Modelo de Pagos - MVP

Arquitectura Empresarial

14-08-2020

Versión 1.3

Itaú

2017

Pagos | Contexto

Objetivo

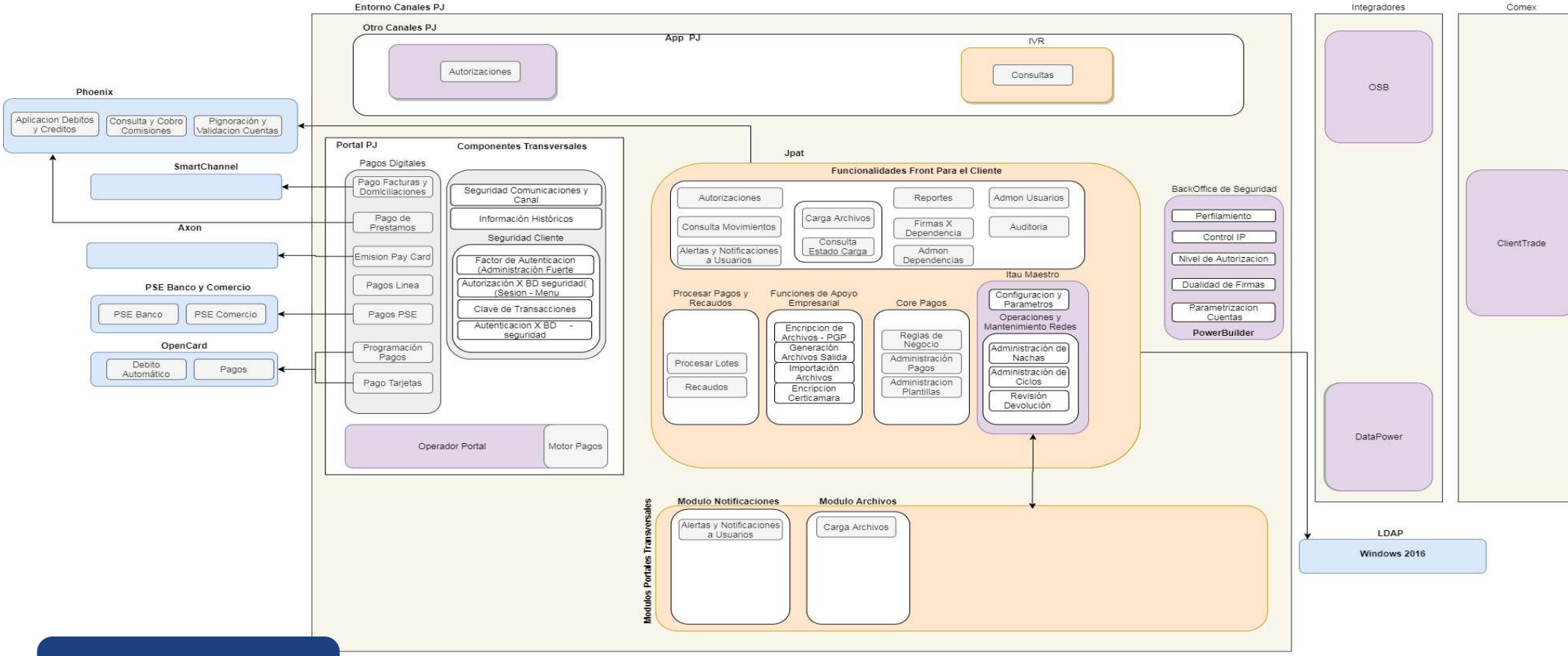
Optimizar el proceso de pagos a terceros buscando mejorar la experiencia del cliente y el flujo del usuario final.

- Activación nuevos Servicios de AWS

Premisas

- Existen componentes transversales de Portal PJ que no son del alcance del proyecto.
- No esta dentro del alcance las modificaciones de Perfiles y usuarios.
- Proceso aplica para clientes existentes.

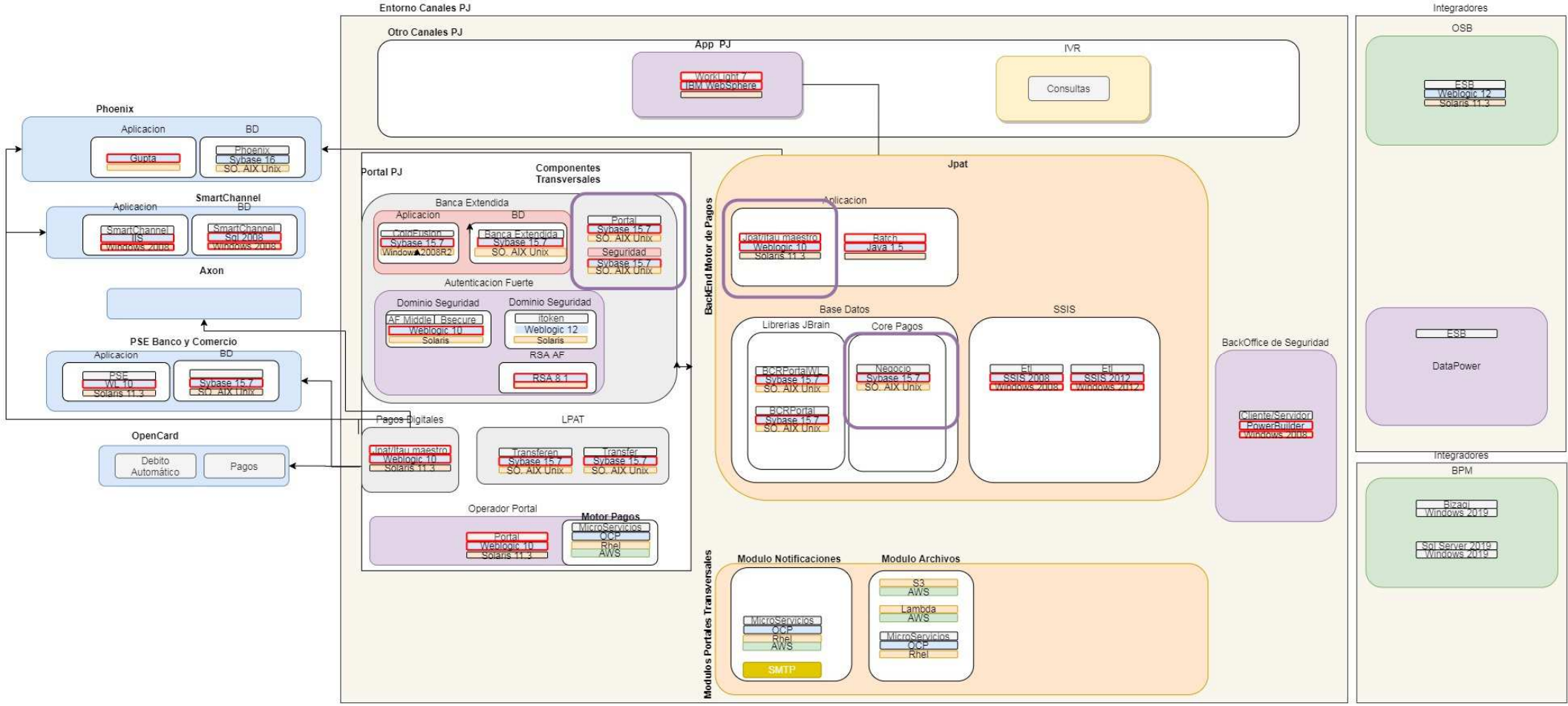
Pagos | Arquitectura Funcional - MVP | Portal PJ



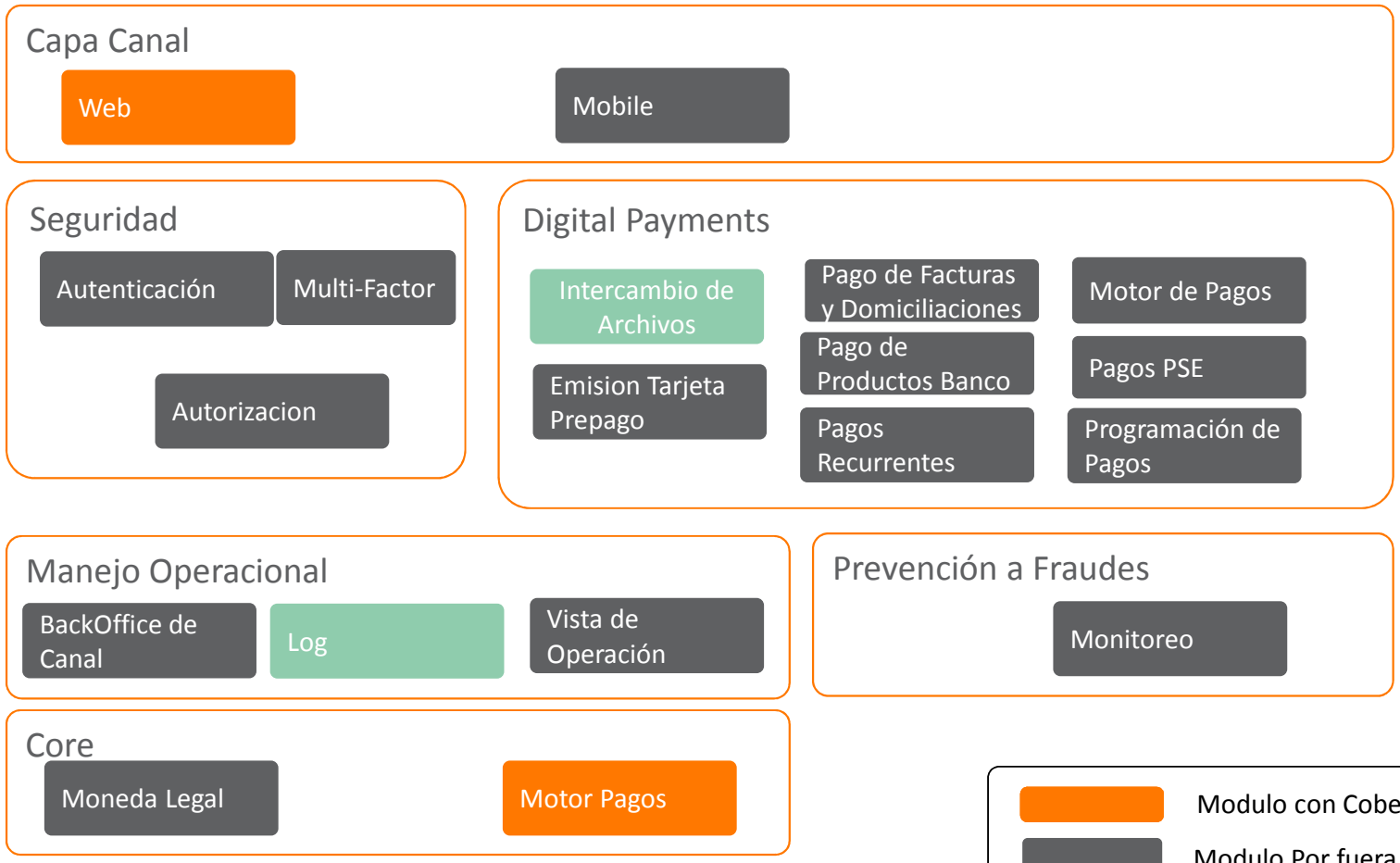
Puntos de Atención

- Se hacer una división del back y del tema de Front.
- Se hace cubrimiento inicial para algunos puntos de componentes transversal
- Jpat sigue con todas las funcionalidades actuales, algunos módulos deberían ser parte del canal y no del back.

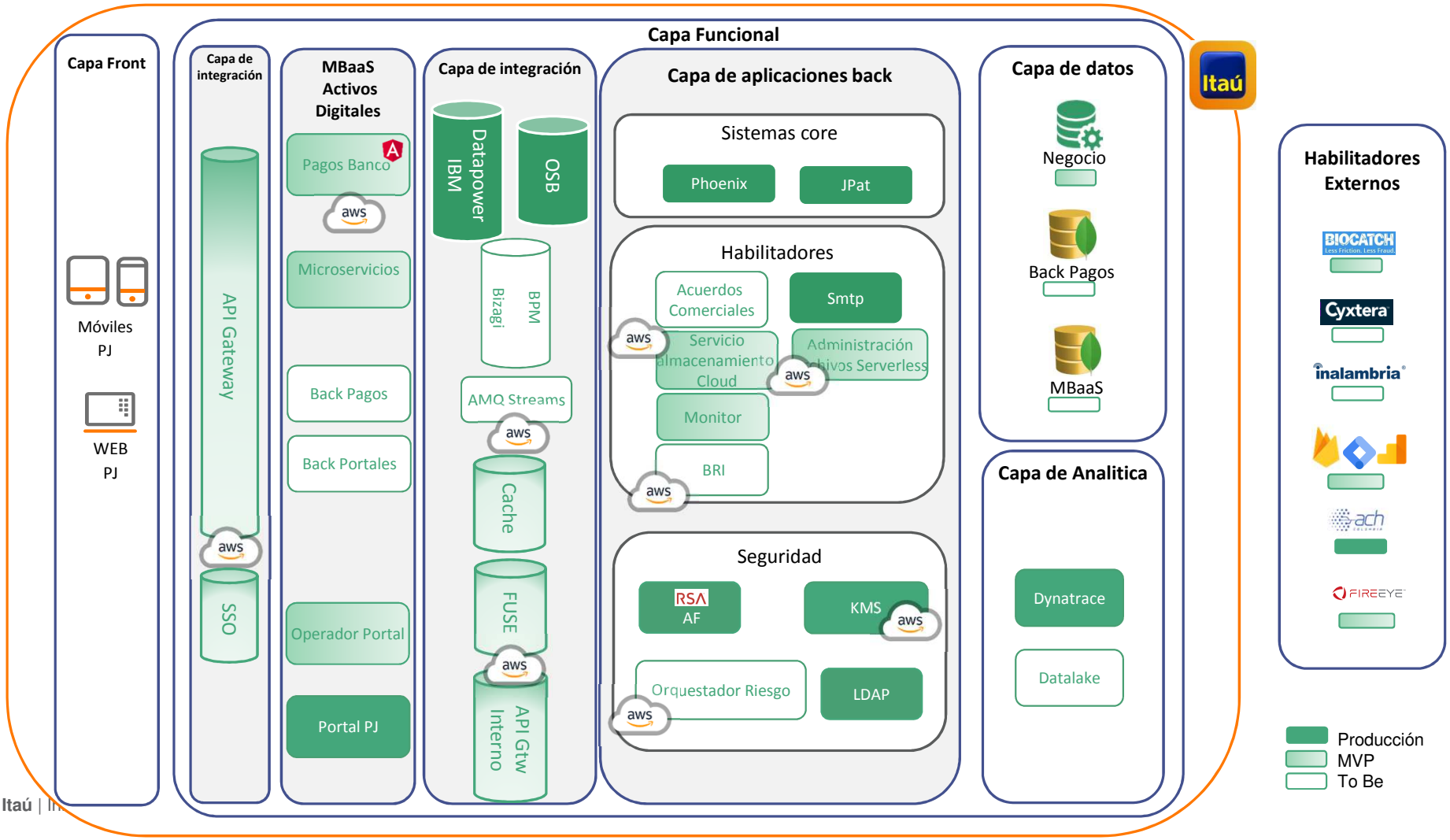
Pagos | Arquitectura Funcional - MVP | Infraestructura



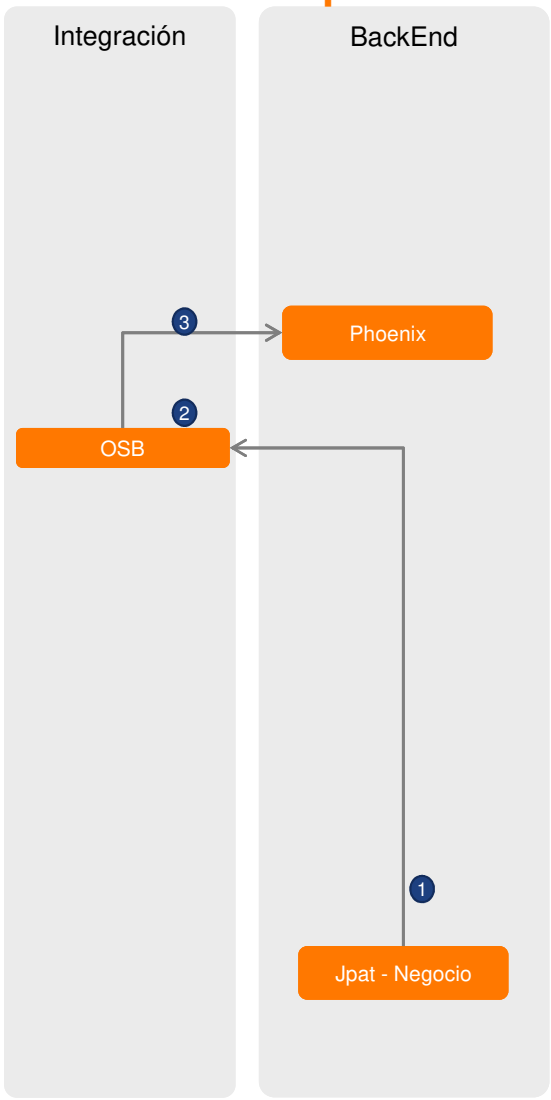
Pagos | Modelo General



Pagos | Arquitectura Componentes

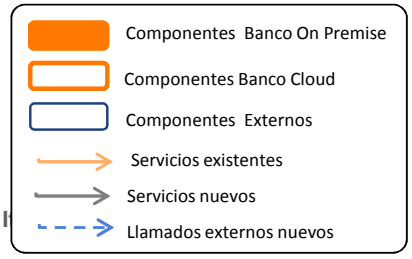


Pagos MVP | Arquitectura Capas | 1. Administración Jpat

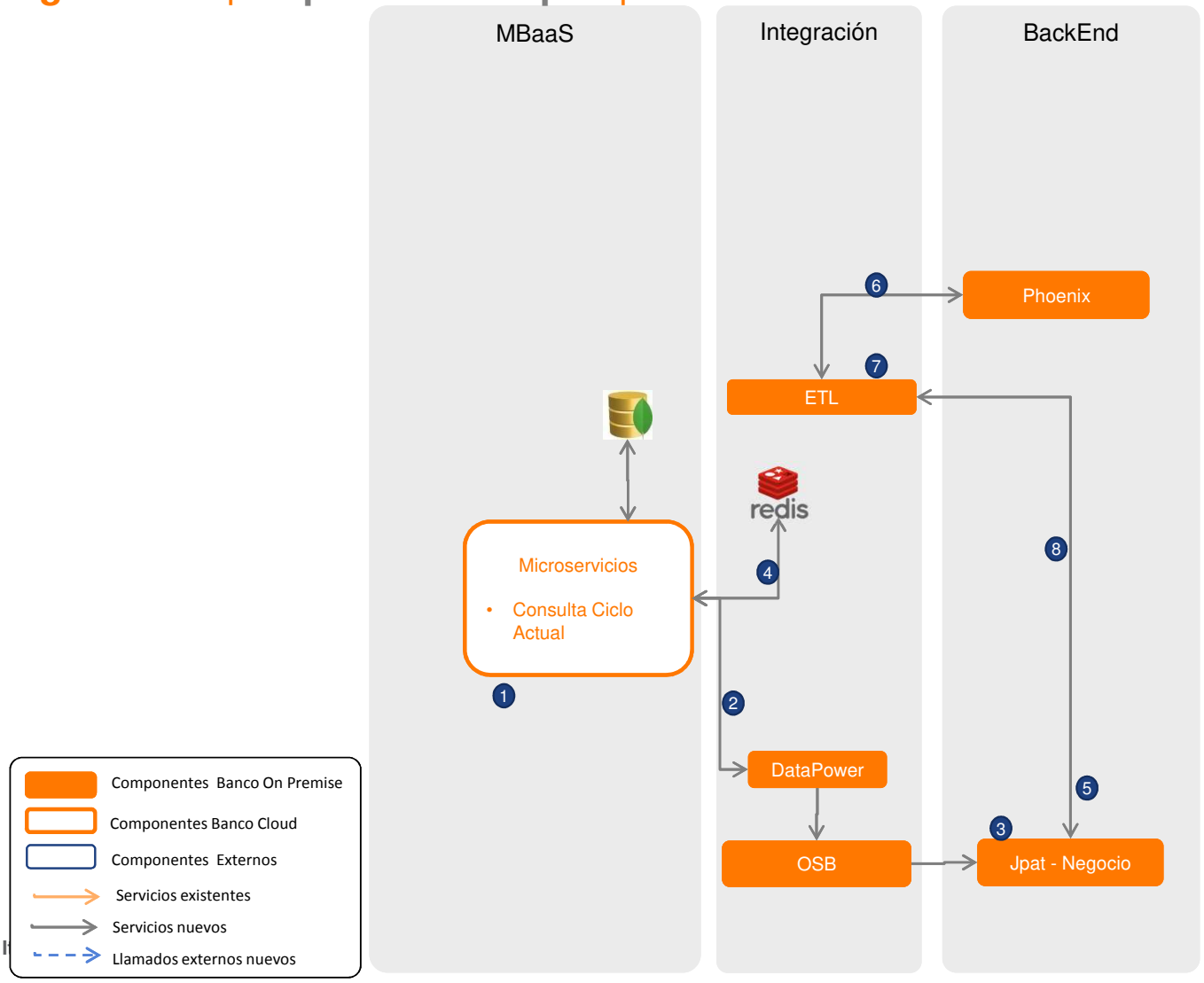


Temas Transversales

1. Para la administración de usuario único, que se realiza sobre el Jpat actual, se modifica la aplicación actúal.
2. Se debe consultar el servicio existente de OSB para consulta de Cliente para consultar el segmento.



Pagos MVP | Arquitectura Capas | 2. General



Temas Transversales

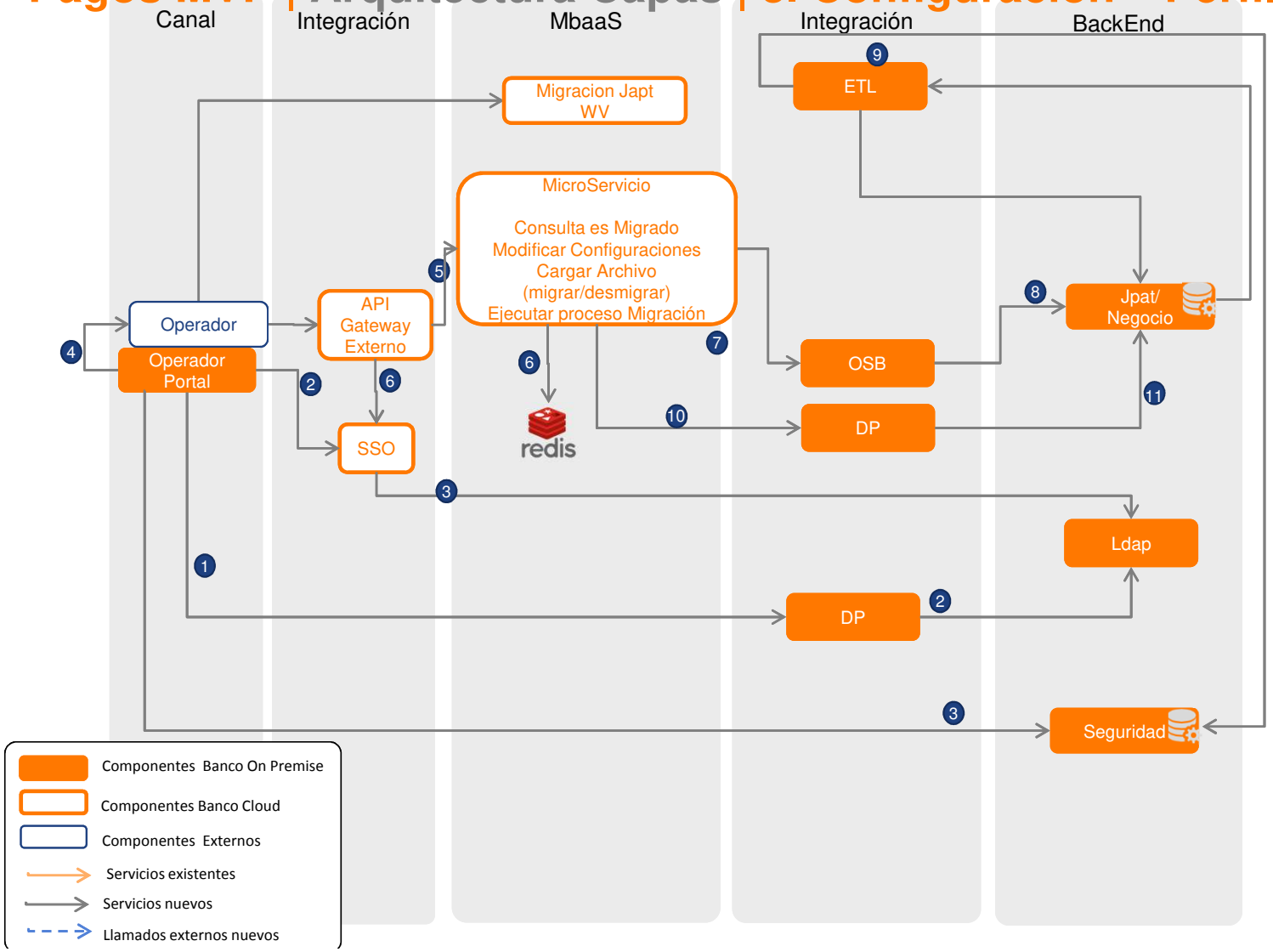
1. Se debe tener un Ms job que cargue la información del ciclo (numero de ciclo y hora inicio y hora finalización del ciclo). Esta información se debe cargar al cache para consulta de todos los clientes. En esta info se debe indicar si esta en ciclo extra temporáneo. Esto se debe actualizar cada x minutos.

5. Cada X tiempo se esta sacando de Jpat las empresas que tienen usuario Único seleccionado.

6. Con la información de las empresas se obtiene de Phoenix la información del segmento asociado, si el segmento cambio se notifica a Jpat.

8. La etl notifica a Jpat y guarda la alerta del cambio de segmento y eliminar la configuración de usuario único.

Pagos MVP | Arquitectura Capas | 3. Configuración – Perfil - Migrados

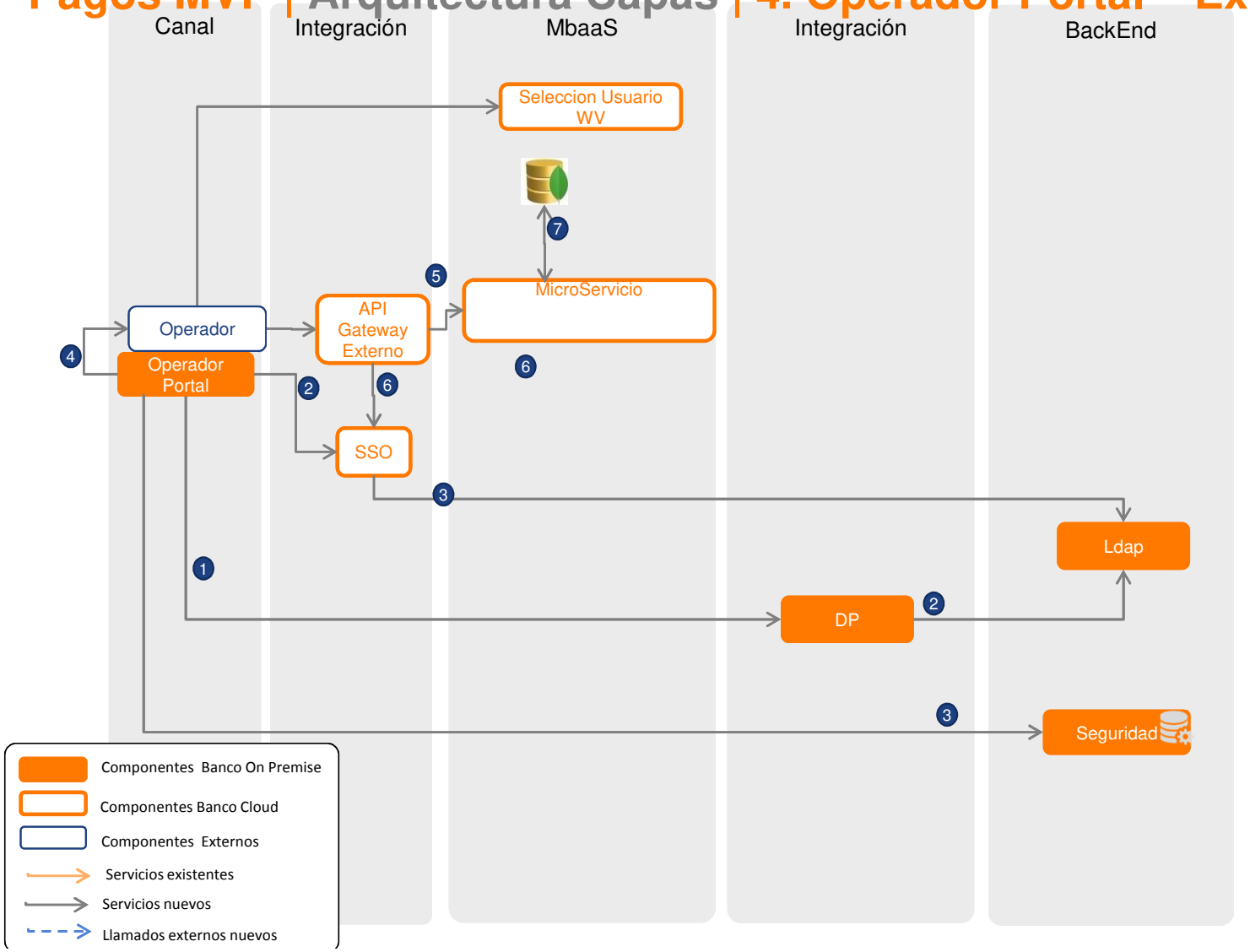


Temas Transversales

1. Se continua haciendo login como hoy día se esa realizando.
2. El Operador Portal relazaría login hacia el SSO con las credenciales del usario.
3. SSO se autentica hacia la capa de Ldap y devuelve el token.
4. Se pasa a la WebApp el token.
6. Se consulta en el cache la información del cliente, si no esta se solicita información del cliente a Negocio por medio del OSB.
9. La ETL se ejecuta y de acuerdo a la tabla de clientes migrados realiza las configuraciones necesarias en Jpat.
10. Se va a cargar el archivo de migración por el operador Portal y se va a entregar el archivo al DP. Se considera que la cantidad de archivos por este medio debe ser muy puntual y no un tema transaccional.

- Para Operador Portal no se hace alcance de la librería de crypto-Vault para este mvp.
- Se plantea que para las opciones de Motor de Pagos se valide en la pagina inicial que el cliente este migrado por medio del cache.

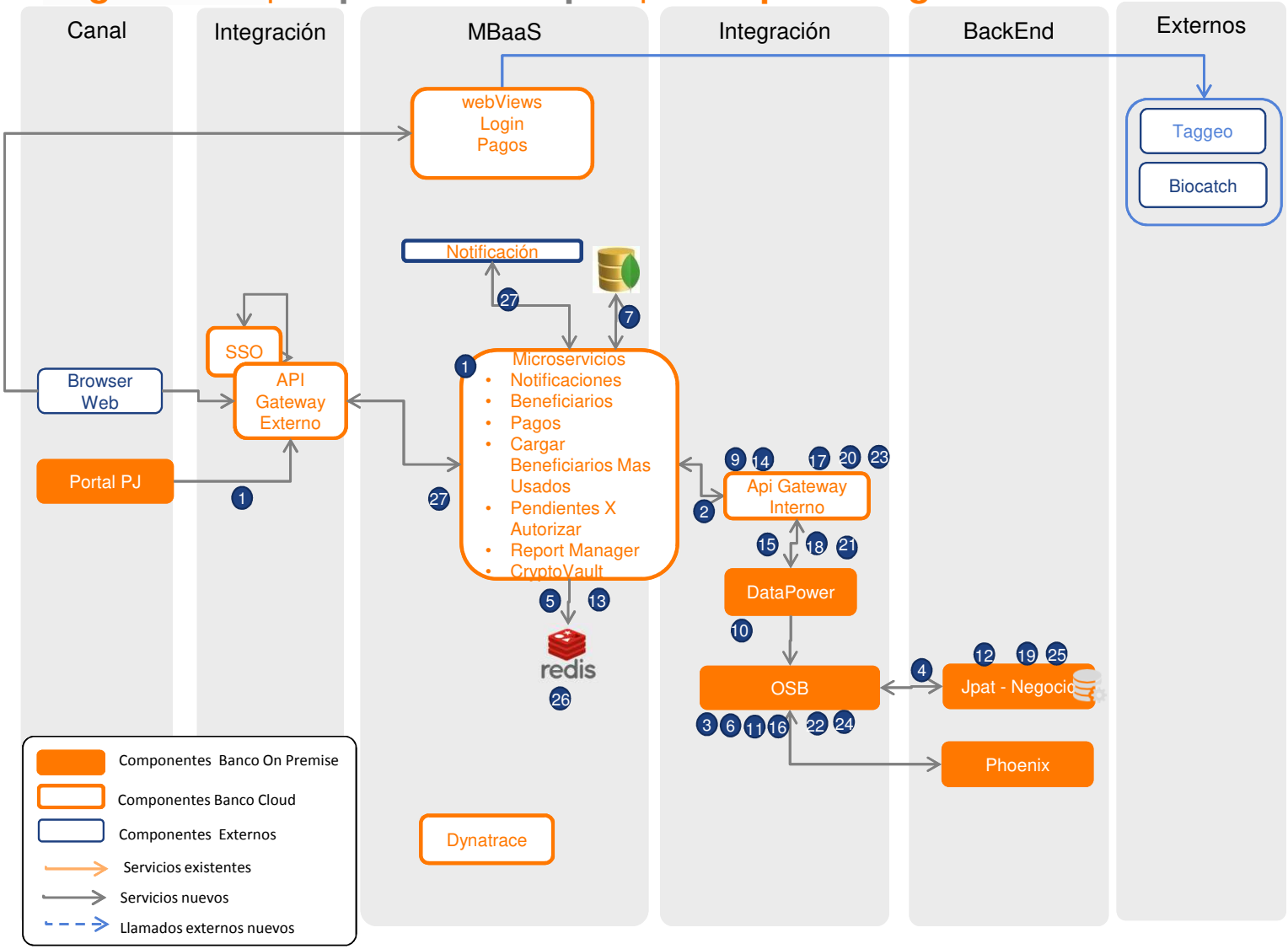
Pagos MVP | Arquitectura Capas | 4. Operador Portal – Experiencia Interna



Temas Transversales

1. Se continua haciendo login como hoy día se esa realizando.
2. El Operador Portal relazaría login hacia el SSO con las credenciales del usario.
3. SSO se autentica hacia la capa de Ldap y devuelve el token.
4. Se pasa a la WebApp el token.
6. Se usa las mismas pantallas del usuario final para mostrarlas a la parte de área central con el la información del usuario seleccionado dentro de Operador Portal.
7. Se debe cargar el tema del perfil de Operador portal para que se tome este como configuración.

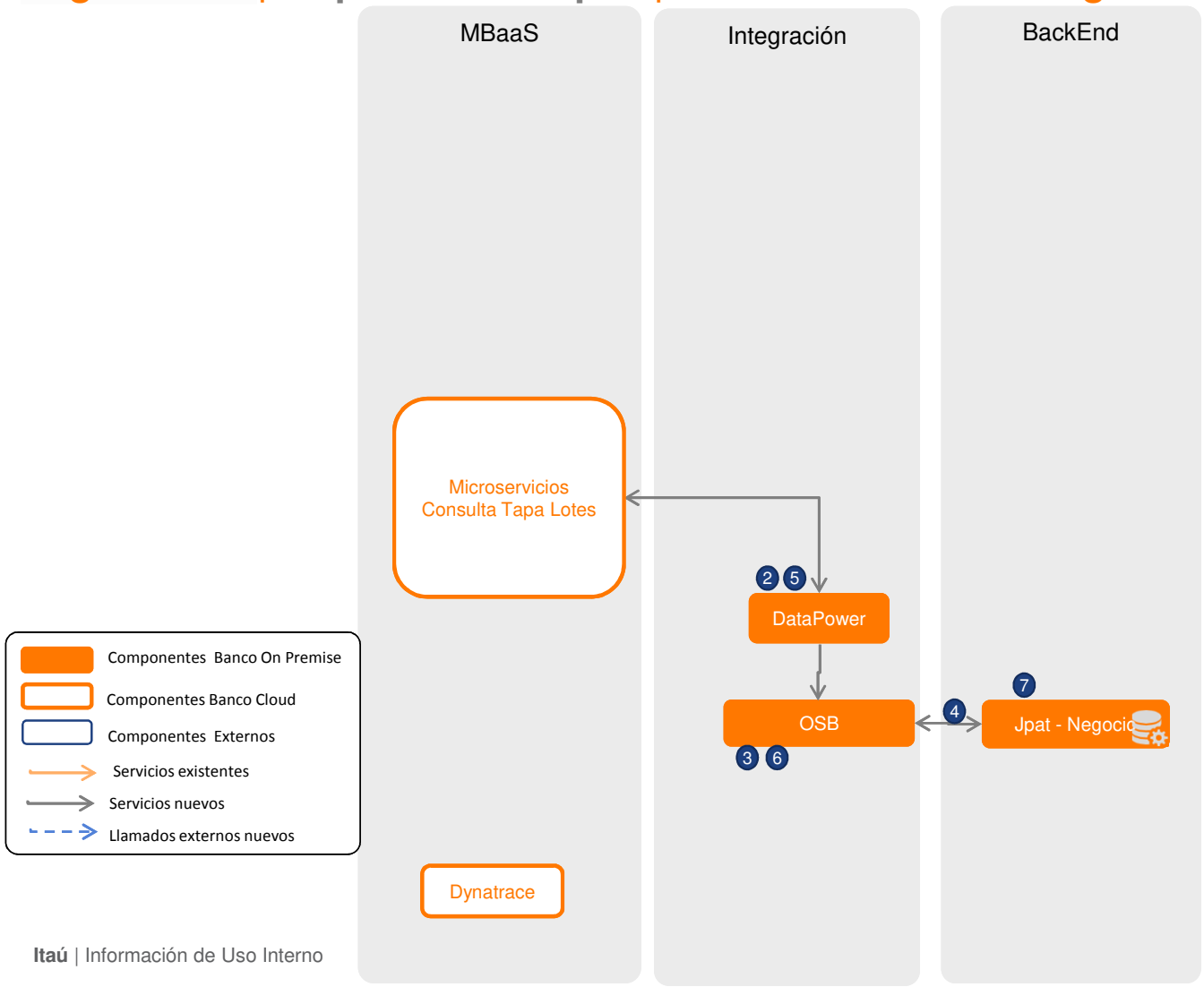
Pagos MVP | Arquitectura Capas | 5. Preparar Pago Manual



Inicio transacción, Cliente ingresa a WV de Pago Manual ya previamente el cliente esta autenticado con las credenciales del cliente y el segundo factor de Autenticación. Debe cumplir con los cifrados de CryptoVault

1. MS obtiene parámetros asociados del tipo de usuario. Se obtiene los parámetros configurados de la empresa, así como las dependencias activas y parametrización asociadas de autorizaciones del usuario. Adicional se carga la lista de perfiles que tiene la empresa con su respectiva identificación.
3. Se consulta por DP hacia OSB
5. Esto se debe almacenar en cache por la sesión del usuario.
7. Se consulta a la BD del MbaaS las opciones y validaciones que se deben activar de acuerdo al usuario. Así como los estados de lotes finales y/o no reusables.
   - Se debe desplegar las opciones al cliente de acuerdo a su perfil.
9. Cuando se registre la información del lote, se debe almacenar en Jpat, vía el OSB
13. Se debe almacenar en Jpat la información en Cache.
    - Cuando se ingrese datos de un beneficiario nuevo, se debe validar si el banco es Itau.
14. Si es Itaú se valida por medio del OSB se debe orquestar que hacia Jpat no existe el cliente y en Phoenix a partir del numero de cuenta sea valido.
17. Posterior a la validación, se debe informar a Jpat el registro del Beneficiario.
20. Cuando se selecciona tercero existente, se debe realizar una consulta por el OSB con un servicios de consulta nombre/Apellido o cedula hacia Jpat
    - Una vez el cliente haga la selección del beneficiario
23. Se debe almacenar la información a Jpat del movimiento asociado al lote y obtener el estado del lote.
26. Para visualizar el resumen se realizara a partir de la información.
27. Para la descarga del PDF se debe generar usando el ms Report Manager con una plantilla diferente.

Pagos MVP | Arquitectura Capas | 6. Visualizar Home Pagos



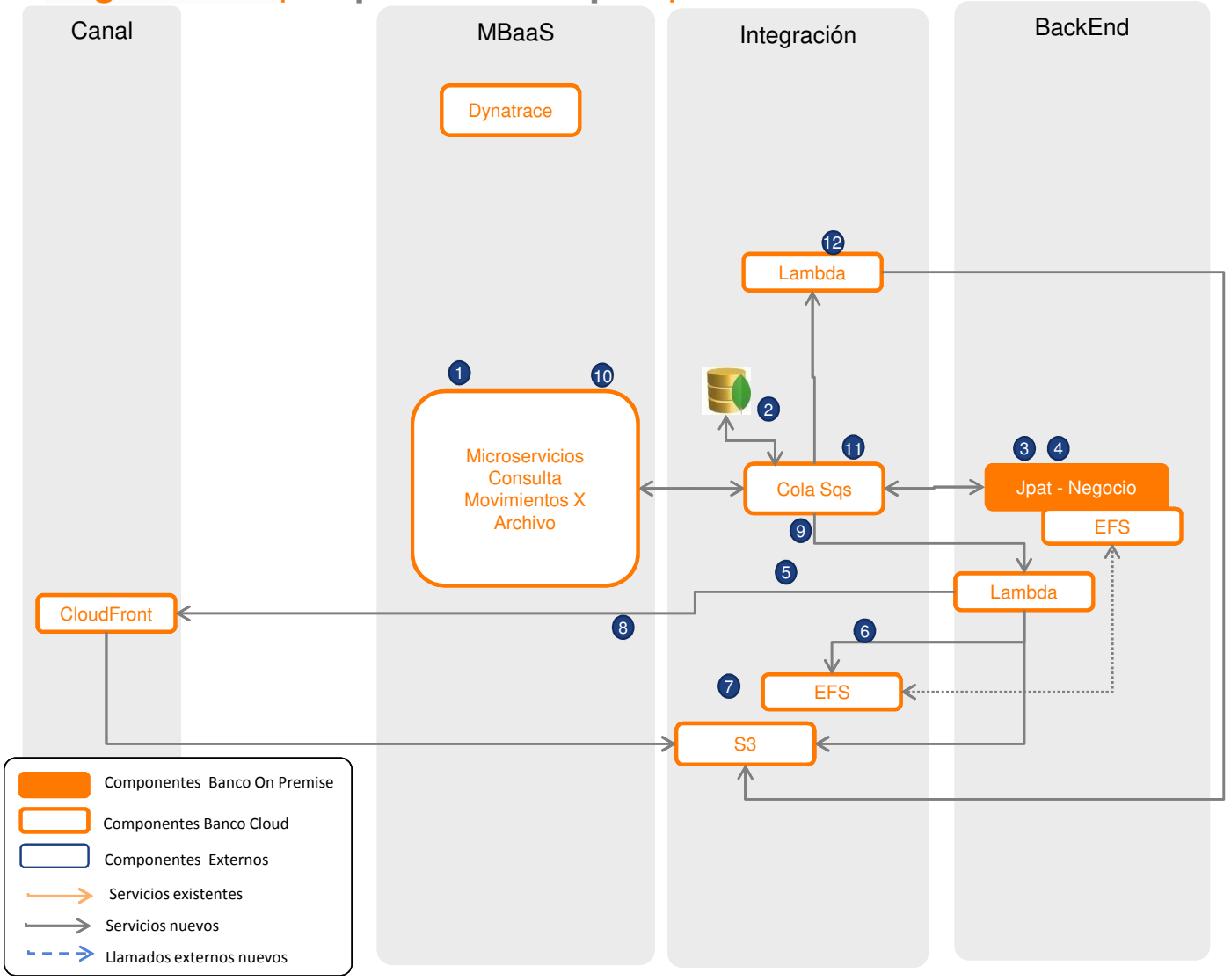
1. Se solicita por medio del MS se hace solicitud de dos servicios, uno con últimos X lotes cerrados y otro servicio de x lotes abiertos.
3. Se solicita la información a Jpat.

6. Una vez el cliente seleccione que desea obtener el detalle de forma manual, se solicita a OSB que se obtenga los x primeros registros a Jpat. La información de esta pagina se despliega el usuario final.
10. Posterior a entregar una pagina, se genera un mensaje a una cola la solicitud de la siguiente pagina, un micro debe estar suscrito a esta cola. El MS invoca el mismo flujo 6 para solicitar la siguiente pagina. Cuando finalice se genera en otra cola mensaje que la información ya esta disponible.

- Cuando se solicite la siguiente pagina se debe revisar la cola para obtener la información para el usuario. Si la información ya esta disponible se debe cargar del cache.

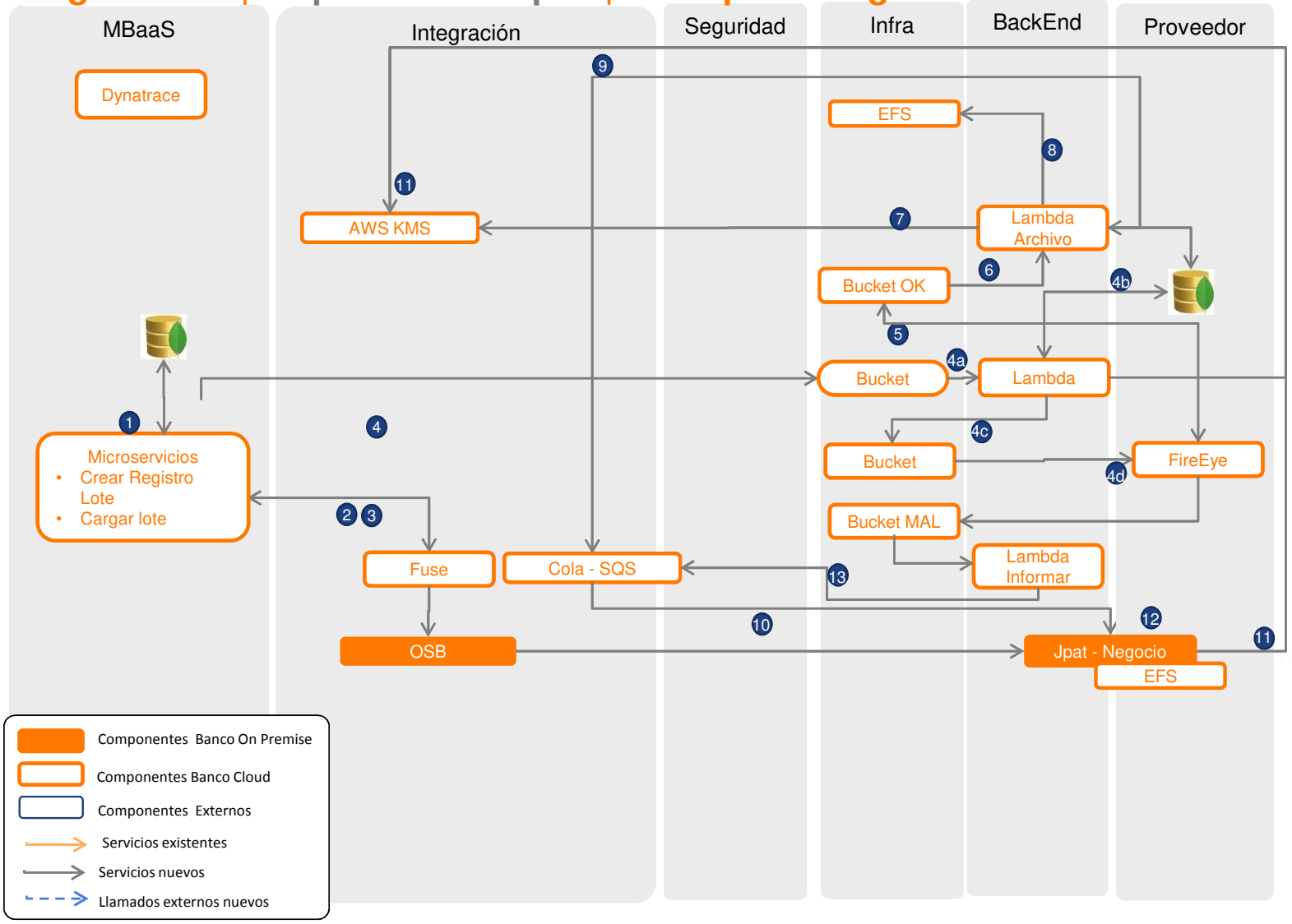
- La selección de los lotes y de las características que se pueden hacer sobre los lotes se debe cambiar de acuerdo a las configuraciones precargadas.

Pagos MVP | Arquitectura Capas | 7. Visualizar Movimientos Desde Archivo



1. Se solicita por medio del MS la información de todos los movimientos del lote, se genera un ID de esta solicitud.
2. Se envía a la cola y se guarda el registro en BD con estado pendiente..
3. Jpat debe desencolar la solicitud del archivo solicitado.
4. Jpat procesa la solicitud genera un archivo CSV y lo entrega en el EFS. El mensaje de respuesta con el nombre del archivo la entrega a una cola y el tipo de archivo solicitado.
5. Lambda lee el mensaje de la cola y con eso puede obtener el archivo de EFS.
7. Convierte el archivo a Excel o al formato Solicitado. El archivo generado lo entrega a S3 y lo elimina del EFS.
8. Posterior lambda solicita a CloudFront la url de descarga del archivo.
9. El resultado lo guarda en la BD con el id del registro.
10. A nivel de la capa front se esta solicitando de acuerdo al ID a la BD si el proceso termino y cual es la URL de descarga.
11. El MS toma la URL para el usuario. Adicional el MS entrega a la cola un mensaje para borrar el archivo.
12. El sqs deja el mensaje 5 minutos y posterior se lo entrega al Lambda para ejecutar.
- Lambda toma el mensaje y elimina sobre el s3 el archivo solicitado.

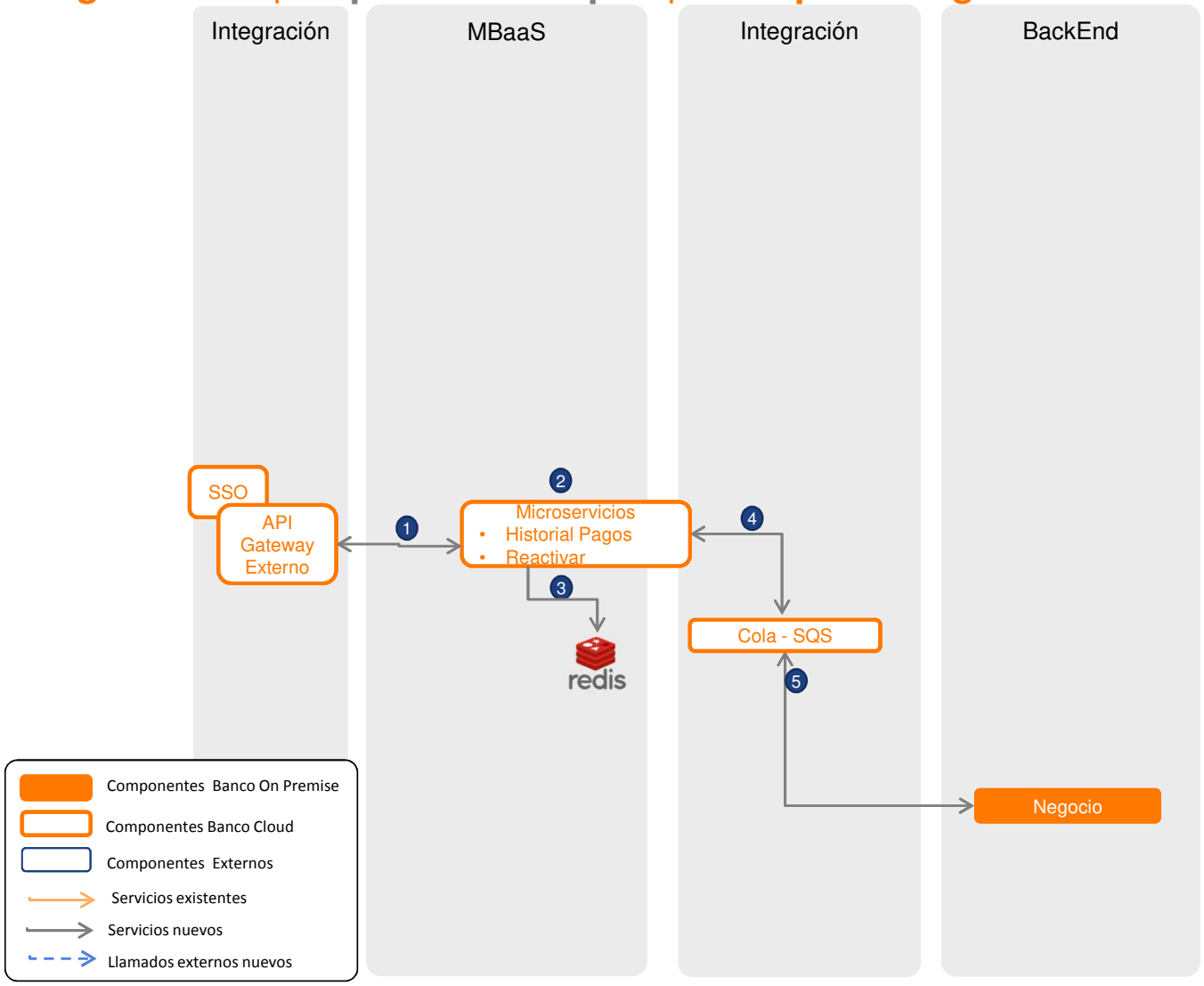
Pagos MVP | Arquitectura Capas | 8. Preparar Pago Archivo



1. Cuando el cliente registre los datos básicos del lote, se debe informar al Back de esta creación.
2. Se almacenan los datos en Jpat.
3. Cuando se va a enviar un archivo se genera un UUID del archivo que se informa a Jpat por medio del flujo 2 en un servicio para esto.
4. Cuando el usuario de la opción de cargar, un MS se encarga de transportar **no** Procesar el archivo y dejarlo en el bucket de S3.
4a. Se dispara una lambda apenas se cargue el archivo y se debe sacar el hash del archivo y después con el resumen del mensaje enviar a KMS a firmar el mensaje.
4b. Se guarda asociado al UUID del archivo el hash de la firma generado por KMS.
4c. Lambda guarda en el bucket destino.
4d. El componente de FireEye de acuerdo al evento del archivo cargado se dispara y revisa el archivo por Malware.
5. Se entrega el archivo cargado libre de virus en otro bucket.
6. Se carga el archivo de Excel y se procesa para convertirlo a un archivo estándar de Jpat.
7. Lambda debe sacar el hash del archivo en formato binario, posterior obtener en la BD la firma obtenida y después enviar a verificar a KMS.
8. Se debe convertir el archivo Excel a formato de Jpat y lo guarda en el EFS, Se debe sacar el hash del archivo y enviar a firmar a KMS.
9. Lambda entrega a la cola el nombre de archivo a procesar y la firma en formato binario.
10. Jpat saca el hash del mensaje y saca el hash del mensaje.
11. Jpat invoca la verificación del hash del mensaje con la firma que recibió.
12. Cuando el mensaje esta validado lo procesa, cuando lo actualiza se cambian estados sobre la base de datos y entrega un mensaje de confirmación a la cola.

Para el uso de llaves asimétricas no pueden ser subidas externas a AWS.

Pagos To be | Arquitectura Capas | 9. Preparar Pago Historial



Temas Transversales

1 El cliente consulta los registros de Servicios de histórico por medio del home para visualizar los registros históricos del cliente (se deben guardar en el cache) y los registros activos del cliente.

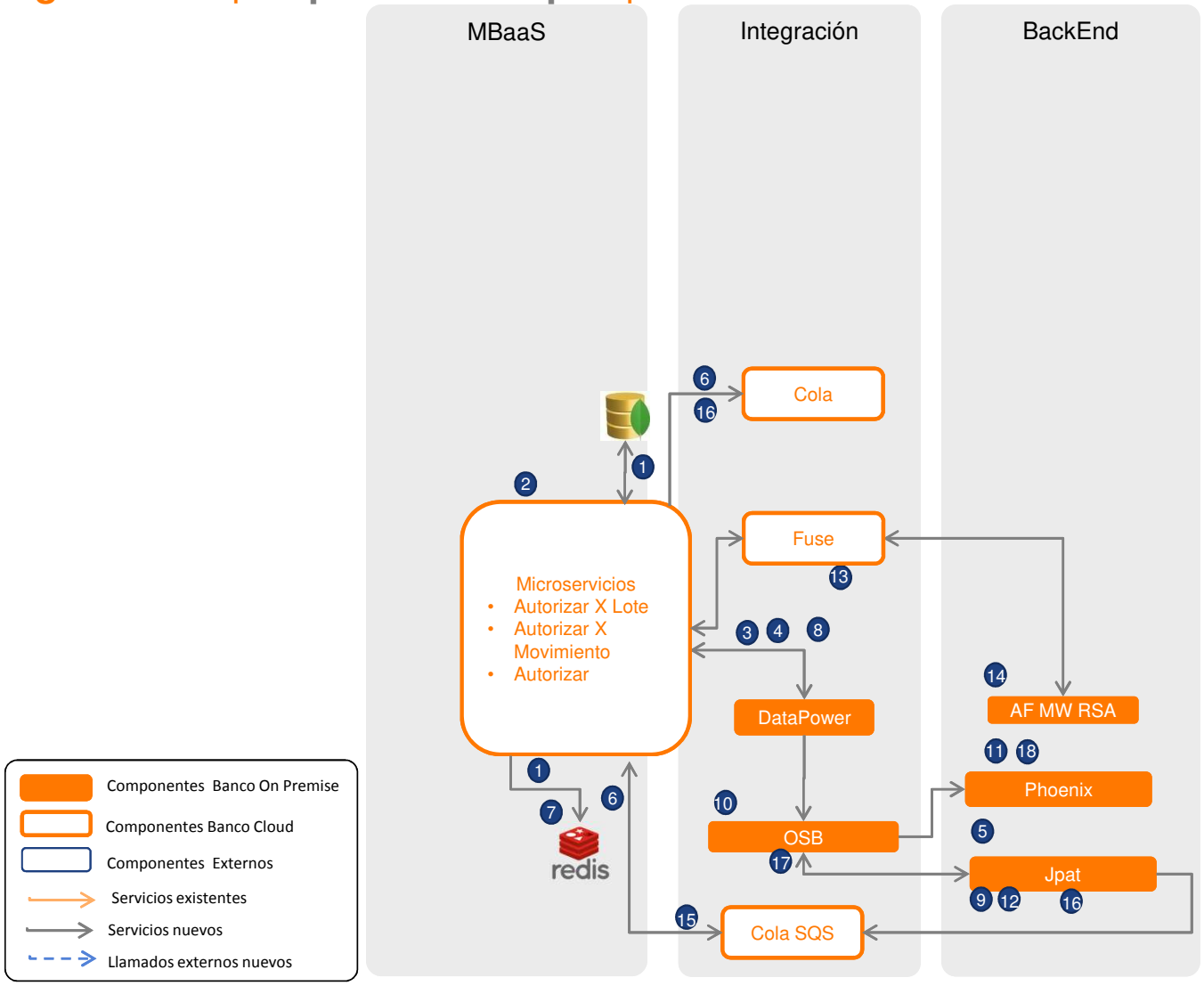
3 MS Historial debe cargar del cache los estados que debe desplegar de las opciones del cliente de acuerdo a su perfil y de los estados de lotes finales y/o no reusables.

4 Una vez el cliente hace la selección del lote y confirma el lote a reactivar, se debe ingresar la información base y posterior se debe lanzar petición al **Back** para generar un nuevo lote activo de acuerdo a la información origen. Se le debe enviar al servicio el UUID del lote a reusar con la nueva información básica.

5 Jpat procesa la petición y cuando realice la modifciacoin adicional a modificar los estados en BD notifica a una nueva cola que el proceso ya finalizo.

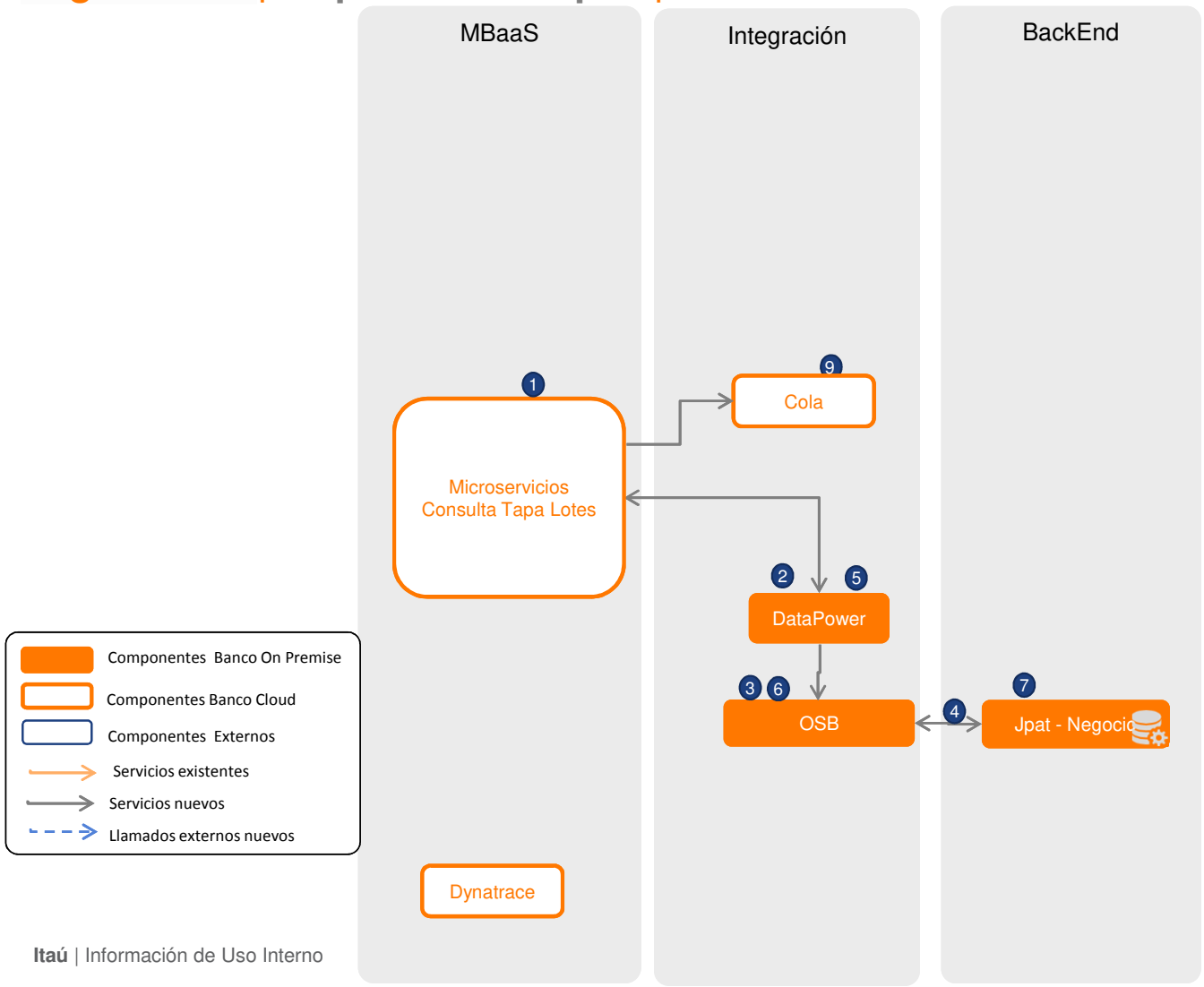
- El cliente puede editar los registros básicos y continuar el proceso como si fuera un Pago Manual.

Pagos To be | Arquitectura Capas | 10. Autorizaciones Pendiente Lotes



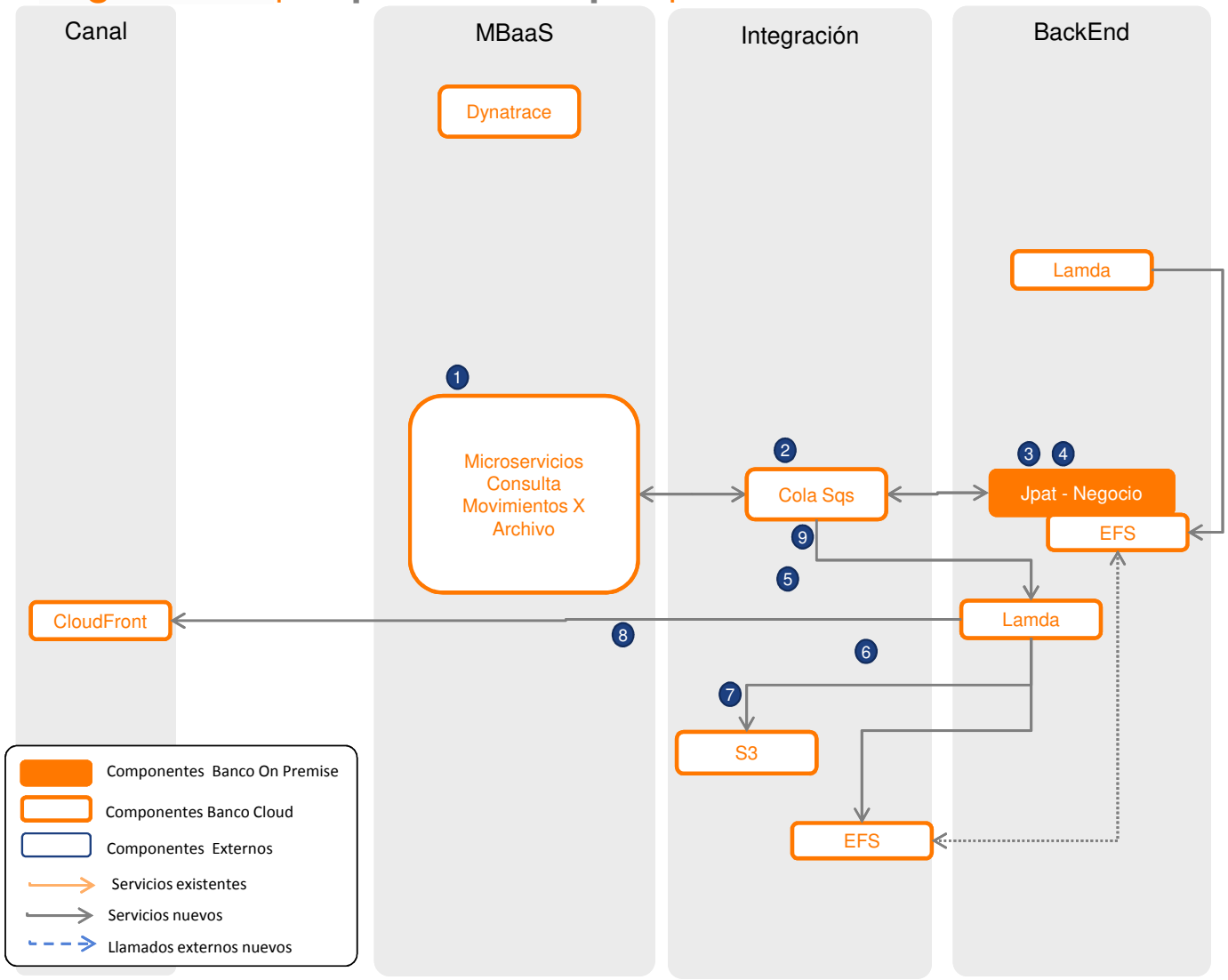
1. MS debe cargar del cache y BD MbaaS los estados que debe desplegar de las opciones del cliente de acuerdo a su perfil y del tipo de firma asociado al cliente.
2. Se deben activar las opciones al cliente de acuerdo al perfil.
   - Se deben cargar los código de cargo que se tienen para esta compañía desde el Back.
3. Una vez el cliente rechaza o eliminar el lote, Se envía la solicitud al Back, el servicio debe devolver el perfil a notificar.
6. Se obtiene todos los clientes con el perfil a notificar del cache asociado a la dependencia y se envía a una cola a Notificar con la identificación del cliente y la plantilla a usar.
7. Una vez el cliente autoriza el lote o el movimiento, se toma el (los) identificadores únicos del registro y se debe validar contra el cache si esta en ciclo extemporáneo.
9. Jpat siempre debe revisar con los datos enviados validar el calculo de cobro de comisión y comisión extemporánea si aplica. Jpat va por medio del OSB va hacia Phoenix.
12. Jpat devuelve los valores a cobrar.
13. Se realiza autenticación de doble factor de cliente por medio de los esquemas actuales
15. MS informa al back por medio de la cola SQS la autorización del identificador del lote(s) o del movimiento(s).
16. Jpat lee de la cola y realiza la lógica e invocación al OSB para ir a Phoenix para los servicios de Pignoracacion/Despignoracion y costo de Trx entre otros.

Pagos MVP | Arquitectura Capas | 11. Home de Terceros



1. Se solicita por medio del MS se hace solicitud de un servicios para obtener los x beneficiarios,
3. Se solicita la información a Jpat.
5. Una vez el cliente seleccione que desea aplicar filtro para campos, se invocar servicio a OSB por medio del Fuse que se obtenga los registros de Jpat. La información se debe paginar por el back.

Pagos MVP | Arquitectura Capas | 12. Visualizar Terceros Desde Archivo

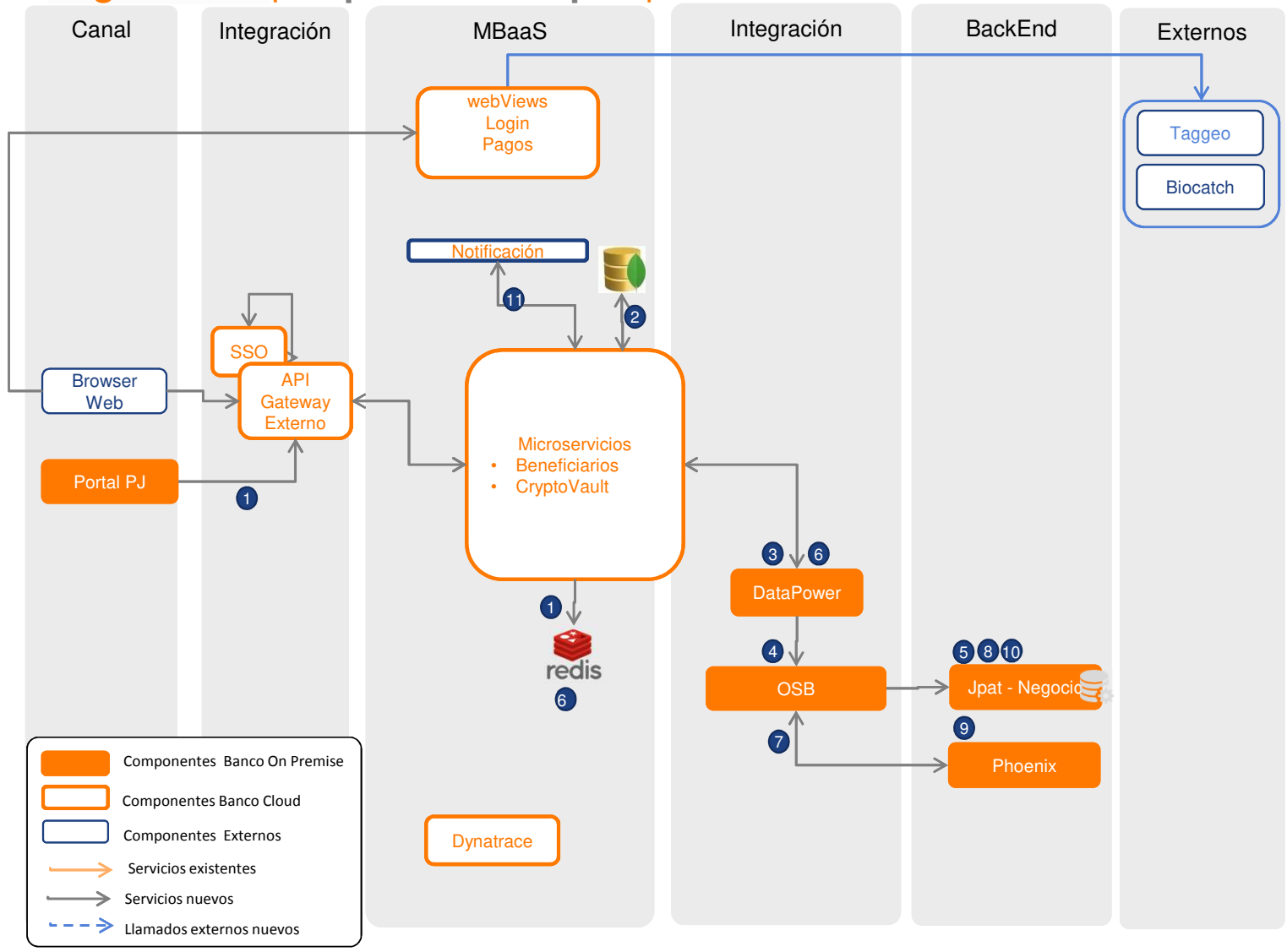


1. Se solicita por medio del MS la información de los beneficiarios del cliente con o sin filtro, la solicitud se guarda en la cola.
3. Jpat debe desencolar la solicitud del archivo solicitado.
4. Jpat procesa la solicitud generar un archivo CSV y lo entrega en el EFS. El mensaje de respuesta con el nombre del archivo la entrega a una cola.
5. Lambda lee el mensaje de la cola y con eso puede obtener el archivo de EFS.
7. Convierte el archivo a Excel o al formato Solicitado. El archivo generado lo entrega a S3.
8. Posterior lambda solicita a CloudFront la url de descarga del archivo.
9. El resultado se lo entrega a la cola para que sea tomado por un MS para entregarle al usuario.

Por medio de un lambda se realice la depuraicon de los archivos de EFS que sean mayor a x horas días de antigüedad.

A nivel de S3 se debe configurar la autodepuración de los archivos a x horas de antiguedad días.

Pagos MVP | Arquitectura Capas | 13. Inscribir Terceros Manual

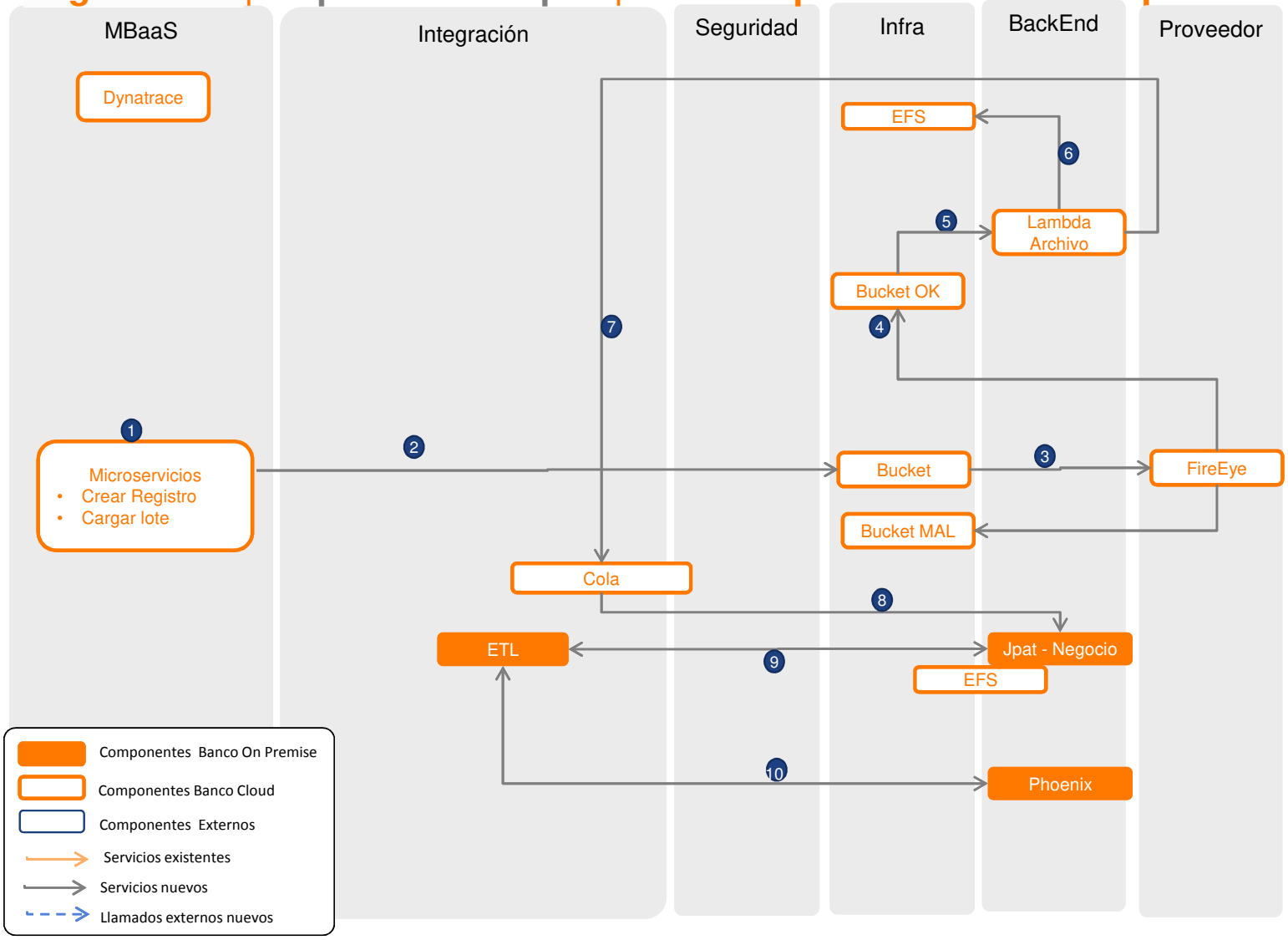


Inicio transacción, Cliente ingresa a WV de Pago Manual ya previamente el cliente esta autenticado con las credenciales del cliente y el segundo factor de Autenticación. Debe cumplir con los cifrados de CryptoVault

1. MS obtiene parámetros asociados a las dependencias que tiene la empresa y de las caracteticas del del cache.
2. Se consulta a la BD del MbaaS las opciones y validaciones que se deben activar de acuerdo al usuario. Así como los estados de lotes finales y/o no reusables.
   - Se debe desplegar las opciones al cliente de acuerdo a su perfil.
3. Cuando se registre la información del tercero, se debe almacenar en Jpat, vía el OSB.
   - Cuando se ingrese datos de un beneficiario nuevo, se debe validar si el banco es Itau.
6. Si es Itaú se valida por medio del OSB hacia Jpat primero a validar que el cliente no exista y sea valido sino debe ir a Phoenix a partir del numero de cuenta y se obtiene la información completa del tercero. Posterior se almacena en Jpat.

11. Posterior se debe notificar al cliente de la inscripción.

Pagos MVP | Arquitectura Capas | 14. Inscripción Beneficiarios por Archivo



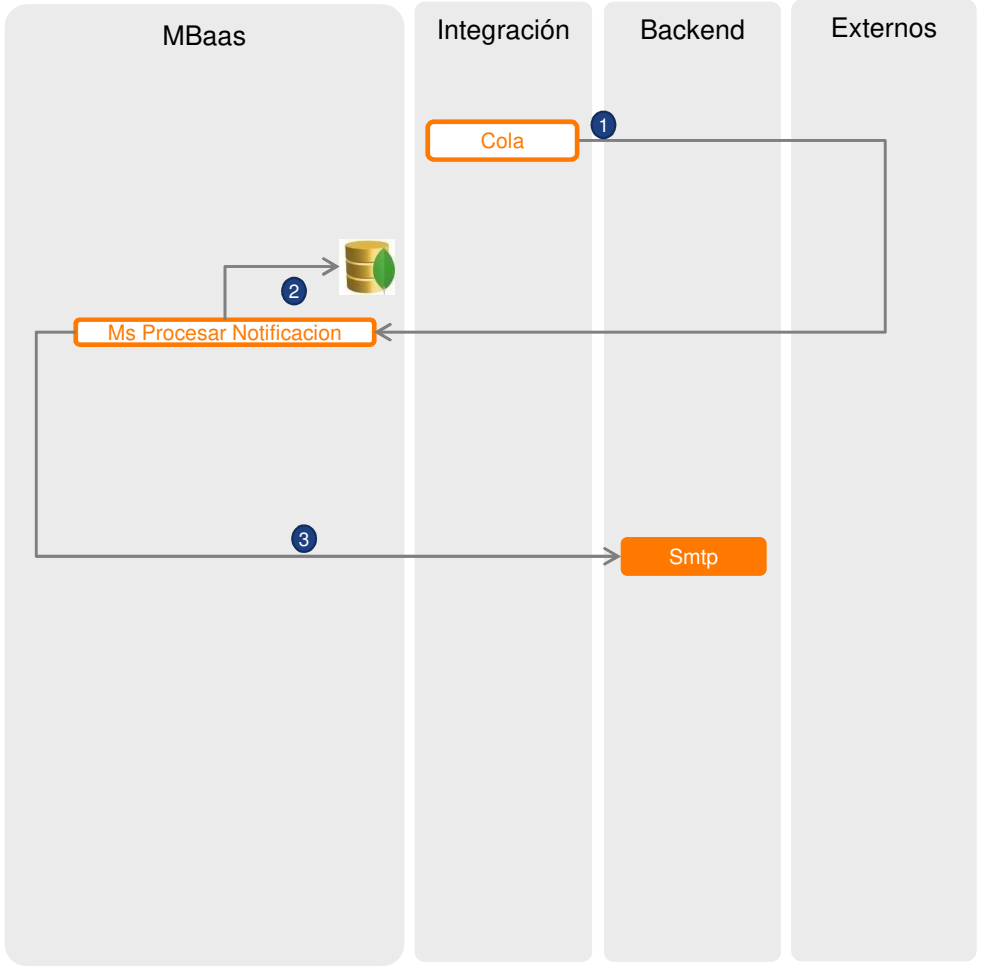
2. Cuando el usuario de la opción de cargar, un MS se encarga de transportar **no** Procesar el archivo y dejarlo en el bucket de S3.
3. El componente de FireEye de acuerdo al evento del archivo cargado se dispara y revisa el archivo por Malware.
4. Se entrega el archivo cargado libre de virus en otro bucket.
5. Se carga el archivo de Excel y se procesa para convertirlo a un archivo estándar de Jpat.
6. Lambda escribe el archivo en el EFS.
7. Lambda entrega a la cola el nombre de archivo a procesar
8. Jpat procesa la cola obtiene el archivo y lo procesa,
9. Jpat por medio de una ETL va a Phoenix a validar los clientes.
10. cuando lo actualiza se cambian estados sobre BD.

* A nivel de Beneficiarios solo ser permite hacer inscripción por medio masivo (la modificación y la eliminación no esta dentro del MVP).

Pagos MVP | Arquitectura Capas | 15*. Modulo de Notificación

Procesos

- Recibir notificación
- Procesar Notificación
- Configurar Plantilla

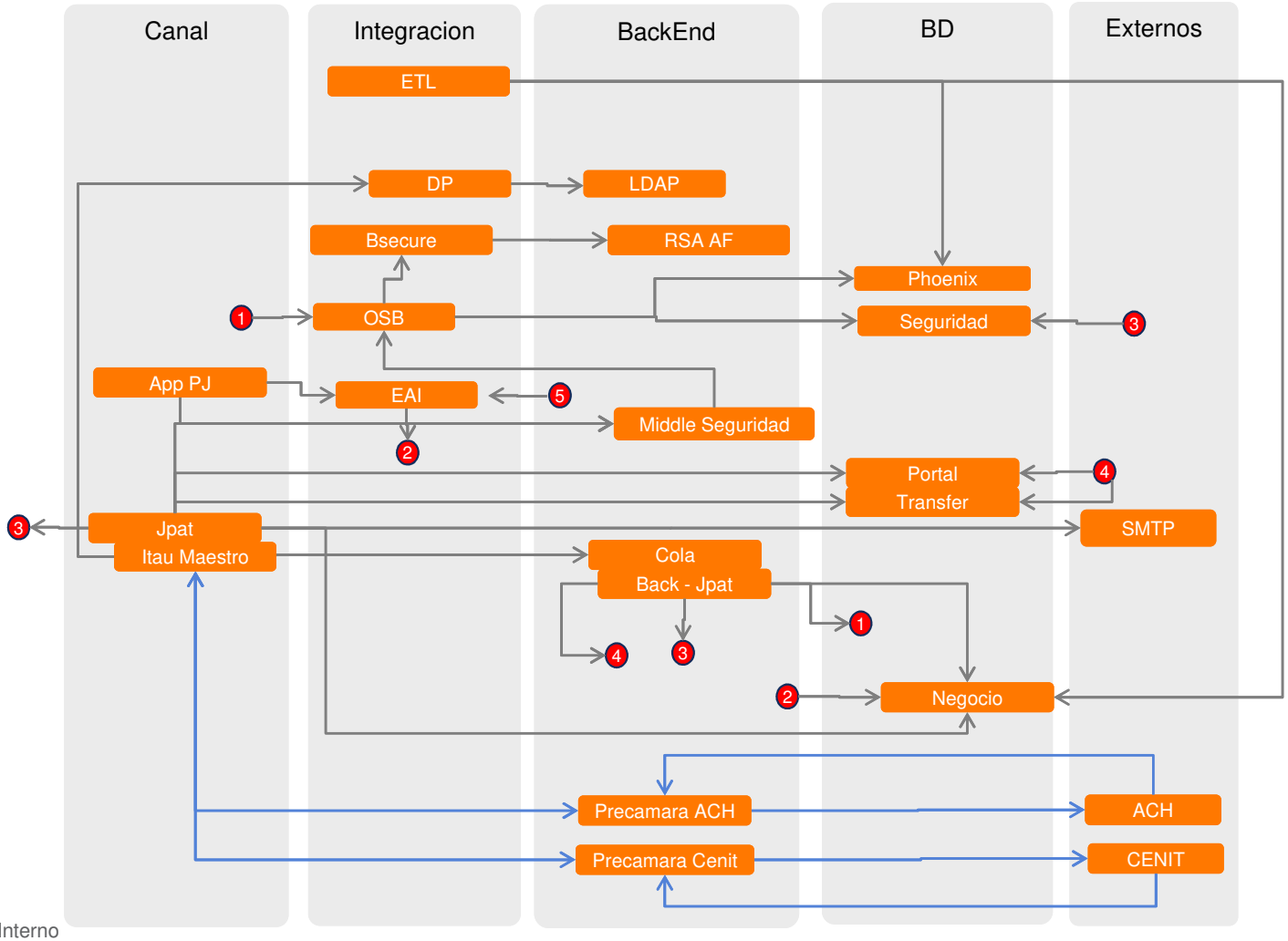


Temas Transversales

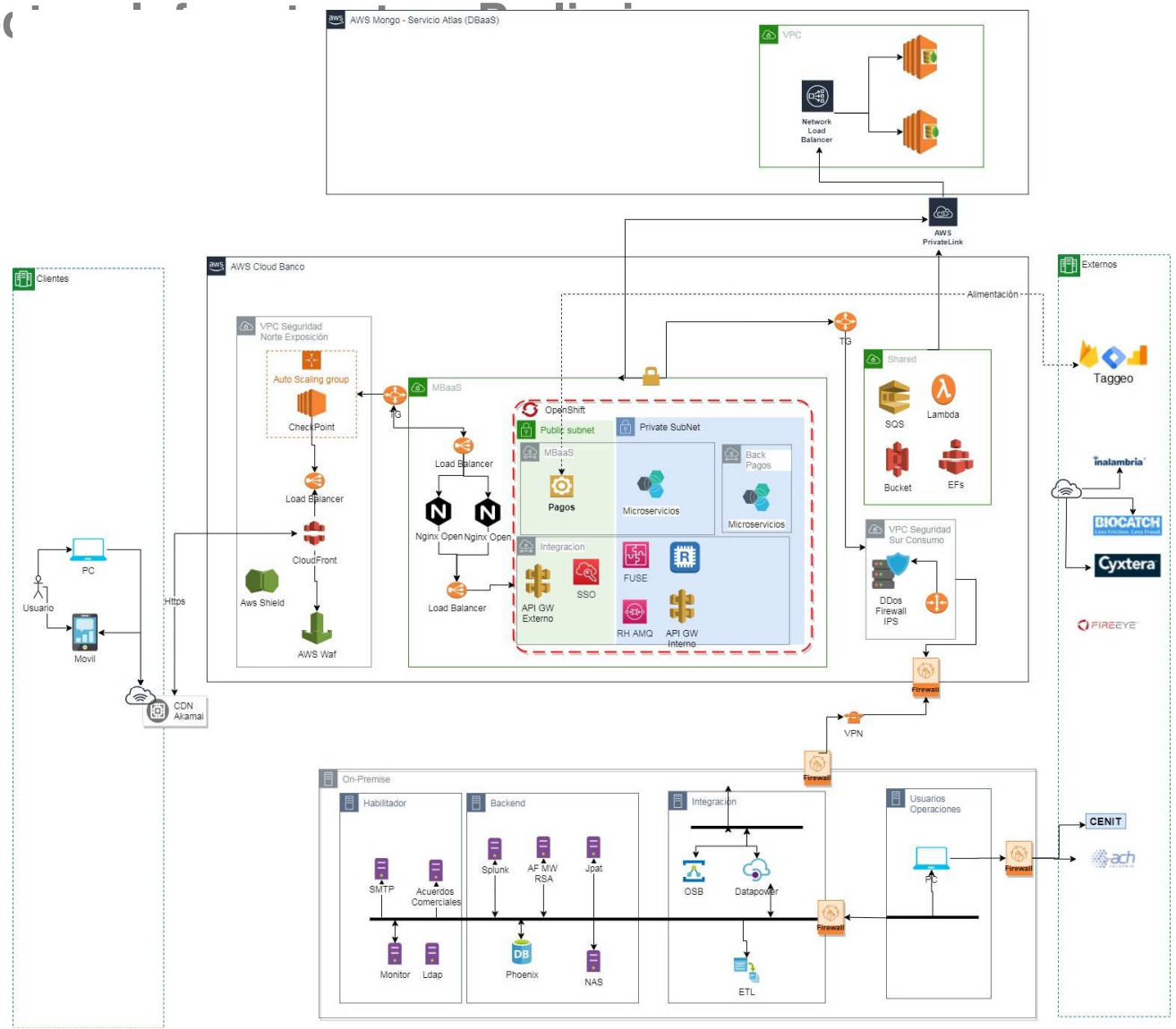
1. Para el procesamiento de los mensajes se haría a partir de MS.
2. EL Ms saca de su BD la plantilla a enviar y el tipo de envió a realizar.
3. De acuerdo a la plantilla a usar se debe envía en este momento únicamente hacia el SMTP.

- Componentes Banco On Premise
- Componentes Banco Cloud
- Componentes Externos
- Componentes a Detallar
- Servicios existentes
- Servicios nuevos

Pagos | Arquitectura Capas – MVP | General



Pagos | Arquitec



Pagos | Puntos Importantes - General

1. Se debe contar con el concepto y la validación de parte de riesgo, seguridad de la información y seguridad IT
2. A nivel de infraestructura se debe considerar una revisión del canal dedicado con AWS, ya que la carga de archivos se tiene estimado aproximado de 20000 archivos al mes. Tamaño máximo aproximado de 2 megas X archivo. Esto se va a cargar en horario hábil por lo cual se debe revisar si se requiere realizar dimensionamiento asociado.
3. La información que se almacene en las colas debe ser persistente.
4. Se debe asegurar el esquema de registro de bitácoras, relacionando como mínimo la información requerida para cumplir normativamente las circulares 042, 052 y 005, así mismo deben quedar claramente identificada la información del cliente, el canal por donde realizó la transacción y la aplicación utilizada.
5. Los componentes serverless de desarrollo deben tener automatización en el despliegue a nivel de código usando Jenkins y gitlab. Es importante cerrar una prueba de concepto para revisar este tema.
6. Infraestructura y/o desarrollo debe asegurar que los componentes instalados en cloud se manejen en esquema de Infraestructure as Code, para proporcionar más agilidad y mejores tiempos de recuperación ante desastres o necesidades de nuevos ambientes.
7. Todo Servicio de AWS debe tener prendida la auditoria para que queden sus registros en CloudTrail y se debe configurar las alarmas sobre la infraestructura en CloudWatch necesarias para garantizar la disponibilidad del servicio.
8. Si hay un cambio a nivel del Perfil Administrador de un parámetro transaccional, el usuario debe salirse para tener el refresco de sus parámetros o configuraciones.
9. Las colas deben proporcionar durabilidad de los mensajes, debe proveer las características para la autenticación y autorización de quien esta realizando la solicitud.
10. Los servicios de OSB se deben realizar basado en Rest, adicional se debe garantizar que toda la información e invocación de servicios en la nube del banco, como coreográficas o llamadas internas en la nube estén siempre usando protocolo seguro (https). Por ultimo se debe garantizar que la invocación desde la nube al primer punto del banco sea también usado protocolo https de acuerdo a los lineamiento de Seguridad de la información.

Pagos | Puntos Importantes - General

1. Se debe asegurar el pipeline de DevSecOps.
2. Se debe asegurar que la información de micros quede almacenada en el registro de Bitacoras. Para la auditoria a nivel de canal se debe asegurar que se almacene de acuerdo al arquitectura ya establecida.
3. La obsolescencia de componentes del back no se revisaran en este primer alcance del MVP, pero todo componente nuevo que se deba crear debe hacerse en una versión soportada.
4. Se debe asegurar a nivel de Jpat que cuando el cliente sea migrado se desactiven las funcionalidades administrativas que no estén cubiertas en el MVP.
5. La configuraciones de la empresa/usuario, como horarios, días laborales entre otros debe cargarse en cache y se debe validar en las diferentes peticiones que haga el usuario final para asegurar su cumplimiento.
6. Para este MVP La carga de archivos no incluye archivos encriptados.
7. El manejo y autenticación de tokens virtuales o físicos no son del alcance del proyecto, por lo que son librerias o proyecto que se usaran como están disponibles.
8. El manejo de auditorias y perfiles no se modificara en el alcance del proyecto se considera que se debe cubrir con las funcionalidades actuales mientras se genera una definición transversal para el portal PJ.
9. La parte de administración que se tiene en Itau Maestro no se modificara. Las nuevas funcionalidades para Operadores se debe realizar en Operador Portal.

Pagos | Puntos Importantes - Seguridad

1. La información entre cloud y el banco deben viajar siempre por el canal dedicado bien sea por VPN o por Direct connect pero nunca deben viajar por internet la comunicación entre AWS y el banco.

2. Se debe asegurar que la información manejada en reposo y en transporte en la nube de AWS este cifrada. Adicional toda comunicación que se haga inclusive en OnPremise debe estar cifrada. A nivel de Mongo y componentes como EFS se deben cifrar en reposo utilizando una llave particular de KMS.

3. Para los servicios de autorización o monetarios expuestos desde Onpremise deben autenticar al menos por un http Basic. Para guardar las contraseñas se debe usar el componente de Secret Manager.

4. Se debe asegurar que a nivel de seguridad la información este protegida en reposo, en transito y cuando se almacene.

5. La información en cache (Bd en memoria) que sea información sensible también debe estar encriptada, se debe cifrar obteniendo la llave de encripcion de KMS.

6. Adicional debe se debe usar https para el transporte de la información. Para el caso de las APIs se debe asegurar que se este usando un modelo de autenticación del canal y en todo momento se tenga el uso de certificados de extremo a extremo.

5. Se debe asegurar que todos los archivos que se carguen en la plataforma deben validarse por la herramienta de prevención de Malware, sin embargo los archivos que sean encriptados no se van a poder cargar para este alcance del MVP.

Pagos | Concepto

1. Se esta planteando el uso de componentes nuevos con una arquitectura Serverless como son los siguientes componentes:
    - Lambda
    - S3
    - EFS
    - SQS

2. Se plantea el uso de un servicio SaaS de un tercero para el análisis de archivos :
    - FireEye Detection On Demand for AWS S3

3. Ya se hizo prueba de Concepto por parte de AE del uso de Lambda, s3 y EFS para validar su compatibilidad.