Diagrama de Contexto:

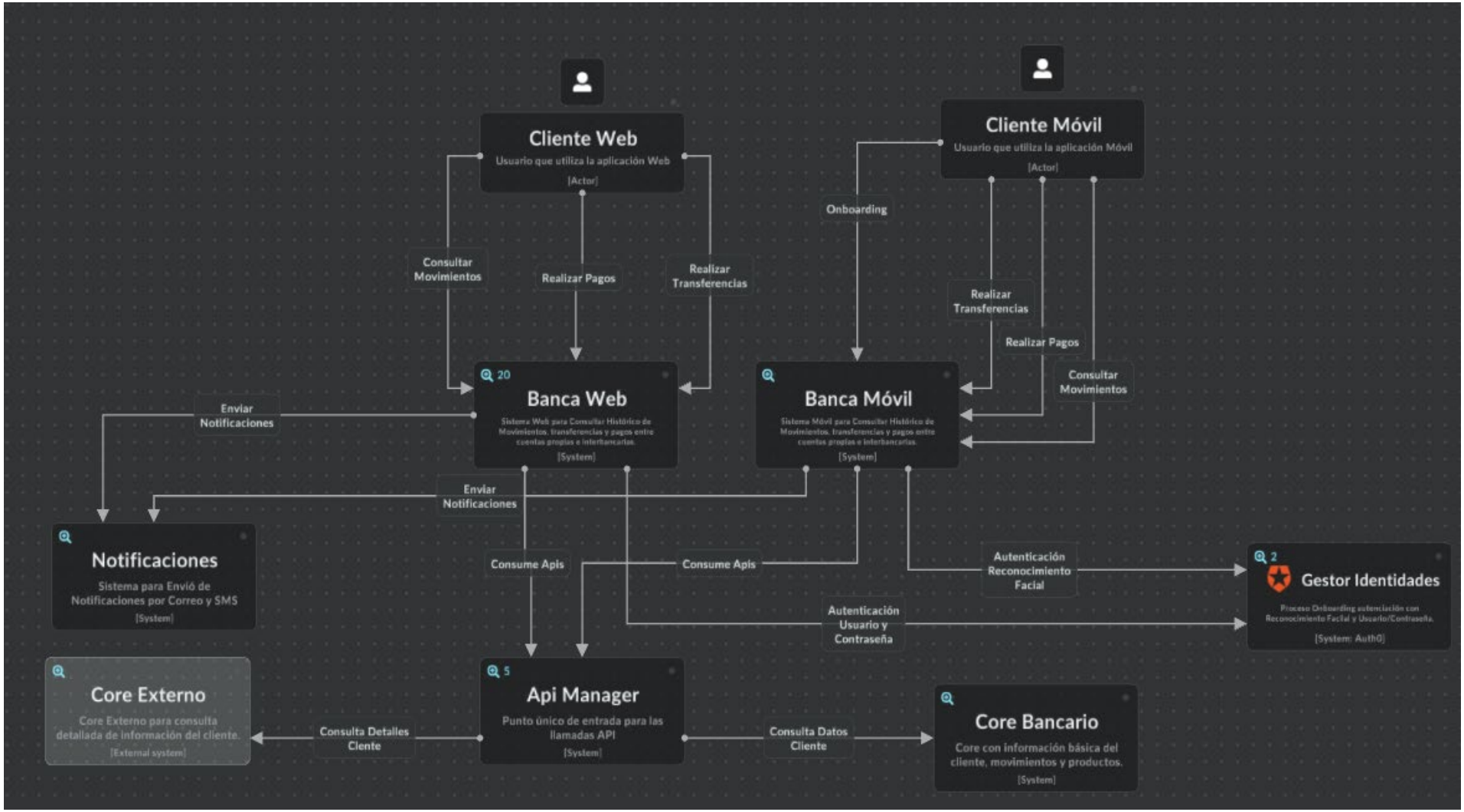


Diagrama de Contenedores:

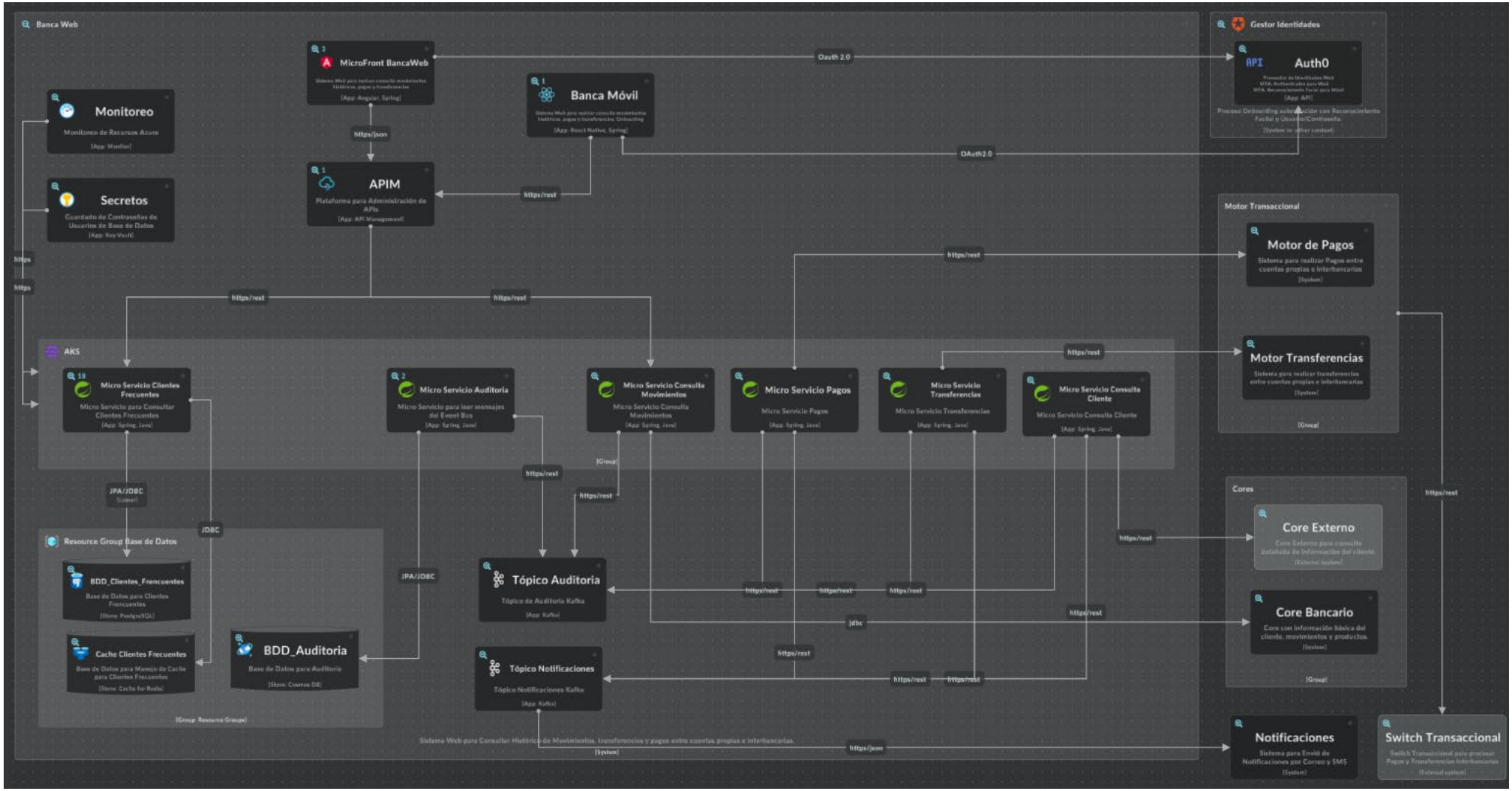


Diagrama de Componentes:

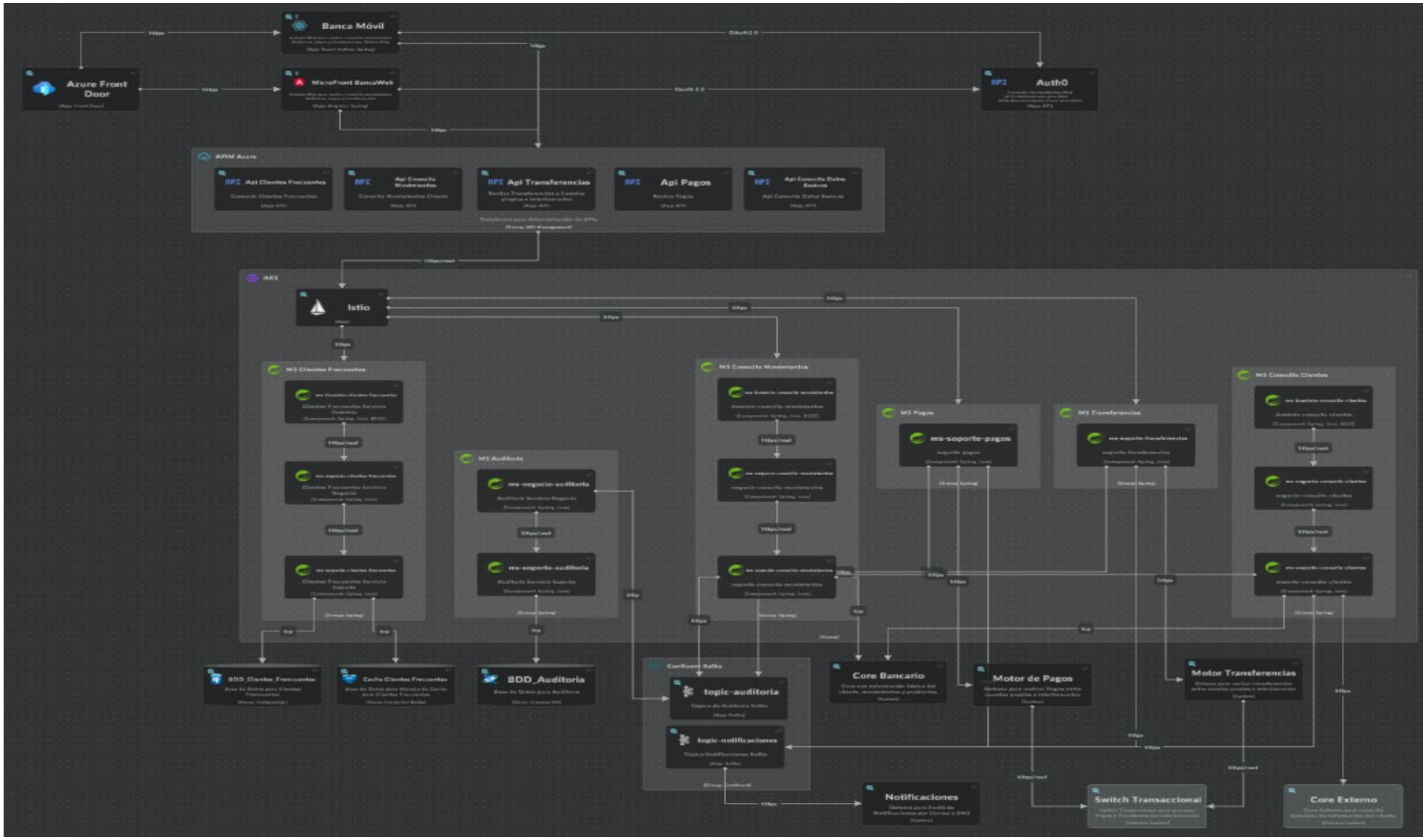
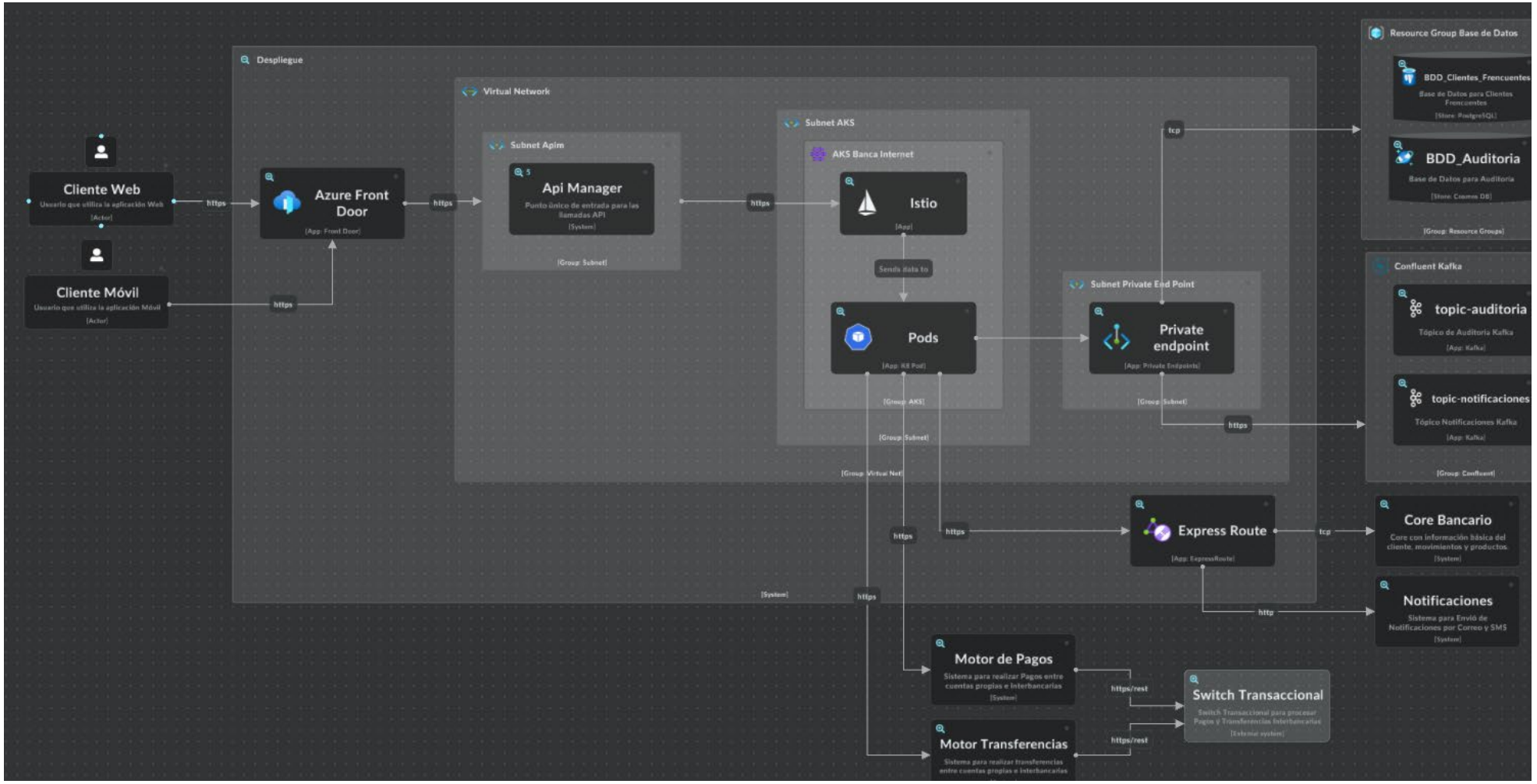

Banca Móvil
Azure Front Door
MicroFront BancaWeb
Auth0
APIM Azure
Api Clientes Frecuentes
Api Consulta Movimientos
Api Transferencias
Api Pagos
Api Consulta Datos Basicos
AKS
Istio
MS Clientes Frecuentes
MS Consulta Movimientos
MS Pagos
MS Transferencias
MS Consulta Clientes
MS Auditoria
ms-soporte-pagos
ms-negocio-auditoria
ms-soporte-auditoria
BDD_Clientes_Frecuentes
Cache Clientes Frecuentes
BDD_Auditoria
Confluent Kafka
topic-auditoria
topic-notificaciones
Core Bancario
Motor de Pagos
Motor Transferencias
Notificaciones
Switch Transaccional
Core Externo

Diagrama de Despliegue:



Flujo Recomendado para Autorización:

Flujo de Código de Autorización con PKCE(Proof Key for Code Exchange), en este flujo el usuario se redirecciona al servidor de autorización (Auth0, Azure Entra ID) para obtener un Código de autorización que se utiliza en el backend para obtener token de acceso a los recursos.

Este fujo de autorización se lo puede implementar en **Auth0.**

Consideraciones:

Elementos Normativos Entidades Financieras:

- **Ley Orgánica de Protección de Datos Personales:**
  Azure Key Vault: Servicio para gestionar y proteger secretos utilizados en aplicaciones.

  Protocolo HTTPS: Un sitio seguro con HTTPS significa que la información sensible, como las contraseñas o los datos bancarios está protegida.

- **Código Orgánico Monetario y Financiero:**
  Azure Monitor: Registrar la actividad de los recursos de Azure para detectar incidentes de seguridad y cumplir con los requisitos de auditoría.

- **Control para la Gestión Integral y Administración de Riesgos Super de Bancos:**
  Auth0: Gestionar la identidad y el acceso a los recursos para que solo las personas autorizadas puedan acceder a información sensible.

- **Normas de Control de la Superintendencia de Bancos:**
  Sistema Notificaciones: Comunicarse con los clientes de manera segura y eficiente.

Alta Disponibilidad, Tolerancia a Fallos:

- Utilizar varias zonas de disponibilidad de Azure.
- Balanceo de carga para distribuir la carga (**Api Manager de Azure**).
- Escalado automático según la demanda (**Azure Kubernetes Services**).
- Escalado horizontal de los Pods (**Horizontal Pod Autoscale en AKS**).
- Réplica automática de Base de Datos (**Azure Cosmos DB para Postgress**).
- Configurar límites para CPU y memoria de los Pods (**Azure Kubernetes Services**).

Recuperación ante Desastres (DR):

- Realizar respaldos automáticos de bases de datos (**Azure Cosmos DB for PostgreSQL**).
- Guardar copias de seguridad en lugares seguros.
- Réplica de datos en varias ubicaciones (**Azure Cosmos DB for PostgreSQL**).
- Utilizar herramientas de virtualización y contenerización (**Azure Kubernetes Services**).

Monitoreo:

- Utilizar herramientas de monitoreo para verificar los tiempos de respuesta, disponibilidad y uso de recursos (**Azure Monitor**).
- Crear alertas para recibir notificaciones (**Azure Monitor**).
- Revisar logs de la aplicación para detectar posibles errores (**Azure Monitor**).