# DOCUMENTO DE ARQUITECTURA

Banca Internet

## HOJA DE CONTROL DOCUMENTAL

| | | | |
|---|---|---|---|
| **Realizado por** | Marco Luna | **Fecha** | 04/09/2024 |
| **Revisado por** | | **Fecha** | |
| **Aprobado por** | | **Fecha** | |

## CONTROL DE VERSIONES

| Versión | Fecha | Descripción |
|---|---|---|
| 1.0 | 04/09/2024 | Versión Inicial |
| | | |

# Tabla de contenido

## OBJETIVOS DEL DOCUMENTO

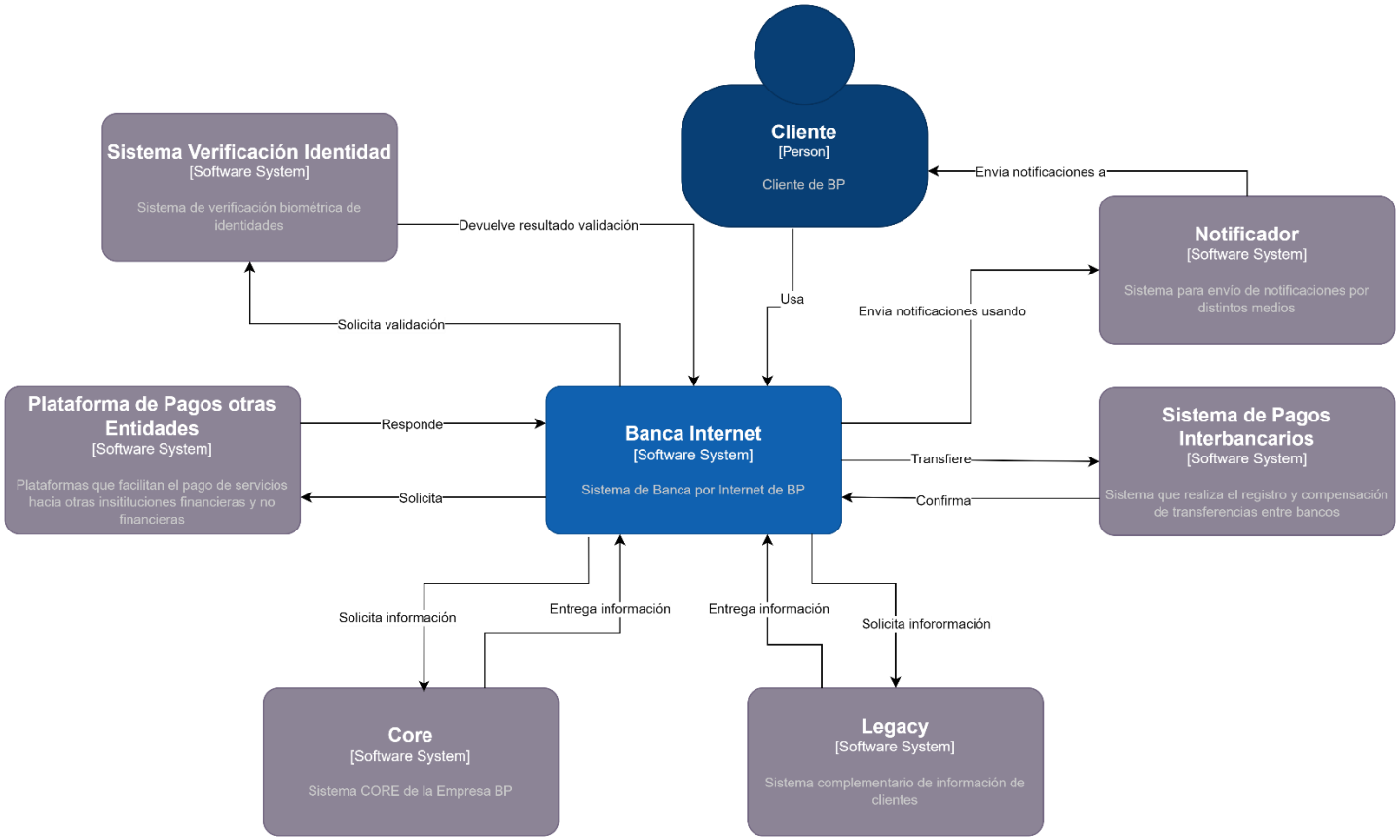
El presente documento busca describir de manera técnica la arquitectura diseñada para la solución Banca por Internet del cliente BP, basado en los requerimientos descritos en las siguientes secciones.

## REQUERIMIENTOS

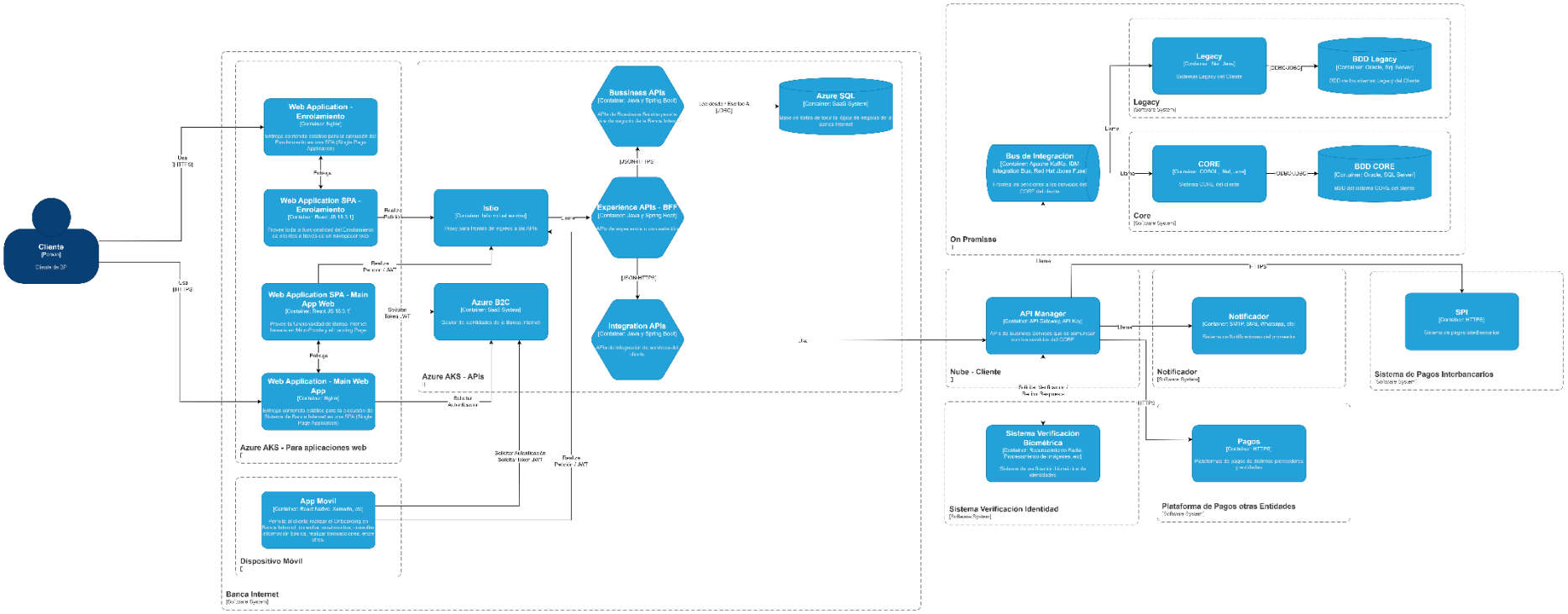
| CODIGO | DESCRIPCIÓN |
|---|---|
| REQ001 | La información de los clientes como movimientos, productos y datos básicos deben extraerse del CORE y del Sistema Complementario |
| REQ002 | Toda transacción/movimiento de los clientes debe ser notificado mediante el componente notificador del sistema.<br><br>El sistema de notificaciones debe enviar mensajes mediante dos mecanismos |
| REQ003 | Tanto la aplicación SPA como MOVIL deben estar construidas mediante un Framework Multiplataforma; la arquitectura propuesta debe proponer dos Frameworks al respecto. |
| REQ004 | La Autenticación debe hacerse mediante el estándar OAuth2.0 utilizando las herramientas que la empresa tiene para el efecto |
| REQ005 | El Onboarding de los clientes en la aplicación MOVIL debe hacerse mediante reconocimiento facial. |
| REQ006 | La Autenticación de los clientes en la Aplicación MOVIL, luego del Onboarding se la debe realizar con usuario y clave, huella digital u otro mecanismo |
| REQ007 | La arquitectura debe contemplar una BDD para registro de log de auditoría y persistencia de información para clientes frecuentes |
| REQ008 | La capa de integración de la arquitectura debe contemplar el uso de un API Gateway. |
| REQ009 | La arquitectura debe contemplar el uso de microservicios con la posibilidad de comunicación con servicios externos. |

# ARQUITECTURA DEL SISTEMA

## DIAGRAMA DE CONTEXTO

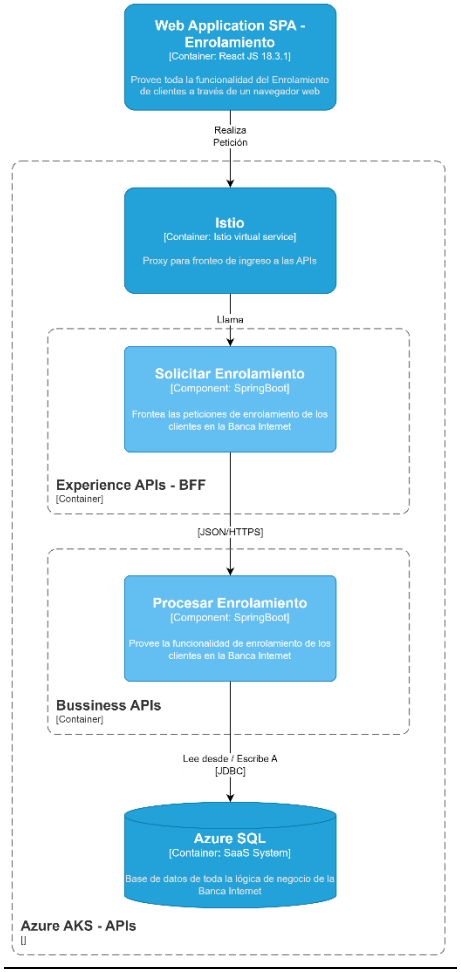


# DIAGRAMA DE CONTENEDORES

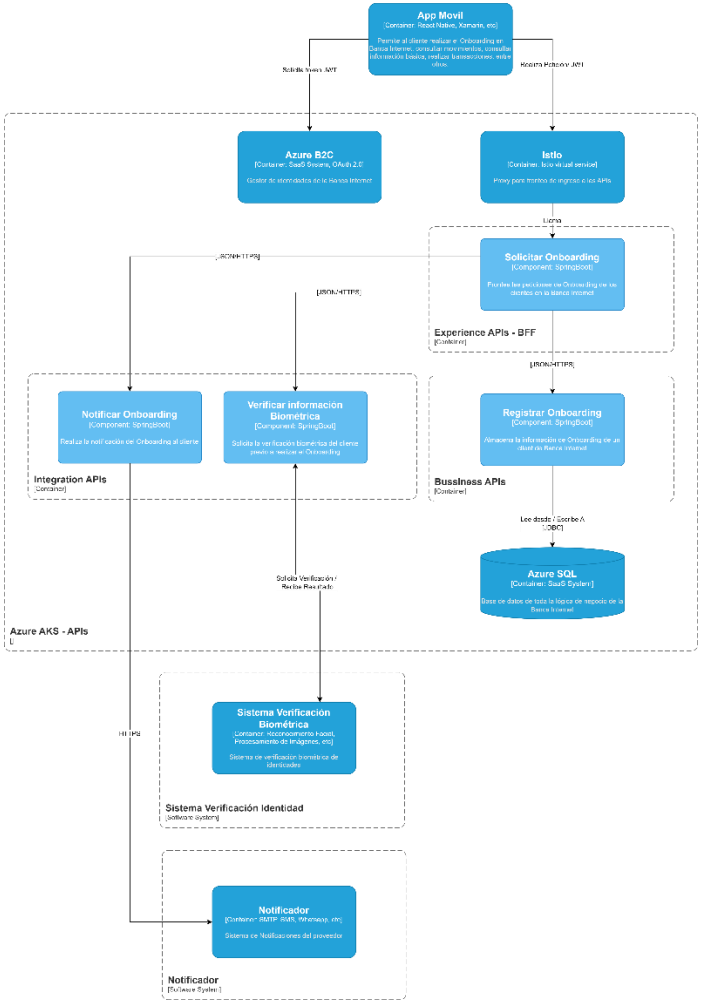


# DIAGRAMAS DE COMPONENTES

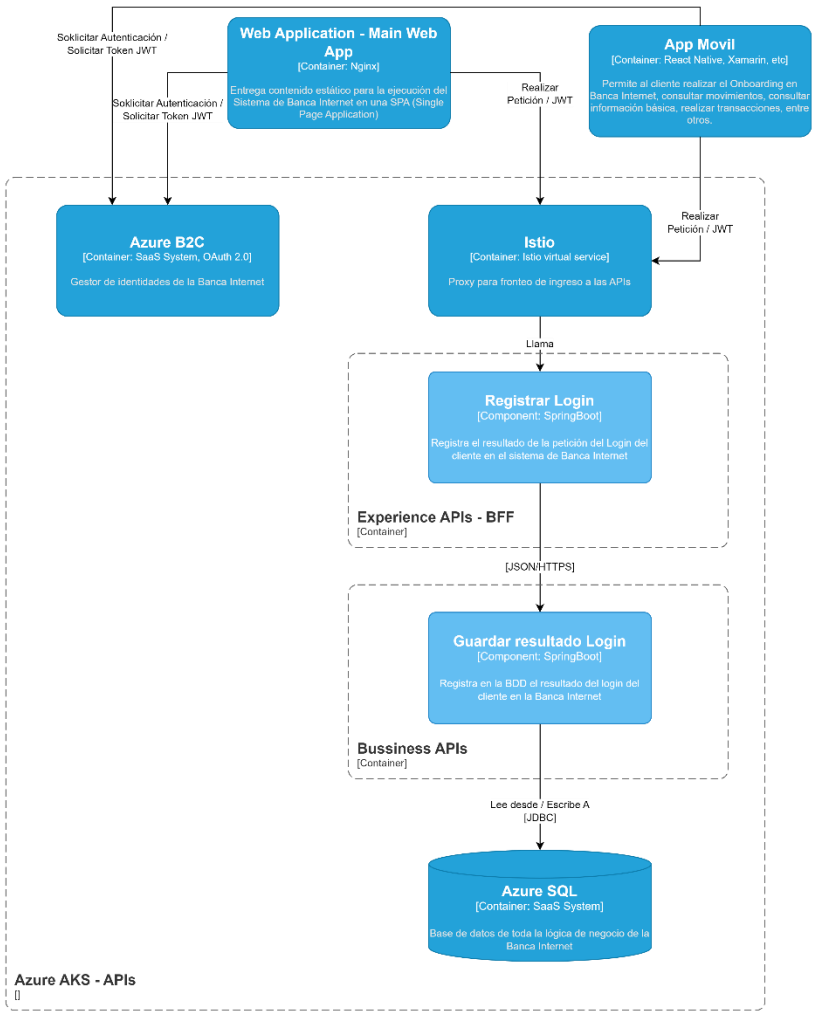
## ENROLAMIENTO EN APP WEB



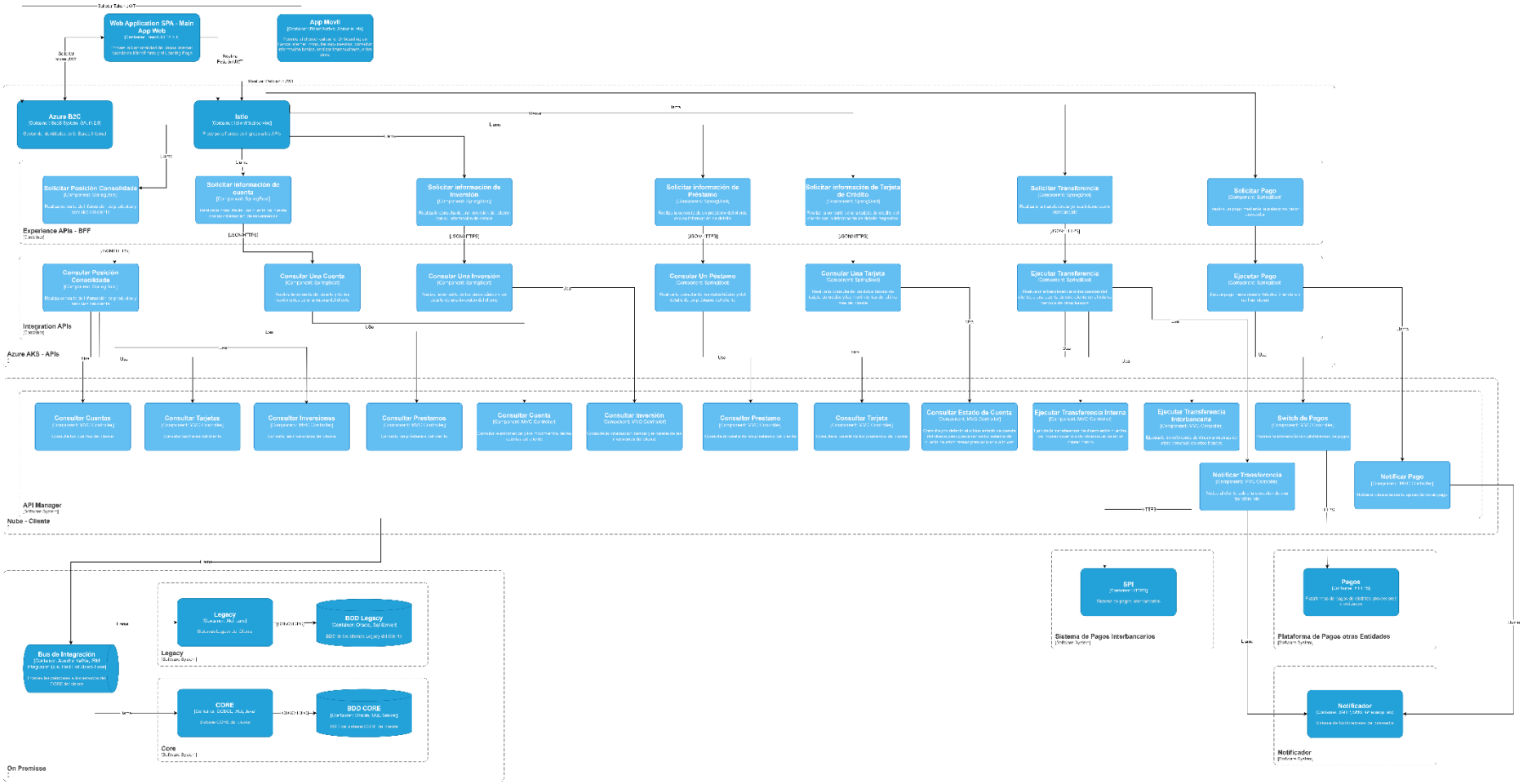
# ONBOARDING APP MOVIL



## LOGIN APP WEB y MOVIL



# TRANSACCIONES APP WEB Y MOVIL



# REQUERIMIENTOS TECNICOS

## 1. REQUERIMIENTO TÉCNICO REQ001

### Detalle del Requerimiento

La información de los clientes como movimientos, productos y datos básicos deben extraerse del CORE y del Sistema Complementario.

### Detalle de la solución

Se creará una Solución Web SPA basada en micro frontends, desplegada mediante NGINX y una App Movil, la cual se propone sea construida ya sea con React Native, Xamarin, .net MAUI, entre otras.

Se propone una capa de APIs agrupados por responsabilidad; por lo tanto, se propone la creación de APIs de experiencia basado en el patrón Backend for Frontend que orqueste las llamadas hacia el resto de APIs, APIs de negocio que permitan manejar la lógica propia del Banca Internet y APIs de integración para el llamado hacia los componentes internos del ecosistema de la empresa BP.

Se asume la existencia de un API Manager que frontee el ingreso de peticiones desde el Internet hacia la red interna de la Empresa BP y hacia los componentes de proveedores terceros e incluso soluciones propias de BP que no sean parte de su sistema CORE o de los sistemas Legacy.

Se asume la existencia de un ESB para fronteo y orquestación de llamadas hacia la infraestructura On Premisse de BP; es decir, su sistema CORE y sus sistemas Legacy.

Se asume que toda la solución estará alojada en la Nube de Azure y por ende se hará uso de los servicios administrados de dicha Nube.

La interacción entre todos estos componentes permitirá la consulta de movimientos, productos, datos básicos, transferencias y pagos por parte de los clientes de BP.

### Seguridad

El esquema de seguridad propone el uso de Azure B2C tanto para la autenticación como para la generación de tokens JWT que permitan el aseguramiento de las APIs.

Se propone la habilitación de ISTIO como front de entrada a las APIs, a fin de generar el Service Mesh.

## 2. REQUERIMIENTO TÉCNICO REQ002

### Detalle del Requerimiento

Toda transacción/movimiento de los clientes debe ser notificado mediante el componente notificador del sistema.

### Detalle de la solución

Para el efecto se asume la existencia de un sistema Notificador existente del lado de BP que permite el envio de notificaciones vía, entre otros, SMS, SMTP, Whatsapp.

Desde el punto de vista de la Arquitectura se propone colocar este componente detrás del API Manager a fin de que pueda ser accedido de manera segura desde internet.

El llamado a los servicios de notificación en el API Manager se lo realizará mediante las APIs de Integración que son, a su vez, llamadas desde las APIs de Experiencia.

Recordar que toda la zona de APIs esta fronteada mediante ISTIO que es por donde entran las peticiones desde la APP Web y Movil

### Seguridad

El aseguramiento de las notificaciones viene dado por la combinación e interacción de Azure B2C, ISTIO y el API Manager

## 3. Requerimiento Técnico REQ003

### Detalle del Requerimiento

Tanto la aplicación SPA como MOVIL deben estar construidas mediante un Framework Multiplataforma; la arquitectura propuesta debe proponer dos Frameworks al respecto.

### Detalle de la solución

Consistente con lo propuesto en la Arquitectura, se propone:

- Para la APP Web, se propone el uso de React JS o Angular JS para su construcción.
- Para la APP Movil, se propone el uso de React Native, Xamarin o .NET MAUI para su construcción.

### Seguridad

N/A

## 4. Requerimiento Técnico REQ004

### Detalle del Requerimiento

La Autenticación debe hacerse mediante el estándar OAuth2.0 utilizando las herramientas que la empresa tiene para el efecto.

### Detalle de la solución

Consistente con lo propuesto en la Arquitectura, se propone:

- Para generación de JWT el uso de Azure B2C.
- Para la autenticación vía SSO tambien el uso de B2C.

### Seguridad

Azure B2C cumple con el estándar Oauth 2.0

## 5. Requerimiento Técnico REQ005

### Detalle del Requerimiento

El Onboarding de los clientes en la aplicación MOVIL debe hacerse mediante reconocimiento facial.

### Detalle de la solución

El proceso de Onboarding que se propone se basa en el llamado, desde la APP Movil, a través de las APIs de Experiencia e Integración y el API Manager, hacia la plataforma de verificación de identidad con uso de biometría de un proveedor tercero.

En este punto es importante mencionar que el request a dichos servicios y su posterior uso dentro de la APP Movil estaría sujeto al uso de un SDK o librerías propias del Proveedor que deben instalarse dentro del dispositivo móvil del cliente.

### Seguridad

El aseguramiento viene dado por la combinación e interacción de Azure B2C, ISTIO y el API Manager; sin perjuicio de que se pueda incluir otro esquema de seguridad exigido por el proveedor tercero.

## 6. Requerimiento Técnico REQ006

### Detalle del Requerimiento

La Autenticación de los clientes en la Aplicación MOVIL, luego del Onboarding se la debe realizar con usuario y clave, huella digital u otro mecanismo.

### Detalle de la solución

La autenticación se propone ya sea mediante un esquema de SSO mediante el uso de Azure B2C en combinación con las APIs internas del dispositivo móvil del cliente para reconocimiento de huella, patrón o pin.

De ser el caso se puede generar un usuario y contraseña propios los cuales serán almacenados en una BDD propia del Sistema de Banca Internet en la Nube; para el efecto, se propone el uso de las APIs de experiencia y de negocio en conjunto con una BDD de Azure SQL.

### Seguridad

Mediante el uso de B2C. Importante mencionar que no se almacenan claves sino que se haría uso de Azure Keyvault para dicho propósito.

## 7. Requerimiento Técnico REQ007

### Detalle del Requerimiento

La arquitectura debe contemplar una BDD para registro de log de auditoría y persistencia de información para clientes frecuentes.

### Detalle de la solución

Si bien se propone la existencia de una BDD de Azure SQL para persistencia de información propia de la Banca Internet; tambien se propone el uso de Dynatrace y de Elastik para telemetría y monitoreo.

Para temas de caché se propone el uso de Redis en lo que corresponda; por ejemplo, configuración centralizada, catálogos, urls, entre otros.

### Seguridad

N/A.

## 8. Requerimiento Técnico REQ008

### Detalle del Requerimiento

La capa de integración de la arquitectura debe contemplar el uso de un API Gateway.

### Detalle de la solución

Como se muestra en las distintas vistas de la arquitectura propuesta, se asume la existencia de un API Manager como front de entrada al ecosistema de BP.

### Seguridad

N/A.

## 9. Requerimiento Técnico REQ009

### Detalle del Requerimiento

La arquitectura debe contemplar el uso de microservicios con la posibilidad de comunicación con servicios externos.

### Detalle de la solución

Como se ha descrito anteriormente se propone una arquitectura desacoplada en varios tipos de APIs como los de experiencia, integración y negocio; además de los componentes desarrollados a nivel del API Manager para integración hacia y desde el ecosistema de BP.

### Seguridad

El aseguramiento viene dado por la combinación e interacción de Azure B2C, ISTIO y el API Manager.

## GLOSARIO DE TERMINOS

| Abreviación | Descripción |
|---|---|
| ISTIO | Gestiona los flujos de tráfico entre servicios, aplica políticas de acceso y agrupa datos de telemetría sin modificar el código de las aplicaciones. Tambien ejecuta acciones de circuit breaker |
| API | Son mecanismos que permiten a dos componentes de software comunicarse entre sí mediante un conjunto de definiciones y protocolos |
| AZURE | Nube de Microsoft |
| AZURE B2C | es una solución de administración de acceso de identidades de clientes (CIAM); cumple con el estándar OAuth 2.0 |