

Devsu LLC

Diseño de Soluciones utilizando el Modelo C4

El **modelo C4** es un enfoque visual para documentar y comunicar la **arquitectura de software** de forma clara y estructurada.

Un buen diagrama de arquitectura de software facilita la comunicación a los equipos de desarrollo y producto, la idea principal es que los diagramas puedan ser entendidos e interpretados por equipos técnicos y no técnicos.

Cuenta con **cuatro niveles de abstracción**, de ahí su nombre:

- Nivel 1: Diagrama de **Contexto**.
- Nivel 2: Diagrama de **Contenedores**
- Nivel 3: Diagrama de **Componentes**
- Nivel 4: Diagrama de **Código** (opcional)

Estos permiten mejorar la documentación de proyectos completos a fin de que la audiencia pueda comprender en qué consiste, como está conformado y cómo se interrelaciona con otros sistemas o servicios.

Repositorio en Github:

<https://github.com/luisalbespgav/aplicardevsu.git>

Objetivo:

Diseñar un **Sistema de Banca por internet**, que permita:

- Crear clientes
- Consultar Información de los clientes
- Realizar transferencias bancarias e interbancarias
- Realizar pagos con debido a cuenta
- Configuración de cupos para transferencias
- Consulta de movimientos Histórico

Consideraciones:

Realizaremos un Análisis y Diseño de un Sistema de Banca Electrónica Web de una entidad BP, considerando los siguientes aspectos:

1. Solo puede ser accedido por clientes del banco
2. Cuenta con un esquema de autenticación y autorización (Azure Entra ID)
3. Cuenta con un modelo de factor de autenticación mediante OTP (Contraseña de un Solo Uso) que se enviará al teléfono celular del usuario como SMS o Push Notification, o email
4. La OTP tiene un tiempo de vigencia de 3 minutos, caso contrario caduca y deniega el acceso
5. Valida que el usuario se encuentre activo en el banco
6. El sistema permite consultar Posición Consolidada y Estados de Cuenta considerando el histórico de movimientos de los clientes
7. Cuenta con una base de datos de Core Bancario y una base de datos de Master Data Management (MDM) con información adicional y detallada del cliente
8. Permite consultar y actualizar cupos para transacciones y pagos de las cuentas de clientes
9. Permite realizar transferencias bancarias e interbancarias
10. Permite realizar pagos de servicios con debido a cuenta
11. Envía un mensaje al usuario (cliente) como SMS o Push Notification, o email, cuando se ha realizado una transacción bancaria
12. Permite guardar logs de auditoría del sistema y transaccionales en un repositorio como Elasticsearch
13. Debe manejar esquemas de anonimización y cifrado para datos sensibles, especialmente los del cliente
14. Debe permitir el registro y uso de acceso biométrico

Fuera de alcance y suposiciones:

1. Se asume que BP cuenta con instalaciones físicas como oficinas y personal no técnico
2. Se asume que BP ya cuenta con computadores para las agencias y solo se requiere para el personal técnico
3. Se asume que BP cuenta con las instalaciones para el desarrollo de Software
4. Se asume que BP no cuenta con licencias y herramientas de desarrollo

Racional Técnico.

Se considera que la solución debe contener las últimas tecnologías del medio, considerando que:

- Estén respaldadas por una empresa o comunidad que garantice su seguridad y continuidad
- Cuenten con certificaciones de seguridad
- Tengan varios años en el mercado considerando la aceptación de empresas y usuarios
- Sean tecnologías multiplataformas
- Estén actualizándose constantemente
- Estén siendo utilizadas por otros bancos

Se considera utilizar tecnologías en la nube en nuestro caso Azure como parte de la solución, debido a que ofrece múltiples ventajas sobre infraestructura On-premise, entre las más importantes destacamos:

- **Escalabilidad y flexibilidad:** La nube permite a las empresas aumentar o disminuir la capacidad de procesamiento de sus aplicaciones según sea necesario, adaptándose a picos de demanda o a cambios en el tráfico. Adicionalmente preparar un servidor en la nube toma minutos con cualquier configuración que se requiera en comparación con On-premise.
- **Mayor velocidad de desarrollo:** facilita el acceso a herramientas y servicios preconfigurados, lo que acelera el proceso de desarrollo y permite a los equipos enfocarse en la innovación.
- **Fácil Acceso global y movilidad:** Se puede acceder a las aplicaciones y datos, y configuración de Nube, desde cualquier lugar solo con una conexión a internet, lo que fomenta la colaboración y la flexibilidad.
- **Reducción de costos:** Se paga solo por los recursos que se utilizan, la nube puede reducir significativamente los costos de infraestructura, mantenimiento y personal. Adicionalmente al contratar un servidor ya cuenta con las licencias de software

Seguridad.

Con el fin de garantizar la seguridad de la información de los clientes, se considera utilizar:

- Protocolos de comunicación HTTPS (NO HTTP)
- Servicio de Akamai como herramienta WAF (Firewall de Aplicaciones Web) y prevención de ataque DDoS (Ataque de Denegación de Servicio Distribuido)
- Servicio recaptcha para proteger de bots que quieran acceder a la aplicación indebidamente
- Anonimizar y/o cifrar datos sensibles de los clientes
- Servicio de cifrado de datos del lado del cliente y del servidor cuando se lo requiera. Azure Cipher.
- Servicio de Azure Key Vault, que es un servicio que permite la gestión segura de claves de cifrado y secretos

Tarjetas de Pago.

Existe un estándar de seguridad de la industria de Tarjetas de Pago (Débito y Crédito) llamado **PCI DSS (Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago)**, se refiere a un conjunto de normas y requisitos de seguridad diseñados para proteger la información de tarjetas de crédito y débito durante su procesamiento y almacenamiento.

PCI DSS es administrado por el **PCI SSC** (Payment Card Industry Security Standards Council), formado por un consorcio de las principales compañías de tarjetas de crédito: Mastercard, Visa, Discover, American Express y JCB, por lo cual cualquier institución financiera relacionada a estas marcas debe cumplir PCI SSC. El cumplimiento con PCI se aplica globalmente a todo vendedor que acepte tarjetas de crédito, débito o prepago.

PCI DSS aborda una serie de amenazas, entre las que se incluyen las siguientes:

- Malware
- Phishing
- Autenticación y control de acceso remoto
- Contraseñas poco seguras
- Software heredado
- Robo de tarjetas

Para nuestro caso no estamos considerando el uso de tarjetas de pago, más sin embargo en caso de requerir el uso de PCI SSC es fácilmente aplicable debido a que la solución planteada cuenta con todos los complementos que ayudan a la seguridad de tratamiento y transporte de datos (HTTPS, Akamai, Cifrado de lado de cliente y servidor), y se cuenta con toda la información de los clientes para poder transmitir en los mensajes **ISO 8583** que son aceptados por las Tarjetas de Crédito, Débito y Prepago.

Ambientes de No Productivos y Productivos.

Se considera contar con 3 ambientes para garantizar la calidad del producto:

➤ **Ambiente de Desarrollo o Develop (No Productivo).**

Ambiente controlado por los desarrolladores con el fin de poder realizar:

- Desarrollo
- Pruebas Unitarias
- Pruebas en pares

➤ **Ambiente de Test o Pruebas (No Productivo)**

Ambiente pre-productivo que permite desplegar los desarrollos realizados por los desarrolladores a fin de probarlos en un ambiente controlado y que el Ingeniero QA pueda validar que el producto cumpla con los requerimientos solicitados.

Debe considerarse que el ambiente de Test debe ser muy parecido al ambiente de Producción, esto significa en cuanto a las condiciones: Balanceador, Capa Media, Base de Datos, Componentes de Red, etc.

Generalmente el tamaño del ambiente de Test es un 20% de la capacidad que tiene el ambiente de Producción.

➤ **Ambiente de Producción (Productivo)**

Ambiente final donde se despliega la solución que va a ver el usuario final.

Debe constar con balanceadores y despliegues en varios nodos a fin de garantizar la Alta disponibilidad.

En caso que sea una aplicación en nube, debe considerarse que la aplicación esté desplegada en diferentes Regiones y/o Zonas, con el fin de que, si resulta una falla o catástrofe en la zona principal, entonces redireccionar a una zona secundaria a fin de garantizar Contingencia.

Existe el **Análisis de Impacto Empresarial (BIA)** que es un proceso sistemático que identifica y analiza las posibles consecuencias de las interrupciones en las funciones críticas del negocio Ayuda a las organizaciones a comprender cómo un desastre, accidente o emergencia podría afectar sus operaciones y proporciona la base para desarrollar estrategias de recuperación.

Análisis Financiero.

Dentro de la solución se consideran el siguiente análisis de Capacidad considerando aquellos CAPEX y OPEX.

CAPEX: Son **Gastos de Capital** o también bienes adquiridos por BP

OPEX: Son **Gastos Operativos** o también bienes alquilados

CAPEX (De Capital)	OPEX (Operacionales)
Compra de Computadores para personal técnico: Desarrolladores, Arquitectos, DevOps, Ingenieros QA, Líderes técnicos, Administradores de Datos, Scrum Master y Product Owners	Alquiler en nube de infraestructura en la nube (IASS)
Cableado Estructurado incluyendo dispositivos de comunicación: Switchs, Routers, Modems, IPs	Alquiler en nube de Plataformas en la nube (PASS)
	Alquiler de Redes WAN/LAN: VPN, Internet, Intranet
	Alquiler en nube de servicios de Autenticación y Autorización, Administración de Usuarios, Envío de Mensajes, etc.
	Alquiler de una plataforma de desarrollo y pruebas en nube para desarrollar la solución

Metodología y Equipos de Trabajo.

Se ha demostrado que los equipos de trabajo Agiles (SCRUM) versus los tradicionales, tienen mejor desempeño en cuanto a los resultados, debido a que se basan en equipos auto disciplinados que priorizan un backlog a fin de construir MVPs (Mínimos Productos Viables) a fin de ir construyendo piezas de legos que conformen un producto final.

Los equipos ágiles priorizan la flexibilidad, la colaboración y la entrega iterativa, adaptándose a los cambios en los requisitos del cliente y entregando valor de forma incremental.

Estimación Alto nivel.

Se considera la siguiente estimación a alto nivel con los costos referenciales de la nube en Azure:

INFRAESTRUCTURA EN LA NUBE DCP y DCA	COSTO MENSUAL
Alquiler en nube de Servidores que requieran configuración personalizada en la nube (IASS). Se debe contratar un Clúster de servidores. Servidores que requieran administración de puertos o configuración personalizada de las aplicaciones, aplica a: - Aplicaciones de usuario - Integración con aplicaciones o servicio externos	18,500
Alquiler en nube de Servidores listos para su uso en la nube (PaaS). Se debe contratar un Clúster de servidores. Se incluye Sistema Operativo y configuración predeterminada Otras aplicaciones - Oracle Database: Base de datos - Elasticsearch	25,000
Alquiler de servicio de Networking, Canales de comunicación entre Servidores, y otros componentes de seguridad como en Azure como: - Azure Virtual Network: VPN - Azure ExpressRoute: Conectividad de red privada de la red corporativa a la nube - Azure Virtual WAN: Conectar oficinas y sitios de forma segura con un portal unificado - Azure VPN Gateway: Utilizar Internet de forma segura para acceder a las redes virtuales de Azure - Azure Network Function Manager: Ampliar la administración de Azure para implementar funciones de red 5G y SD-WAN en dispositivos perimetrales - Azure Application Gateway: Equilibrador de carga de tráfico web - Firewalls	12,000
Alquiler en nube de servicios de Autenticación y Autorización, Administración de Usuarios, Envío de Mensajes, etc. - Azure Entra ID - OAuth 2.0 - Facephi - Kafka - Azure Key Vault - Azure Communication Services: Envío de mensajes SMS, Notification, email. - Akamai: Balanceador, CDN y Seguridad WAF (Firewall) y anti DDoS - dynatrace: monitoreo	4,500
Alquiler de una plataforma de desarrollo y pruebas en nube para desarrollar la solución:	9,500
	TOTAL MENSUAL
	69,500
	TOTAL ANUAL
	834,000

Equipos de Trabajo:

Para desarrollar el proyecto de BP, deben conformarse equipos SCRUM, que se enfoque en definir un backlog y trabaje en Hitos (MVPs) a fin de ir construyendo la solución que requiere BP.

Por el tamaño del proyecto se considera crear Sprints de 2 semanas a fin de garantizar el entregable.

Se recomienda crear equipos SCRUM cuyos miembros deben estar conformados por:

MIEMBROS	Número	RESPONSABILIDAD	COSTO UNITARIO	COSTO MENSUAL
PO (Product Owner)	1	Encargado de definir y priorizar el Backlog para el equipo	5,000	5,000
Arquitecto	1	Encargado de realizar las definiciones técnicas para entregarlas al equipo de desarrollo. Realizar avanzadas técnicas	4,000	4,000
Desarrollador Front End	1	Desarrollar las pantallas para las aplicaciones, considerando temas de seguridad y aplicando estándares	3,000	3,000
Desarrollador Back End	1	Desarrollar la aplicación de backend para las aplicaciones, considerando temas de seguridad y aplicando estándares, estas deben contener lógica y deben integrarse a las APIs de Negocio	3,000	3,000
Desarrollador Capa Media	2	Desarrollar APIs de Negocio y Microservicios que contengan la lógica de negocio y	3,000	6,000
QA	1	Encargado de realizar las pruebas del sistema a fin de garantizar su calidad.	3,000	3,000
		TOTAL MENSUAL		24,000
		TOTAL ANUAL		288,000

Se debe considerar equipos de apoyo que apoyen a los equipos de trabajo para garantizar el cumplimiento de los hitos planificados:

MIEMBROS	Número	RESPONSABILIDAD	COSTO UNITARIO	COSTO MENSUAL
Project Management	2	Managers de Proyectos que coordina con los equipos SCRUM que los avances de los proyectos vayan de acuerdo a los cronogramas	6,000	12,000
Líder Técnico	2	Manager Técnico de Proyectos, que coordina con los equipos SCRUM y establece un gobierno para coordinar que los desarrollos se integren. Es Facilitador Técnico. Establece Gobiernos para que no se realice trabajo duplicado, especialmente en la Capa Media.	5,000	10,000
Scrum Master	3	Facilitadores y garantizar que los equipos cumplan con el Marco Agile	3,000	9,000
Devops	3	Encargado de despliegues a ambientes de Pruebas y Producción. Preparación de servidores y componentes en nube para los proyectos.	3,000	9,000
Administradores BDD	2	Encargado de Administrar las Bases de Datos, asegurar los respaldos y sincronización de datos entre DCP y DCA	3,000	6,000
Administradores Plataformas	2	Encargado de Administrar los servidores, networking, tanto de nube como On-premise, asegurar los respaldos y sincronización de aplicaciones entre DCP y DCA	3,000	6,000
Seguridad	3	Garantizar la seguridad de cada desarrollo antes de ponerlo en producción	3,000	9,000
Normativas	3	Asegurar el cumplimiento de los informes que deben entregarse a los Entes de Control, y aplicar las nuevas normativas	3,000	9,000
		TOTAL MENSUAL		70,000
		TOTAL ANUAL		840,000

Se considera que el proyecto debe estar construido en un año calendario, para lo cual se considera tener al menos 6 equipos de Trabajo y un equipo de apoyo:

EQUIPO	Número	RESPONSABILIDAD	COSTO UNITARIO	COSTO MENSUAL
Equipos SCRUM	6	Desarrollo de Sistema de Banca por internet	24,000	144,000
Equipo de apoyo	1	Asegurar la metodología y cumplimiento del proyecto en cada Etapa o Fase. Mantenimiento de la Plataforma.	70,000	70,000
		Infraestructura de Servidores y Red DCP y DCA		69,500
		TOTAL MENSUAL		283,500
		TOTAL ANUAL		3,402,000

El proyecto al primer año tendría una estimación aproximada de \$3.402.000 (tres millones cuatrocientos dos mil) dólares americanos.

Cronograma de Actividades:

A continuación, se detalla un cronograma con las actividades y tareas del equipo SCRUM, y otros actores intervenientes en el proyecto.

Consideraciones:

- Se consideran Sprints de 2 semanas con el fin de garantizar los entregables
- Se consideran todas las ceremonias Scrum
- Diariamente se realiza la Ceremonia de Daily de 15 minutos para alinear al equipo Scrum
- No se están considerando días festivos
- Solo se despliega a ambiente productivo el fin de semana correspondiente al segundo sprint de cada mes. Se despliega el desarrollo del Sprint 1 y 2.

17	Despliegue Ambiente Productivo	DevOps, Desarrolladores, QA, arquitecto	9	26/9/2026	27/9/2026																	
18	Marco Ágil Ceremonia 1: Planning	Todo el equipo SCRUM	9	28/9/2026	28/9/2026																	
18	Desarrollo de la Aplicación Sistema de Banca por internet	Desarrolladores, Arquitecto	10	29/9/2026	5/10/2026																	
18	Preparación de pruebas QA	QA, PO, Arquitecto	10	29/9/2026	5/10/2026																	
18	Despliegue a ambientes de Test 1	DevOps, desarrolladores	10	6/10/2026	6/10/2026																	
18	Ejecutar Pruebas QA	QA, desarrolladores	10	7/10/2026	7/10/2026																	
18	Ajustes Desarrollo	Desarrolladores, Arquitecto	10	8/10/2026	8/10/2026																	
18	Despliegue a ambientes de Test 2	DevOps, desarrolladores	10	8/10/2026	8/10/2026																	
18	Ejecutar Pruebas QA 2	QA, desarrolladores	10	9/10/2026	9/10/2026																	
18	Definición de Backlog para siguiente Sprint	PO, Arquitecto	10	30/9/2026	2/10/2026																	
18	Desglose en HU, Tareas y Actividades	Arquitecto	10	2/10/2026	6/10/2026																	
18	Avanzada Backlog	Todo el equipo SCRUM	10	9/10/2026	9/10/2026																	
18	Marco Ágil Ceremonia 2: Sprint Review	Todo el equipo SCRUM	10	9/10/2026	9/10/2026																	
18	Marco Ágil Ceremonia 3: Sprint Retrospectiva	Todo el equipo SCRUM	10	9/10/2026	9/10/2026																	
19	Marco Ágil Ceremonia 1: Planning	Todo el equipo SCRUM	10	12/10/2026	12/10/2026																	
19	Desarrollo de la Aplicación Sistema de Banca por internet	Desarrolladores, Arquitecto	10	13/10/2026	19/10/2026																	
19	Preparación de pruebas QA	QA, PO, Arquitecto	10	13/10/2026	19/10/2026																	
19	Despliegue a ambientes de Test 1	DevOps, desarrolladores	10	20/10/2026	20/10/2026																	
19	Ejecutar Pruebas QA	QA, desarrolladores	10	21/10/2026	21/10/2026																	
19	Ajustes Desarrollo	Desarrolladores, Arquitecto	10	22/10/2026	22/10/2026																	
19	Despliegue a ambientes de Test 2	DevOps, desarrolladores	10	22/10/2026	22/10/2026																	
19	Ejecutar Pruebas QA 2	QA, desarrolladores	10	23/10/2026	23/10/2026																	
19	Definición de Backlog para siguiente Sprint	PO, Arquitecto	10	14/10/2026	16/10/2026																	
19	Desglose en HU, Tareas y Actividades	Arquitecto	10	16/10/2026	20/10/2026																	
19	Avanzada Backlog	Todo el equipo SCRUM	10	23/10/2026	23/10/2026																	
19	Marco Ágil Ceremonia 2: Sprint Review	Todo el equipo SCRUM	10	23/10/2026	23/10/2026																	
19	Marco Ágil Ceremonia 3: Sprint Retrospectiva	DevOps,	10	24/10/2026	25/10/2026																	
19	Despliegue Ambiente Productivo	Desarrolladores, QA, arquitecto	10	24/10/2026	25/10/2026																	
20	Marco Ágil Ceremonia 1: Planning	Todo el equipo SCRUM	10	26/10/2026	26/10/2026																	
20	Desarrollo de la Aplicación Sistema de Banca por internet	Desarrolladores, Arquitecto	11	27/10/2026	2/11/2026																	
20	Preparación de pruebas QA	QA, PO, Arquitecto	11	27/10/2026	2/11/2026																	
20	Despliegue a ambientes de Test 1	DevOps, desarrolladores	11	3/11/2026	3/11/2026																	
20	Ejecutar Pruebas QA	QA, desarrolladores	11	4/11/2026	4/11/2026																	
20	Ajustes Desarrollo	Desarrolladores, Arquitecto	11	5/11/2026	5/11/2026																	
20	Despliegue a ambientes de Test 2	DevOps, desarrolladores	11	5/11/2026	5/11/2026																	
20	Ejecutar Pruebas QA 2	QA, desarrolladores	11	6/11/2026	6/11/2026																	
20	Definición de Backlog para siguiente Sprint	PO, Arquitecto	10	28/10/2026	30/10/2026																	
20	Desglose en HU, Tareas y Actividades	Arquitecto	11	30/10/2026	3/11/2026																	
20	Avanzada Backlog	Todo el equipo SCRUM	11	6/11/2026	6/11/2026																	
20	Marco Ágil Ceremonia 2: Sprint Review	Todo el equipo SCRUM	11	6/11/2026	6/11/2026																	
20	Marco Ágil Ceremonia 3: Sprint Retrospectiva	Todo el equipo SCRUM	11	6/11/2026	6/11/2026																	
21	Marco Ágil Ceremonia 1: Planning	Todo el equipo SCRUM	11	9/11/2026	9/11/2026																	
21	Desarrollo de la Aplicación Sistema de Banca por internet	Desarrolladores, Arquitecto	11	10/11/2026	16/11/2026																	
21	Preparación de pruebas QA	QA, PO, Arquitecto	11	10/11/2026	16/11/2026																	
21	Despliegue a ambientes de Test 1	DevOps, desarrolladores	11	17/11/2026	17/11/2026																	
21	Ejecutar Pruebas QA	QA, desarrolladores	11	18/11/2026	18/11/2026																	
21	Ajustes Desarrollo	Desarrolladores, Arquitecto	11	19/11/2026	19/11/2026																	
21	Despliegue a ambientes de Test 2	DevOps, desarrolladores	11	19/11/2026	19/11/2026																	
21	Ejecutar Pruebas QA 2	QA, desarrolladores	11	20/11/2026	20/11/2026																	
21	Definición de Backlog para siguiente Sprint	PO, Arquitecto	11	11/11/2026	13/11/2026																	
21	Desglose en HU, Tareas y Actividades	Arquitecto	11	13/11/2026	17/11/2026																	
21	Avanzada Backlog	Todo el equipo SCRUM	11	20/11/2026	20/11/2026																	
21	Marco Ágil Ceremonia 2: Sprint Review	Todo el equipo SCRUM	11	20/11/2026	20/11/2026																	
21	Marco Ágil Ceremonia 3: Sprint Retrospectiva	Todo el equipo SCRUM	11	2																		

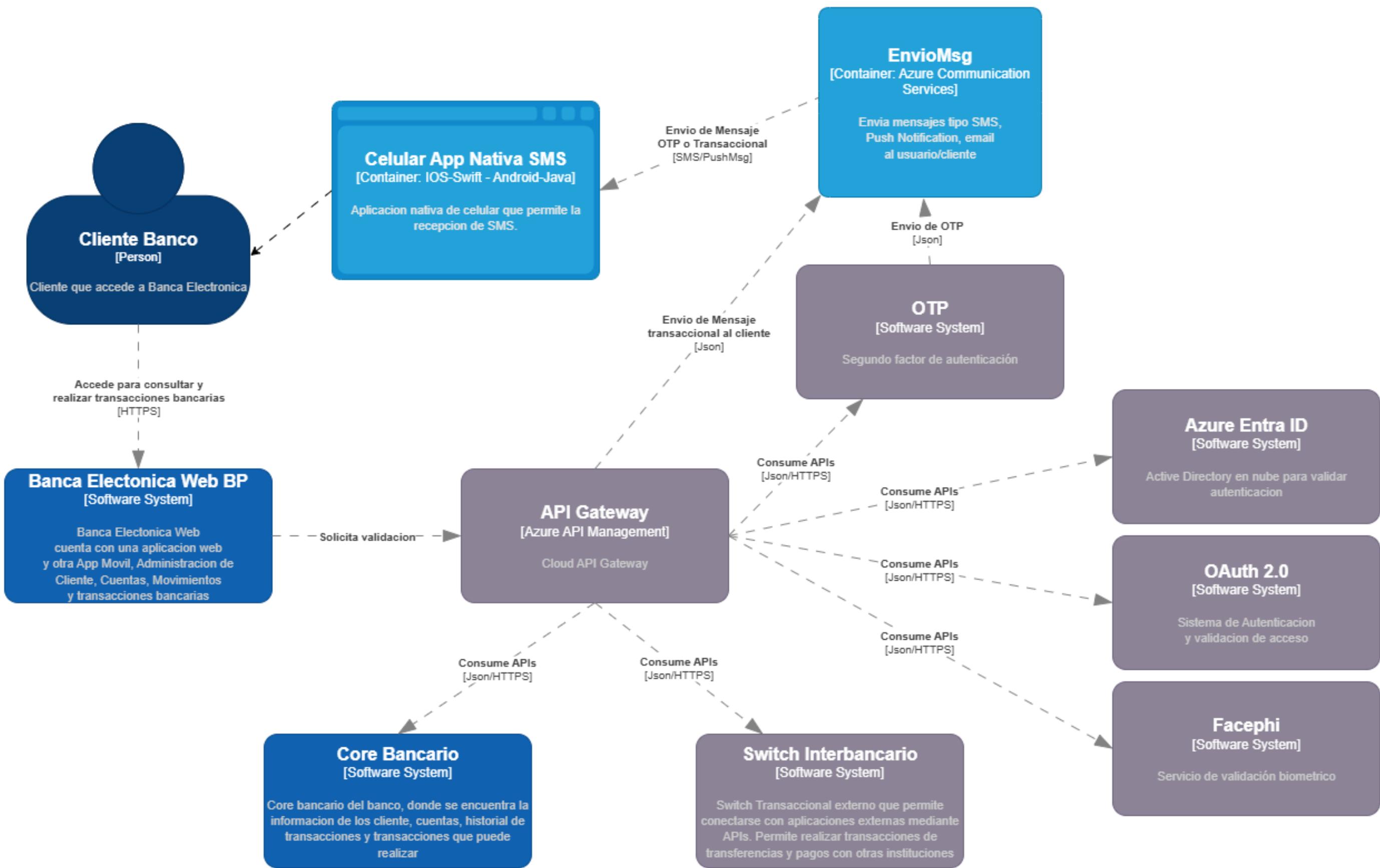
Nivel 1: Diagrama de Contexto.

El Diagrama de Contexto muestra el nivel más general del sistema a analizar, los usuarios que interactúan con el sistema, los sistemas externos con los que se relaciona, y las interacciones que tiene cada elemento con el sistema.

Para nuestro caso exponemos el Diagrama de Contexto de la **Banca por Internet BP**, llamada **Banca Electronica Web BP**. Tiene las siguientes consideraciones:

- Los clientes acceden a la Banca Electronica Web BP, utiliza un protocolo seguro HTTPS (Web)
- El sistema se integra con un API Gateway que permite administrar las APIs para que tengan gobernanza y seguridad. Las APIs cuentan con microservicios que tienen las reglas de negocio. Esta es la capa media del sistema
- Se integra con Azure Entra ID para realizar el proceso validación de usuarios del sistema
- Se integra con OAuth 2.0 para realizar el proceso validación de Autenticación y Autorización para usuarios del sistema. También administra los tokens de sesión para los usuarios
- Se integra con Facephi para realizar el registro y validación biométrica del sistema
- Cuenta con un servicio de OTP (One Time Password) que actúa como segundo factor de autenticación para acceder a la aplicación
- Se integra con un sistema de mensajería que permite comunicar la OTP y otros mensajes tales como el ingreso al sistema, transacciones realizadas (pagos o transferencias) o ingresos fallidos. El mensaje llega a los dispositivos celulares de los clientes, esto con el fin de que el cliente sea notificado inmediatamente de sus interacciones con el sistema.

BANCA POR INTERNET BP -- DIAGRAMA DE CONTEXTO



Nivel 2: Diagrama de Contenedores.

El Diagrama de Contenedores muestra la estructura del Sistema en un alto nivel. Descompone el sistema en aplicaciones, servicios, bases de datos, etc. Ayuda a entender cómo se distribuyen las responsabilidades y las interacciones que tiene cada elemento con el sistema.

Nuestro diagrama de contenedores tiene las siguientes consideraciones:

- Los clientes acceden a la **Banca Electronica Web BP**, utiliza un protocolo seguro HTTPS (Web) y se comunica con un Balanceador **Akamai** que actúa como una capa de protección y redirige el control hacia la aplicación Web o Móvil dependiendo el acceso.

Akamai cuenta con seguridad **WAF** (Web Application Firewall) que protege a la aplicación contra ataques dirigidos a la capa de aplicación. También cuenta con **protección DDoS** que se centra en mitigar ataques de gran volumen que buscan sobrecargar el servidor y negar el acceso al servicio.

- El sistema cuenta con una **aplicación SPA** (Single page Application) que permite acceder a la aplicación desde un navegador web. Las SPA ofrecen una experiencia de usuario más rápida y fluida, similar a una aplicación nativa, y se destacan por su mayor velocidad y capacidad de respuesta.

Para desarrollar la aplicación se elige la última versión estable de Angular ya que es un framework robusto para el desarrollo de aplicaciones web, especialmente adecuado para proyectos grandes y complejos. Asimismo, Angular tiene un muy buen rendimiento y tiene el soporte de una gran empresa como Google.

Se integra con reCAPTCHA a fin de que se evite que un Bot trate de ingresar a la aplicación ilegalmente.

La aplicación debe estar desplegada en un clúster AKS de al menos 3 nodos en balanceo, cada nodo debe contener la misma aplicación, en caso que supere el 80% de uso de los nodos, entonces debe desplegarse un nodo adicional. Con esto se garantiza la Alta Disponibilidad. Esto se denomina Escalamiento Horizontal.

- Para desarrollar la **aplicación Móvil** se decide utilizar Flutter. Si bien existen otros lenguajes con mas tiempo en el mercado y que son multiplataforma como el caso de React Native (Javascript/Typescript), o los nativos Kotlin para Android y Swift para IOS, Flutter está ganando popularidad debido a que su lenguaje Dart es fuertemente tipado y corrige errores desde un inicio, no así Javascript. Además, Flutter permite escribir una sola aplicación para Android e IOS, claro considerando las particularidades de cada lenguaje.

- El sistema cuenta con una **aplicación Back End** misma que contiene la lógica de la aplicación (no de negocio) y que permite comunicar la aplicación SPA y Móvil con los Servicios de Capa Media y de autenticación.

Esta aplicación se encuentra desarrollada en la última versión LTS de SpringBoot/Java.

- El sistema se integra con un API Gateway que actúa como un API Management para administrar las APIs para que tengan gobernanza y seguridad.

Las APIs cuentan con microservicios que tienen las reglas de negocio y que permiten acceder a los datos de la aplicación.

En esta capa se encuentran grupo de APIs que permiten realizar:

- **LoginAuth y Validacion OTP:** APIs de validaciones de autenticación de usuario y OTP
- **API de Negocio:** Grupo de APIs de negocio que permiten consultar información de clientes, crear clientes y realizar transacciones bancarias e interbancarias con cuentas de los clientes
- **Microservicios de Negocio:** Grupo de Microservicios de negocio que permiten consultar información de clientes, crear clientes y realizar transacciones con cuentas de los clientes.

También permiten invocar el microservicio **Cypher**, que permite realizar anonimización y desanonimización, y cifrado y descifrado de datos. Esto es útil para guardar la información sensible de los clientes.

También se integra con otros servicios externos, tales como:

- **Azure Communication Services**, para envío de mensajes SMS, Push Notifications o email
- **Azure Entra ID**, para consultar los datos de los usuarios del sistema
- **Facephii**, para registro y consulta biométrica
- **Oauth 2.0**, para validación de Autenticación y Autorización para usuarios del sistema.
También administra los tokens de sesión para los usuarios

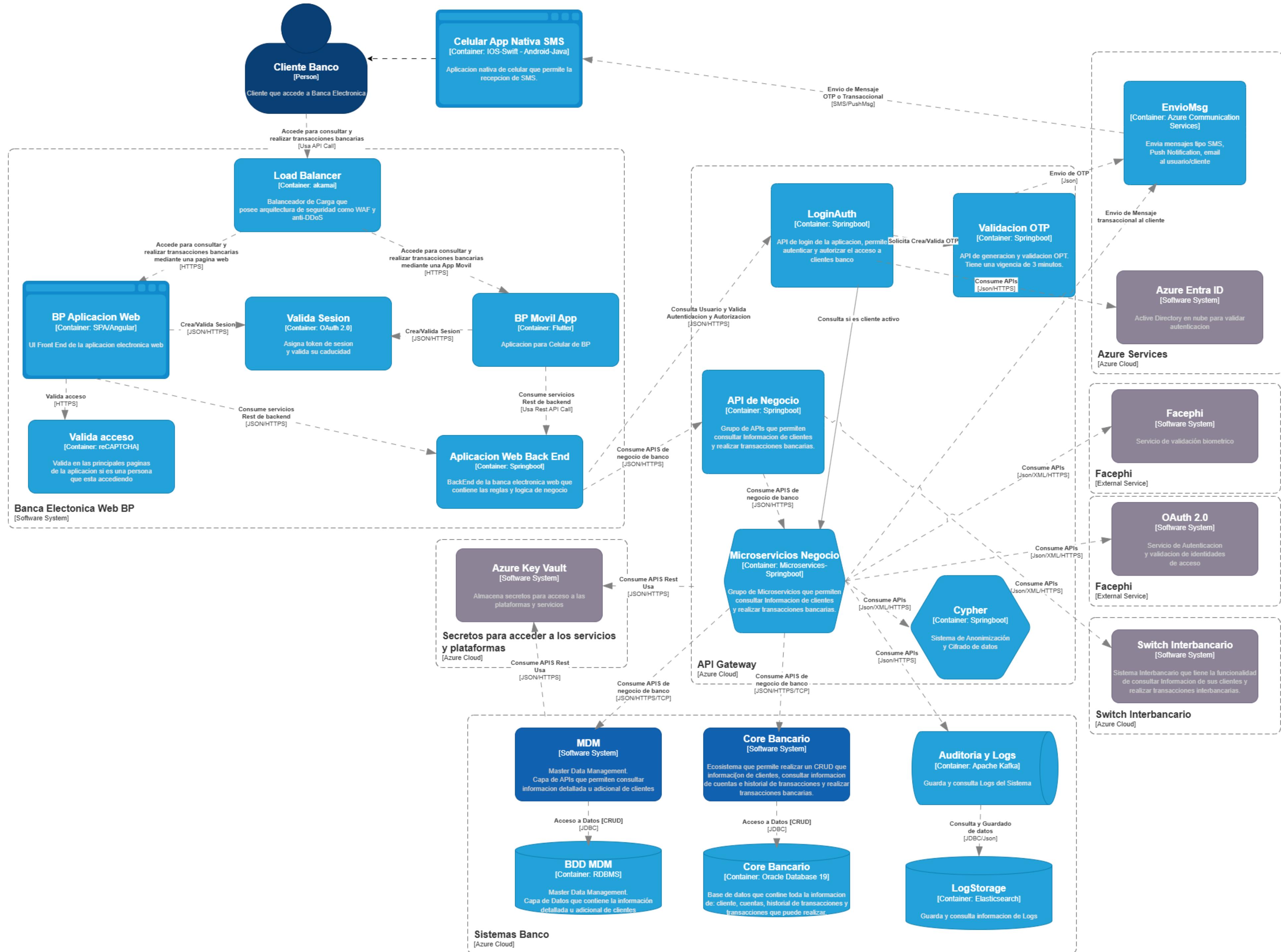
En esta capa se realiza la integración con:

- **El Core Bancario**, que almacena la información de clientes y realizar transacciones bancarias
- **MDM**, que contiene la información adicional y detallada de los clientes de BP

- **Auditoria y Logs**, permite guardar los Logs de auditoría.

Cabe recalcar que las capas de APIs, Microservicios, Core bancario, MDM y Logs de auditoría, se integran con Azure Key Vault para guardar las claves y secretos para acceder a: APIs, Microservicios y Bases de Datos. Azure Key Vault trabaja con OAuth 2.0.

BANCA POR INTERNET BP -- DIAGRAMA DE CONTENEDORES



Nivel 3: Diagrama de Componentes.

El Diagrama de Componentes profundiza en detalle cada contenedor o servicio del diagrama de contenedores, para mostrar los componentes internos de cada uno y cómo se relacionan entre sí. Visualiza la lógica de negocio y funciones específicas.

El diagrama de componentes es un detalle más profundo del diagrama de contenedores (anterior), desglosamos los contenedores y servicios tomando en consideración:

Los clientes acceden a la **Banca Electronica Web BP** comunicándose con un Balanceador **Akamai** que actúa como una capa de protección (Firewall) y redirige el control hacia cada aplicación, Web o Móvil dependiendo el acceso.

La capa media y de Datos están atados al servicio de Azure Key Vault que guarda los secretos y llaves para acceder a cada una de estas capas.

Las páginas de “**BP Aplicacion Web**” y “**BP Móvil App**” cuentan con una integración con reCAPTCHA que permite validar que el usuario que ingrese a la aplicación no sea un Bot que esté tratando de ingresar.

Las Capas “**BP Aplicacion Web**” y “**BP Móvil App**” son aplicaciones que cuentan con opciones y pantallas atadas a Métodos y Eventos que realizan ciertas funcionalidades dentro de las aplicaciones, y a su vez estas están integradas a APIs y Microservicios que conectan a los datos y otros servicios externos. Mencionemos cada una a continuación:

BP Aplicación Web y BP Movil App (Front Web y Movil) <Angular>	Aplicacion Web Back End (Back End del Front) <Java>	API de Negocio (APIs de Negocio - Integración) <Springboot>	Microservicios Negocio (Microservicios Negocio - Lógica y Reglas de Negocio) <Springboot>	Core Bancario (Microservicios de Core) <Java>	Bases de Datos	Otras Aplicaciones	Servicios Externos
Azure Key Vault Almacena secretos para acceso a las plataformas y servicios							
Auth Funcionalidad de pantalla Login y Autenticación para acceso a la aplicación, tanto web como móvil.	<p>Valida Usuario Lógica de Login, integra las validaciones de acceso a la aplicación</p> <p>Consulta Estado Cliente Consulta si el Cliente/Usuario está en estado es Activo</p> <p>Genera y Valida OTP Autentica el usuario Valida Usuario y Contraseña</p> <p>Administración Datos Cliente CRUD la información del cliente. Permite consultar, crear, actualizar y eliminar información relacionada al cliente de BP.</p> <p>Guardar Log Auditoria** Permite Guardar el Log de Auditoria transaccional de los movimientos que realiza el usuario</p>	<p>Consultar y Validar Usuario Autentica el usuario y valida Usuario y Contraseña</p> <p>// Autenticación y Autorización Autentica y Autoriza las identidades de acceso de usuario</p> <p>// Validación Biométrica Realiza el registro y validación biométrica del cliente</p> <p>LoginAuth</p> <p>// Genera OTP Solicitud de generación de OTP y enviar al celular del cliente Tiempo de vigencia 3 minutos posterior caduca.</p> <p>// Valida OTP Valida si el No. OTP es válido y está vigente.</p> <p>// Validación Biométrica Realiza el registro y validación biométrica del cliente</p> <p>// Administración Datos Cliente CRUD la información del cliente. Permite consultar, crear, actualizar y eliminar información relacionada al cliente de BP.</p> <p>// Consulta Datos Cliente Consulta la posición Consolidada del cliente</p>	<p>// Clientes CRUD de información de clientes</p> <p>BDD Core Bancario Base de datos que contiene toda la información de: cliente, cuentas, historial de transacciones y transacciones que puede realizar</p> <p>BDD Core Bancario Base de datos que contiene toda la información de: cliente, cuentas, historial de transacciones y transacciones que puede realizar</p> <p>BDD Core Bancario Base de datos que contiene toda la información de: cliente, cuentas, historial de transacciones y transacciones que puede realizar</p> <p>BDD Core Bancario Base de datos que contiene toda la información de: cliente, cuentas, historial de transacciones y transacciones que puede realizar</p>	<p>RDBMS</p>			<p>Azure Entra ID Active Directory en nube para validar autenticación</p> <p>OAuth 2.0 Servicio de Autenticación y validación de identidades de acceso</p> <p>Facephi Servicio de validación biométrico</p> <p>EnvioMsg < Azure Communication Services> Envía mensajes tipo SMS, Push Notification, email al usuario/cliente. Comunica OTP, ingreso al sistema y los movimientos transaccionales realizados.</p> <p>Facephi Servicio de validación biométrica</p> <p>EnvioMsg < Azure Communication Services></p>
Información Cliente Consulta la información del cliente para presentarla en pantalla	<p>Administración Datos Cliente CRUD la información del cliente. Permite consultar, crear, actualizar y eliminar información relacionada al cliente de BP, consume servicios Rest de backend.</p> <p>Guardar Log Auditoria** Permite Guardar el Log de Auditoria transaccional de los movimientos que realiza el usuario</p>	<p>// MDM Consulta Datos Adicionales Cliente Consulta de información adicional y detallada del cliente</p> <p>Administración Datos Cliente CRUD la información del cliente. Permite consultar, crear, actualizar y eliminar información relacionada al cliente de BP.</p>	<p>// MDM Consulta Datos Adicionales Cliente Consulta información adicional y detallada del cliente</p> <p>// Validación Biométrica Realiza el registro y validación biométrica del cliente</p> <p>// Administración Datos Cliente CRUD la información del cliente. Permite consultar, crear, actualizar y eliminar información relacionada al cliente de BP.</p> <p>// Consulta Datos Cliente Consulta la posición Consolidada del cliente</p>	<p>MDM</p> <p>MDM Clientes CRUD de información adicional de clientes</p> <p>BDD MDM Master Data Management. Capa de Datos que contiene la información detallada u adicional de clientes.</p> <p>BDD Core Bancario Base de datos que contiene toda la información de: cliente, cuentas, historial de transacciones y transacciones que puede realizar</p> <p>BDD Core Bancario Base de datos que contiene toda la información de: cliente, cuentas, historial de transacciones y transacciones que puede realizar</p>	<p>CYPHER</p> <p>Anonimización Anonimización y Desanonimización de Datos.</p> <p>Cifrado Cifrado y Descifrado de Datos.</p> <p>CYPHER</p> <p>Anonimizacion Anonimización y Desanonimización de Datos.</p> <p>Cifrado Cifrado y Descifrado de Datos.</p>		<p>Facephi Servicio de validación biométrica.</p> <p>EnvioMsg < Azure Communication Services> Envía mensajes tipo SMS, Push Notification, email al usuario/cliente. Comunica OTP, ingreso al sistema y los movimientos transaccionales realizados.</p>
Posición Consolidada Consulta la posición. Consolidada del cliente	<p>Consulta posición Consolidada Consulta la posición Consolidada del cliente</p> <p>Guardar Log Auditoria** Permite Guardar el Log de Auditoria transaccional de los movimientos que realiza el usuario</p>	<p>Consulta Movimientos - Cuentas del cliente Consulta los movimientos de cuentas bancarias del cliente, así como su posición Consolidada.</p>	<p>// Consulta Movimientos - Cuentas del cliente Consulta los movimientos de cuentas bancarias del cliente</p> <p>// Consulta Datos Cliente Consulta la posición Consolidada del cliente</p>	<p>// Clientes CRUD de información de clientes</p> <p>// Consulta Movimientos Consulta de Movimientos de cuentas de clientes banco.</p> <p>// Cuentas CRUD de información de cuentas bancarias</p>	<p>BDD Core Bancario Base de datos que contiene toda la información de: cliente, cuentas, historial de transacciones y transacciones que puede realizar.</p>		<p>EnvioMsg < Azure Communication Services> Envía mensajes tipo SMS, Push Notification, email al usuario/cliente. Comunica OTP, ingreso al sistema y los movimientos transaccionales realizados.</p>

BP Aplicación Web y BP Movil App (Front Web y Movil) <Angular>	Aplicacion Web Back End (Back End del Front) <Java>	API de Negocio (APIs de Negocio - Integración) <Springboot>	Microservicios Negocio (Microservicios Negocio - Lógica y Reglas de Negocio) <Springboot>	Core Bancario (Microservicios de Core) <Java>	Bases de Datos	Otras Aplicaciones	Servicios Externos
Estado de Cuenta Consulta información del estado de cuenta del cliente	Consulta Estado de Cuenta Consulta información del estado de cuenta del cliente	Consulta Movimientos - Cuentas del cliente Consulta los movimientos de cuentas bancarias del cliente, así como su posición Consolidada.	// Consulta Movimientos - Cuentas del cliente Consulta los movimientos de cuentas bancarias del cliente // Consulta Datos Cliente Consulta la posición Consolidada del cliente	 // Clientes CRUD de información de clientes // Consulta Movimientos Consulta de Movimientos de cuentas de clientes banco. // Cuentas CRUD de información de cuentas bancarias	 BDD Core Bancario Base de datos que contiene toda la información de: cliente, cuentas, historial de transacciones y transacciones que puede realizar.	// CYPHER Anonimización Anonimización y Desanonimización de Datos. Cifrado Cifrado y Descifrado de Datos.	EnvioMsg < Azure Communication Services> Envía mensajes tipo SMS, Push Notification, email al usuario/cliente. Comunica OTP, ingreso al sistema y los movimientos transaccionales realizados.
Configuración de Cupos Consulta y Actualiza Cupos para las cuentas del cliente.	Configuración de Cupos Consulta y Actualiza Cupos para las cuentas del cliente	Configuración de Cupos Consulta y Actualiza Cupos para las cuentas del cliente	// Configuración de Cupos CRUD de información de cuentas bancarias // Consulta Datos Cliente: Consulta la posición Consolidada del cliente	 // Clientes CRUD de información de clientes // Cuentas CRUD de información de cuentas bancarias	 BDD Core Bancario Base de datos que contiene toda la información de: cliente, cuentas, historial de transacciones y transacciones que puede realizar.	// CYPHER Anonimización Anonimización y Desanonimización de Datos. Cifrado Cifrado y Descifrado de Datos.	EnvioMsg < Azure Communication Services> Envía mensajes tipo SMS, Push Notification, email al usuario/cliente. Comunica OTP, ingreso al sistema y los movimientos transaccionales realizados.
Realizar Pagos Permite realizar pagos desde las cuentas del cliente	Transacciones Pagos Permite realizar pagos desde las cuentas del cliente bancarias e interbancarias.	Transacciones bancarias Permite realizar Pagos y Transferencias bancarias e interbancarias desde las cuentas del cliente.	// Transacciones bancarias Microservicio que permite realizar Pagos y Transferencias bancarias e interbancarias desde las cuentas del cliente. // Consulta Datos Cliente Consulta la posición Consolidada del cliente	 // Clientes CRUD de información de clientes // Cuentas CRUD de información de cuentas bancarias // Transacciones Transferencias bancarias Débito y Crédito que afectan a las cuentas del cliente [Transferencias y Pagos]	 BDD Core Bancario Base de datos que contiene toda la información de: cliente, cuentas, historial de transacciones y transacciones que puede realizar.	// CYPHER Anonimización Anonimización y Desanonimización de Datos. Cifrado Cifrado y Descifrado de Datos.	Switch Interbancario Sistema Interbancario que tiene la funcionalidad de consultar información de sus clientes y realizar transacciones interbancarias. EnvioMsg < Azure Communication Services> Envía mensajes tipo SMS, Push Notification, email al usuario/cliente. Comunica OTP, ingreso al sistema y los movimientos transaccionales realizados.
Realizar Transferencias Permite realizar Transferencias bancarias e interbancarias desde las cuentas del cliente.	Transacciones Transferencias Permite realizar Transferencias bancarias e interbancarias desde las cuentas del cliente	Transacciones Transferencias Permite realizar Pagos y Transferencias bancarias e interbancarias desde las cuentas del cliente	// Transacciones bancarias Microservicio que permite realizar Pagos y Transferencias bancarias e interbancarias desde las cuentas del cliente. // Consulta Datos Cliente Consulta la posición Consolidada del cliente	 // Clientes CRUD de información de clientes // Cuentas CRUD de información de cuentas bancarias // Transacciones Transferencias bancarias Débito y Crédito que afectan a las cuentas del cliente [Transferencias y Pagos]	 BDD Core Bancario Base de datos que contiene toda la información de: cliente, cuentas, historial de transacciones y transacciones que puede realizar.	// CYPHER Anonimización Anonimización y Desanonimización de Datos. Cifrado Cifrado y Descifrado de Datos.	Switch Interbancario Sistema Interbancario que tiene la funcionalidad de consultar información de sus clientes y realizar transacciones interbancarias. EnvioMsg < Azure Communication Services> Envía mensajes tipo SMS, Push Notification, email al usuario/cliente. Comunica OTP, ingreso al sistema y los movimientos transaccionales realizados.
	*** Guardar Log Auditoria Permite Guardar el Log de Auditoria transaccional de los movimientos que realiza el usuario	Guardar Log Auditoria Guarda el Log de Auditoria transaccional de los movimientos que realiza el usuario	Guardar Log Guarda el Log de Auditoria transaccional de los movimientos que realiza el usuario		Elasticsearch BDD LogAuditory Base de datos de Logs de Auditoria, que permite realizar análisis en tiempo real.	Kafka Log Auditory Servicio Pub/Sub que encola los registros de Logs para guardarlo en la BDD	

*** Redireccionamiento para el guardado de Logs en la Capa de Back End.

BANCA POR INTERNET BP -- DIAGRAMA DE COMPONENTES



Nivel 4: Diagrama de Código (opcional).

El Diagrama de Código representa detalles técnicos como clases, métodos, interfaces o módulos, que son los componentes más pequeños a nivel de programación. Útil para desarrolladores que necesitan comprender la implementación y lógica de cada componente

Se indica un diagrama muy general de clases relacionado al Sistema de Banco.

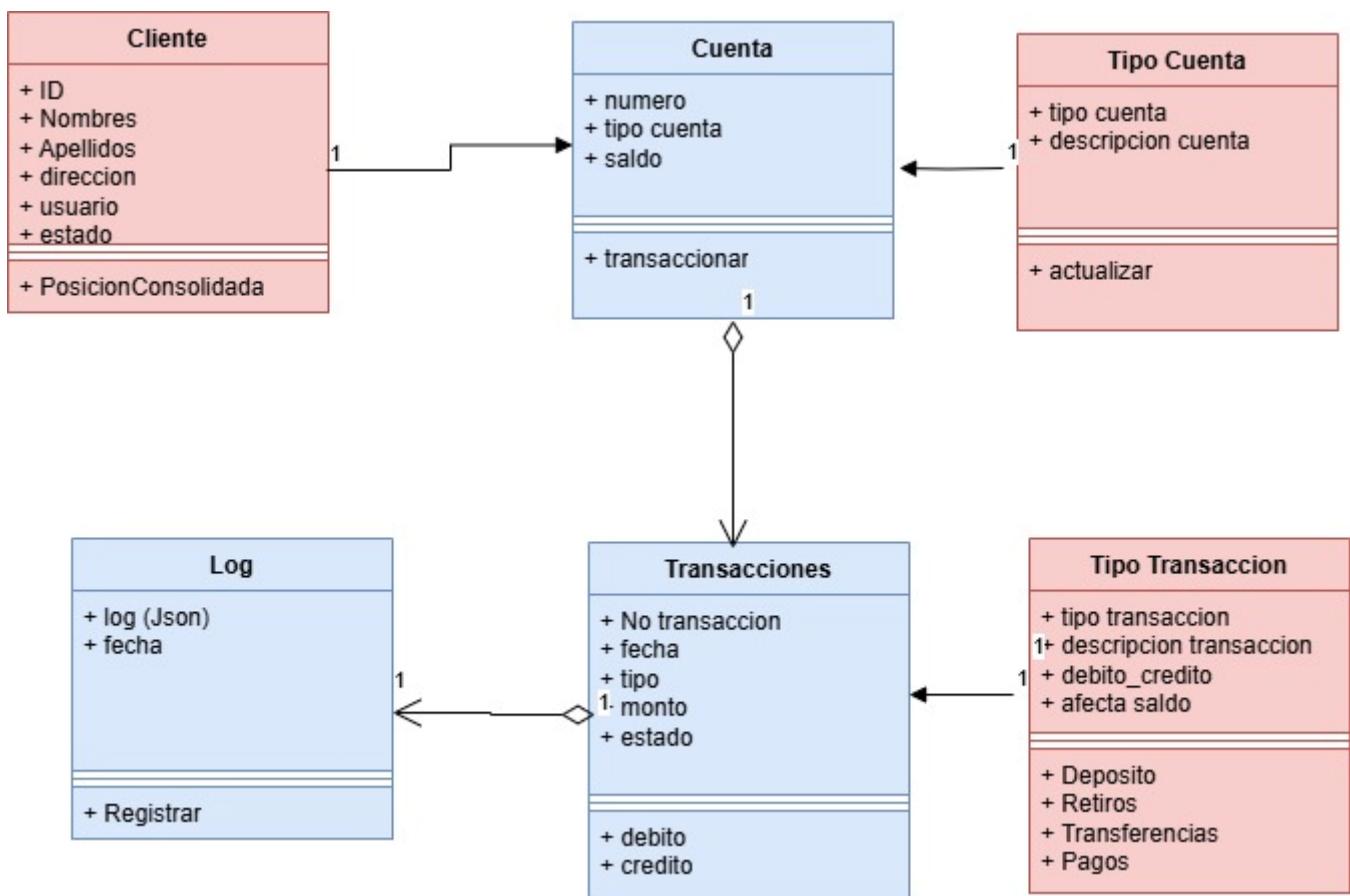


Diagrama de Despliegue.

El Diagrama de Despliegue representa gráficamente la disposición física de los componentes de software en nodos de hardware, ya sean físicos (On-premise) o en nube, facilitando la comprensión de la arquitectura de un sistema. Adicionalmente ilustra cómo se distribuyen los artefactos de software en el hardware. Estos diagramas son esenciales para visualizar la topología del sistema y entender cómo interactúan los componentes de software y hardware.

El siguiente diagrama solo representa el ambiente de producción.

Como parte de la solución, se considera:

- El usuario ingresa desde una página web la sitio <https://www.bp.com>
- La configuración del DNS lo redirecciona a un Load Balancer que tiene la dirección IP: 1.1.x.121/122, para esto utilizamos la aplicación **Akamai** que cuenta con seguridad WAF (Firewall de Aplicaciones Web) y prevención de ataque DDoS (Ataque de Denegación de Servicio Distribuido), esto previene que puedan realizar ataques de fuerza a la aplicación.

Se utiliza la herramienta de monitoreo **dynatrace**, que actúa como un servicio de monitoreo estático que valida si la página y/o aplicación móvil se encuentran activas y disponibles.

- La aplicación cuenta con una página de contingencia con IP: 1.1.x.10 en caso de **Fuera de Servicio o Mantenimientos Programados**. Esta página esta desarrollada en Angular y desplegada en un AKS dentro de la aplicación
- La aplicación se encuentra desplegada en Azure Cloud, y se despliega en 2 Regiones y/o Zonas, con el fin de que, si resulta una falla o catástrofe en la zona principal, entonces redireccionar a una zona secundaria a fin de garantizar Contingencia. Ambas regiones tienen las mismas capacidades y configuración, a excepción de las direcciones IP:
 - La aplicación principal o DCP (Data Center Principal) se encuentra en la Región A
 - La aplicación secundaria de respaldo contingente o DCA (Data Center Alterno) se encuentra en la Región B
- La aplicación se encuentra desplegada en un Clúster de AKS (Azure Kubernetes Service) IP: 1.10.x.x/24 donde se despliegan los diferentes componentes de la aplicación: Front y Back
- Cuenta con un API Management de Azure para la gobernanza y despliegues de APIs
- La solución cuenta con una Capa Media que se encuentra desplegada en un Clúster de AKS IP: 1.20.x.x/23 donde se despliegan los diferentes microservicios de negocio que interactúan con la lógica de negocio y los Datos que se encuentran en las diferentes Bases de Datos

- Las Bases de Datos se encuentran desplegadas en un Clúster de Bases de Datos de Azure. Aquí se encuentran desplegadas las diferentes bases de datos: Core, MDM, Log Storage
- Considerando que los datos se van actualizando constantemente, en la Región A, para que la Región B de contingencia, se utiliza un servicio de Azure SQL replica, que permite sincronizar la información en tiempo real
- Para notificar a los usuarios acerca de los movimientos realizados, se utilizan 2 servicios independientes de **Azure Communication Services** el primero con IP: 1.11.x.110 y el segundo con IP: 1.11.x.111, y con el fin de garantizar que los usuarios sean comunicados, se utiliza un **servicio Pub/Sub** como Kafka para encolar los mensajes que son enviados por la aplicación.

Otra opción para solventar el tema de comunicación es utilizar el patrón Circuit Breaker que permite actúa como un disyuntor en un sistema eléctrico (On/Off), monitoreando el éxito y el fracaso de las solicitudes a un servicio y bloqueando temporalmente futuras solicitudes si las fallas superan un umbral, lo que permite que el servicio fallido se recupere potencialmente, en otras palabras apaga un servicio que este saturado de peticiones y prende el respaldo, y permite que el primero termine con las solicitudes y recepte nuevas solicitudes.

Utilizar un servicio Pub/Sub y Circuit Breaker son 2 patrones de diseño que se pueden utilizar para solventar el tema de comunicación.

- La solución se encuentra integrada con otros servicios para su funcionamiento, mismos que se encuentran en Azure, Google Cloud y otros:
 - Azure Cloud:
 - Azure Key Vault, para guardar claves y secretos de la aplicación y base de datos
 - Azure Entra ID, para administrar los usuarios
 - Kafka, administrado de mensajes y colas
 - Google Cloud:
 - reCAPTCHA, para validar que es una persona que accede a la aplicación
 - Otros:
 - Dynatrace, herramienta de monitoreo
 - Oauth 2.0, herramienta de
 - Facephi, validación biométrica

Existe el **Análisis de Impacto Empresarial (BIA)** que es un proceso sistemático que identifica y analiza las posibles consecuencias de las interrupciones en las funciones críticas del negocio Ayuda

a las organizaciones a comprender cómo un desastre, accidente o emergencia podría afectar sus operaciones y proporciona la base para desarrollar estrategias de recuperación.

