**Diagrama de Contexto del Sistema**

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.

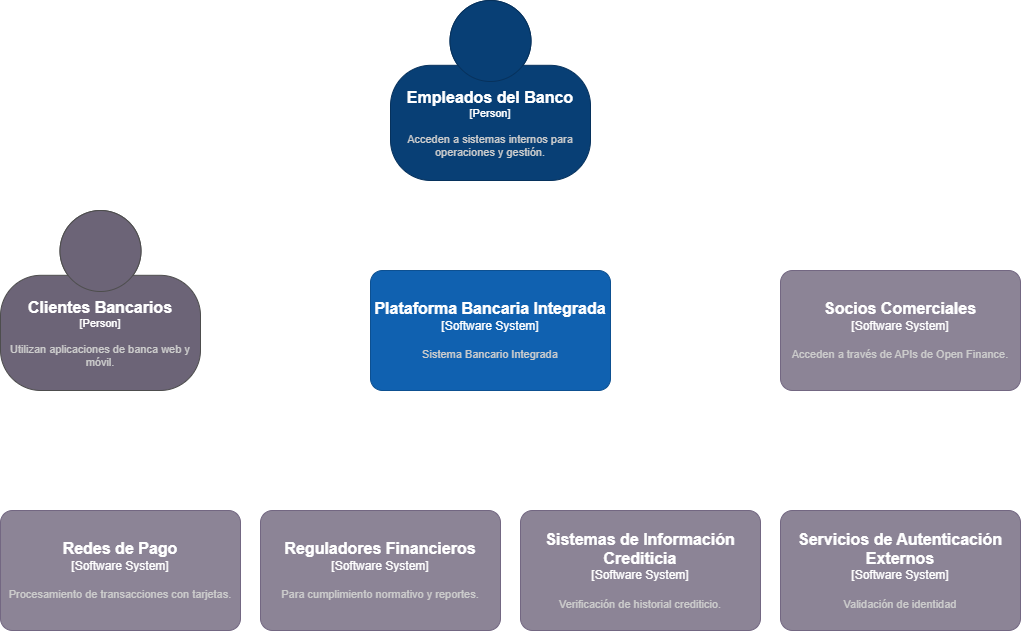
****

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.

1. **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.

1. **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.

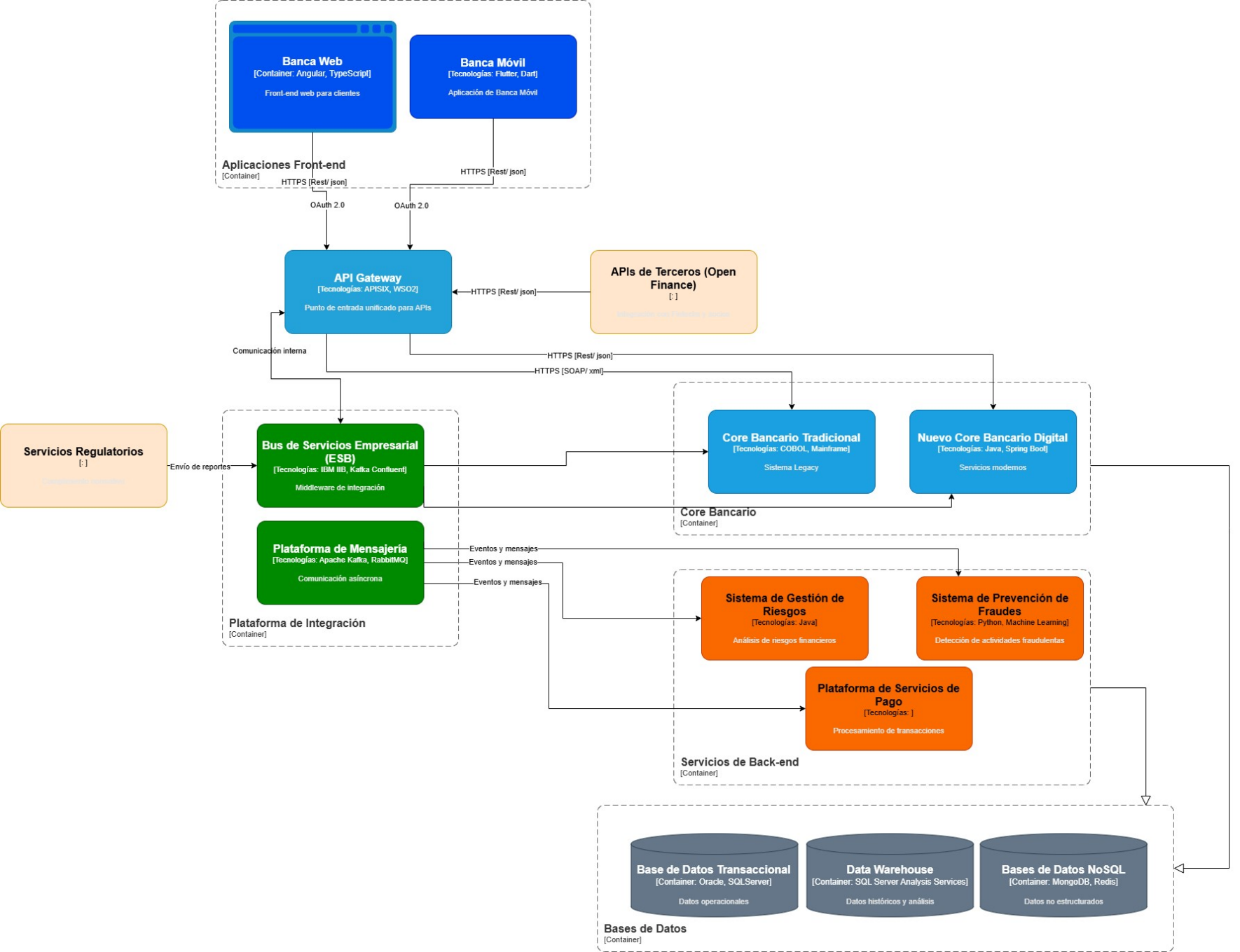


Ilustración 2. Diagrama de Contenedores

**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.