garantizando la continuidad del servicio.

Se implementan sistemas de monitoreo y observabilidad que supervisan continuamente el rendimiento, disponibilidad y estado de los servicios y la infraestructura. Herramientas como Prometheus y Grafana recopilan métricas y generan dashboards en tiempo real. Se configuran alertas que notifican al equipo de operaciones sobre anomalías, fallos o degradación del rendimiento, permitiendo una respuesta rápida antes de que los problemas afecten a los usuarios finales.

Para cumplir todos estos aspectos se debe desarrollar un Plan de Recuperación ante Desastres que define procedimientos detallados para restaurar los servicios en caso de una interrupción mayor. Esto incluye incluye:

- **Análisis de Impacto en el Negocio**: Identifica las funciones críticas y establece prioridades para la recuperación.
- **Objetivos de Tiempo de Recuperación y Punto de Recuperación**: Define el tiempo máximo aceptable para la restauración de servicios y la pérdida máxima de datos tolerable.
- **Procedimientos de Recuperación**: Pasos específicos para restaurar sistemas y datos, incluyendo roles y responsabilidades.
- **Comunicación y Coordinación**: Protocolos para mantener informados a los equipos internos, clientes y partes interesadas durante y después de un incidente.

Modelo de gobierno de APIs y servicios

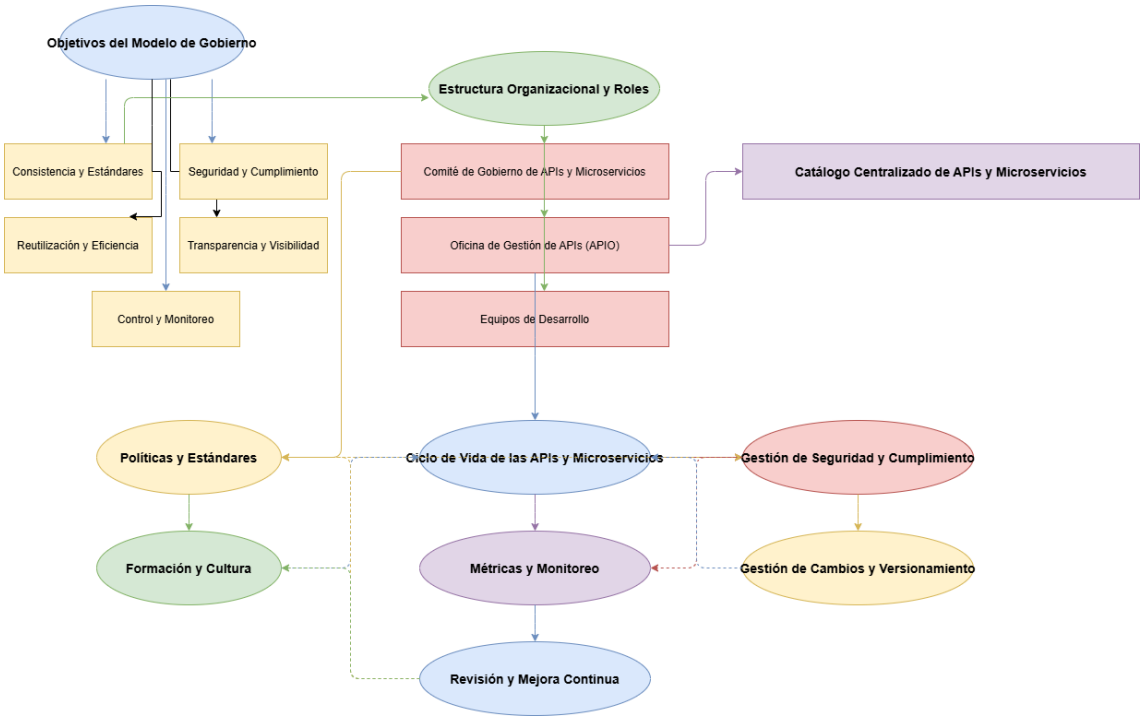

Ilustración 4. Modelo de Gobierno de APIs y microservicios

El modelo de gobierno para APIs y microservicios es esencial en una organización bancaria para garantizar que su desarrollo, implementación y mantenimiento se realicen de manera consistente y alineada con los objetivos del negocio y las políticas de seguridad. Este modelo establece objetivos claros, como la consistencia y estándares en el diseño y documentación, seguridad y cumplimiento normativo (incluida la Ley Orgánica de Protección de Datos Personales), reutilización y eficiencia de componentes, transparencia y visibilidad mediante un inventario actualizado, y control y monitoreo proactivo del rendimiento y uso de las APIs y microservicios.

La estructura organizacional propuesta incluye un **Comité de Gobierno de APIs y Microservicios**, encargado de definir políticas y estrategias, conformado por representantes de Tecnología, Seguridad, Cumplimiento, Negocio y Arquitectura. La **Oficina de Gestión de APIs (APIO)** es responsable de implementar estas políticas, coordinar el ciclo de vida de las APIs, proporcionar soporte a los equipos de desarrollo y mantener el catálogo centralizado. Los **equipos de desarrollo** son quienes construyen y mantienen las APIs y microservicios siguiendo los estándares establecidos, colaborando estrechamente con la APIO. El ciclo de vida estándar abarca desde la planificación y diseño hasta el retiro, incluyendo fases de desarrollo, validación, despliegue, operación y monitoreo.

Se establecen políticas y estándares que deben seguir todos los equipos, cubriendo aspectos como el diseño de APIs (estilo RESTful, consistencia en nomenclatura, versionamiento), seguridad (autenticación y autorización con OAuth 2.0 y JWT, encriptación con HTTPS/TLS, gestión de claves), documentación accesible y actualizada, y prácticas de pruebas y calidad (cobertura de pruebas, análisis de código, revisión por pares). Un catálogo centralizado facilita la visibilidad y gestión de las APIs. La gestión de seguridad y cumplimiento incluye evaluaciones periódicas, políticas de acceso basadas en roles y gestión de incidentes. Además, se promueve una cultura de capacitación continua y colaboración, apoyada por herramientas y tecnologías de

soporte como plataformas de API Management y pipelines de CI/CD. La revisión y mejora continua del modelo permiten adaptarlo ante cambios tecnológicos o estratégicos, asegurando su efectividad y alineación con los objetivos del banco.