

Quito, 17 de septiembre de 2025

Estimados
DEVSU

Referencia: ARQUITECTO DE SOLUCIONES – SECTOR BANCARIO

De mi consideración:

Reciba un cordial saludo de parte de Víctor Barrionuevo Bolaños, experto en Tecnologías de la Información, y conocedor que la empresa DEVSU a la cual usted pertenece, se encuentra en la búsqueda de un “Arquitecto de Soluciones – Sector Bancario” para Ecuador, me permite poner a su disposición mi hoja de vida y el ejercicio práctico requerido en el proceso de selección, en la cual usted podrá apreciar que tengo más de 25 años de experiencia en el campo de IT, de los cuales los últimos 12 años he estado liderando las áreas de tecnologías de importantes instituciones; como son: Banco Central del Ecuador, Corporación Nacional de Telecomunicaciones CNT EP y la Corporación Financiera Nacional.

El haber trabajado y adquirido conocimiento de diferentes áreas de Tecnologías de la Información (Infraestructura de TI, Seguridad Informática, Desarrollo de Software, Gestión de Procesos y Servicios de TI, entre otros) me han brindado la experiencia necesaria para liderar equipos de trabajo durante la implementación de varios proyectos de transformación digital; así como también, la oportunidad para desempeñarme como consultor tecnológico en varias instituciones.

Por favor sírvase aceptar mi aplicación para el cargo de ““Arquitecto de Soluciones – Sector Bancario””, para lo cual adjunto mi hoja de vida, a través de la cual podrá validar que dispongo de las aptitudes, habilidades y experiencia necesarias para contribuir con su organización, en la consecución de sus objetivos estratégicos.

Le agradezco por su tiempo y quedo a la espera de su respuesta; y si lo considera necesario, poder reunirnos y compartir con ustedes mi experiencia.

Saludos,
Víctor Barrionuevo

Email: vbarriouevob@yahoo.com
Teléfono: (593) 0999457534
Dirección: Urb. La Colina 400, Calle Manabi y Guayas
Sangolqui - Ecuador

DEVSU

Ejercicio Practico

Informe de la Arquitectura Sistema Bancario vía Internet

Victor Barrionuevo Bolaños
Quito, 17 de septiembre de 2025

Tabla de contenido

1.	ANTECEDENTES	4
2.	OBJETIVO	4
3.	DESARROLLO	5
3.1	Arquitectura de la Solución.	5
3.1.1	Contexto del Sistema.	5
3.1.2	Contenedores del Sistema.	7
3.1.3	Componentes del Sistema.	10
3.2	Diagramas Complementarios del Sistema.	12
3.3	Consideraciones de Seguridad y Marco Normativo.	12
3.4	Consideraciones de Alta Disponibilidad y Contingencia.	13
4.	FIRMA DE RESPONSABILIDAD	14

Índice de Ilustraciones

Ilustración 1. Diagrama de Contexto - Sistema Bancario Internet	5
Ilustración 2. Diagrama de Contenedores - Sistema Bancario Internet.....	7
Ilustración 3. Diagrama de Componentes - Sistema Bancario Internet.....	10

1. ANTECEDENTES

El presente informe corresponde al ejercicio práctico solicitado por la DEVSU como parte del proceso de postulación para el cargo de “Arquitecto de Soluciones – Institución Bancaria”

2. OBJETIVO

Elaborar la arquitectura de la solución para un Sistema Bancario vía Internet que cumpla con las siguientes características.

Diseñar un sistema de banca por internet, en este sistema los usuarios podrán acceder al histórico de sus movimientos, realizar transferencias y pagos entre cuentas propias e interbancarias.

Toda la información referente al cliente se tomará de 2 sistemas, una plataforma Core que contiene información básica de cliente, movimientos, productos y un sistema independiente que complementa la información del cliente cuando los datos se requieren en detalle.

Debido a que la norma exige que los usuarios sean notificados sobre los movimientos realizados, el sistema utilizará sistemas externos o propios de envío de notificaciones, mínimo 2.

Este sistema contará con 2 aplicaciones en el Front, una SPA y una Aplicación móvil desarrollada en un Framework multiplataforma.

Ambas aplicaciones autenticarán a los usuarios mediante un servicio que usa el estándar OAuth2.0, para el cual no requiere implementar toda la lógica, ya que la compañía cuenta con un producto que puede ser configurado para este fin; sin embargo, debe dar recomendaciones sobre cuál es el mejor flujo de autenticación que se debería usar según el estándar.

Tenga en cuenta que el sistema de Onboarding para nuevos clientes en la aplicación móvil usa reconocimiento facial, por tanto, su arquitectura deberá considerarlo como parte del flujo de autorización y autenticación, a partir del Onboarding el nuevo usuario podrá ingresar al sistema mediante usuario y clave, huella o algún otro método específico alguno de los anteriores dentro de su arquitectura, también puede recomendar herramientas de industria que realicen estas tareas y robustezca su aplicación.

El sistema utiliza una base de datos de auditoría que registra todas las acciones del cliente y cuenta con un mecanismo de persistencia de información para clientes frecuentes, para este caso proponga una alternativa basada en patrones de diseño que relacione los componentes que deberían interactuar para conseguir el objetivo.

Para obtener los datos del cliente el sistema pasa por una capa de integración compuesta por un API Gateway y consume los servicios necesarios de acuerdo con el tipo de transacción, inicialmente usted cuenta con 3 servicios principales, consulta de datos básicos, consulta de movimientos y transferencias que realiza llamados a servicios externos dependiendo del tipo, si considera que debería agregar más servicios para mejorar el rendimiento de su arquitectura o agregar más servicios para mejorar la respuesta de información a sus clientes, es libre de hacerlo.

Se debe incluir los siguientes diagramas en el diseño de la solución:

- Diagrama de Contexto
- Diagrama de Contenedores
- Diagrama de Componentes

3. DESARROLLO

3.1 Arquitectura de la Solución.

Para una mejor comprensión del diseño arquitectónico propuesto para el Sistema Bancario vía Internet se ha establecido utilizar el modelo C4; por lo cual, en el presente ejercicio se han establecido los diagramas de contexto, de contenedores y de componentes.

Se realizará un enfoque por cada nivel contexto, contenedor y componente, describiendo los componentes identificados; como son: tecnologías, componentes y protocolos.

Finalmente, se incluye en el presente diseño los diagramas de Landscape y Deployment para una mejor comprensión de la arquitectura propuesta.

3.1.1 Contexto del Sistema.

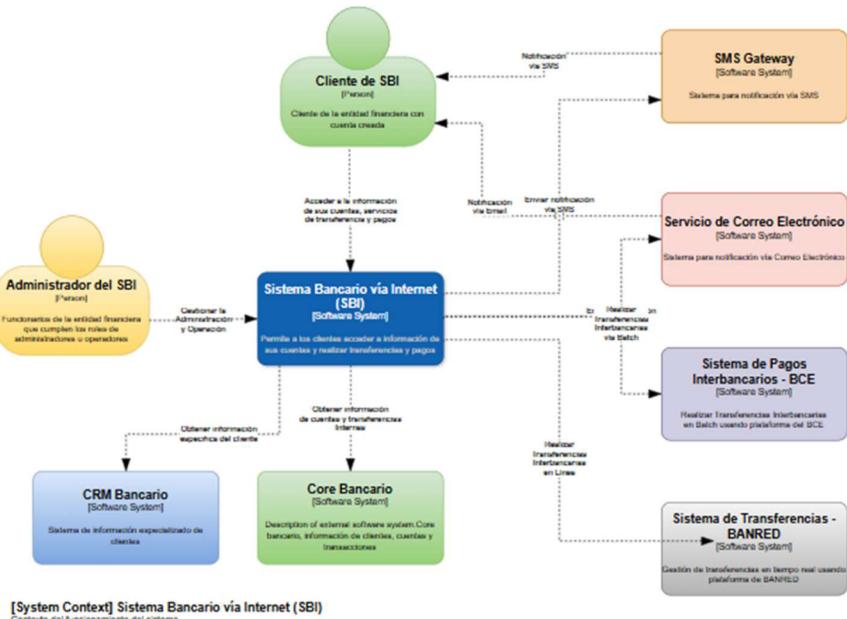


Ilustración 1. Diagrama de Contexto - Sistema Bancario Internet

En el Contexto del Sistema se identifican dos actores que interactúan con el sistema que son los clientes y administrador/operator.

Cliente del SBI: son clientes de la institución bancaria con un o varias cuentas creadas en la entidad bancaria. Los clientes podrán acceder a los servicios del Sistema Bancario vía Internet (estados de cuentas, servicios de transferencia y pagos) a través de la aplicación web usando un browser (Firefox, Edge, Chrome) o mediante una aplicación para dispositivo móvil (smartphone Apple iOS o Android).

Administrador/Operador del SBI: corresponde al personal o staff de la institución financiera, la cual cumple con los roles de administrador y operador del Sistema Bancario vía Internet, los cuales accederán al sistema a través de una aplicación web que les permita realizar las actividades de: gestionar la lógica o reglas del negocio, orquestación de transacciones, parametrización, monitoreo, consultas, solución de incidentes, entre otros.

Adicionalmente, se estable la integración a través de API con sistemas especializados que dispone la institución y con sistemas o pasarelas de pagos y transferencias interbancarias.

Sistemas especializados del Core Bancario: este sistema proveerá la información de las cuentas de los clientes, sus reglas o lógica de negocio, movimientos de las cuentas y estados de cuenta; las transacciones que se realicen a través del Sistema Bancario vía Internet se registraran en el Core Bancario.

Sistema CRM de clientes: este sistema especializado proveerá información complementaria de los clientes, para de esta manera poder ofrecer una visión integral de los productos y servicios que dispone el cliente en la institución bancaria.

Sistema de Pagos Interbancario BCE: sistema especializado externo provisto por el Banco Central del Ecuador, el mismo que permite realizar transferencias interbancarias en Batch y gestionar pagos de servicios con todo el ecosistema financiero.

Sistema de Transferencias de BANRED: sistema especializado externo provisto por el BANRED, el mismo que permite realizar transferencias interbancarias en línea y gestionar pagos de servicios con las instituciones adscritas a BANRED

Finalmente, se requiere de la integración con servicios de notificación, el primero es vía correo electrónico y el segundo vía Gateway SMS, este servicio permitirá remitir a los clientes información de OTP, alertas de movimientos, confirmaciones, mensajes informativos, entre otros

Notificación vía correo electrónico: provisto como un servicio en nube, el cual puede ser implementado a través de Amazon Simple Email Service (SES), Azure Communication Services (ACS), Gmail API, SendGrid. Se deberá implementar este servicio vía SMTP y API, lo cual nos dará un esquema de contingencia.

Notificación vía SMS: considerando un esquema de alta disponibilidad y contingencia para el servicio, se recomienda implementar un esquema híbrido mediante el uso de un Gateway SMS local, el cual tenga la primera opción para gestionar las notificaciones, con ello se solventarían temas asociados a costos y cumplimiento de normativa emitida por los organismos de control (Superintendencia de Bancos); y como una segunda prioridad y en caso de fallo del primero, el uso de un servicio en nube, para lo cual se pueden explorar las opciones de Amazon SNS (Simple Notification Service), Azure Communication Services (ACS), Twilio.

Se anexa al presente informe el Diagrama de Contexto del Sistema Bancario vía Internet.

3.1.2 Contenedores del Sistema.

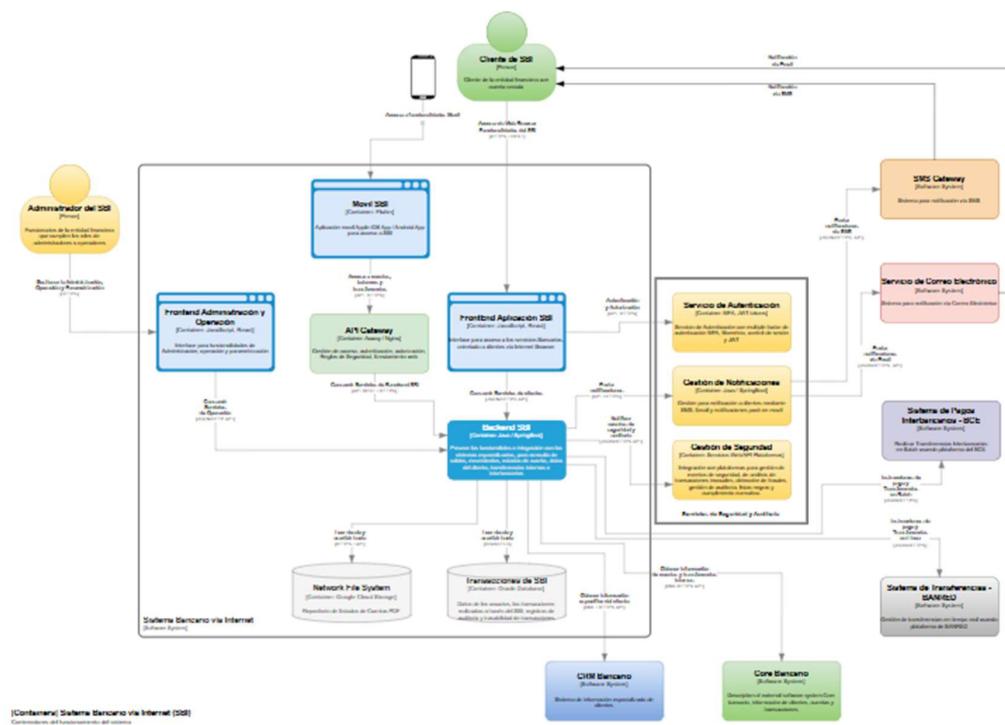


Ilustración 2. Diagrama de Contenedores - Sistema Bancario Internet

A nivel de contenedores se heredan los mismos usuarios, sistemas especializados y servicios de notificación, de acuerdo a lo establecido el diagrama de contexto del sistema. Adicionalmente, a nivel de Contenedores del sistema se identifican los siguientes componentes:

FrontEnd de Administración y Operación: provee la interface para brindar las funcionalidades o servicios para establecer la lógica o reglas del negocio, orquestación de transacciones, parametrización, monitoreo, consultas, solución de incidentes, entre otros. El acceso se realizará desde las estaciones clientes a través de navegadores web (Firefox, Edge, Chrome) a través de un servicio seguro vías HTTPS.

En referencia al framework de trabajo para este contenedor, se analizó la utilización de herramientas como React y Angular, las dos herramientas presentan un buen rendimiento, están muy bien posicionadas a nivel nacional; sin embargo la selección para este proyecto sería React usando JavaScript, esta decisión se la realiza considerando que se encuentra altamente difundida en el país y su curva de aprendizaje es rápida, lo cual facilitaría el establecer un equipo de trabajo con experiencia en la utilización de esta herramienta. Adicionalmente, se podrán cumplir los requerimientos de seguridad, mantenibilidad, escalabilidad y cumplimiento de estándares.

FrontEnd Aplicación SBI: provee la interface para brindar las funcionalidades o servicios a los clientes del Sistema Bancario vía Internet, a través de la cual se establecerán los servicios de acceso, autenticación y autorización en el sistema, información de los productos o servicios a los cuales tiene acceso el cliente, consulta de estados de cuenta, realizar transferencias internas, transferencias interbancarias, pagos de servicios, entre otros. El acceso se realizará desde las estaciones clientes a través de navegadores web (Firefox, Edge, Chrome) a través de un servicio seguro vías HTTPS.

En referencia al framework de trabajo para este contenedor, se analizó la utilización de herramientas como React y Angular, las dos herramientas presentan un buen rendimiento, están muy bien posicionadas a nivel nacional; sin embargo la selección para este proyecto sería React usando JavaScript, esta decisión se la realiza considerando que se encuentra altamente difundida en el país y su curva de aprendizaje es rápida, lo cual facilitaría el establecer un equipo de trabajo con experiencia en la utilización de esta herramienta. Adicionalmente, se podrán cumplir los requerimientos de seguridad, mantenibilidad, escalabilidad y cumplimiento de estándares.

FrontEnd Aplicación Móvil: provee una aplicación móvil para brindar las funcionalidades o servicios a los clientes del Sistema Bancario vía Internet, a través de la cual se establecerán los servicios de acceso, autenticación y autorización en el sistema, información de los productos o servicios a los cuales tiene acceso el cliente, realizar transferencias internas, transferencias interbancarias, pagos de servicios, entre otros. El acceso se realizará desde dispositivos móviles (Apple iOS y Android) a través de un servicio seguro vías HTTPS y conexión con el BackEnd del SBI mediante un API Gateway.

En referencia al framework de trabajo para este contenedor, se analizó la utilización de herramientas como Flutter y React Native, las dos herramientas presentan un buen rendimiento, están muy bien posicionadas y líderes en el desarrollo de aplicaciones móviles; sin embargo la selección para este proyecto sería Flutter, esta decisión se la realiza considerando que se encuentra altamente difundida en el país y su curva de aprendizaje es rápida, lo cual facilitaría el establecer un equipo de trabajo con experiencia en la utilización de esta herramienta. Adicionalmente, el respaldo de Google para esta herramienta garantiza estabilidad y sostenibilidad en el tiempo.

API Gateway: es el componente que permite el acceso de la aplicación móvil a los servicios que brinda el BackEnd del Sistema Bancario vía Internet. Este componente es el punto de acceso único de la aplicación móvil y brinda los servicios a través de un canal seguro con TLS, cumple con las funciones autenticación OAuth2, gestiona el acceso (logger y auditoria), enruta a los servicios de BackEnd.

Para la implementación del API Gateway se pueden utilizar servicios en nube (AWS API Gateway, Azure API Management (APIM)); así como plataformas OnPremise tales como Axway API Gateway. Considerando que el sistema está orientado hacia clientes móviles la recomendación sería la utilización de una plataforma en nube como AWS API Gateway.

BackEnd del Sistema SBI: este contendor se encarga de atender los requerimientos realizados por las interfaces del FrontEnd, provee la lógica para procesar las transacciones y conectar con los sistemas especializados y de esta manera brindar los servicios; se convierte en el core del Sistema Bancario vía Internet; ya que gestiona, las

conexiones con los sistemas Core Bancario, CRM Bancario, Sistemas de Pagos Interbancarios BCE, Sistema Transferencias de BANRED.

Adicionalmente, el BackEnd del SBI permite la integración con las plataformas de notificación vía correo electrónico y mensajes SMS; así como integración con las plataformas de seguridad, auditoria, control de acceso, autenticación y autorización.

Desde la perspectiva tecnológica la implementación del BackEnd puede realizarse mediante un Framework con soporte de Java, ya sea estos alojados en la nube en ambientes virtualizados o en plataformas OnPremise. Para la implementación del proyecto se recomendaría alojar los mismos en un proveedor de nube con Spring Boot. El uso de ambientes virtualizados garantizará el crecimiento vertical y horizontal de recursos en caso de ser requerido; así como, la disponibilidad del servicio y esquemas de contingencia.

Sistema Almacenamiento Red: repositorio digital para almacenar los estados de cuenta de los clientes. Algunas consideraciones que se deben tomar en cuenta para almacenar esta información en la nube son: seguridad (encriptación, control de acceso, disponibilidad, confidencialidad), uso de metadatos para gestionar la búsqueda, asociación con clientes, indexación y clasificación de la información; y costo de mantener el almacenamiento en línea, por lo cual se requiere un esquema de archive en la nube para almacenar la información menos acezada.

Este servicio será implementado mediante un servicio en nube que permita las funcionalidades de un Gestor de Contenido Empresarial (ECM). Considerando que para el proyecto se ha definido la utilización de servicios AWS , se plantea los siguientes componentes: Amazon Simple Storage Service (S3) para almacenamiento de datos en línea, Amazon S3 Glacier para archive de datos; y Amazon DynamoDB para gestión de metadatos.

Base de Datos del Sistema SBI: la instancia de Base de Datos del Sistema Bancario vía Internet, almacenará la información de las transacciones realizadas en el sistema y de los usuarios del mismo. Esta componente estará resguardada por un firewall de Base de Datos y debe permitir esquema de encriptación de datos en reposo, auditoria de las transacciones de la base datos.

Para implementar este contenedor se puede explorar las alternativas de Bases de Datos transaccionales SQL tales como Oracle, PostgreSQL, SQL Server, entre otras. Considerando los volúmenes de transaccionalidad que se esperaría de este tipo de sistemas debemos disponer de un esquema robusto y seguro con esquemas de alta disponibilidad y contingencia. Para implementar este proyecto se recomendaría la utilización de Oracle, considerando que en el mercado local existe un alto número de profesionales con experiencia en su manejo, que es un líder en el mercado local en la implementación de sistemas críticos y que dispone de las herramientas para garantizar alta disponibilidad, seguridad. Este componente también podría estar alojado en la infraestructura de WAS a través del servicio de Amazon RDS Oracle.

Adicionalmente, se incluyen servicios asociados a seguridad y auditoria que deben ser consumidos por el Sistema Bancario vía Internet por los API de integración especializados de cada plataforma; entre los cuales están:

Servicios de Autenticación: soporte de autenticación mediante OAuth2, soporte de múltiple factor de autenticación (MFA), onboarding de Biométría, control de sesión y gestión de tokens JWT

Servicios para la Gestión de Notificaciones: son los servicios de notificación de correo electrónico y mensajería SMS tal como se describió en el diagrama de contexto del sistema.

Servicios para la Gestión de Seguridad y Auditoría: este componente permite la integración con plataformas para gestión de eventos de seguridad (SIEM), Plataforma de Data Lost Prevention (DLP), de análisis de transacciones inusuales y detección de fraudes, gestión de auditoría, manejo de listas negras OFAC, de monitoreo de funcionamiento de los servicios web del sistema y otras herramientas que permitan el cumplimiento normativo.

Se anexa al presente informe el Diagrama de Contenedores del Sistema Bancario vía Internet

3.1.3 Componentes del Sistema.

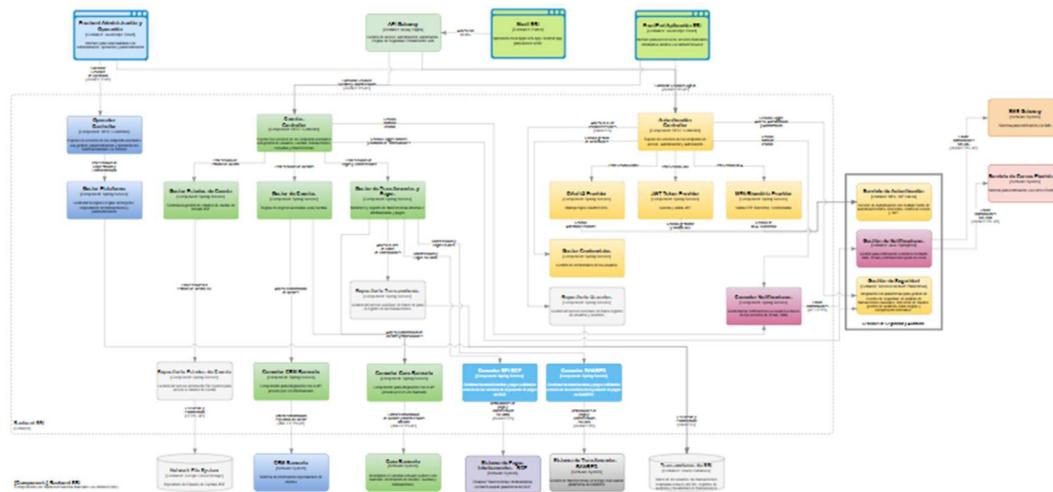


Ilustración 3. Diagrama de Componentes - Sistema Bancario Internet

En referencia a los componentes identificados para el Sistema Bancario vía Internet se han identificado los siguientes componentes.

Controlador de Autenticación: expone los servicios de los EndPoints de acceso, autenticación y autorización, hacia los clientes del sistema. Este es un componente dentro de un BackEnd basado en servicios REST con Spring Boot.

OAuth2 Provider: se encarga de la autenticación y autorización de las conexiones y peticiones al sistema, gestiona el token JWT para validar los requerimientos.

JWT Provider: se encarga de proveer el Token JWT para el proceso de autenticación y autorización de las transacciones y peticiones al sistema así como validar que los tokens sean válidos, no se encuentren expirados.

MFA/Biométrico Provider: se encarga de proveer acceso a los sistemas de autenticación de múltiple factor, para incorporar un segundo factor de autenticación, adicional al usuario y password; adicionalmente se encarga de la integración con el sistema de OnBoarding y validación en base a Biometría.

Gestor de Credenciales: este componente contiene la lógica del sistema para la gestión de los usuarios y sus credenciales. Este es un componente dentro de un BackEnd basado en servicios REST con Spring Service.

Controlador de Cuentas: expone los servicios de los endpoints de cuentas, transacciones, consultas, transferencias y pagos, hacia los clientes del sistema. Este es un componente dentro de un BackEnd basado en servicios REST con Spring Boot.

Gestor de Estados de Cuenta: este componente contiene la lógica del sistema para la gestión de los usuarios y sus credenciales. Este es un componente dentro de un BackEnd basado en servicios REST con Spring Service.

Repositorio de Estados de Cuenta: este componente contiene la lógica del sistema para la gestión de los estados de cuenta en formato PDF. Este es un componente dentro de un BackEnd basado en servicios REST con Spring Service.

Gestor de Cuentas: este componente contiene la lógica del sistema para la gestión de las cuentas y de las reglas de negocio asociadas a las cuentas. Este es un componente dentro de un BackEnd basado en servicios REST con Spring Service.

Gestor de Transferencias y Pagos: este componente contiene la lógica del sistema para la gestión, monitoreo y registro de las transacciones de transferencias internas e interbancarias, el pago de servicios. Este es un componente dentro de un BackEnd basado en servicios REST con Spring Service.

Repositorio de Transacciones: este componente maneja la persistencia en base de datos para el registro de las transacciones ejecutadas por los usuarios.

Repositorio de Usuarios: este componente maneja la persistencia en base de datos para el registro de los usuarios, perfiles y registro de acceso.

Controlador de Operaciones: expone los servicios de los endpoints para la operación y administración del Sistema Bancario vía Internet, hacia los administradores y operadores del staff de la institución bancaria. Este es un componente dentro de un BackEnd basado en servicios REST con Spring Boot.

Gestor de la Plataforma: este componente contiene la lógica del sistema para las administración y operación del sistema, y configurar las reglas del negocio, orquestación de transacciones y parametrización. Este es un componente dentro de un BackEnd basado en servicios REST con Spring Service.

Conector de Notificaciones: componente de integración que sirve como puente entre tu BackEnd y los servicios de notificación vía correo electrónico y SMS, este componente

debe ser desarrollado en base a las tecnologías y protocolos expuestos por el servicio de notificación.

Conector Core Bancario: componente de integración que sirve como puente entre tu BackEnd y los servicios provistos por el Core Bancario, este componente debe ser desarrollado en base a las tecnologías y protocolos expuestos por el Core Bancario.

Conector CRM Bancario: componente de integración que sirve como puente entre tu BackEnd y los servicios provistos por el CRM Bancario, este componente debe ser desarrollado en base a las tecnologías y protocolos expuestos por el CRM Bancario.

Conector SPI BCE: componente de integración que sirve como puente entre tu BackEnd y los servicios provistos por Sistema de pagos Interbancarios del BCE, este componente debe ser desarrollado en base a las tecnologías, protocolos expuestos y norma técnica de integración definido por el SPI del BCE.

Conector Transferencia BANRED: componente de integración que sirve como puente entre tu BackEnd y los servicios provistos por Sistema de Transferencias de BANRED, este componente debe ser desarrollado en base a las tecnologías, protocolos expuestos y norma técnica de integración definido por BANRED.

Se anexa al presente informe el Diagrama de Componentes del Sistema Bancario vía Internet

[3.2 Diagramas Complementarios del Sistema.](#)

Se han establecido diagramas complementarios con son el Diagrama de Landscape y el diagrama de Deployment.

En el diagrama de Landscape se muestra una vista de alto nivel del Sistema Bancario vía Internet y su interrelación con otros sistemas y servicios que brinda la institución bancaria.

El diagrama de Deployment esta enfocado a los componentes de infraestructura que son requeridos para la implementación y despliegue del Sistema Bancario vía Internet, en el cual se puede apreciar la relación con los componentes tales como Firewall de Aplicaciones Web, Firewall de Base de Datos, Balanceadores de carga local y geográfico y firewall de acceso perimetral.

Se anexa al presente informe el Diagrama de Landscape y Deployment del Sistema Bancario vía Internet.

[3.3 Consideraciones de Seguridad y Marco Normativo.](#)

El Sistema Bancario vía Internet deberá cumplir con un estricto marco normativo, el cual esta enfocado a garantizar la confidencialidad, integridad y disponibilidad del sistema y sus datos, entre los marcos normativos aplicables podemos mencionar los siguientes:

- Normas de Control para la Gestión del Riesgo, incluidas en la Norma de control para las entidades de los sectores financieros público y privado, emitida por la Superintendencia de Bancos.
- Ley de protección de datos personales

- Estándar PCI DSS (Payment Card Industry – Data Security Standard)
- Estándar ISO/IEC 27001 Sistema de Gestión de la Seguridad de la Información
- Norma ISO 20022 Intercambio de Datos en el Sector Financiero
- Esquema Gubernamental de Seguridad de la Información (aplicable al sector financiero público)
- Normas de Control Interno (aplicable al sector financiero público)
- Política de seguridad de la información elaborada por la Institución bancaria

Entre las herramientas de seguridad necesarias para garantizar un ecosistema seguro para el Sistema Bancario vía Internet, se pueden mencionar a las siguientes:

- Firewall de Aplicaciones Web (WAF)
- Firewall perimetral
- Firewall de Base de Datos
- Sistema de Prevención y Detección de Intrusiones (IPS/IDS)
- Denegación de Servicio Distribuido (DDoS)
- Data Lost Prevention (DLP)
- Gestor de Eventos de Seguridad de la Información (SIEM)
- Sistema antifraude y análisis de transacciones inusuales
- Servicio de Listas de Sanciones (SLS) de la OFAC – Listas Negras
- Servicio para encriptación de bases de datos
- Plataforma de monitoreo de servicios y aplicaciones web
- Utilización de certificados digitales para los dominios de los servicios y de esta manera exponer los servicios a través de puertos seguros, minimizando el riesgo de Phishing.
- Servicios provistos por empresas especializadas para mitigar el riesgo de Phishing y evaluar el nivel de seguridad del sistema.

En referencia al proceso de autenticación y autorización de los clientes utilizando un servicio basado en el estándar OAuth2, se podría incorporar el siguiente flujo:

1. El cliente móvil o aplicación Web realiza el requerimiento de autenticación ingresando sus credenciales en el servidor de autorización (OAuth).
2. El servidor de autorización atiende el requerimiento.
3. El cliente obtiene el Access Token JWT y el Refresh Token.
4. El API Gateway valida el Access Token remitido por el cliente.
5. El API Gateway redirecciona las solicitudes a los servicios provistos por el BackEnd.

3.4 Consideraciones de Alta Disponibilidad y Contingencia.

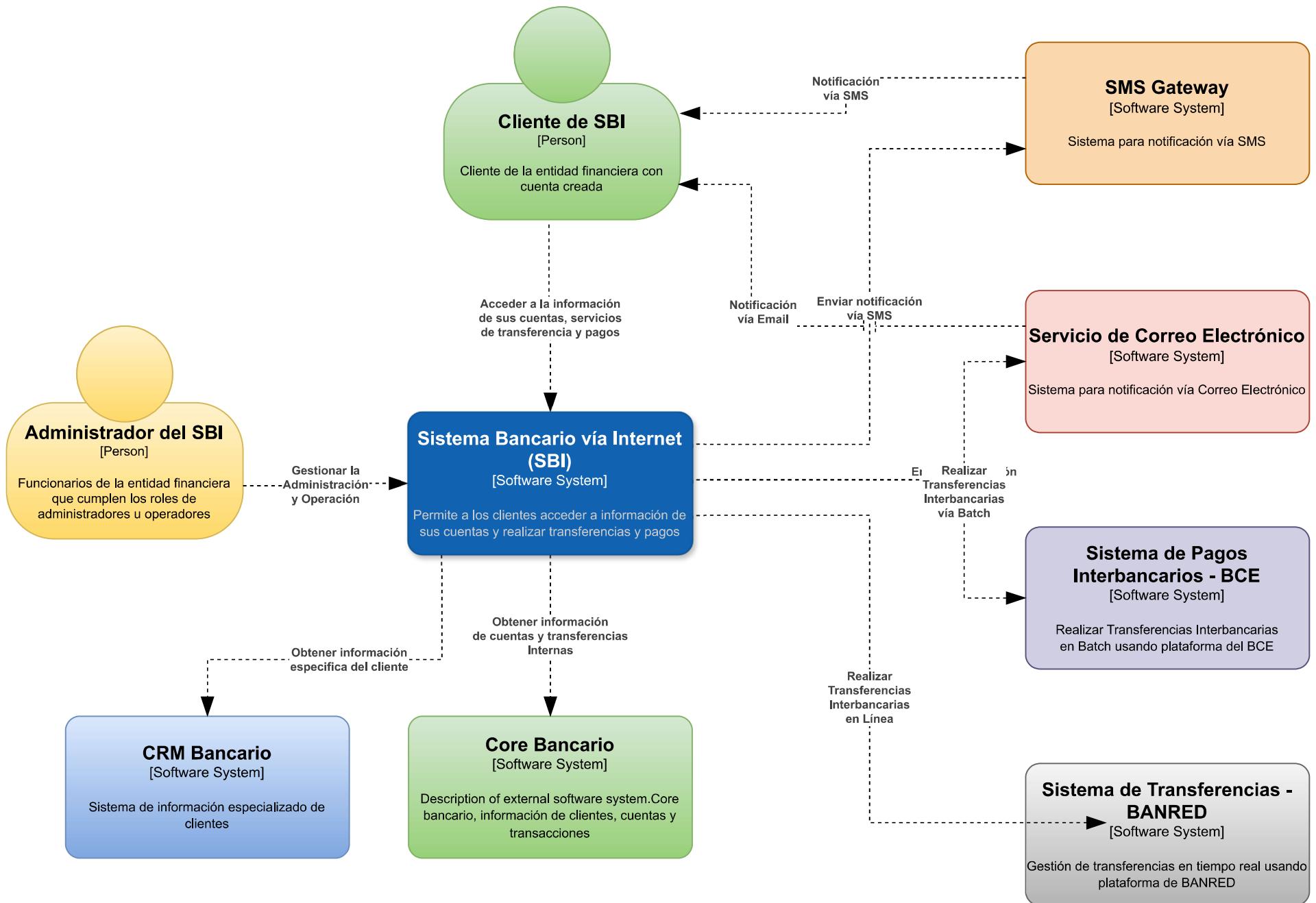
En referencia a los esquemas de alta disponibilidad y contingencia, para el Sistema Bancario vía Internet se han considerado los siguientes aspectos:

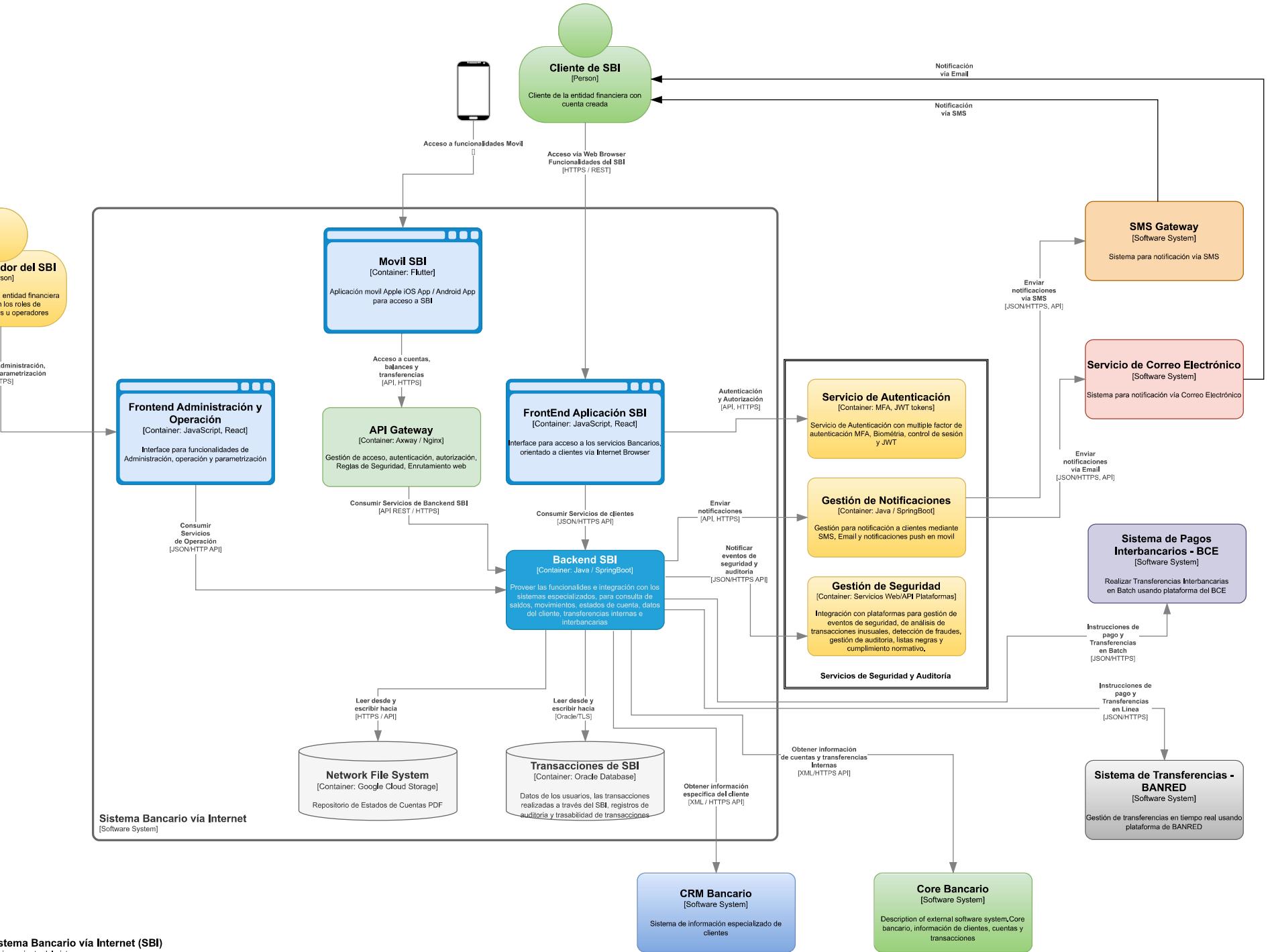
- Implementar el acceso a los servicios a través de un Firewall de Aplicaciones (WAF) localizado en la nube, el cual adicionalmente permitirá cumplir con el control de ataques de Denegación de Servicio (DDoS).
- Implementación de Balanceadores de Carga Geográficos, el cual permitirá acceder a una granja de servidores virtualizados, lo cual garantiza la alta disponibilidad, la redundancia geográfica; así como, la capacidad de crecimiento horizontal y vertical de recursos.

- Implementación de un Firewall perimetral de Nueva Generación, en el cual se configurarán esquemas de segmentación de la red y zonas seguras (DMZ) para los componentes expuestos hacia los clientes.
- Implementación de Balanceadores de Carga Local, los cuales permitirán un acceso a una granja de servidores virtualizados que alojarán el BackEnd, lo cual garantiza la alta disponibilidad, la redundancia geográfica; así como, la capacidad de crecimiento horizontal y vertical de recursos.
- Implementar los componentes en servidores virtualizados o servicio en nube provistos por un proveedor especializado como son los servicios de AWS, lo cual permite garantizar la alta disponibilidad y contingencia para varios de los componentes del diseño.
- Implementación de la base de datos del sistema en un servicio en nube, lo cual permite garantizar la alta disponibilidad y contingencia; adicionalmente se deberá generar una replica de la información a una segunda instancia de la base datos; así como los esquemas de respaldos correspondientes.

4. FIRMA DE RESPONSABILIDAD

Elaborado por: Victor Barrionuevo Bolaños	
---	--





[Containers] Sistema Bancario vía Internet (SBI)
Contenedores del funcionamiento del sistema

