UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Sistema de gestión de datos en el proceso de autenticaciónpara emisores en la empresa ALIGNET S.A.C.

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:
Ingeniero de Sistemas

AUTORES:

Pinto Pintos, Katelyn Zarelly (ORCID: 0000-0001-5680-2836)
Zúñiga Huaraca, Kenny Wilfredo (ORCID: 0000-0002-8898-4600)

ASESORA

Mg. Rosa Menéndez Mueras (ORCID: 0000-0003-2403-7679)

LÍNEA DE INVESTIGACIÓN:

Sistemas de Información y Comunicaciones

Lima - Perú

2021

DEDICATORIA

A mi madre querida Maibee porque me ayudó en las buenas y en las malas, además de haberme dado la vida, siempre confió en mí. A la memoria mi padre Albino, quien me educo e inspira a ser una mejor persona y obtener una carrera profesional. Su ejemplo me dio fuerzas cuando quise rendirme.

Pinto Pintos, Katelyn Z.

A Dios todo poderoso, A mis Padres Luzmila y Juan por el apoyo incondicional y haber estado en todo momento para poder lograr los objetivos trasados en mi trayectoria universitaria. A todas las personas especiales que me acompañaron en esta etapa, aportando a mi formación tanto profesional y como ser humano.

Zúñiga Huaraca, Kenny W.

AGRADECIMIENTO

A Dios por brindarnos salud, fortaleza y capacidad; también hacemos extenso este reconocimiento a todos los maestros, quienes nos han dado las pautas para nuestra formación profesional; y por último a todos quienes conforman la empresa Alignet, por habernos abierto las puertas, permitiendo la accesibilidad a sus instalaciones.

INDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

INDICE DE ANEXOS

RESUMEN

El presente trabajo de investigación se desarrolló con la problemática de ¿Cuál es la influencia de un sistema de gestión de datos en el proceso de autenticación para emisores en la empresa ALIGNET S.A.C.? El objetivo de la investigación fue determinar la influencia de un sistema de gestión de datos en el proceso de autenticación para emisores en la empresa ALIGNET SAC.

Alignet es una empresa especializada en brindar soluciones tecnológicas y de seguridad para comercio electrónico y métodos de pago. El estudio cuenta con una investigación aplicada, diseño de investigación preexperimental y como instrumento de recolección de datos la ficha de registro, que midió el promedio de 30 registros de transacciones diarias de Alignet.

El resultado demuestra que el sistema de gestión de datos tiene el efecto esperado en el rendimiento con una mejora significativa a una variación 6%y 4%. En conclusión, se logró medir un aumento el porcentaje de transacciones autorizadas de 6% y disminuir el porcentaje de transacciones denegadas en una 4%.

Palabras claves: Sistema de gestión de datos, Autenticación para emisores, protocolo 3D Secure, comercio electrónico.

ABSTRACT

This research work was developed with the problem of what is the influence of a data management system in the authentication process for issuers in the company ALIGNET S.A.C.? The objective of the research was to determine the influence of a data management system in the authentication process for issuers in the company ALIGNET SAC.

Alignet is a company specialized in providing technological and security solutions for electronic commerce and payment methods. The study has an applied research, pre-experimental research design and as a data collection instrument the registration form, which measured the average of 30 Alignet daily transaction records.

The result shows that the data management system has the expected effect on performance with a significant improvement at a 6% and 4% variation. In conclusion, it was possible to measure an increase in the percentage of authorized transactions of 6% and a decrease in the percentage of denied transactions by 4%.

Keywords: Data Management System, Authentication for issuers, 3D Secure Protocol, Electronic Commerce.

I. INTRODUCCIÓN

Para observar la influencia actual a nivel mundial del comercio electrónico, se tiene que analizar su aplicación, ya que "[…] apoyarse en tecnologías como el comercio móvil, la transferencia electrónica de fondos […], el procesamiento de transacciones en línea, el intercambio electrónico de datos (EDI), […] y los sistemas automáticos de recopilación de datos." (Kütz, 2016, p. 16). En ese contexto la empresa Alignet provee soluciones tecnológicas y de seguridad para comercio electrónico y métodos de pago, contando con más de 40 entidades financieras como clientes distribuidos en 11 países, brindando como servicio el Autentication Costumer Service (ACS) para emisores.

En el último año la empresa Alignet ha tenido un incremento de clientes que ha llevado a evaluar los procesos de gestión, para poder controlar el número elevado de transacciones con el propósito de mejorar los procesos para los emisores. Se debe mencionar que el porcentaje de transacciones denegadas del mes de setiembre del 2020 es 18% (ver Anexo 6), cifra alarmante que ha empezado a preocupar a la organización, ya que, con respecto al año pasado durante el mismo periodo, se presenta un incremento del 8% (ver Anexo 6), este problema es generado debido a que las transacciones no pasan el proceso de autenticación por datos incorrectos. Además, el porcentaje de transacciones autorizadas del mismo mes es 67% (ver Anexo 6), el cual también se ha visto afectado ya que la reducción con respecto al año pasado es del 19% (ver Anexo 6) provocando una perdida considerable en los ingresos. Es necesario mencionar que los procesos de autenticación se tienen que alinear a la nueva normativa que exige la utilización de un nuevo protocolo. Además, las diferentes marcas como Visa, MasterCard, Diners Club y American Express están estableciendo una serie de nuevas políticas para aquellos comercios que transaccionen almacenando información de los tarjetahabientes, haciendo énfasis en temas de seguridad. Cabe recalcar que cada marca maneja normas diferentes, lo que aumenta la complejidad en la implementación.

El proceso de autenticación denominado ACS empieza cuando el tarjetahabiente brinda la información de su tarjeta al realizar una compra en línea, cuanta más

información transmita del tarjetahabiente, más segura será la identificación y se tendrá menos posibilidades de experimentar un fraude (a no ser que se detecte que es una compra potencialmente fraudulenta, entonces se solicitará algún tipo de verificación de identidad). Este dato adicional puede ser una clave dinámica por SMS o correo electrónico para confirmar la compra.

Por consiguiente, una posible solución puede ser la implementación de nuevos servicios, con el fin de reducir las transacciones denegadas y aumentar el porcentaje de transacciones autorizadas para emisores en donde se requiere mayor información del tarjetahabiente, incluso es necesario que los emisores puedan tener un sistema de reportería personalizado, por ello se desarrollará un sistema de gestión de datos en el proceso de autenticación para emisores, el cual cargará los datos de las tarjetas de manera individual, permitiendo gestionar las transacciones ingresadas así como la visualización de su respectivo status. También se crearán usuarios para cada emisor con diferentes permisos, tomando en cuenta que solo podrán visualizar y gestionar datos de sus tarjetahabientes. Además, se propone crear un nuevo proceso denominado enrolamiento masivo de datos que consta del envío de un archivo plano cifrado por el servicio SFTP, el cual contiene los datos de múltiples tarjetas que requieren registrar, actualizar o eliminar en la base de datos. Luego de haber procesado esos datos, se creará un archivo de resultados en el cual indicará que tarjetas se han logrado procesar con éxito y cuál fue el error en caso de no llegar a finalizar el flujo correcto. Otra solución sería realizar cambios directamente en base de datos a pedido del cliente a través de solicitudes de soporte cada vez que se presente incidencias sobre falla de autenticación de una transacción, esto conllevaría a que el proceso sea más tardado y generaría costos operativos directamente en la empresa Alignet, pero evitaría todos los costos de desarrollo en un sistema de gestión.

Entonces, los autores de esta investigación formulan el problema general así ¿Cuál es la influencia de un sistema de gestión de datos en el proceso de autenticación para emisores en la empresa ALIGNET S.A.C.?, y como problemática específica de la siguiente manera: ¿Cuál es la influencia de un sistema de gestión de datos en el

porcentaje de transacciones denegadas en el proceso de autenticación para emisores en la empresa ALIGNET S.A.C.? y ¿Cuál es la influencia de un sistema de gestión de datos en el porcentaje de transacciones autorizadas en el proceso de autenticación para emisores en la empresa ALIGNET SAC?

La investigación se justifica de manera económica “con el fin de encontrar pistas de mejorar […] los procesos comunicación y colaboración entre los diferentes bancos del sistema bancario peruano que permitan disminuir las pérdidas” (NEGRILLO, 2019, p. 4). La investigación propone la implementación de un sistema en el sector financiero para producir resultados económicos beneficiosos para la empresa, de manera similar sucede en este caso, se plantea implementar un sistema que permita que los emisores o bancos puedan transaccionar con sus tarjetas de manera online, sin impedimentos, y sobre todo de manera segura reduciendo en gran medida el porcentaje de transacciones denegadas y aumentando el porcentaje de transacciones autorizadas. Adicional a ello, el incremento de valor en los contratos que tiene Alignet con los Emisores se verá incrementado de manera sustancial.

La investigación se justifica de manera practica porque existe la necesidad de los emisores que se monitoree en tiempo real las transacciones mediante la etapa de autenticación y autorización, administrar de manera efectiva la información de los tarjetahabientes, que el emisor brinde soporte a sus clientes con sus tarjetas en cualquier momento sin depender o consultar con Alignet. Con el sistema de gestión el emisor está totalmente informado de cada uno de sus clientes.

El proyecto se justifica de manera operativa por que actualmente la empresa Alignet realiza todo tipo de corrección de datos del tarjetahabiente en el proceso de autenticación que ingresa a solicitud del cliente (emisores) mediante un ticket de atención de solicitud de soporte provocando cargas operativas. Por ello, la implementación de un sistema de gestión de datos en el proceso de autenticación para emisores puede reducir la carga operativa en la organización además que brindará funcionalidades adicionales de personalización por emisor.

De esta manera los autores proponen como objetivo general, determinar la influencia de un sistema de gestión de datos en el proceso de autenticación para

emisores en la empresa ALIGNET SAC, y como objetivos específicos: determinar la influencia de un sistema de gestión de datos en el porcentaje de transacciones denegadas en el proceso de autenticación para emisores en la empresa ALIGNET SAC y determinar la influencia de un sistema de gestión de datos en el porcentaje de transacciones autorizadas en el proceso de autenticación para emisores en la empresa ALIGNET SAC.

De esta manera los autores proponen como hipótesis general de un sistema de gestión de datos mejorará el proceso de autenticación para emisores en la empresa ALIGNET SAC, y como hipótesis específicas: un sistema de gestión de datos disminuirá el porcentaje de transacciones denegadas del proceso de autenticación para emisores en la empresa ALIGNET SAC y un sistema de gestión de datos aumentará el porcentaje de transacciones autorizadas en el proceso de autenticación para emisores en la empresa ALIGNET .

II. MARCO TEÓRICO

Se realizó una revisión de distintos gestores de repositorios referente a nuestra variable dependiente e independiente los cuales se han tomado como antecedentes:

Para Gonzales (2017), estudió la relación de aceptación de clientes y el desarrollo de la banca electrónica en el Perú. El tipo de investigación es social-explicativa-cuantitativa y como diseño de investigación es no experimental - transversal. Se utilizó como muestra a los 4 principales bancos del Perú, tomando 385 clientes de ambos sexos de Lima en el rango de 25 y 64 años, además pertenecientes al sector socioeconómico A, B, C. Se concluyó que el crecimiento de la banca electrónica depende de la aprobación de los clientes con este canal de atención; el 48% de clientes mencionaron que hicieron uso de los servicios electrónicos, y de ese resultado, el 41% define su frecuencia de uso como “Rara vez”. Asimismo, recomendó que en el futuro se incentive la aceptación que tienen los clientes con la banca en línea y promueva la educación financiera.

Este antecedente permitió dar un mayor enfoque a los bancos o emisores y su relación de aceptación con los tarjetahabientes, estos estudios previos permiten que evaluar la importancia de un sistema de gestión de datos que ayude a los emisores a tomar medidas acertadas para llegar de manera correcta al usuario final.

Para Orihuela y Otros (2019), estudió los factores que no permitan la adopción del comercio electrónico en los negocios que funcionan en el centro comercial Constitución. El tipo de investigación es del tipo básico y el diseño de investigación no experimental. Se utilizó como muestra el centro comercial Constitución, realizando un estudio no-probabilístico con la participación de los dueños; Se concluyó que los responsables de los 220 negocios en el periodo de julio y agosto en el 2018 presentan factores de conocimiento, de entorno y organizacionales, lo cuales son limitantes para acoger el comercio electrónico en los negocios del lugar. Se debe mencionar que la tecnología no es una limitante, más bien es un incentivo, debido a los resultados que se obtuvieron al recolectar información de 160 dueños y personas responsables de los negocios. Asimismo, recomendó implementar un

modelo de eCommerce, el Mall Online, que reduce las limitaciones que tienen los negocios para adoptar el comercio en línea, ya que toma a mayor cantidad de negocios para este modelo de negocio en donde los procesos estarán centralizados en una sola plataforma virtual, además los productos o servicios serán comercializados a modo de stand online.

Este antecedente permitió dar un mayor enfoque a las limitaciones que presenta el comercio peruano y la importancia de un modelo tecnológico que permita gestionarlos datos de manera virtual.

Para Gonzales (2016), estudió el planteamiento de herramientas de seguridad web esenciales que se puedan aplicar en empresas que cuentan con una tienda de ventas por internet desarrollada en Prestahop, Ecuador. El tipo de investigación es experimental y diseño comparativo. Como muestra se utilizó los protocolos de recolección de datos se en donde se estructuraron siguiendo el reporte de Arcotel en el 2015 haciendo un análisis al uso del Internet en Ecuador, también se realizó un estudio experimental, el desarrollo del sistema informático se fundamentó para contrarrestar ataques que impidan el desarrollo de la empresa. Como resultado las personas urbanas de ecuador que tienen acceso a internet (37%) en comparación a la población rural (9.1%), este análisis se realizó entre los años 2010 y 2013. Las conclusiones indican que el internet en ecuador ha evolucionado en porcentajes que superan el 300% obligando a las pequeñas, medianas y grandes empresas a implementar una nueva forma para generar ingresos como son las tiendas online. Asimismo, las recomendaciones indican que mantener actualizado el software ayuda de manera favorable al tema de seguridad en donde se corrigen vulnerabilidades.

Este antecedente permitió dar un mayor enfoque a la seguridad que ofrece una plataforma y la importancia de poder controlar los riesgos,así como cumplir con las normas o estándares de calidad.

Según Ardizzi (2017), Estudió la falta de análisis empírico sobre la relación en la innovación en métodos de autenticación y la adopción del usuario con los instrumentos de pago digitales además de abordar un tema importante en términos

de implicaciones políticas como la adopción masiva de autenticación fuerte de clientes (SCA) y su impacto negativo en la experiencia de usuario. Tipo de investigación explicativa y diseño experimental. Utilizó como muestra el número de transacciones de comercio electrónico en Italia, con tarjetas de crédito y débito, realizando un estudio explicativo, además detectó el crecimiento anual de un 20% en el periodo 2011 – 2016, encontrando alrededor de 400 millones de tarjetas utilizadas a través de internet, calculando la tasa de crecimiento de transacciones "remotas" es cuatro veces mayor que las presenciales. Como resultado de estudio concluyo que la estimación de un modelo de ecuación apoya la hipótesis de efectos negativos de un cierto método de autenticación de dos factores (como el protocolo 3-D secure) en el usuario-experiencia durante el periodo 2012 – 2016. Tales resultados son robustos tanto en panel estático de especificaciones de datos (modelos EF – efectos fijos) y dinámicos (estimador GMM a la Arellano - Bond). Sin embargo, se interpretó estos resultados de manera dinámica en donde simplemente se confirman que la experiencia de usuario no debe de ser subestimada por el legislador.

Este antecedente permitió dar un mayor enfoque sobre el proceso de autenticación y como afecta en la experiencia de compra del tarjetahabiente, evaluando la seguridad y complejidad en el proceso de autenticación de una compra.

Según Marchal y otros, (2019), Estudió el diseño de una solución para detectar fraude de comercio electrónico organizado. Esta investigación es de tipo de investigación experimental y diseño experimental. Utilizó como muestra la agrupación técnica en pedidos en el sitio web de Zalando, realizando un estudio experimental la agrupación de 6 millones de pedidos en el 2019. Se concluyó que se detectó el 26,2% de fraude y falsas alarmas del 0.1% de pedidos legítimos con un 35% de precisión, por lo que se concluyó que cancelar pedidos legítimos de buenos clientes por un posible fraude genera mala experiencia al cliente y esto puede afectar de manera perjudicial la satisfacción del cliente provocando la disminución de la rentabilidad de un servicio en línea. Asimismo, recomendó que la

maniobrabilidad de un sistema de detección de fraude se tendría que evaluar de manera subjetiva en diferentes comercios minoristas en línea.

Este antecedente permitió dar un mayor enfoque sobre la importancia del índice de fraude y como puede afectar significativamente de manera negativa en los ingresos de una organización.

Según Miranda y otros (2015), estudió la implementación de un sistema de monitoreo de la infraestructura tecnológica para medir la disponibilidad del servicio de autorizaciones en Diners Club del Ecuador y un modelo de medición automática del proceso de negocio de autorizaciones en Diners Club del Ecuador que permita obtener información en línea del desempeño del proceso que soporte decisiones adecuadas y oportunas. Utilizó como muestra las autorizaciones por la empresa Datafast utilizando como estudio preexperimental con la participación del el área de Tecnología y el área de crédito cuya ubicación dentro de la estructura organizacional en Diners Club del Ecuador en el año 2014. Como resultado del estudio se concluye la metodología Business Service Management (BSM), tuvo como beneficios a los técnicos, los cuales pueden identificar tempranamente la falla de un componente y consecuentemente poder dar una solución en menos tiempo, también a los jefes de tecnología porque pueden medir la disponibilidad de los servicios tecnológicos con los cuales pueden saber el tipo de servicio que están brindando como organización y si están o no cumpliendo con sus objetivos. Además, a los gerentes de tecnología, quien recibe la información que generan los otros dos niveles los cuales son utilizados para la planificación mediante el conocimiento del nivel de uso de los recursos tecnológicos. Asimismo, recomendó que para completar el circulo de monitoreo y extender los beneficios por fuera del área de tecnología, se debe extender el monitoreo del desempeño de los procesos de negocios, es decir, no solo saber si el servicio funciona o no funciona, sino saber si está cumpliendo con las metas propuestas del negocio.

Este antecedente permitió dar un mayor enfoque al monitoreo de transacciones gracias al sistema de gestión que nos permite tener mayor visión de las acciones a tomar.

Ñique (2016), Estudió la implementación de solución de autenticación segura basada en doble factor en una entidad del estado. El tipo de investigación es del tipo aplicada. Se utilizó como muestra la protección de los recursos como el acceso del correo interno de la empresa, el acceso remoto VPN SSL, la consola de administración de firewall, cinco sistemas web internos, treinta y cinco computadoras de escritorio con sistema operativo Windows, diez computadoras portátiles también con Windows y ciento cincuenta usuarios, el total para esta muestra fueron considerados doscientos tres recursos como activos de información las que fueron clasificados como información, software y personas. Se debe de mencionar que con la implementación de este proyecto se logró reducir un 45% de los riesgos de acceso no autorizado de usuarios internos, así como externos a recursos informáticos importantes de la empresa, además debido a la centralización del control de acceso de los servicios informáticos, se llegó a mejorar los procesos de administración de control de acceso lógico de usuarios a los servicios y sistemas que necesitan para realizar sus labores. Asimismo, recomendó que se implementen servidores réplicas para contar con mayor capacidad de contingencia para la plataforma principal, además que se podría desplegar estos servidores de autenticación como réplicas en sedes remotas o redes físicamente lejanas, con el fin de reducir la distancia física que recorre el tráfico de los eventos de autenticación y así optimizar el tiempo de respuesta de la plataforma.

Este antecedente permitió dar un mayor enfoque a la importancia de la seguridad sobre la autenticación de usuario para proteger los activos de la empresa, en este caso, para el presente proyecto al trabajar con data sensible de clientes finales y entidades financieras, será necesario una autenticación de doble factor, para esta solución se consumirá la API de OKTA especializada en la autenticación de identidad en internet.

Según Bombón (2018), Estudió los canales electrónicos, autenticación y monitoreo en el sistema financiero de la cooperativa de ahorro y crédito Kullki Wasi de la ciudad de Ambato. Como tipo de investigación utilizó la modalidad bibliográfica – documental. No se llegó a realizar el muestreo porque la población es reducida y es

de fácil acceso, por ello la muestra viene a ser la misma población por el número limitado de personas. La población para el análisis, así como estudio es el departamento de sistemas y el departamento de contabilidad de la cooperativa de ahorro y crédito Kullki Wasi Ltda., la cual se encuentra ubicada en la calle B. Juan Benigno Vela, Ambato 180150 de la ciudad de Ambato en el periodo 2018. Como resultado del estudio se concluyó que con la implementación de un sistema web en la Cooperativa de Ahorro y Crédito Kullki Wasi, mejoró el proceso operativo de las transacciones, consultas y monitoreo, todo esto siendo de mucha ayuda para los socios así como para los empleados del departamento de créditos, además se obtuvieron resultados satisfactorios en las interacciones como el acceso al sistema, transacciones internas, transacciones externas, consultas (saldos, créditos e inversiones), en el simulador de crédito y monitoreo (Créditos - Morosidad). Asimismo, recomendó a todos los usuarios finales que revisen el manual para entender el funcionamiento de los procesos individualmente, así evitando errar en los parámetros de la aplicación, además el software debe de estar bajo la responsabilidad del departamento de sistemas con la finalidad de corregir posibles errores que se puedan presentar con el tiempo.

Este antecedente permitió dar un mayor enfoque a los beneficios en la mejora de los procesos operacionales dentro de una organización, así como la importancia de la supervisión del equipo de sistemas sobre el área de operaciones.

A continuación, se presentarán los conceptos relacionados a las variables planteadas en este proyecto de investigación:

Según Hernández & Hernández (2018), el comercio electrónico consiste en vender bienes y servicios, por una web o aplicación para móviles en donde se permite realizar operaciones comerciales. De esta manera los comercios usan las plataformas electrónicas para ofrecer una gran variedad de productos y servicios de manera atractiva hacia el consumidor. (p. 25)

Un sistema de gestión de datos es una colección de procedimientos y personas que procesan información. Implica la recopilación, procesamiento, almacenamiento y recuperación de información. Quizás la herramienta más obvia es la computadora.

Sin embargo, es solo una de las muchas herramientas necesarias. Otras "herramientas" son las herramientas y formularios de recopilación de datos, los protocolos de gestión de datos, los mecanismos de control de calidad, los documentos, las instalaciones de almacenamiento para medios impresos y electrónicos y los mecanismos de recuperación. (Schoenbach, 2014, p. 40)

Según Caballero (2014), El proceso de autenticación basada en riesgos comienza con la recopilación de grandes cantidades de información, y el aprendizaje automático ayuda a analizar estos datos y usarlos para asignar una "puntuación de riesgo" a cada transacción. Por ejemplo, cambiar direcciones IP o compras inusualmente grandes; las soluciones de autenticación basadas en riesgos han demostrado ser muy precisas; según informes de MasterCard, algunas empresas han reducido el fraude en un 90%. (p. 36)

La seguridad de la información incluye asegurarse de que la organización comprenda, asuma, gestione y minimice los riesgos de seguridad de la información de forma documentada, sistemática, estructurada, repetible y eficaz, y la adapte a los cambios en la empresa. Riesgo, medio ambiente y tecnología. (Tarazona, 2017, p. 137)

Permite a clientes muy dispersos y proveedores para interactuar y ejecutar transacciones de compra. Cada paso de la contratación El proceso se captura electrónicamente y todos los datos de la transacción se enrutan automáticamente, reduciendo tiempo y costo de adquisición. Si se implementa correctamente, la contratación electrónica puede ofrecer enormes valores para las empresas de diferentes formas. (Kuzt, 2016, p. 30)

Transacción rechazada se refiere a la denegación de una tarjeta de crédito que se está utilizando como método de pago. Hay varias razones por las que una tarjeta puede ser rechazada y estas incluyen fondos insuficientes en la cuenta, que la tarjeta no está activada o que la tarjeta es robada o cancelada. Las razones más comunes por las que se rechaza una tarjeta son una fecha de vencimiento incorrecta y un número de tarjeta incorrecto. Por lo general, estos son el resultado de un error del usuario al ingresar los números. (Rodríguez, 2014, p. 92)

A continuación, se presentará conceptos relacionados para el desarrollo del Sistema de gestión de datos como la arquitectura del software, la metodología y las tecnologías.

Para esta investigación en el desarrollo del sistema de gestión de datos se hará uso del lenguaje de programación Python. Según Pérez y otros (2014), los lenguajes de programación son la herramienta básica de construcción de programas. En el caso python ha ido ganando popularidad en comunidades de software libre, científica y educacional, por su sencillez y posibilidad de concentrarse en los problemas. (p. 20)

Así como también se hará uso de la base de datos no relacional mongodb. Según Bellido (2016), MongoDB es un sistema de base de datos NoSQL multiplataforma de licencia libre. El patrón de arquitectura utilizado para el sistema de gestión de datos será el de microservicios. López y Maya lo define como: “Pequeños servicios autónomos que trabajan juntos”.

La metodología Scrum es un proceso de desarrollo de software iterativo y en evolución, generalmente utilizado en un entorno basado en el desarrollo de software ágil. Los trabajos se organizan en ciclos llamados Sprints, y estas iteraciones suelen durar de dos a cuatro semanas. Durante cada sprint, el equipo seleccionará una lista priorizada de necesidades del cliente, denominada historias de usuario, para que las funciones desarrolladas primero sean las más valiosas para los clientes. Al final de cada sprint, se entregará un producto potencialmente lanzable/distribuible/ comerciable. (Diaz,2017, p. 56)

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

De acuerdo al nivel de análisis y los requisitos para la realización de la investigación, se determina que la investigación es un tipo de aplicación, porque se basa en el uso de conocimientos teórico-prácticos para resolver problemas o determinar el nivel de problemas. influencias.

La investigación aplicada tiene como objeto el estudio de un problema destinado a la acción. La investigación aplicada puede aportar hechos nuevos… si proyectamos suficientemente bien nuestra investigación aplicada, de modo que podamos confiar en los hechos puestos al descubierto, la nueva información puede ser útil y estimable para la teoría. (Baena,2017, p. 140)

El diseño de investigación poblaciones experimental, el investigador no sólo se encuentra en condiciones prácticas de llevar a cabo un experimento, sino que conoce también, en buena medida, la naturaleza del fenómeno que investiga. (Baena,2017, p. 143)

La investigación realizada tiene un diseño experimental porque las variables dependientes se miden y comparan mediante conocimientos teóricos y prácticos. De acuerdo con los requerimientos de la investigación, se van a intervenir las variables de medida en un contexto controlado y repetible.

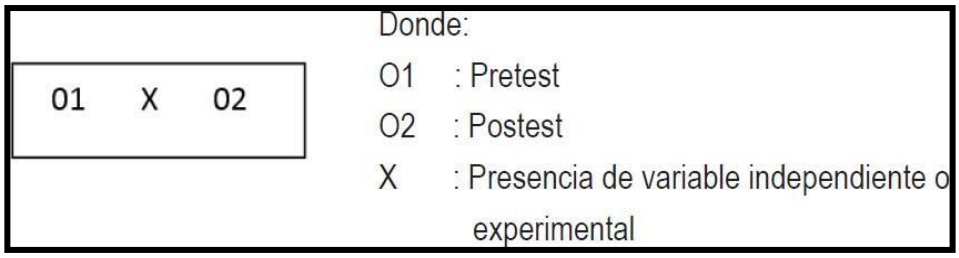


Figura 1 Diseño pretest postest con un solo grupo

Fuente: Mejía, Reyes y, Sánchez 2018

Leyenda:

X: Variable independiente (Sistema de gestión de datos) Es la influencia de la Gestión de datos en el desempeño del proceso de autenticación para emisores en Alignet SAC.

Mediante la evaluación previa (pretest) y posterior (postest) se determinará el grado porcentual de influencia en el proceso de autenticación para emisores de la organización.

O1: Pretest; medición experimental del desempeño del proceso de autenticación para emisores antes de la implementación del sistema de gestión de datos. Esta medición será contrastada con la medición postest.

O2: Postest; medición experimental del desempeño del proceso de autenticación para emisores después de la implementación del sistema de gestión de datos de la organización.

3.2. Variables y operacionalización

Definición conceptual

Variable independiente: Sistema de gestión de datos

Se define como el conjunto de procedimientos y personas por medio de los cuales se procesa la información. Involucra la recolección, manipulación, almacenamiento, y recuperación de información (Schoenbach,2014, p. 40)

Variable dependiente: Proceso de autenticación

El proceso de autenticación basado en el riesgo comienza con la recopilación de grandes volúmenes de información y el aprendizaje automático ayuda a analizar estos datos y usarlos para asignar a cada transacción un "puntaje de riesgo''. Los factores que se utilizan para evaluar el riesgo varían. Por ejemplo, una dirección IP que cambia constantemente o una compra anormalmente grande. Las soluciones de autenticación basadas en el riesgo han demostrado ser muy precisas. (Caballero,2014, p. 36)

Definición Operacional

Variable dependiente: Proceso de autenticación

Para medir la variable proceso de autenticación se utilizará la ficha de registro. Esta variable cuenta con una dimensión (Eficacia) la cual se divide por 2 indicadores (porcentaje de transacciones denegadas y porcentaje de transacciones autorizadas), para cada uno de ellos se utilizará formulas.

Indicadores

El primer indicador que se utilizara en esta investigación es el porcentaje de transacciones denegadas, así como se muestra la fórmula establecida para su medición.

$$PTD = \frac{\text{CANTIDAD DE TRANSACCIONES DENEGADAS}}{TOTAL\ DE\ TRANSACCIONES}\ X\ 100$$

Figura 2: Formula de porcentaje de transacciones denegadas

Fuente: López, Pedro

El segundo indicador que se utilizara en esta investigación es el porcentaje de transacciones autorizadas, así como se muestra la formula establecida para su medición.

$$PTA = \frac{\text{CANTIDAD DE TRANSACCIONES AUTORIZADAS}}{TOTAL\ DE\ TRANSACCIONES}\ X\ 100$$

Figura 3. Formula de porcentaje de transacciones autorizadas

Fuente: López, Pedro

3.3. Población, muestra y muestreo

Población

Según De la orden y Pimienta (2017), la población se refiere a todos los elementos que se ven afectados por el fenómeno o circunstancias específicas que fomentan la investigación. Estos elementos pueden ser personales o causales, también están limitados a un área específica, a un tiempo y espacio específicos. (p. 205)

En este trabajo de investigación se obtuvo un total de 30 registros de transacciones del mes de septiembre. En donde la organización utiliza estos registros en función de la experiencia para evaluar el porcentaje de transacciones denegadas y autorizadas. El registro del estudio corresponde a una evaluación de un mes (lunes a domingo), de la cual se obtendrán datos para medir el porcentaje de transacciones denegadas y el porcentaje de transacciones autorizadas.

Durante el pleno funcionamiento del ACS de la organización, los registros se pueden obtener directamente del área de TI de Alignet SAC.

CRITERIO DE INCLUSIÓN	CRITERIO DE EXCLUSIÓN
Rango de fechas del 1 de septiembre al 30 de septiembre delos registros diarios de transacciones.	Registros diarios fuera del rango de fecha de inclusión.

Tabla 1 Criterios de Inclusión y Exclusión

Fuente: 3.3. Población, muestra y muestreo

Elaboración: Propia.

Muestra

Según Baena (2017), indico que la muestra se refiere al subgrupo general que se está cuantificando. Este subgrupo debe contener las mismas características y entorno simbólico que la población. Por su generalización, esta última permite obtener resultados representativos de la población total. (p. 150)

El análisis especifica que cuando el número total de elementos es inferior a 50, la muestra se puede considerar como la muestra completa. De acuerdo con la situación anterior, debido a la pequeña población, la muestra estará conformada por todos los elementos de la población encuestados en el desarrollo del proyecto.

Muestreo

Para obtener muestras, es importante realizar procedimientos de muestreo. El procedimiento se basa en una selección sistemática de determinados elementos representativos de la población. Comparado con el análisis general, la importancia de aplicar este programa es reducir costos y tiempo. (Baena,2017, p. 152)

Por lo tanto, como la población es pequeña y solo tiene acceso a la muestra que será de 30 registros diarios, entonces no se hará el muestreo probabilístico.

3.4. Técnicas e instrumentos de recolección de datos.

Según Hernandez (2018) Las herramientas de recopilación de datos se utilizan para recopilar información en el proceso de investigación y desarrollo. Se pueden dividir en dos partes: indirecta (cuestionarios, pruebas, etc.) y directa (entrevistas, observaciones, etc.). Estas herramientas se aplican sobre la base de una muestra representativa de la población total. (p. 198)

TECNICA	INSTRUMENTO
Técnica de fichaje (De La Orden, y otros, 2017)	**Guía de Observación** GO 01: Recolección de valores de porcentaje de transacciones autorizadas GO 02: Recolección de valores de porcentaje de transacciones denegadas. (Ver Anexos)

Tabla 2Técnica e instrumento del proyecto

Fuente: 3.4. Técnicas e instrumentos de recolección de datos.

Elaboración: Propia.

Técnica de Recolección de Datos

La técnica del fichaje se basa en la ubicación y reconocimiento de los datos en las fuentes de información (muestra) a fin de lograr desarrollar el análisis recto o derivado de la problemática del estudio. (Escudero, 2018, p. 112)

Instrumentos de Recolección de Datos

La herramienta elegida para esta investigación es la ficha de registro. En el desarrollo del proyecto se utilizarán dos fichas de registros. La primera ficha de registro se desarrolló para recopilar información sobre el porcentaje de transacciones denegadas (ver Anexo 3). La segunda ficha de registro es para recopilar información sobre el porcentaje de transacciones aprobadas (ver Anexo 3). Ambos documentos fueron recolectados dentro de los 30 días antes y después de la implementación del proyecto, que tiene como objetivo medir el impacto del sistema de gestión de datos en el proceso de autenticación para emisor de Alignet S.A.C.

La ficha de registro se basa en anotaciones físicas de datos o resultados obtenidos durante el desarrollo de un proyecto de investigación. Permite el mantenimiento de un registro organizativo de los datos obtenidos con el fin de procesar su análisis y determinar el cumplimiento del estudio. (De la Orden Hoz, y otros, 2017, p. 128)

Del mismo modo, al diseñar un instrumento (ficha de registro) para la recolección de datos, se deben considerar dos criterios importantes: validez y confiabilidad. - Validez

Según Hernandez (2018), al evaluar el concepto de validez, se refiere al nivel de precisión en la definición de las variables de investigación de la evaluación instrumental. El nivel de evaluación debe expresar qué tan cerca mide el concepto teórico de la variable (indicador) de manera práctica. La validez consiste en validez de contenido, criterios y constructo. (p. 130)

Validez de Contenido

La validez de contenido se refiere a la capacidad de una herramienta para incluir aspectos suficientes o más importantes de las variables que está tratando de medir.

Validez de Criterio

La validez de los criterios se basa en que la primera herramienta debe proporcionar resultados similares (parcial o mayoritariamente) ya que la segunda también mide las mismas variables.

Validez de Constructo

Al expresar el grado de correspondencia entre los datos obtenidos de la variable (a través del instrumento) y la teoría bibliográfica relacionada con ella, se puede mejorar la efectividad de la estructura.

Para el presente estudio se tomará una validez basada en el contenido mediante el juicio de experto.

Confiabilidad

La confiabilidad de los instrumentos depende principalmente de la precisión de sus muestras representativas con resultados razonables y consistentes. (Hernandez, 2018, p.133)

Las búsquedas especifican la confiabilidad de los documentos, permiten asegurar que el desarrollo se basa en la realidad, estos a su vez representan las características y resultados reales de todo el proceso de investigación.

El proyecto de investigación desarrolló contenidos adecuados para fichas de registro, que pueden ser verificados mediante juicio de expertos. El desarrollo de esta verificación hará que las herramientas de recolección de datos (fichas de registro) sean más confiables.

3.5. Procedimientos

La recolección de los datos y conocimiento del desarrollo de la investigación fue coordinada con la empresa dentro de un periodo de 30 días del mes de septiembre.

Para recopilar los datos, se recopilan dentro de los 30 días de un mes (de lunes a domingo) en la oficina de Tecnología de Información de Alignet SAC entre las 2 a.m. y las 10 p.m. todos los meses (según el número de empleados de la organización). El análisis se desarrolla antes y después de la aplicación del sistema de gestión de datos para cumplir con los requisitos de datos para su posterior análisis y evaluación.

Los datos se obtienen a través del módulo de administrador del software Alignet Aplication Management (AAM), que proporciona informes y luego proporciona la

ficha de registro correspondiente para su posterior aprobación por parte del jefe del área de TI y utilizada como evidencia importante en ella. Indicadores de diagnóstico.

Después de aplicar la investigación, realizaremos nuevas mediciones en los indicadores para complementar los indicadores anteriores para que la investigación produzca el análisis final en Alignet S.A.C. Al finalizar el análisis, se redactará un informe concluyente y se remitirá al responsable del campo para su posterior aprobación y archivo.

3.6. Métodos de Análisis de datos.

Se establece que el estudio desarrolla un análisis cuantitativo, ya que se basa en el análisis de los valores numéricos obtenidos en las fichas de registro y sus representaciones gráficas que estos derivan.

Así mismo, el análisis se realiza en un primer instante bajo la representación gráfica y detallada de los datos obtenidos en las fichas durante la evaluación de los indicadores. En esta etapa de análisis se busca representar de forma estadística la información obtenida durante la ejecución del estudio. Esto último constituyéndose como el análisis descriptivo de los datos del proyecto de investigación y que se soportan en la estadística descriptiva.

La estadística descriptiva, a la cual también se denomina estadística básica, es aquella que se encarga de establecer las relaciones de análisis de los datos en función a su tipo y las operaciones que se aplican entre ellas. Busca expresar la complejidad de los datos en gráficos accesibles a los interesados.

Posterior a este primer análisis se realizará el contraste de los datos. Se pone en contraste los datos recabados antes y después de la implementación del sistema de gestión de datos. Con este contraste metódico se busca obtener un análisis real de la influencia del sistema de gestión de datos de la empresa Alignet S.A.C. y con ello determinar si los objetivos e hipótesis de la investigación fueron desarrollados de manera total, parcial o si surgieron nuevos eventos que requieran estudios adicionales. Para esta fase se emplea herramientas de la estadística inferencial.

La estadística inferencial, también denominada estadística de segundo nivel, permite evaluar las congruencias o diferencias entre las poblaciones que son tomadas en las muestras del estudio. Dependiendo de la orientación este tipo de estadística puede ser paramétrica o no paramétrica.

3.7. Aspectos Éticos

El estudio basa su desarrollo en los principios fundamentales de todo trabajo de investigación. Se busca formar el principio de justicia al desarrollar una utilidad de beneficio para la empresa Alignet SAC, buscando el bienestar de la misma en toda la implementación del proyecto. Así mismo, busca ejecutar de manera competente y dedicada cada fase del método científico, que está asociado al desarrollo del presente estudio. El estudio parte del consentimiento explícito de la organización.

El proyecto también se desenvuelve dentro de los lineamientos proporcionados por la Oficina de Investigación y la Escuela Profesional de Ingeniería de Sistemas de la Universidad Cesar Vallejo – Sede Ate (Resolución de Consejo Universitario N° 0389 – 2017/UCV). Se desarrolla una investigación que cumple con los requerimientos del diseño cuantitativo de enfoque científico.

El presente estudio tiene especial cuidado en el uso de los concepto teóricos y bibliográficos de otros autores (Decreto Legislativo N° 822 – Ley Sobre el Derecho de Autor). Se redacta de manera clara cada uno de estos aportes siguiendo la normativa del ISO 690 – 2, referenciando a sus autores y modo de obtención del material.

La investigación válida la selección de la metodología a implementar para la variable independiente: Sistema de gestión de datos, en base a la evaluación de expertos. Los expertos responderán a un documento de validación de la metodología, permitiendo optar por la metodología más apropiada para la investigación.

Finalmente, el estudio presenta información acerca de la empresa Alignet SAC. La información asociada fue tratada bajo los lineamientos de La Ley 29733 – Ley de Tratamiento de Datos Personales, a fin de conservar la integridad de la misma y la transparencia en los fines para los cuales son dispuestos (ISO/IEC 29100).

IV. RESULTADOS

El trabajo desarrollado en el presente estudio fue estructurado y desarrollado con el propósito de establecer la influencia exacta y cuantificable del Sistema de gestión de datos. En el caso particular de la empresa Alignet posterior a la implementación de la tecnología. A continuación, se muestran los resultados en base a la problemática principal y especificas:

El presente estudio tuvo como objetivo principal medir la influencia del sistema de gestión de datos en la empresa Alignet. El cálculo de la influencia está basado en el análisis de los indicadores considerados importantes tales como porcentaje de transacciones denegadas y porcentaje de transacciones autorizadas. Basados en los datos que se recaban conforme se integra la propuesta un sistema de gestión en el proceso de autenticación, se puede evidenciar cambios sustanciales en los indicadores. (Ver Gráfico 1)

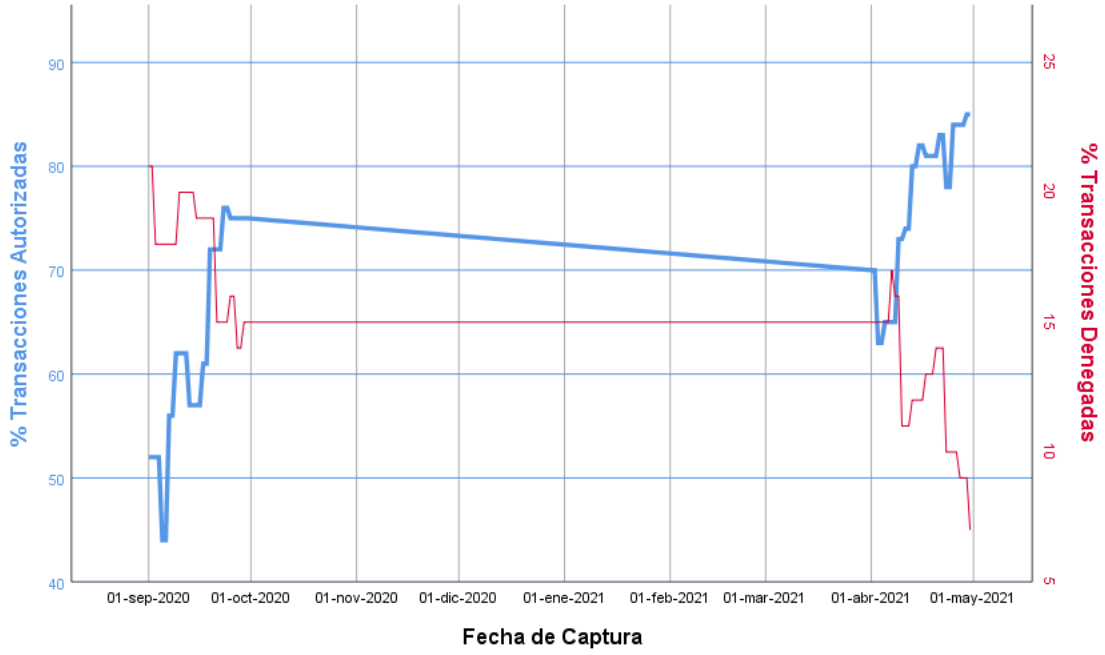


Gráfico 1Indicadores de influencia en el Proceso de Autenticación para emisores en la Empresa Alignet.

Fuente: Anexos

Elaboración: IBM SPSS Statistisc v. 26

Tipo de Medición		% Transacciones Denegadas	% Transacciones Autorizadas
Pretest	Media	17,73	63,20
	N	30	30
	% de suma total	58,7%	45,2%
Postest	Media	12,50	76,53
	N	30	30
	% de suma total	41,3%	54,8%
Total	Media	15,12	69,87
	N	60	60
	% de suma total	100,0%	100,0%

Tabla 3 Evaluación de mediciones pre y post test de indicadores

Fuente: Anexo

Elaboración: IBM SPSS Statistisc v. 26

Antes de la implementación del Sistema de Gestión en el Proceso de Autenticación, los indicadores se encontraban por debajo del requerimiento de la organización. Esto evidenciaría que las transacciones no podían culminar su proceso de autenticación por datos incorrectos, tarjetas no enroladas, tarjetas bloqueadas por el emisor o transacción incompleta. La medición de indicadores expresa el estado de la influencia del proceso de autenticación, porque la influencia es directamente proporcional al porcentaje de transacciones autorizadas (cuanto mayor son las transacciones autorizadas, mayor es la influencia). De manera similar, la influencia del proceso de autenticación es inversamente proporcional al porcentaje de transacciones denegadas (cuanto menor sea el porcentaje de transacciones denegadas, mejor será la influencia del proceso de autenticación). Considerando el cuadro cronológico de los datos, los resultados muestran que el sistema de gestión de datos en el proceso de autenticación de la empresa Alignet tiene el impacto esperado en la influencia, es decir, una mejora significativa. De la misma manera, se puede concluir que la implementación del sistema siempre tiende a mejorar la influencia a medida que se agregan datos de los tarjetahabientes.

Si analizamos el porcentaje de transacciones autorizadas en detalle, mide las transacciones culminadas con éxito en la etapa de autenticación; según las observaciones, este indicador ha sufrido los cambios más importantes. Cada transacción registrada representa el valor promedio del porcentaje de transacciones autorizadas en cada día en orden cronológico, y se usa para representar las transacciones completas. El porcentaje de transacciones autorizadas se mantuvo en 0.67 (67%) en el tiempo antes del final de la implementación del sistema. El bajo porcentaje de este indicador se debe a la poca información actualizada de los tarjetahabientes y otras observaciones. Al final del proyecto, este indicador pasó a ser 0,73 (73%) como valor de medida promedio en las transacciones, manteniendo así el mejor desempeño del proceso de autenticación y del servicio que gestionan los emisores de la empresa Alignet. (Ver Gráfico 2)

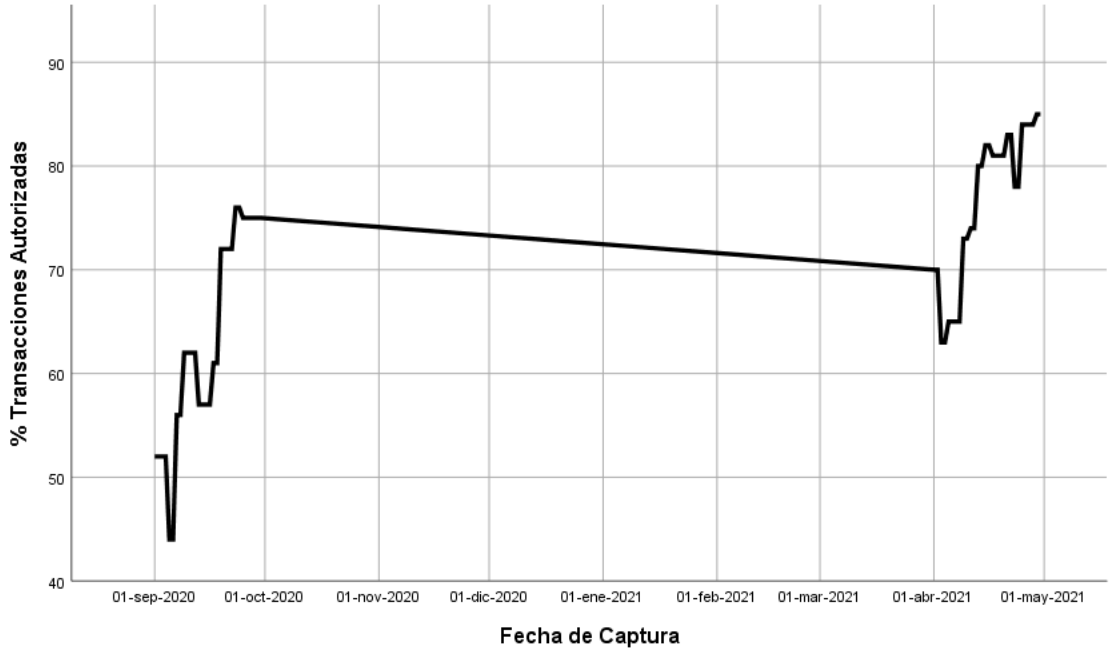


Gráfico 2 Evolución del porcentaje de transacciones Autorizadas.

Fuente: Anexos

Elaboración: Propia

De esta forma, las transacciones realizadas por internet se transmiten del sistema dentro de un rango de porcentaje aceptable para los emisores. Reduce los

problemas de autenticación entre los tarjetahabientes y la pérdida de transacciones para la empresa Alignet.

Al evaluar las transacciones denegadas por día de la organización, se determinan los indicadores que se pueden cambiar para beneficiar el desempeño. El porcentaje de transacciones denegadas es de aproximadamente 18 %, aunque este valor no genera pérdidas amplias de transacciones, sí afecta el rendimiento. Después de utilizar el sistema de gestión en el proceso a autenticación, este porcentaje se ha convertido en un promedio de 14%. El cambio de 4% constituye un cambio importante en la cantidad de transacciones que no se pierden por falta de información del tarjetahabiente. Este porcentaje debe reducirse, lográndose a medida que se desarrolla la investigación. (Ver Gráfico 3)

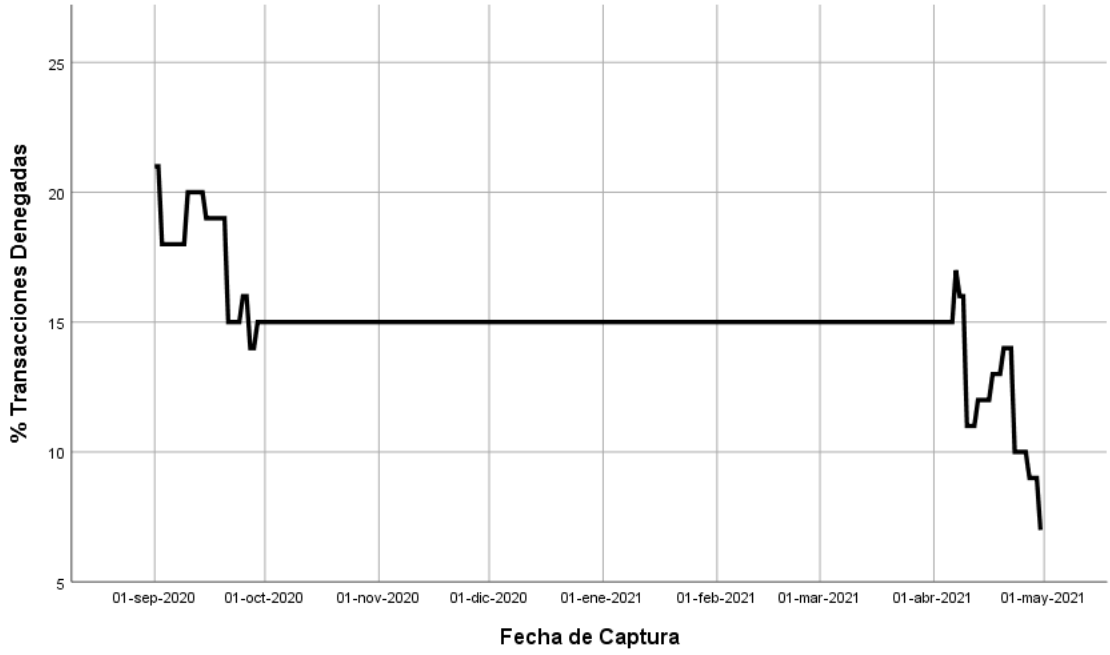


Gráfico 3Evolución del porcentaje de transacciones Denegadas.

Fuente: Anexo

Elaboración: Propia

La mejora de este indicador supone una disminución de su valor, puede mantener actualizados los datos de los emisores de la empresa Alignet incluso cuando los tarjetahabientes no transaccionen de manera online. El porcentaje reducido permite

a los emisores ampliar la posibilidad de transaccionar de los clientes. Para reducir las transacciones denegadas, es necesario establecer una frecuencia de actualización de los datos de los tarjetahabientes y eliminar datos redundantes, que constituyen duplicación de campos en las bases de datos y consumen recursos. A partir de estos valores, se puede decir que los supuestos realizados en el desarrollo de este trabajo de investigación son positivos. En otras palabras, cuando se utiliza un sistema de gestión de datos, se mejora el proceso de autenticación.

V. DISCUSION

Este trabajo de investigación tuvo como objetivo determinar influencia de un sistema de gestión de datos en el proceso de autenticación para emisores en la empresa Alignet S.A.C. Del capítulo anterior, en donde se deriva una serie de información proveniente del cálculo del porcentaje de transacciones autorizadas y transacciones denegadas se obtiene una serie de aseveraciones que son de suma importancia para alcanzar nuestro propósito.

Los resultados de investigación comprueban la hipótesis propuesta. Se afirma que un sistema de gestión de datos mejorará el proceso de autenticación para emisores en la empresa Alignet S.A.C., Del trabajo de implementación del proyecto se obtuvo que el porcentaje de transacciones autorizadas ha presentado un incremento del 6% y la reducción del porcentaje de transacciones denegadas en 4%. Siendo un balance positivo para todos los emisores y usuarios, estos últimos que realizan operaciones en la línea porque menos transacciones fueron truncadas pudiendo finalizar con éxito el proceso de autenticación. Ante estos resultados encontrados podemos inferir que mas usuarios han podido realizar sus operaciones de pagos de servicios sin ningún problema provocando que se vuelvan a utilizar este medio de pago.

A partir de los hallazgos encontrados, aceptamos la hipótesis alternativa general que establece que existe una relación de dependencia entre el desarrollo de banca electrónica y la aceptación de los clientes en toda lima metropolitana.

Estos resultados guardan relación con lo que sostiene Gonzales (2017), quien señala que el crecimiento de la banca electrónica depende de la aprobación de los clientes con este canal de atención porque el 84.9% de los usuarios se encuentran satisfecho y muy satisfechos. Por lo que sí el usuario al tener una mala experiencia al presentar problemas en sus métodos de pago, pueden provocar que no lo sigan utilizando o simplemente preferir otras alternativas en el mercado. Por ello se debe de mantener la data de los usuarios actualizada por los bancos para que no presenten problemas en el procedimiento de autenticación al momento de adquirir un bien o servicio y así evitar los datos incorrectos. Disminuir la fricción es uno de

los objetivos importantes para que el cliente vuelva a preferir estos medios de pago y pueda afianzar su preferencia para así con ello incrementar la demanda y el desarrollo de la banca electrónica que abre las puertas a muchos comercios a través de las tecnologías brindadas por Alignet hacia los emisores. Adicional a ello también se acepta la hipótesis general de Orihuela y otros (2019) que menciona que el factor tecnológico no actúa como una limitante, sino como un incentivo a la adopción del comercio electrónico como parte de las actividades en los negocios. Gracias a los resultados encontrados se puede entender la importancia positiva de un sistema de gestión de datos puede aportar al crecimiento del comercio en línea

En cuanto al porcentaje de transacciones denegadas, aceptamos la hipótesis de efectos negativos de un determinado método de autenticación de dos factores como el protocolo 3-D Secure en el usuario – experiencia. Estos resultados guardan relación con lo que sostiene Ardizzi (2017), quien señala que la experiencia del usuario no debe ser subestimada por el responsable de la formulación de políticas y que el problema ya ha sido abordado por las recientes directrices sobre seguridad de pagos por internet que requieren autentificación de cliente fuerte para pagos en línea. Además, la idea de permitir excepciones del requisito de autenticación fuerte de clientes es coherente con la posibilidad de hacer que el inicio del pago sea más fácil de usar. Incluso se menciona que no existe una tecnología de seguridad única para todos y los proveedores de servicios pueden implementar diferentes tipos de métodos de autenticación de dos factores para la banca electrónica con diferentes niveles de usabilidad. En el proceso de autenticación existe deferentes criterios al momento autenticar una transacción en donde cada una de ellas pueden afectar directamente al porcentaje de transacciones denegadas, un claro ejemplo puede ser el tema de montos superados los cuales usarán la data que se tiene registrado en el enrolamiento masivo o enrolamiento por API, en este caso puede ser el número de teléfono. Si la clave OTP no le llega al usuario porque no se tiene actualizado o simplemente no lo tiene registrado puede provocar que se pierda la autenticación de la transacción y que la experiencia de usuario se vea afectada considerablemente.

VI. CONCLUSION

De este trabajo de investigación se pueden extraer una serie de conclusiones, Aquellos que son muy útiles para comprender las relaciones entre un sistema de gestión de datos y el proceso de autenticación. Considerando los valores de proceso, discusión y análisis de la implementación de un sistema de gestión de datos bajo las características mostradas, considerando los resultados del porcentaje de las transacciones autorizadas y denegadas en la empresa Alignet, podemos sacar conclusiones:

Primero: Un sistema de gestión de datos mejorará el proceso de autenticación para emisores en la empresa ALIGNET SAC

En este proyecto de investigación se determinó la influencia positiva de un sistema de gestión de datos en el proceso de autenticación para emisores en la empresa ALIGNET SAC, porque en comparación con el valor inicial obtenido en el estudio se logró aumentar el porcentaje de transacciones autorizadas en un 6% y reducir el porcentaje de transacciones denegadas en un 4%, favoreciendo a los cliente de la empresa (emisores) a quienes va dirigido este producto con la finalidad de gestionar de una manera más eficiente sus tarjetas emitidas para el proceso de autenticación.

Segundo: un sistema de gestión de datos aumentará el porcentaje de transacciones autorizadas en el proceso de autenticación para emisores en la empresa ALIGNET SAC.

En cuanto al porcentaje de transacciones autorizadas tomadas en este trabajo de investigación, los resultados se tomaron en el rango del mes de septiembre del 2020 presentando como resultado 67% (2749698 transacciones autorizadas) y los resultados al finalizar este proyecto en el mes de abril del 2021 son de 73% (3736036 transacciones autorizadas). Este resultado indica fuertemente un crecimiento favorable de las transacciones que han podido ser autenticadas correctamente. Gracias a este resultado favorable los clientes de Alignet (emisores) incrementarán sus transacciones positivas, adicionando que podrán administrar sus tarjetas enroladas, directamente desde la plataforma.

Tercero: un sistema de gestión de datos disminuirá el porcentaje de transacciones denegadas del proceso de autenticación para emisores en la empresa ALIGNET SAC

En esta investigación se determinó la influencia de un sistema de gestión de datos en el porcentaje de transacciones denegadas en el proceso de autenticación para emisores en la empresa ALIGNET SAC, podemos establecer que la hipótesis planteada en este proyecto es favorable porque fue posible reducir la proporción de transacciones denegadas de un promedio de 18% a 14%; en donde inicialmente se calcularon 778 201 transacciones en el mes de septiembre del año 2020 y después de la implementación de este proyecto se obtuvo una mejora teniendo como resultado 607 344 transacciones en el mes de abril del año 2021 al final del proyecto.

Los resultados indican una mejora significativa en las métricas seleccionadas para evaluar el impacto en el proceso de autenticación de identidad del emisor de Alignet. Demostrar la eficiencia del sistema de gestión de datos como un agregado de valor para todos clientes emisores de la empresa.

VII. RECOMENDACIONES

1. Respecto a este proyecto se recomienda a futuro realizar mejoras, cambios y actualizaciones hacia nuevos requerimientos del cliente, para mantener el producto actualizados y que se ajuste a los requerimientos de los clientes emisores.

2. Se recomienda usar la tecnología de microservicios en la plataforma de alojamiento AWS por objetivos específicos o tareas para poder darle manteniendo o asistencia ante una incidencia rápidamente además de poder distribuir la carga, tener una fluidez y continuidad en el servicio.

3. Se recomienda alinear el producto a las nuevas versiones del protocolo 3D-SECURE que puedas presentarse a futuro, para poder tener disponible el servicio.

4. Se recomienda a las áreas administrativas generar un manual de usuario para los clientes y así evitar que el mal uso sea por parte del usuario nivel administrador o visor.

5. Realizar pruebas de rendimiento y performance del procesamiento de archivos para enrolamiento masivo y todo el sistema para lograr tener una acción preventiva que se pueda ir mejorando y permitir la disponibilidad del servicio continuo.

6. Poner alertas en el CPUs Utilization (Percent),DB Connections(count),Freeable Memory(MB),Write Latency(Milliseconds),Read Latency(Milliseconds),Network Receive Througput(MB/Second) para poder monitorear el consumo de recursos de la DB de la aplicación en los servicios de AWS y prever posibles incidentes de lentitud o perdidas del servicio.

REFERENCIAS

ANDRADE CHIMBA, Christian David. 2016. Implementación de herramientas de seguridad web en una tienda de ventas por internet desarrollada en Prestashop. Quito : Universidad de las Américas, 2016.

ARDIZZI, Guerino. 2017. Innovation in costumer authentication methods, card-based internet payments and user experience: empirical evidence from Italy. Join ECB-BI conference, Roma, Italia : 2017.

BAENA PAZ, GUILLERMINA. 2017. Metodología de la Investigación. Mexico : Grupo Editorial Patria, 2017. 978-607-744-748-1.

Base de datos NoSQL: MongoDB. Bellido Sanchez, Sergio. 2015. Mexico : s.n., 2015.

BORGHELLO, Cristian. 2019. Segu.Info: Noticias sobre seguridad de la información. [En línea] 23 de Diciembre de 2019. [Citado el: 2 de Octubre de 2020.] https://blog.segu- info.com.ar/2019/12/metodos-de-autenticacion-disponibles.html.

Caballero, Jimmy. 2014. AUTENTICACIÓN BASADA EN RIESGOS (RBA). [aut. libro] JIMMY CABALLERO, JORGE RICARDO y LADINO MARTÍNEZ. AUTENTICACIÓN BASADA EN RIESGOS (RBA). bogota : UNIVERSIDAD CATOLICA DE COLOMBIA, 2014.

Challenger-Pérez, Ivet, Díaz-Ricardo, Yanet y Becerra-García, Roberto Antonio. 2014. El lenguaje de programación Python. Cuba : Universidad de Holguín, 2014. 1027-2127.

Daniel López, Edgar Maya. 2017. Arquitectura de Software basada en Microservicios para. Ecuador : Universidad Técnica del Norte, 2017.

De la Orden Hoz, Arturo y Pimienta Prieto, Julio Herminio. 2017. Metodología de la investigación: competencia aprendizaje vida. Mexico : Pearson, 2017. 978-607-32-3932-5.

DURÁN, AURA MARÍA PINTO y ADIANA MARÍA TORO GIRALDO. 2014. AUTENTICACIÓN BASADA EN RIESGOS (RBA). BOGOTA : UNIVERSIDAD CATOLICA DE COLOMBIA FACULTAD DE INGENIERIA, 2014.

ESCUDERO, C. y CORTEZ, L. 2018. Técnicas y métodos cualitativos para la investigación científica. Machala : Editorial UTMACH, 2018.

GONZALES, Angie Katherine. 2017. El desarrollo de la banca electrónica y la aceptación de los clientes de lima metropolitana de los 4 principales bancos del perú. Universidad San Ignacio de Loyola, Lima, Perú : 2017.

HERNÁNDEZ Ramos, Eva María y Hernandez Barrueco, Luis. 2018. Manual de comercio electrónico.s.l. : margen books, 2018. 9788417313630.

HERNÁNDEZ, R. y MENDOZA, C. 2018. Metodología de la Investigación: Las rutas cuantitativa, cualitativa y mixta. Mexico : McGraw-Hill, 2018. 978-1-4562-6096-5.

KÜTZ, Martin. 2016. Introduction to E-Commerce: Combining Business and Information Technology. Alemania : bookbon.com, 2016. 9788740315202.

LARRÁN, Jorge y MURIEL DE LOS REYES, M. J. 2007. La banca por internet como innovación tecnológica en el sector bancario. Vigo, España : Investigaciones Europeas de Dirección y Economía de la Empresa, 2007. 11352523.

MARCHAL, Samuel y SZYLLER, Sebastián. 2019. Detecting organized eCommerce fraud using scalable categorical clustering. Proceedings of the 35th Annual Computer Security Applications Conference, EEUU : 2019.

MEJÍA, K., REYES, C. y SÁNCHEZ, H. 2018. Manual de términos en investigación científica, tecnológica y humanística. Lima : Universidad Ricardo Palma, Vicerrectorado de Investigación, 2018. 978-612-47351-4-1.

MIRANDA, Mera y PATRICIO, Rene. 2015. Monitoreo de la infraestructura de TI y modelo de medición automática del proceso de autorizaciones en tiempo real de Diners Club del Ecuador. Universidad de las Fuerzas Armadas, Sangolquí, Ecuador : 2015.

NEGRILLO, Ricardo Alberto. 2019. Impacto de una guía de cooperación organizacional en la reducción de perdidas por fraude tecnológico del banco continental. Lima : Universidad Nacional Agraria la Molina, 2019.

ORIHUELA, Gabriela y SIUCE, Giuliana Ysela. 2019. Factores que limitan la adopción del comercio electrónico en los negocios del centro comercial Contitución de Huancayo. Universidad Continental, Huancayo, Perú : 2019.

SCHOENBACH, Victor J. 2014. Gestion y analisis de datos. s.l. : epidemiolog.net, 2014.

TARAZONA T., Cesar H. 2017. AMENAZAS INFORMÁTICAS Y SEGURIDAD DE LA INFORMACIÓN. AMENAZAS INFORMÁTICAS Y SEGURIDAD DE LA INFORMACIÓN. s.l. : Etek Internacional, 2017.

ANEXOS

Anexo 2: Matriz de consistencia

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES	DIMENSIONES	INDICADOR
Principal	**General**	**General**	**Independiente**		
¿Cuál es la influencia de un sistema de gestión de datos en el proceso de autenticación para emisores en la empresa ALIGNET S.A.C.?	Determinar la influencia de un sistema de gestión de datos en el proceso de autenticación para emisores en la empresa ALIGNET SAC	Un sistema de gestión de datos que mejorará el proceso de autenticación para emisores en la empresa ALIGNET SAC	sistema de gestión de datos		
Específicos	**Específicos**	**Específicos**	**Dependiente**		
¿Cuál es la influencia de un sistema de gestión de datos en el porcentaje de transacciones denegadas en el proceso de autenticación para emisores en la empresa ALIGNET S.A.C.?	Determinar la influencia de un sistema de gestión de datos para reducir el porcentaje de transacciones denegadas en el proceso de autenticación para emisores en la empresa ALIGNET SAC	Un sistema de gestión de datos disminuirá el porcentaje de transacciones denegadas del proceso de autenticación para emisores en la empresa ALIGNET SAC	proceso de autenticación	Eficacia	porcentaje de transacciones denegadas
¿Cuál es la influencia de un sistema de gestión de datos en el porcentaje de transacciones autorizadas en el proceso de autenticación para emisores en la empresa ALIGNET SAC?	Determinar la influencia de un sistema de gestión de datos en el porcentaje de transacciones autorizadas en el proceso de autenticación para emisores en la empresa ALIGNET SAC	Un sistema de gestión de datos aumentará el porcentaje de transacciones autorizadas en el proceso de autenticación para emisores en la empresa ALIGNET SAC			porcentaje de transacciones autorizadas

Anexo 3: Matriz de operacionalización

Variable	Definición conceptual	Dimensiones	Indicadores
Sistema de gestión de datos	El sistema de gestión de datos es el conjunto de procedimientos y personas por medio de los cuales se procesa la información. Involucra la recolección, manipulación, almacenamiento, y recuperación de información. Talvez la herramienta más visible es la computadora; sin embargo, es meramente una de tantas herramientas necesarias. Otras "herramientas" son los instrumentos y los formularios de recolección de datos, el protocolo de gestión de datos, los mecanismos de control de calidad, documentación, instalaciones de almacenamiento tanto para el papel como los medios electrónicos, y los mecanismos de recuperación. (Schoenbach,2014)	La seguridad de la información consiste en garantizar que los riesgos de la seguridad de la información son conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías. (Rayme,2017)	transacción rechazada se refiere a la denegación de una tarjeta de crédito que se está utilizando como método de pago. Hay varias razones por las que una tarjeta puede ser rechazada y estas incluyen fondos insuficientes en la cuenta, que la tarjeta no está activada o que la tarjeta es robada o cancelada. Las razones más comunes por las que se rechaza una tarjeta son una fecha de vencimiento incorrecta y un número de tarjeta incorrecto. Por lo general, estos son el resultado de un error del usuario al ingresar los números. (Rodríguez, 2014)
Proceso de autenticación	El proceso de autenticación basado en el riesgo comienza con la recopilación de grandes volúmenes de información y el aprendizaje automático ayuda a analizar estos datos y usarlos para asignar a cada transacción un "puntaje de riesgo". Los factores que se utilizan para evaluar el riesgo varían. Por ejemplo, una dirección IP que cambia constantemente o una compra anormalmente grande. Las soluciones de autenticación basadas en el riesgo han demostrado ser muy precisas. (Caballero,2014)	Eficacia	Permite a clientes muy dispersos y proveedores para interactuar y ejecutar transacciones de compra. Cada paso de la contratación El proceso se captura electrónicamente y todos los datos de la transacción se enrutan automáticamente, reduciendo tiempo y costo de adquisición. Si se implementa correctamente, la contratación electrónica puede ofrecer enormes valores para las empresas de diferentes formas. (Kuzt, 2016)

Anexo 4 Instrumento de recolección de datos

FICHA DE REGISTRO						
DIMENSIÓN:				Eficacia	**FECHA:**	01/09/2020
INDICADOR:				Porcentaje de transacciones denegadas	**DURACIÓN:**	30 días
INVESTIGADORES:				Pinto Pintos, Katelyn Zarelly Zuñiga Huaraca, Kenny	**AREA:**	TI
EMPRESA:				Alignet S.A.C.	**FORMULA:**	
PROCESO DE OBSERVACION:				Autenticación	$PTD = \frac{Cantidad\ de\ transacciones\ denegadas}{Total\ de\ transacciones} x\ 100$	
TIPO:				Pre-Test		
N°	**FECHA 2020**			**Transacciones denegadas**	**Total de transacciones**	**Promedio**
	MES	**DIA**	**FECHA**			
1	**SETIEMBRE**	Martes	01/09/2020	37976	180839	21%
		Miércoles	02/09/2020	24575	117027	21%
		Jueves	03/09/2020	26568	147603	18%
		Viernes	04/09/2020	30780	171005	18%
		Sábado	05/09/2020	24730	137390	18%
		Domingo	06/09/2020	30713	170628	18%
		Lunes	07/09/2020	23770	132058	18%
		Martes	08/09/2020	32702	181682	18%
		Miércoles	09/09/2020	31840	176891	18%
		Jueves	10/09/2020	37137	185688	21%
		Viernes	11/09/2020	30256	151282	20%

		Sábado	12/09/2020	22008	110042	20%
		Domingo	13/09/2020	31365	156829	20%
		Lunes	14/09/2020	24229	121148	20%
		Martes	15/09/2020	26089	137311	19%
		Miércoles	16/09/2020	27660	145584	19%
		Jueves	17/09/2020	30767	161936	19%
		Viernes	18/09/2020	26483	139388	19%
		Sábado	19/09/2020	22565	118764	19%
		Domingo	20/09/2020	26509	139524	19%
		Lunes	21/09/2020	18626	124176	15%
		Martes	22/09/2020	22012	146753	15%
		Miércoles	23/09/2020	23490	156604	15%
		Jueves	24/09/2020	23352	155680	15%
		Viernes	25/09/2020	23718	148240	16%
		Sábado	26/09/2020	20460	127878	16%
		Domingo	27/09/2020	14205	101467	14%
		Lunes	28/09/2020	22258	158990	14%
		Martes	29/09/2020	19374	129164	15%
		Miércoles	30/09/2020	21984	146562	15%
TOTAL				788064	4378133	18%

FICHA DE REGISTRO			
DIMENSIÓN:	Eficacia	**FECHA:**	01/09/2020
INDICADOR:	Porcentaje de transacciones autorizadas	**DURACIÓN:**	30 días

INVESTIGADORES:				Pinto Pintos, Katelyn Zarelly Zuñiga Huaraca, Kenny	**AREA:**	TI
EMPRESA:				Alignet S.A.C.	**FORMULA:**	
PROCESO DE OBSERVACION:				Autenticación	$PTA = \frac{Cantidad\ de\ transacciones\ autorizadas}{Total\ de\ transacciones} \times 100$	
TIPO:				Pre-Test		
N°	**FECHA 2020**			**Transacciones autorizadas**	**Total de transacciones**	**Promedio**
	MES	**DIA**	**FECHA**			
1	**SETIEMBRE**	Martes	01/09/2020	94036	180839	52%
		Miércoles	02/09/2020	60854	117027	52%
		Jueves	03/09/2020	76753	147603	52%
		Viernes	04/09/2020	88922	171005	52%
		Sábado	05/09/2020	60451	137390	44%
		Domingo	06/09/2020	75076	170628	44%
		Lunes	07/09/2020	73952	132058	56%
		Martes	08/09/2020	101741	181682	56%
		Miércoles	09/09/2020	109672	176891	62%
		Jueves	10/09/2020	115126	185688	62%
		Viernes	11/09/2020	93794	151282	62%
		Sábado	12/09/2020	68226	110042	62%
		Domingo	13/09/2020	89392	156829	57%
		Lunes	14/09/2020	69054	121148	57%
		Martes	15/09/2020	78267	137311	57%
		Miércoles	16/09/2020	82982	145584	57%
		Jueves	17/09/2020	98780	161936	61%
		Viernes	18/09/2020	85026	139388	61%

		Sábado	19/09/2020	85510	118764	72%
		Domingo	20/09/2020	100457	139524	72%
		Lunes	21/09/2020	89406	124176	72%
		Martes	22/09/2020	105662	146753	72%
		Miércoles	23/09/2020	119019	156604	76%
		Jueves	24/09/2020	118316	155680	76%
		Viernes	25/09/2020	111180	148240	75%
		Sábado	26/09/2020	95908	127878	75%
		Domingo	27/09/2020	76100	101467	75%
		Lunes	28/09/2020	119242	158990	75%
		Martes	29/09/2020	96873	129164	75%
		Miércoles	30/09/2020	109921	146562	75%
TOTAL				2933349	4378133	67%

FICHA DE REGISTRO			
DIMENSIÓN:	Eficacia	**FECHA:**	01/04/2021
INDICADOR:	Porcentaje de transacciones denegadas	**DURACIÓN:**	30 días
INVESTIGADORES:	Pinto Pintos, Katelyn Zarelly Zuñiga Huaraca, Kenny	**AREA:**	TI
EMPRESA:	Alignet S.A.C.	**FORMULA:**	
PROCESO DE OBSERVACION:	Autenticación	$PTD = \frac{Cantidad\ de\ transacciones\ denegadas}{Total\ de\ transacciones} x\ 100$	
TIPO:	Post-Test		
	FECHA 2021		**Promedio**

N°	MES	DIA	FECHA	Transacciones denegadas	Total de transacciones	
1	ABRIL	Jueves	01/04/2021	18144	123250	15%
		Viernes	02/04/2021	25361	169078	15%
		Sábado	03/04/2021	17334	115566	15%
		Domingo	04/04/2021	23298	155325	15%
		Lunes	05/04/2021	26740	178273	15%
		Martes	06/04/2021	18480	123955	15%
		Miércoles	07/04/2021	36242	213192	17%
		Jueves	08/04/2021	23508	146928	16%
		Viernes	09/04/2021	18860	117880	16%
		Sábado	10/04/2021	24184	219858	11%
		Domingo	11/04/2021	21322	195422	11%
		Lunes	12/04/2021	22774	202021	11%
		Martes	13/04/2021	22384	186541	12%
		Miércoles	14/04/2021	26863	223861	12%
		Jueves	15/04/2021	21973	190874	12%
		Viernes	16/04/2021	24032	200267	12%
		Sábado	17/04/2021	16496	126897	13%
		Domingo	18/04/2021	24067	185136	13%
		Lunes	19/04/2021	20525	157888	13%
		Martes	20/04/2021	19742	141561	14%
		Miércoles	21/04/2021	26995	192824	14%
		Jueves	22/04/2021	19507	137887	14%
		Viernes	23/04/2021	12036	120363	10%
		Sábado	24/04/2021	12590	125907	10%
		Domingo	25/04/2021	13347	133471	10%

		Lunes	26/04/2021	19626	189484	10%
		Martes	27/04/2021	10656	118403	9%
		Miércoles	28/04/2021	15022	166918	9%
		Jueves	29/04/2021	14533	161482	9%
		Viernes	30/04/2021	10703	152914	7%
TOTAL				589434	4873426	14%

FICHA DE REGISTRO						
DIMENSIÓN:				Eficacia	**FECHA:**	01/04/2021
INDICADOR:				Porcentaje de transacciones autorizadas	**DURACIÓN:**	30 días
INVESTIGADORES:				Pinto Pintos, Katelyn Zarelly Zuñiga Huaraca, Kenny	**AREA:**	TI
EMPRESA:				Alignet S.A.C.	**FORMULA:**	
PROCESO DE OBSERVACION:				Autenticación	$PTA = \frac{Cantidad\ de\ transacciones\ autorizadas}{Total\ de\ transacciones} \times 100$	
TIPO:				Post-Test		
N°	**FECHA 2021**			**Transacciones autorizadas**	**Total de transacciones**	**Promedio**
	MES	**DIA**	**FECHA**			
1	**ABRIL**	Jueves	01/04/2021	86275	123250	70%
		Viernes	02/04/2021	118354	169078	70%
		Sábado	03/04/2021	72806	115566	63%
		Domingo	04/04/2021	97854	155325	63%
		Lunes	05/04/2021	115877	178273	65%
		Martes	06/04/2021	80570	123955	65%
		Miércoles	07/04/2021	138574	213192	65%

		Jueves	08/04/2021	95503	146928	65%
		Viernes	09/04/2021	86103	117880	73%
		Sábado	10/04/2021	160496	219858	73%
		Domingo	11/04/2021	144612	195422	74%
		Lunes	12/04/2021	149495	202021	74%
		Martes	13/04/2021	149232	186541	80%
		Miércoles	14/04/2021	179088	223861	80%
		Jueves	15/04/2021	156516	190874	82%
		Viernes	16/04/2021	164218	200267	82%
		Sábado	17/04/2021	102786	126897	81%
		Domingo	18/04/2021	149960	185136	81%
		Lunes	19/04/2021	127889	157888	81%
		Martes	20/04/2021	114664	141561	81%
		Miércoles	21/04/2021	160043	192824	83%
		Jueves	22/04/2021	114846	137887	83%
		Viernes	23/04/2021	93883	120363	78%
		Sábado	24/04/2021	98207	125907	78%
		Domingo	25/04/2021	112115	133471	84%
		Lunes	26/04/2021	159166	189484	84%
		Martes	27/04/2021	99458	118403	84%
		Miércoles	28/04/2021	140211	166918	84%
		Jueves	29/04/2021	137259	161482	85%
		Viernes	30/04/2021	129976	152914	85%
TOTAL				3391257	4873426	73%

Anexo 5: Carta de aceptación

CARTA DE ACEPTACION

"SISTEMA DE GESTIÓN DE DATOS EN EL PROCESO DE AUTENTICACIÓN PARA EMISORES EN LA EMPRESA ALIGNET S.A.C., MIRAFLORES - 2020"

Mediante el presente documento se certifica:

Que Pinto Pintos, Katelyn Zarelly, identificada con DNI: 70100999 estudiante de Escuela de Ingeniería de Sistemas de la Universidad Cesar Vallejo y Zúñiga Huaraca, Kenny Wilfredo, identificada con DNI: 48512213 estudiante de Escuela de Ingeniería de Sistemas de la Universidad Cesar Vallejo, han sido aceptados por nuestra empresa para realizar su proyecto de investigación, dando conformidad que la empresa Alignet brindara toda la información necesaria para la elaboración de la presente investigación "SISTEMA DE GESTIÓN DE DATOS EN EL PROCESO DE AUTENTICACIÓN PARA EMISORES EN LA EMPRESA ALIGNET S.A.C., MIRAFLORES - 2020".

Como condiciones contractuales, los estudiantes esta obligado a no divulgar ni usar para fines personales la información, será usado exclusivamente para el desarrollo de la presente investigación.

Miraflores, 01 de abril de 2021

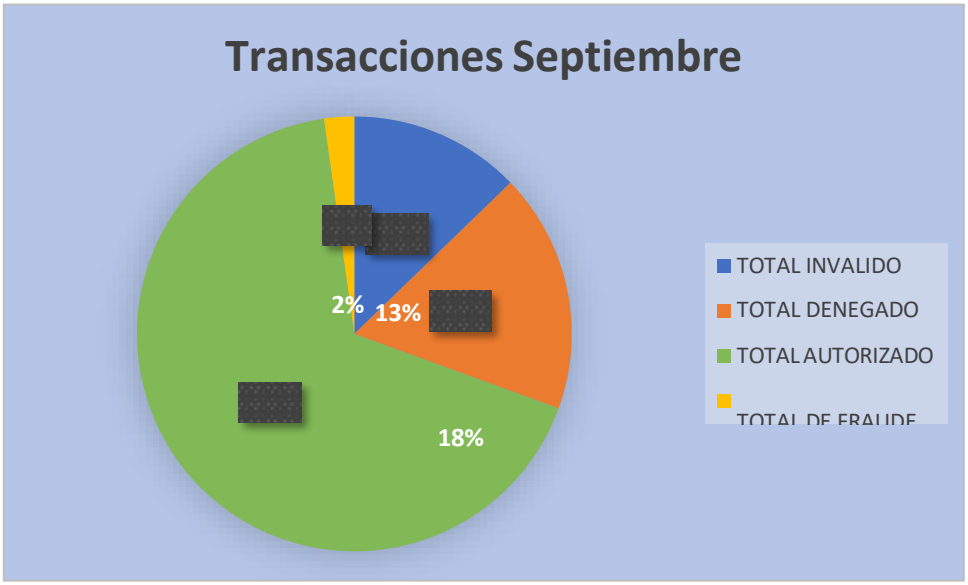
DocuSigned by:
Luis Gamarra
F4A43C4F8AEC424...

LA EMPRESA
GAMARRA ROIG LUIS ERNESTO
GERENTE GENERAL

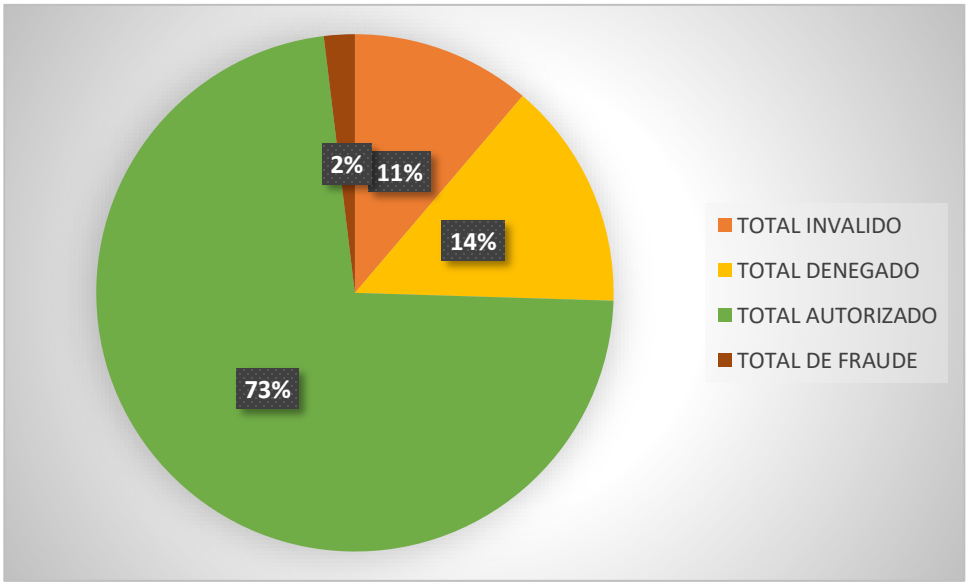
DocuSigned by:
Javier De la Cruz
C493BA1694DB455...

LA EMPRESA
DE LA CRUZ COSTA JAVIER EDUARDO
GERENTE DE ADM. Y FINANZAS

Anexo 6: Gráfica de transacciones del mes de septiembre – Pretest



Anexo 7: Gráfica de transacciones del mes de abril – Postest


2%
11%
14%
73%
TOTAL INVALIDO
TOTAL DENEGADO
TOTAL AUTORIZADO
TOTAL DE FRAUDE

Anexo 8: Marco de trabajo ágil

ENROLAMIENTO MASIVO

RFC 047 - Enrolamiento Masivo SFTP

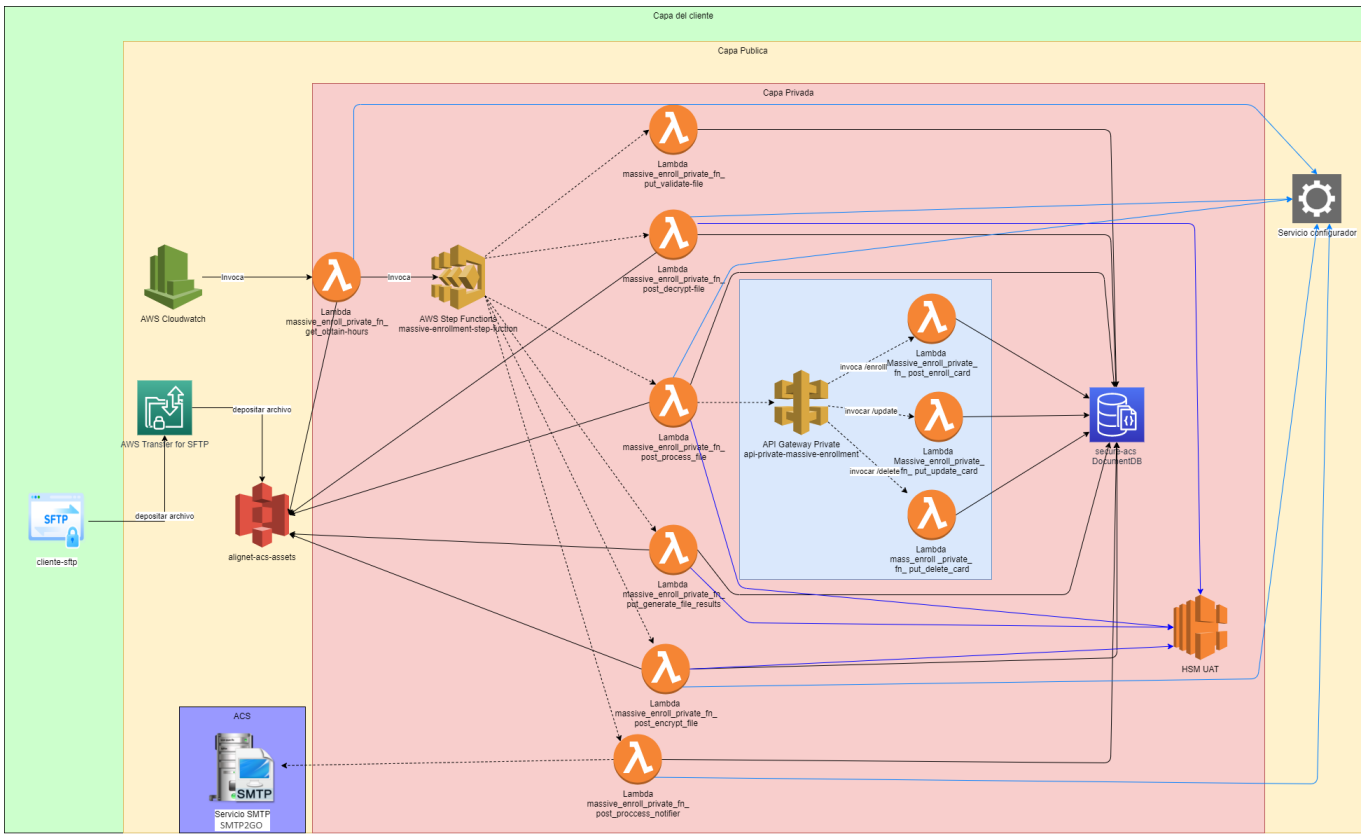
Generalidades del alcance

El aplicativo de Enrolamiento masivo de tarjetas permite enrolar, actualizar y eliminar las tarjetas enviadas por el emisor en un archivo de texto plano depositadas en un directorio de un servidor SFTP creado para el cliente.

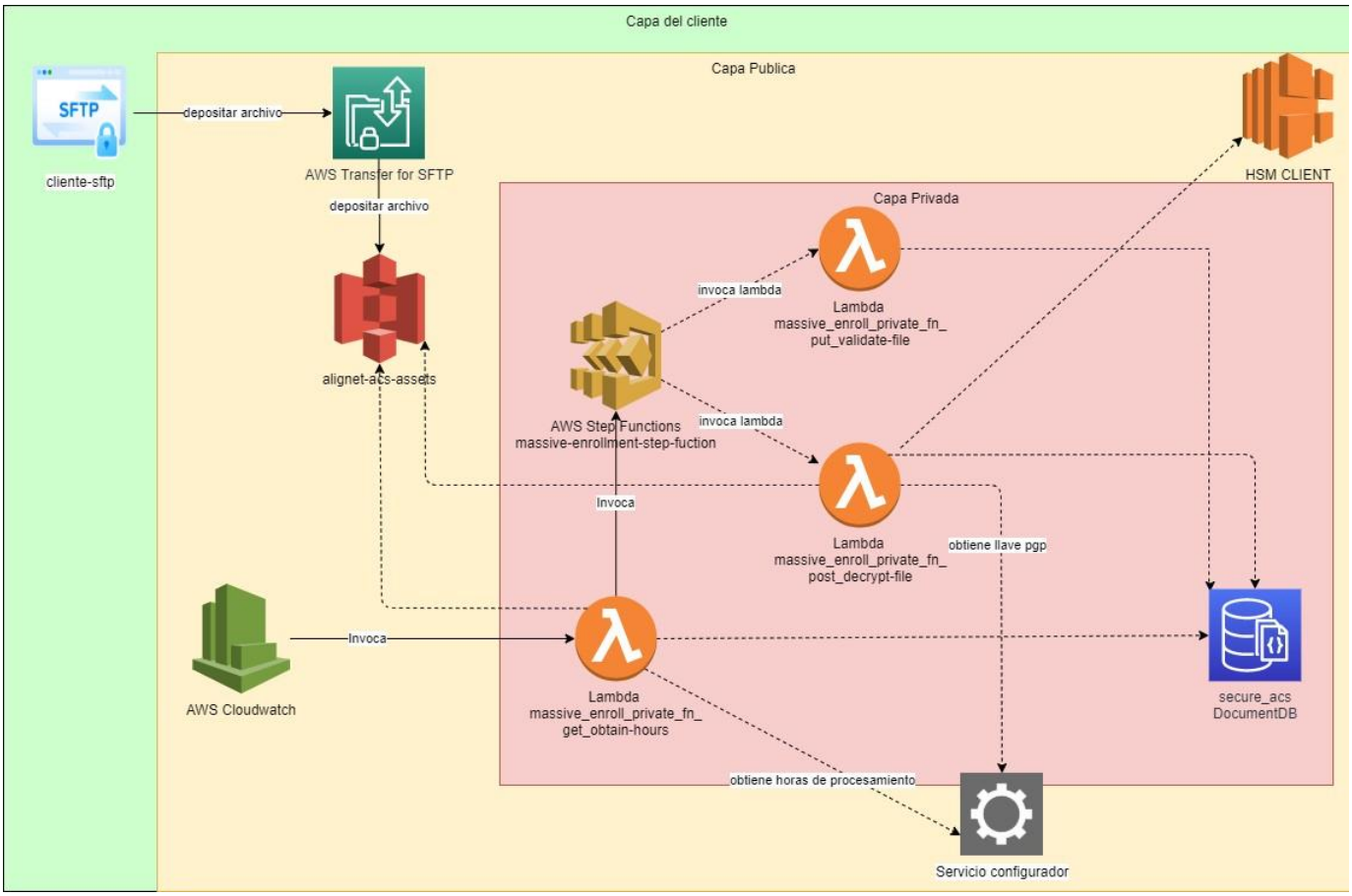
Se procesará el archivo plano, que dará como resultado otro archivo plano con los resultados de los registros procesados y no procesados y el motivo de error cuando aplique. Las marcas con las que puede trabajar los emisores son:

- Visa
- Mastercard
- American Express
- Diners

Arquitectura Enrolamiento Masivo consolidado



RFC 047 - Obtención y validación de archivos



Deposito de archivo:

El emisor dejara un archivo plano cifrado con llave PGP en su carpeta IN para procesarlo. Para este deposito, el emisor deberá emplear un cliente SFTP donde deberá usar las credenciales generadas para el emisor y conectarse al servicio AWS Transfer for SFTP el cual internamente redirigirá el archivo al servicio S3 alignet-acs-assets.

Obtención de archivo:

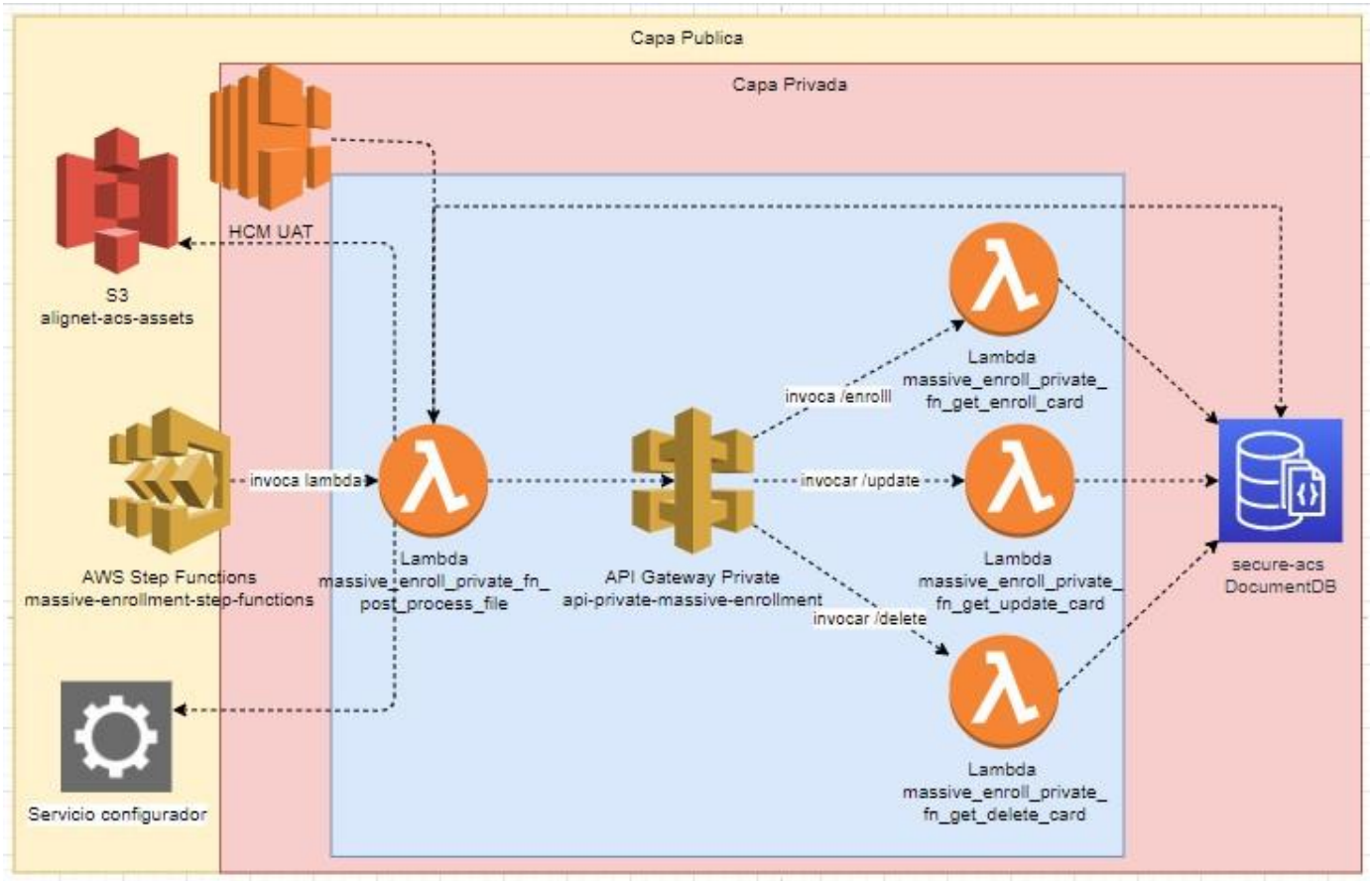
Se usara el cloudwatch para levantar el Lambda massive_enroll_private_fn_get_obtain-hours que se comunicara con el servicio configurador para obtener las horas de procesamiento de cada emisor y la base de datos ACS. Estas horas de invocación son configuradas en base de datos que son comparadas con la hora actual en AWS CloudWatch. Cuando obtenga un archivo el procederá a guardar el nombre del archivo en la base de datos Secure-acs.

Validación de archivo:

El AWS step Functions invocara al Lambda massive_enroll_private_fn_put_validate-file se comunicara con la base de datos Secure-acs para validar el nombre del archivo y la encriptacion del archivo, por ultimo el AWS step Functions invocara al

Lambda massive_enroll_private_fn_post_decrypt-file el cual obtendrá la llave pgp del servicio configurador y hsm para desencriptar el archivo.

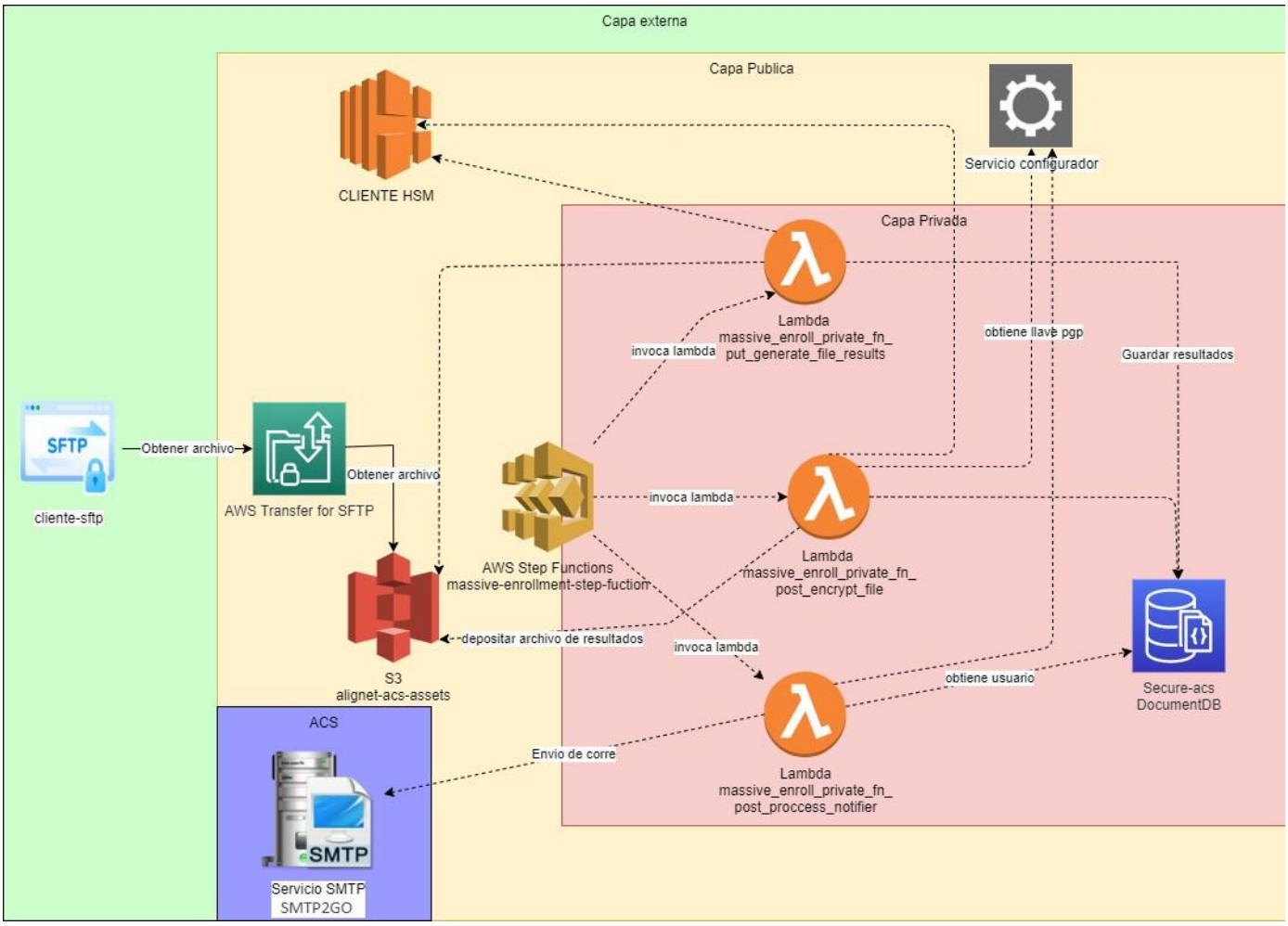
RFC 047 - Procesamiento de archivos



Procesamiento de archivo:

El AWS Step Functions invocara al Lambda process-file que dará lectura del archivo, el cual debera ser obtenido desde el S3 alignet-acs-assets. Dependiendo del tipo de proceso a realizar (Enrolamiento, Actualizacion o Eliminacion), sera invocado el API api-private-massive-enrollment que enviara la tarjeta a procesar al Lambda enroll-card que lo ejecutara y guardara en la base de datos; si fuera una actualización lo enviara al Lambda update-card y por ultimo si fuera una eliminación lo enviaría al Lambda delete-card, luego de ejecutarse cada lambda se guardara en la base de datos de cardaccount.

RFC 047 - Generación de resultados



Generación de resultados: AWS step functions Massive-enrollment-step-function-Logs invoca el Lambda generate-file-results que generara un archivo de resultados y un archivo de log, se guardara en la base de datos de ACS coleccion file, siguiente se invoca el Lambda encrypt-file que obtendrá las llave pgp del servicio configurador para encriptar el archivo y se comunica con el HSM Client luego guardara los archivos de resultados encriptado y log en S3 alignet-acs-assets para que se guarde en la carpeta del cliente-sftp.

Notificación de resultados:El Lambda process-notifier consultara a la base de datos ACS para obtener los usuario a los cuales se les notificara (los textos son configurables en base de datos) con el servicio smtp via correo electronico de que ya se proceso el archivo o cual es el error del procesamiento. tambien procedera a eliminar el archivo enviado en la carpeta IN

Listado de Mensajes de Error

Código	Mensaje	Versión del ACS	Etapa - Proceso
000	Procesado correctamente	1.0	Enrolamiento
001	No posee los parámetros requeridos, debe ser [Total campos requeridos]	1.0	Enrolamiento
002	No posee una tarjeta valida (nulo o vacío).	1.0	Enrolamiento
003	No posee una tarjeta válida para la marca enviada.	1.0	Enrolamiento
004	No posee una tarjeta válida para el emisor, no hay registros del Bin.	1.0	Enrolamiento
005	La tarjeta 445566 *** *** 0001 está afiliada.	1.0	Enrolamiento
006	La tarjeta 445566 *** *** 0001 está bloqueada.	1.0	Enrolamiento
007	La tarjeta 445566 *** *** 0001 esta eliminada.	1.0	Enrolamiento
008	La tarjeta 445566 *** *** 0001 no se pudo procesar, no se guardó la información.	1.0	Enrolamiento
009	El valor de la tarjeta enviado si es numérico, pero no cumple con la longitud.	1.0	Enrolamiento
012	El valor del celular enviado si es numérico, pero no cumple con la longitud	1.0	Enrolamiento
013	No posee celular valido (no es numérica).	1.0	Enrolamiento
014	El valor del celular es nulo o vacío.	1.0	Enrolamiento
015	El email no cumple con la longitud.	1.0	Enrolamiento
016	El email no tiene formato válido.	1.0	Enrolamiento
017	El valor del email es nulo o vacío.	1.0	Enrolamiento
018	El valor del prefijo celular enviado si es numérico, pero no cumple con la longitud.	1.0	Enrolamiento
019	No posee prefijo valido (no es numérica).	1.0	Enrolamiento
020	El valor del prefijo es nulo o vacío.	1.0	Enrolamiento
025	No se encuentra la tarjeta 445566 *** *** 0001 en los registros de base de datos.	1.0	Enrolamiento
027	La tarjeta no se pudo procesar, no se eliminó la información.	1.0	Enrolamiento
028	La tarjeta 445566 *** *** 0001 ya se encuentra eliminada.	1.0	Enrolamiento
029	La tarjeta no se encuentra registrada.	1.0	Enrolamiento
030	El Bin de la tarjeta no está configurado para el emisor.	1.0	Enrolamiento
031	El formato de la tarjeta es inválido.	1.0	Enrolamiento
032	El emisor tiene habilitado la opción de realizar operaciones con la marca enviada	1.0	Enrolamiento
033	El emisor no tiene habilitado en la marca el método de	1.0	Enrolamiento

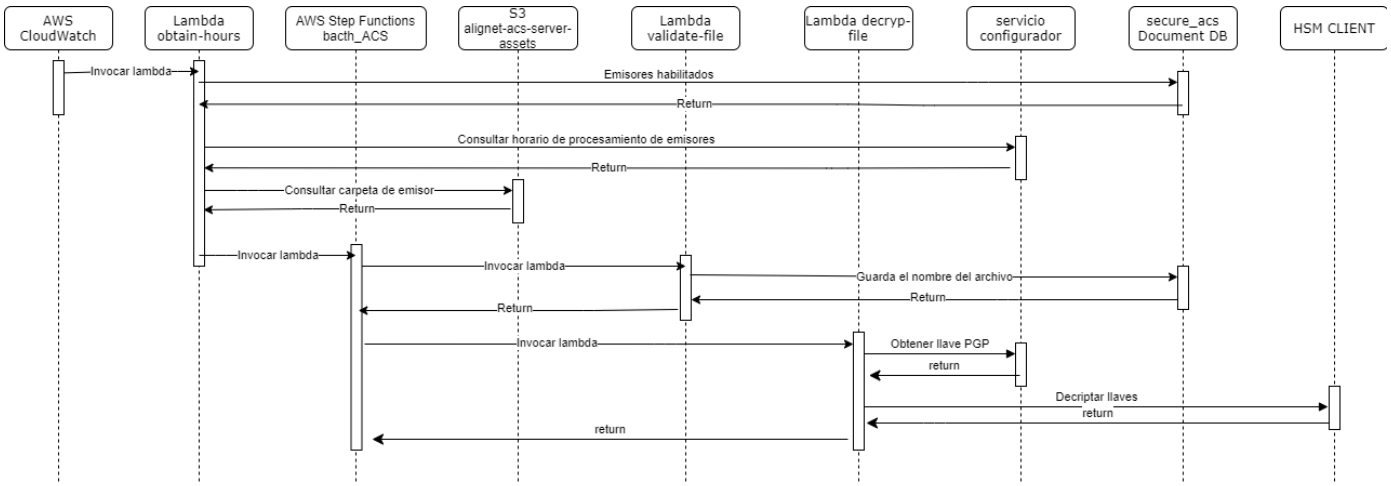
	autenticación enviado		
034	Tipo de Operación no válido	1.0	Enrolamiento
035	Valor de Marca no permitido	1.0	Enrolamiento
099	No procesado	1.0	Enrolamiento

RFC 047 - Diagramas - Flujo

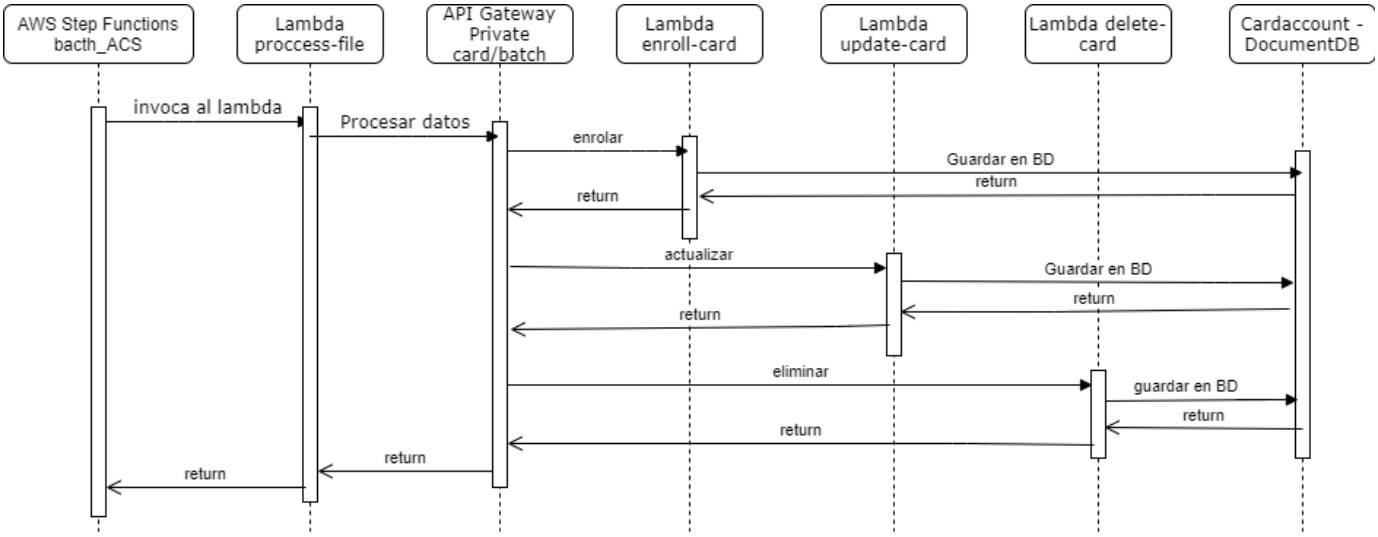
A continuación se detallan los diagramas de flujo del proceso de enrolamiento masivo. Se ha separado en tres procesos que se realizan de manera secuencial donde se tiene como punto de partida la invocación que realiza el AWS CloudWatch al AWS Step Functions para el inicio del flujo de trabajo. Se estará contemplando timeouts adecuados para las invocaciones sincronías a los servicios. Adicional-mente, se considerara la utilización de calentadores para los servicios Lambda.

Obtención y validación de archivo

En el diagrama de flujo siguiente se describe la secuencia del archivo depositado por el emisor por los componentes del servicio. Este proceso es iniciado por el AWS CloudWatch, en base a horas definidas para la invocación del AWS Step Functions.



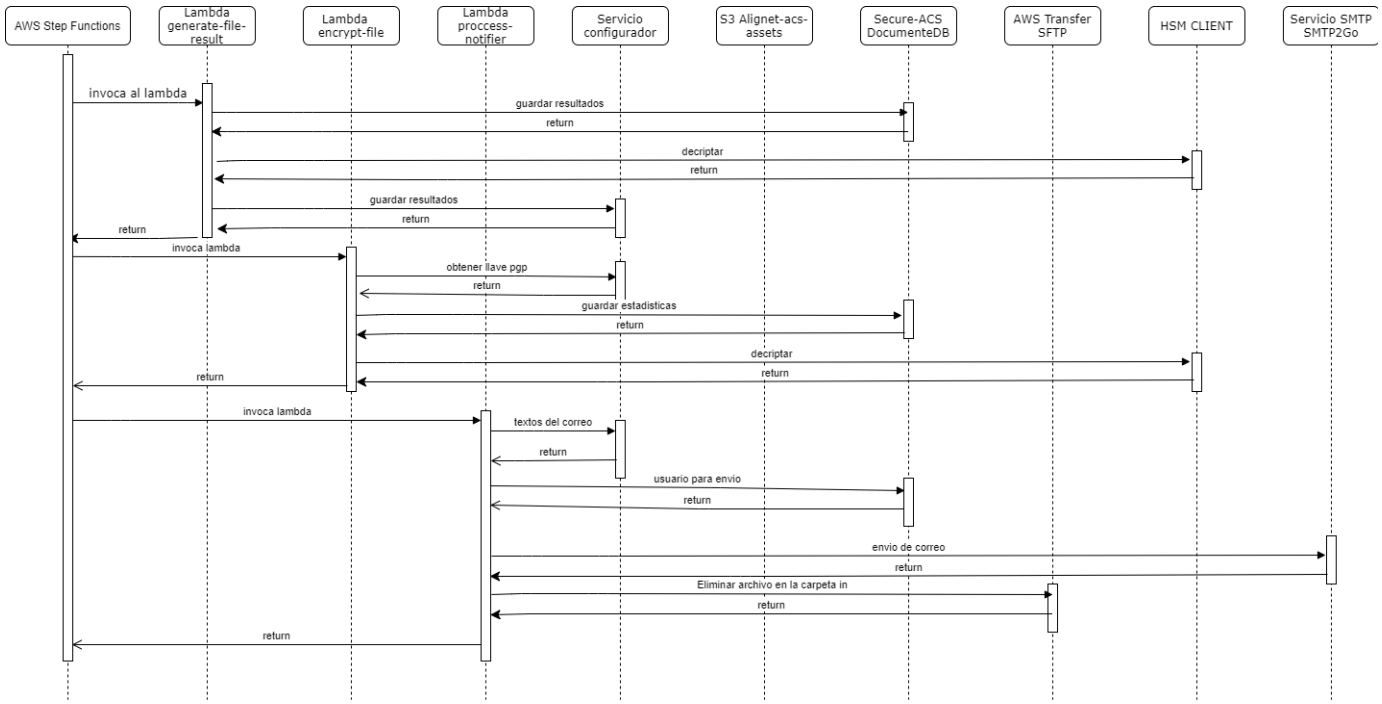
Procesamiento de archivo



En el diagrama de flujo siguiente se describe la secuencia del archivo luego de ser validado, el archivo sera procesado por los componentes.

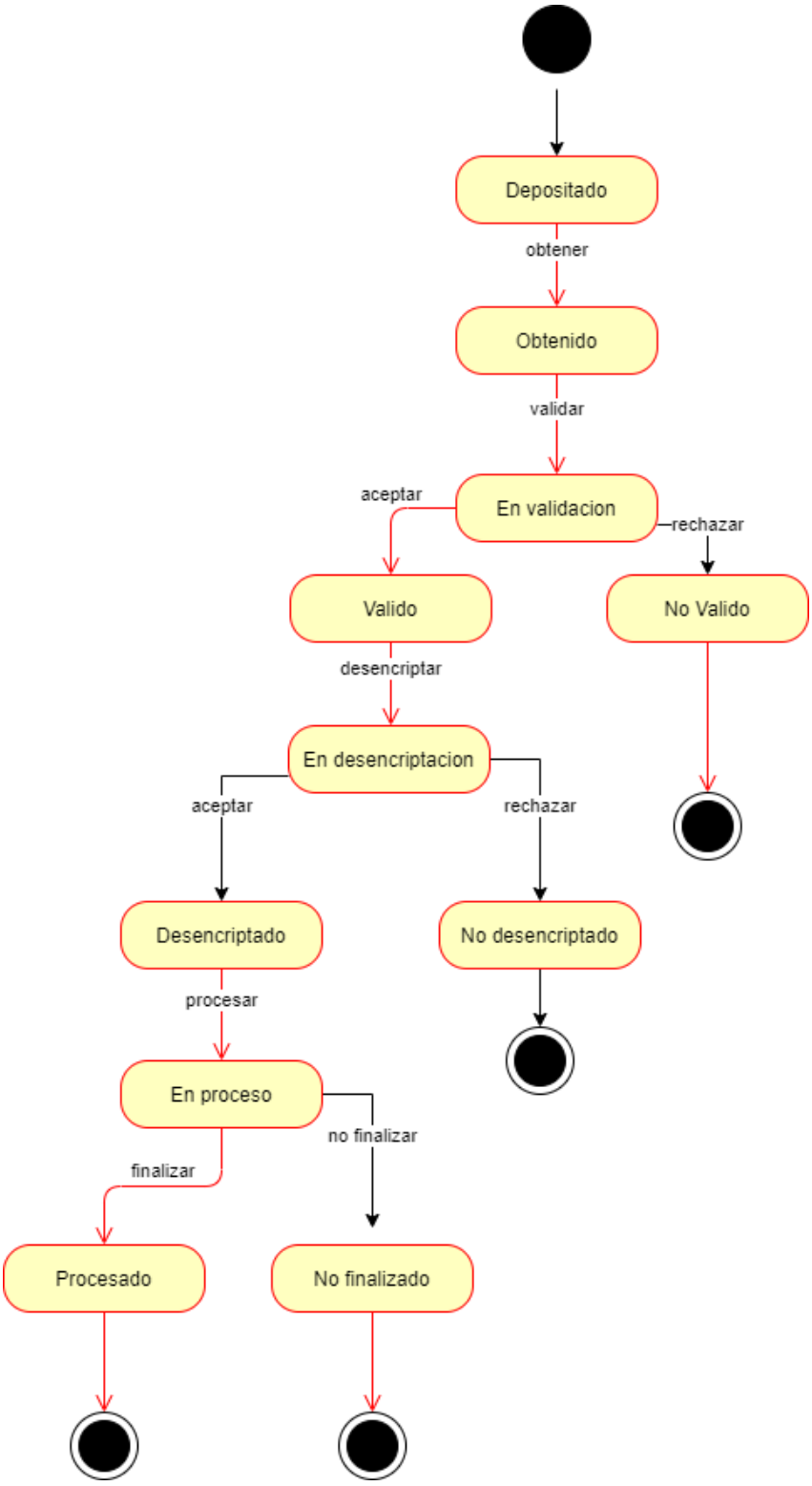
Generación de resultado

En el diagrama de flujo siguiente se describe la secuencia de la generacion de los archivos de resultado y log, el archivo sera procesado por los componentes y depositar lo en la carpeta del cliente sftp.

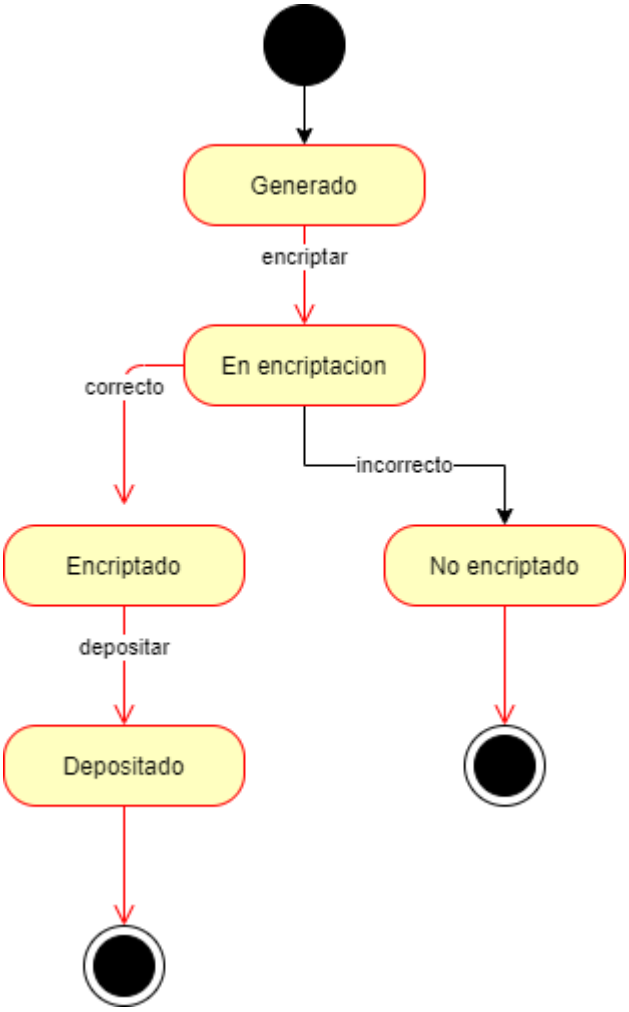


RFC 047 - Diagramas - Estado

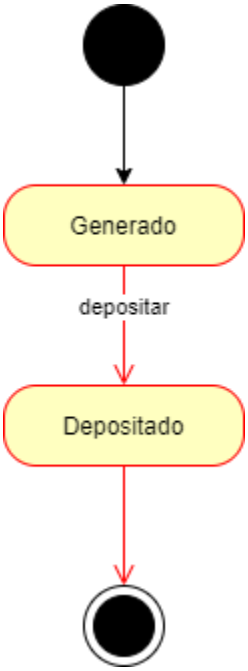
Archivo de entrada



Archivo de resultado

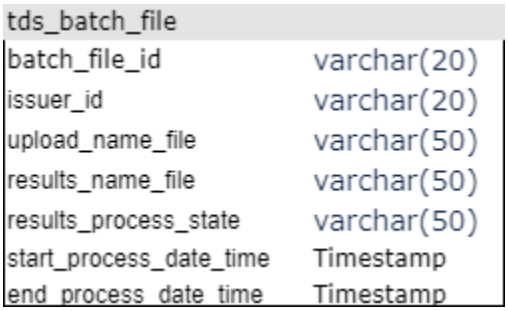


Archivo de log



RFC 047 - Modelo de datos

La base de datos de la Carga Masiva estará conformada por data maestra y/o de configuraciones para las entidades como emisores.



COLECCIONES

tds_batch_file

Column name	Type	Description
batch_file_id	varchar(20)	Identificador del registro
issuer_id	varchar(20)	Identificador del emisor
upload_name_file	varchar(50)	Nombre de archivo subido
results_name_file	varchar(50)	Nombre de archivo de resultados
results_process_state	varchar(50)	Estado del proceso del archivo de resultados
start_process_date_time	Timestamp	Fecha y tiempo en que se inicio el proceso de carga masiva
end_process_date_time	Timestamp	Fecha y tiempo en que finalizo el proceso de carga masiva

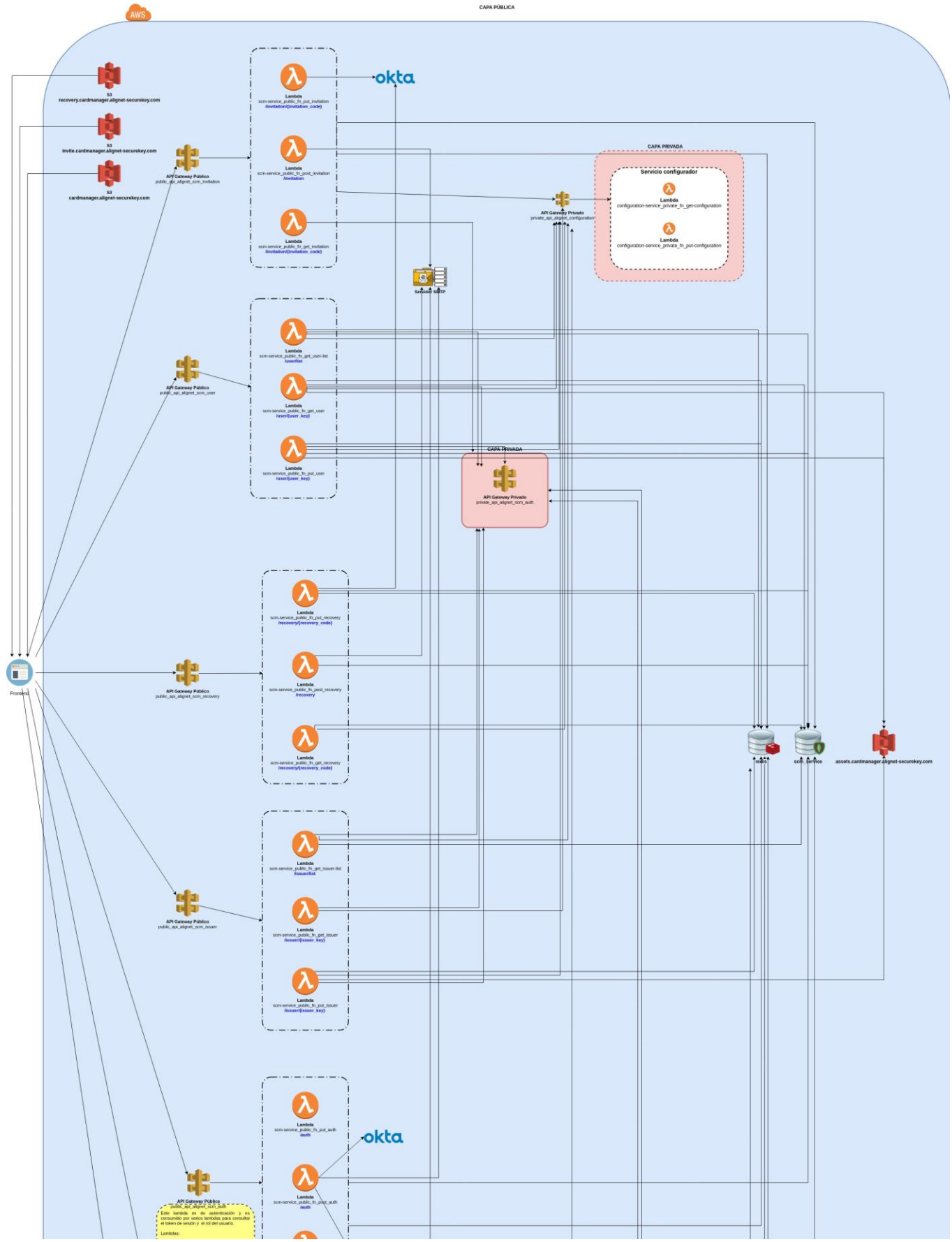
RFC 063- Reglas de contraseña(add y update)

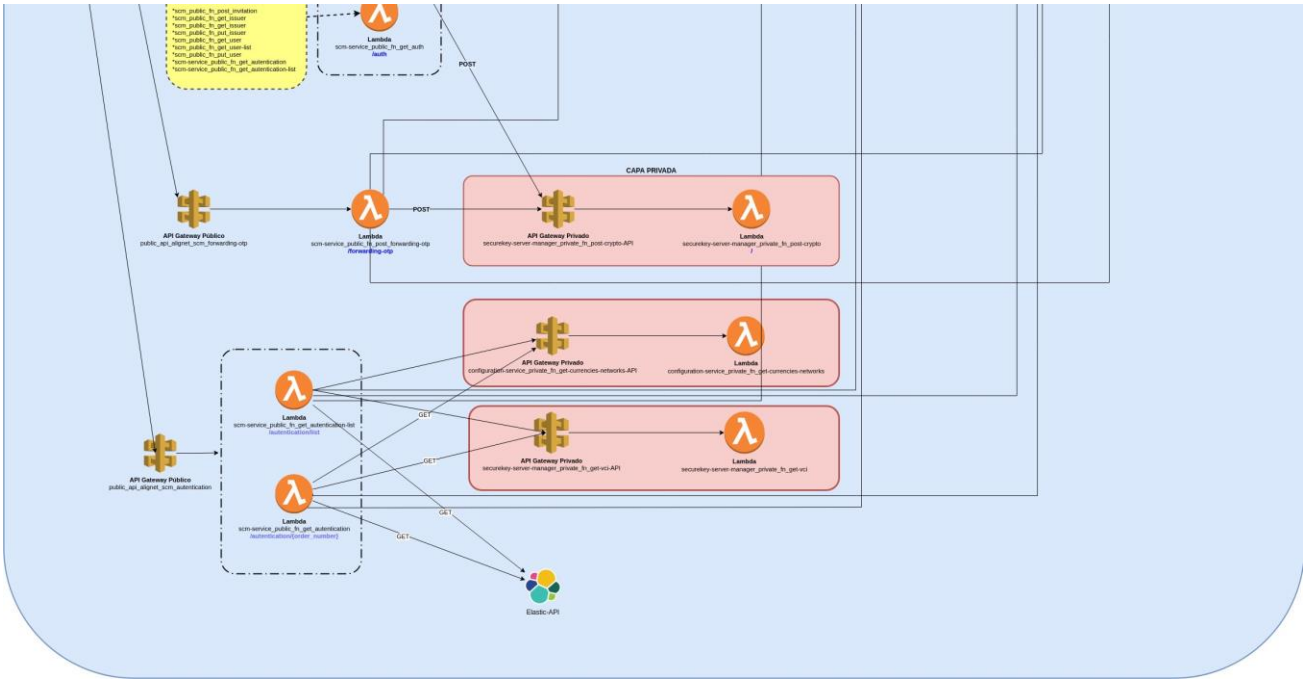
En este RFC se explicara las formas que se optaron para cumplir las condiciones de las POLITICAS DE CONTRASEÑAS.

Politicas del Proyecto	Soluciones
Longitud mínima de 8 caracteres	Se valida en el front end (el boton de aceptar se bloquea) y back end (se coloca una condicional el cual si no cumple con la longitud devuelven un error)
Contraseñas complejas con valores alfanuméricos y caracteres especiales.	Se valida en el front end (se valida lo que se coloca en la casilla) y en el Okta(servicio que administra el login y password)
Las nuevas contraseñas no puedan ser iguales que las 8 últimas contraseñas utilizadas por el usuario	Se valida desde el Redis, se guardan las claves en el cache y mediante el codigo se valida si se repite o si ya tiene 8 claves, en este caso, se elimina al ultima y se agrega la nueva.
Las contraseñas deben ser modificadas por lo menos cada 90 días.	En el Okta se configuro las reglas de contraseña, se le activo y coloco que cada 90 dias va a expirar la contraseña actual.
Máxima longitud es de 10 caracteres para la contraseña.	Se valida en el front end (el boton de aceptar se bloquea) y back end (se coloca una condicional el cual si no cumple con la longitud devuelven un error)
Autenticar todas las ID de usuario, sistemas y aplicaciones con una contraseña.	se realiza la validacion con la contraseña que se almacena en el okta y en el cache.
Las cuentas de usuario deben ser bloqueadas después de más de 3 intentos de ingreso inválidos.	Se realiza el bloqueo de la cuenta al tercer intento.
Requerir que una vez que una cuenta de usuario se bloquee siga bloqueada hasta que el Administrador de Sistemas restablezca la cuenta	Al tercer inteto la cuenta se bloquea por completo, la unica forma de desbloquear es eliminando la cuenta del registro de reitentos.
Requerir que el tiempo ocioso para cerrar el sistema/sesión sea máximo 15 minutos.	
Eliminar o desactivar a los usuarios inactivos por lo menos cada 90 días.	

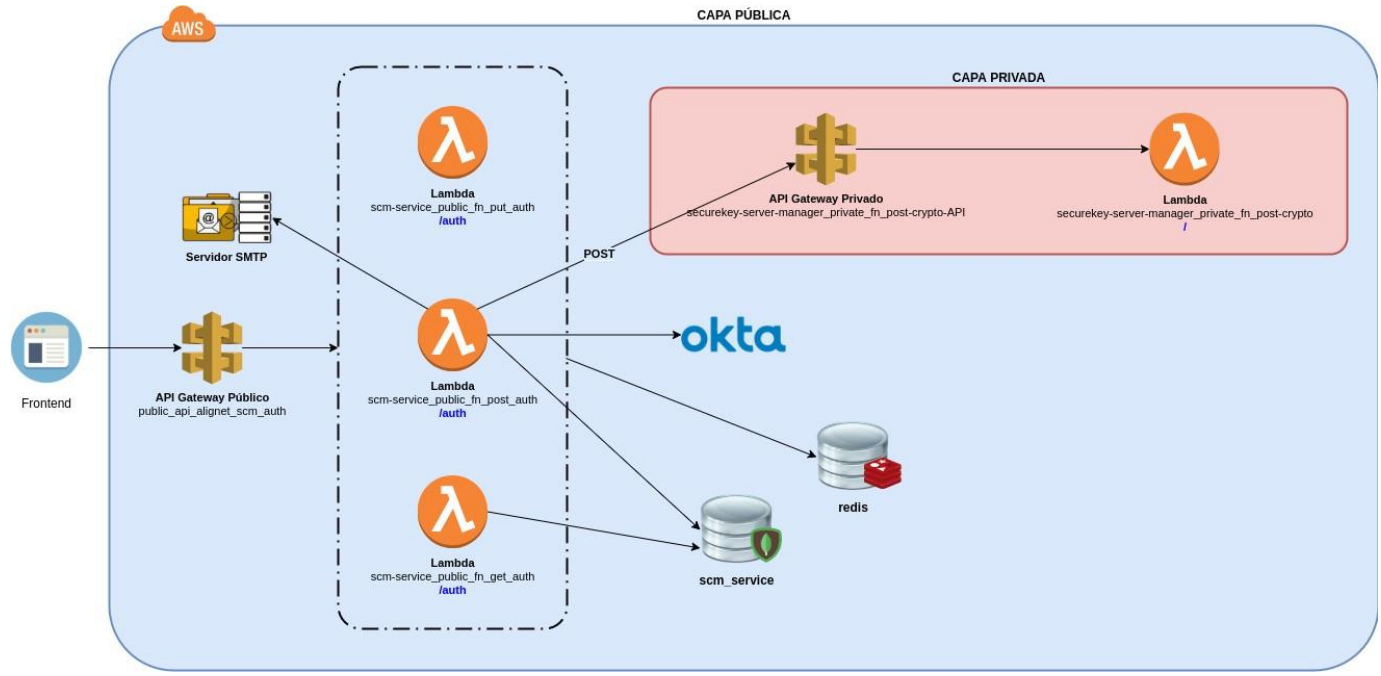
SISTEMA WEB SECUREKEY CARD MANAGER

RFC 063 - Diagrama general de arquitectura





RFC 063 - Login

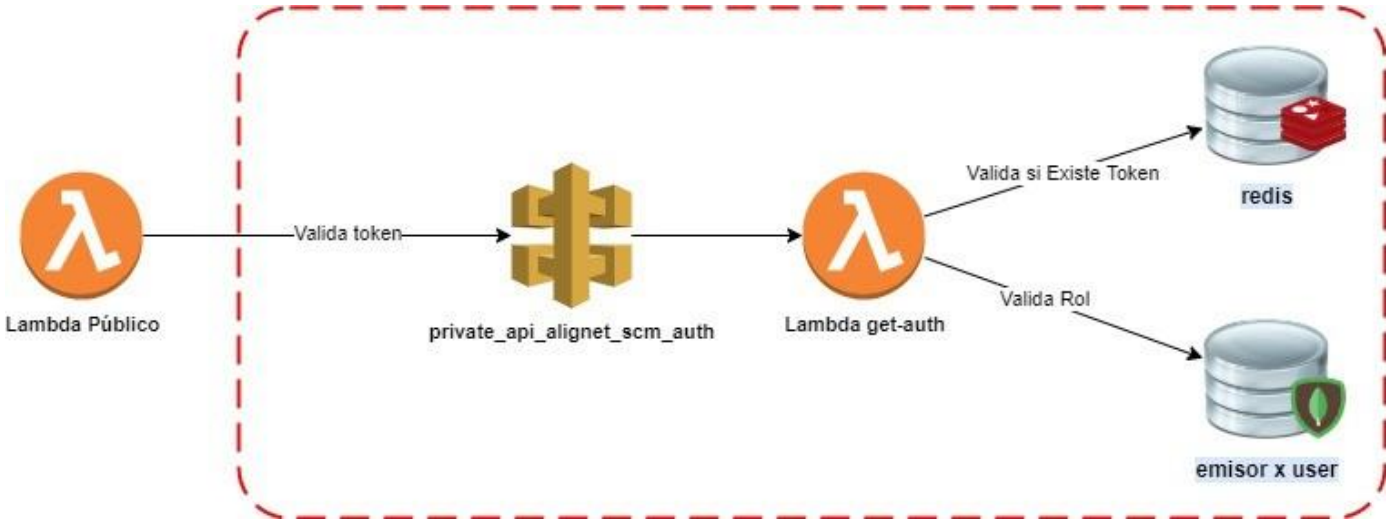


Observación:

Se reutilizará componente perteneciente al proyecto SecureKey Server Manager.

El nombre del componente es Crypto y su función es generar un código de 6 dígitos para luego ser usado como código OTP.

RFC 063 - Validación de Sesión



*OKTA API: Servicio de autenticación https://developer.okta.com/

**Se considera soporte para mas de un proveedor de autenticación

Para los servicios del SAC se requiere incluir un token de Autenticación en los Headers de las consultas. Este token se usa para validar el acceso, roles y permisos antes de continuar con la consulta

Validación de Token

Se consume el lambda “get - auth” que es el encargado de validar el token

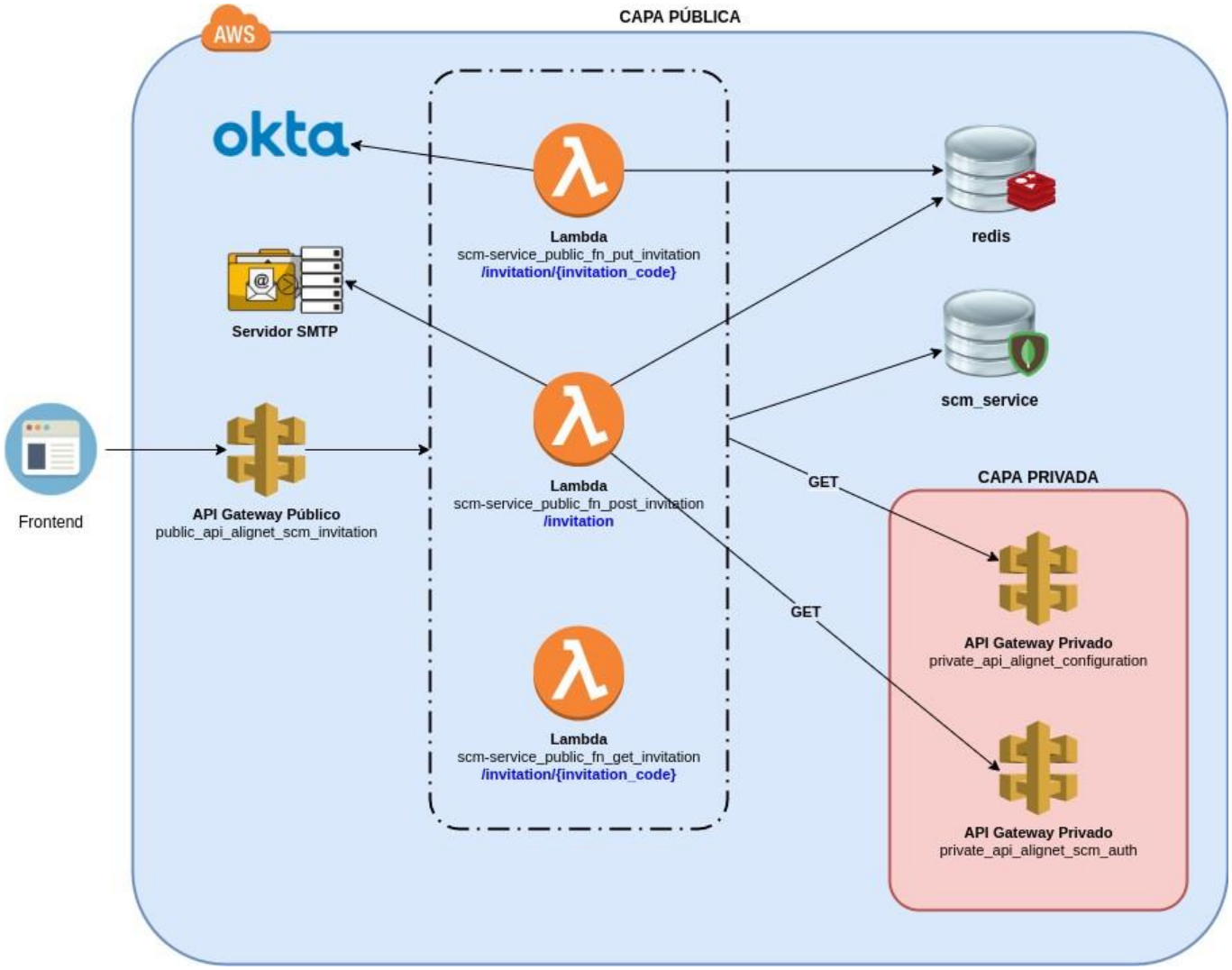
Primero el token se valida con los registros de sesiones para verificar si

Cumple con la doble autenticación

No ha expirado

Se valida el token con el servicio de OKTA para verificar que el token sigue siendo válido

RFC 063 - Invitación

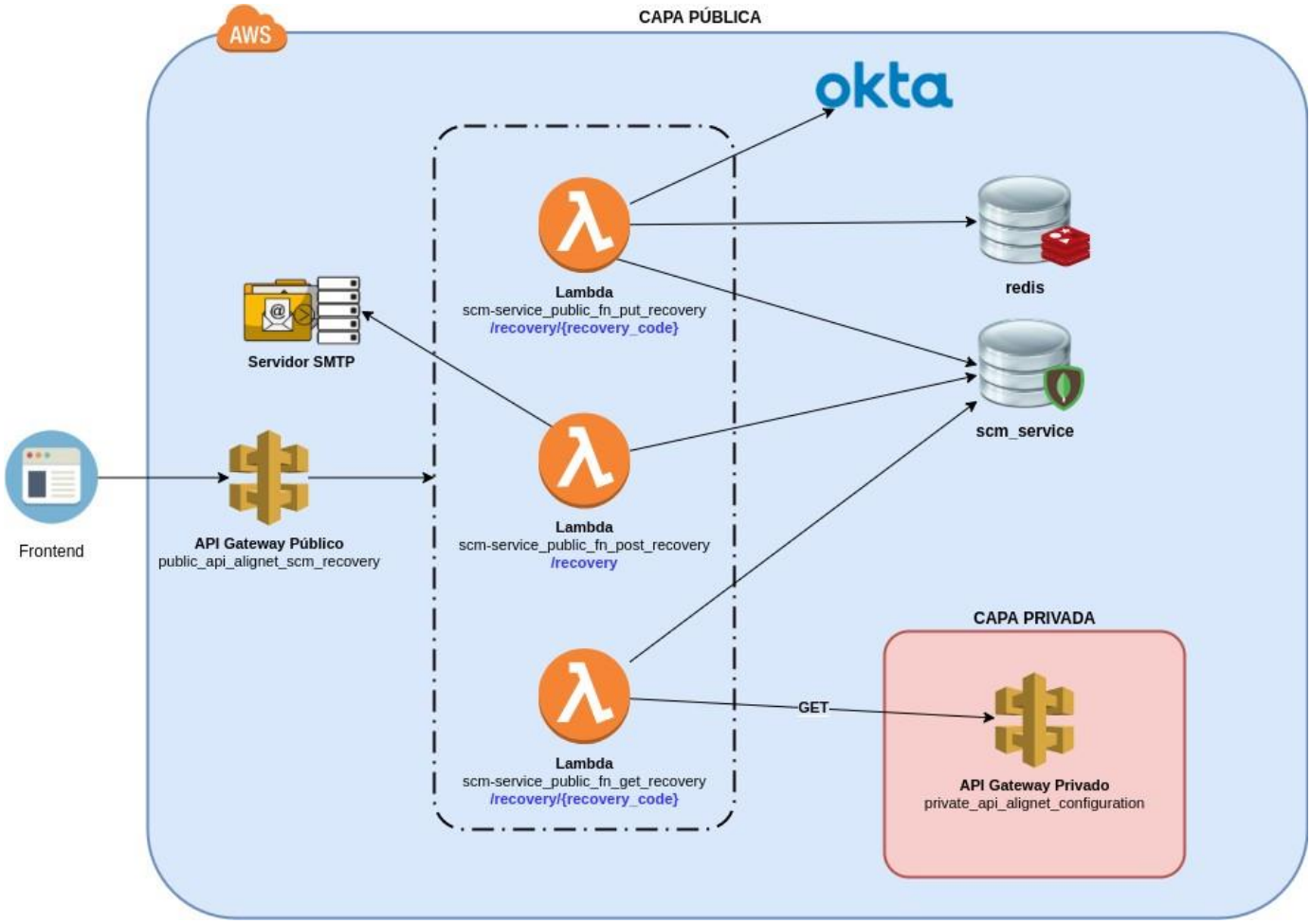


Observación:

Por temas de comunicación entre los componentes del Servicio Configurador y SecureKey Card Manager (Servicio de Login) se vió la necesidad de crear un API Gateway Privado para el Servicio de Login. El nombre del API Gateway Privado es private_api_alignet_scm_auth.

Existen ambos API Gateway, el público (public_api_alignet_scm_auth) para la comunicación con la parte Front y el privado (private_api_alignet_scm_auth) para la comunicación con los componentes internos de la capa privada.

RFC 063 - Recuperación de contraseña



*OKTA API: Servicio de autenticación https://developer.okta.com/

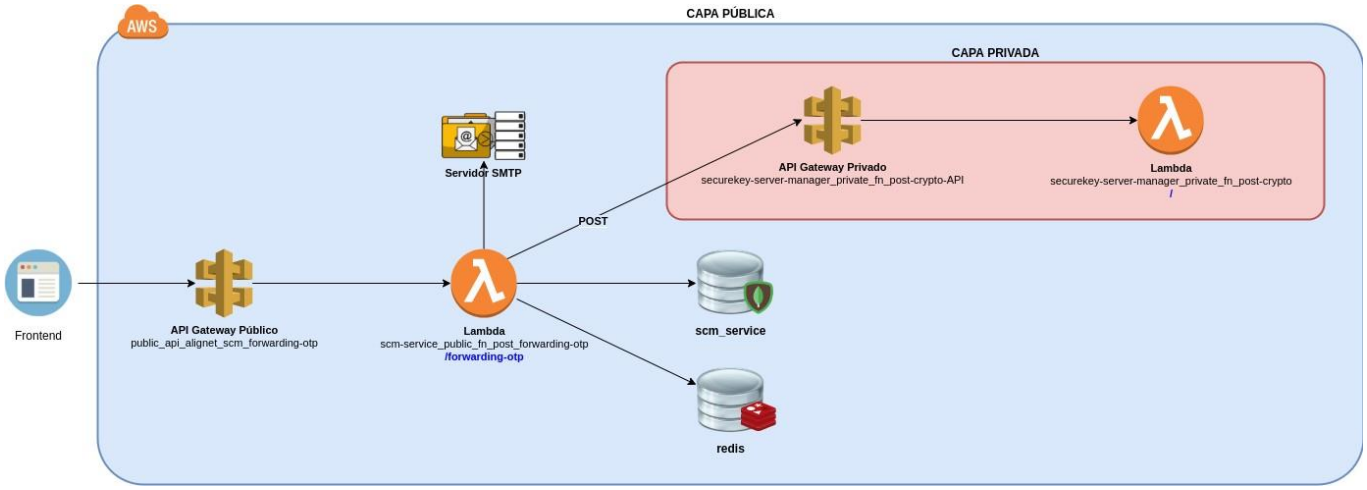
**Se considera soporte para mas de un proveedor de autenticación

Recuperar Contraseña - /recovery

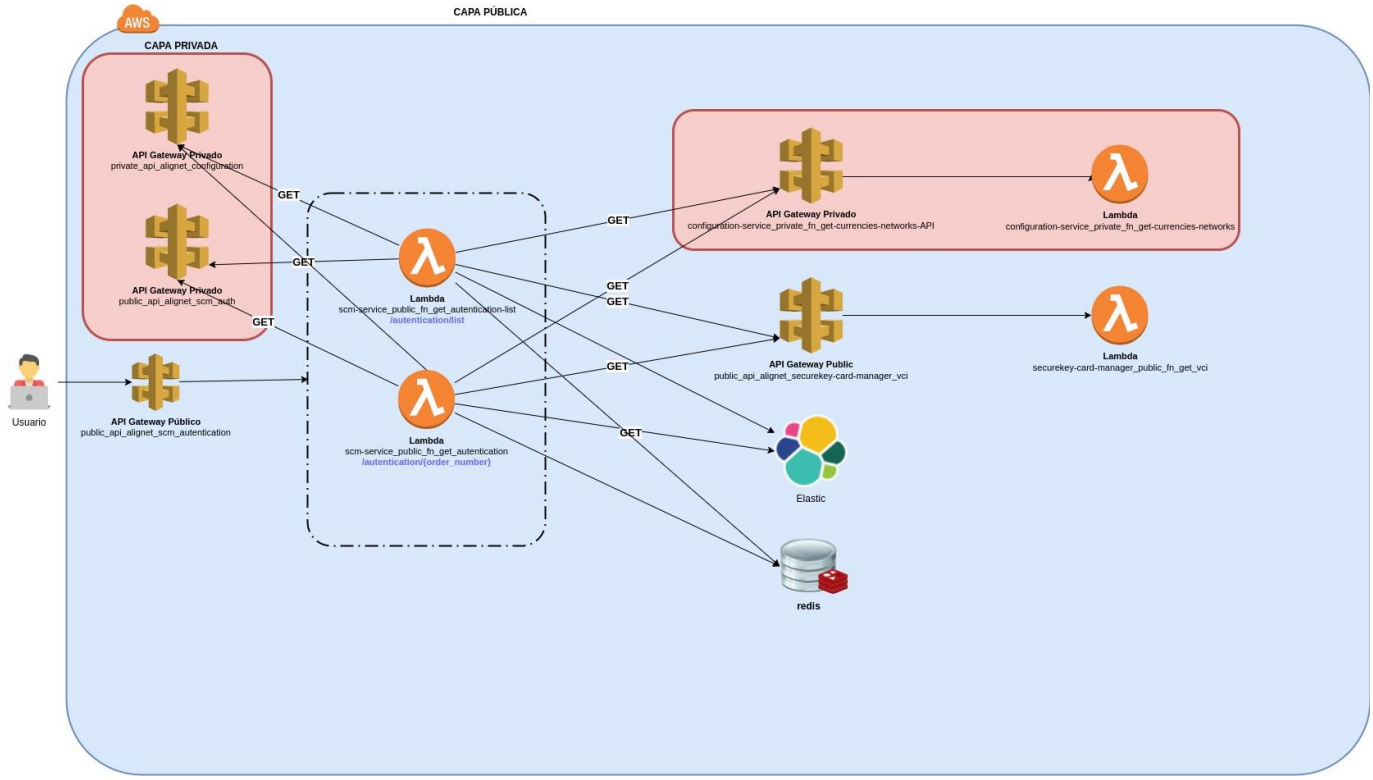
El usuario solicita la recuperación de contraseña indicando su correo, el lambda “post - recovery” se encarga de generar la solicitud de recuperación a través del API de OKTA

OKTA gestiona el flujo de recuperación de contraseña: Envío de correo de recuperación y actualización de contraseña

RFC 063 - Reenvío de código OTP

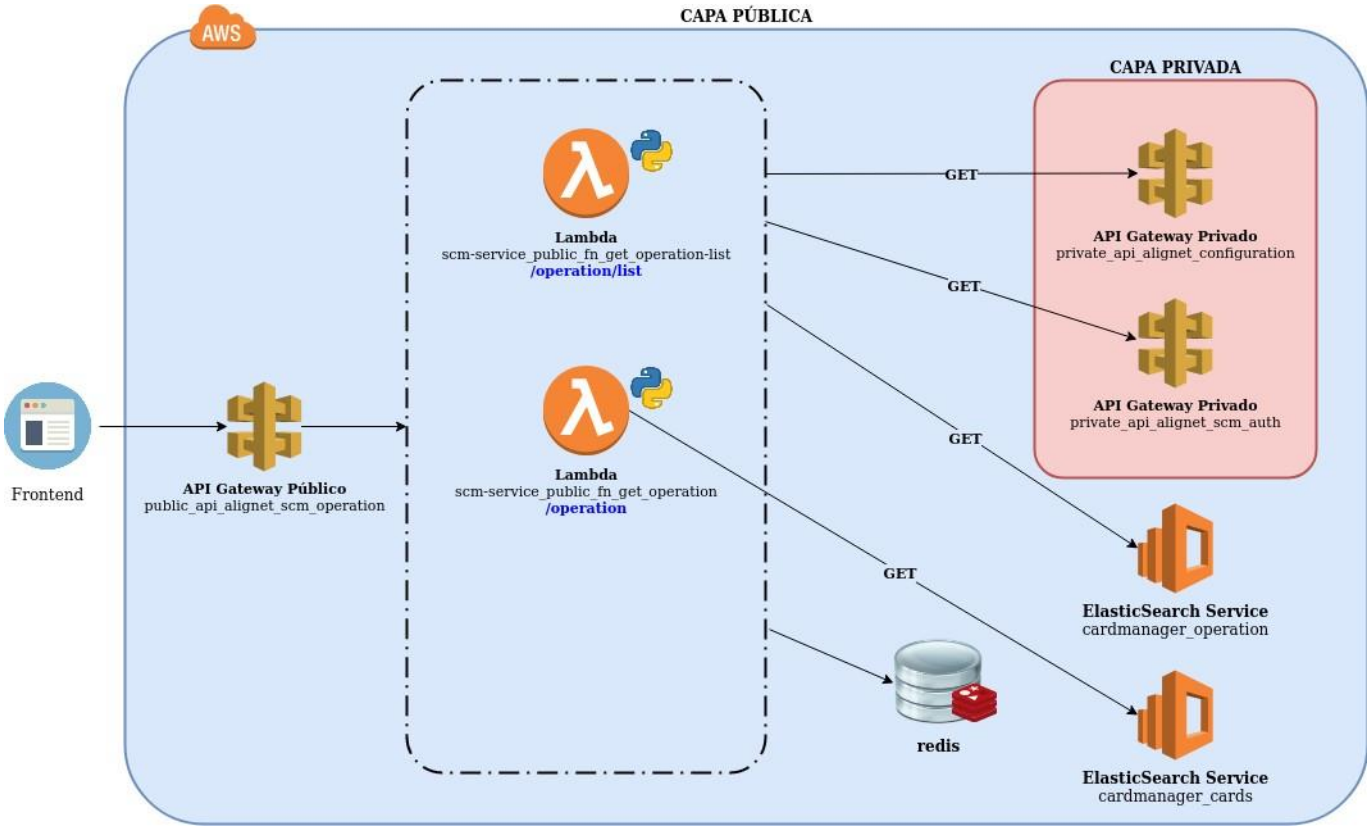


RFC 063 - Autenticaciones



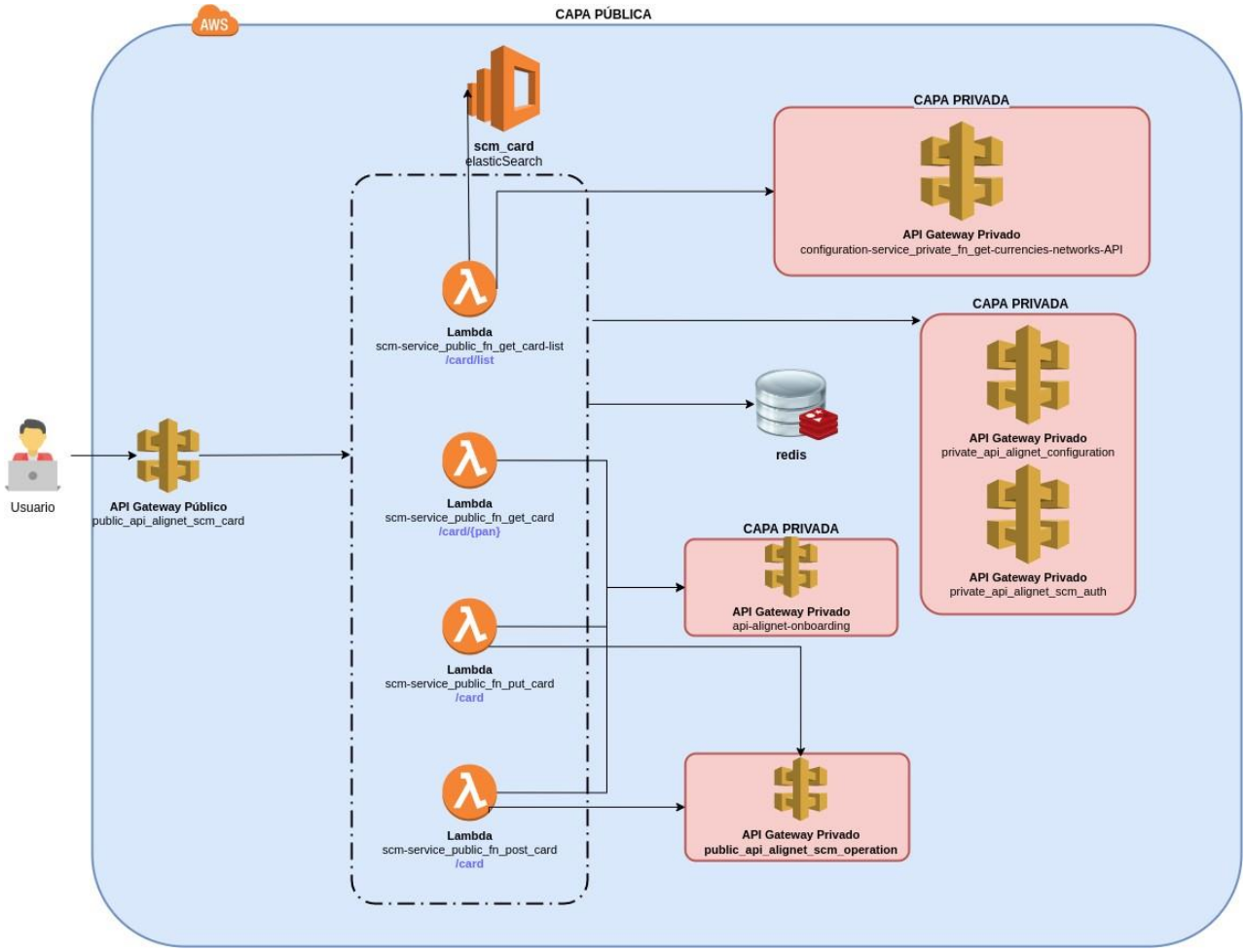
Componente	Tipo	Protocolo	Url	Descripción
public_api_alignet_scm_autentication	API GATEWAY	REST API	/autentication	Recurso en api gateway con protocolo rest.
scm-service_public_fn_get_autentication	LAMBDA	REST - GET	/autentication	Lambda encargado de mostrar los detalles correspondientes a una autenticación.
scm-service_public_fn_get_autentication-list	LAMBDA	REST - GET	/autentication /list	Lambda encargado de mostrar los datos correspondientes mediante un filtro específico de una lista de autenticaciones.
configuration-service_private_fn_get-currencies-networks	LAMBDA	REST - GET	/currencies	Lambda usado para obtener los datos con referente al tipo de moneda.
securekey-server-manager_public_fn_get- vci	LAMDA	REST - GET	/vci	Lambda usado para obtener el resultado de autemticación.

RFC 063 - Operaciones



Componente	Tipo	Protocolo	Url	Descripción
public_api_alignet_scm_operation	API GATEWAY	REST API	/operation	Recurso en api gateway con protocolo rest
scm-service_public_fn_get_operation-list	LAMBDA	REST - GET	/operation/list	Lambda encargado de mostrar los datos correspondientes mediante un filtro específico de una lista de operaciones
scm-service_public_fn_get_operation	LAMBDA	REST - GET	/operation	Lambda encargado de mostrar los datos correspondientes a una operación
scm-service_public_fn_get_export	LAMBDA	REST - GET	/operation /export	Lambda común encargado de realizar la exportación de archivos csv

RFC 063- Tarjetas

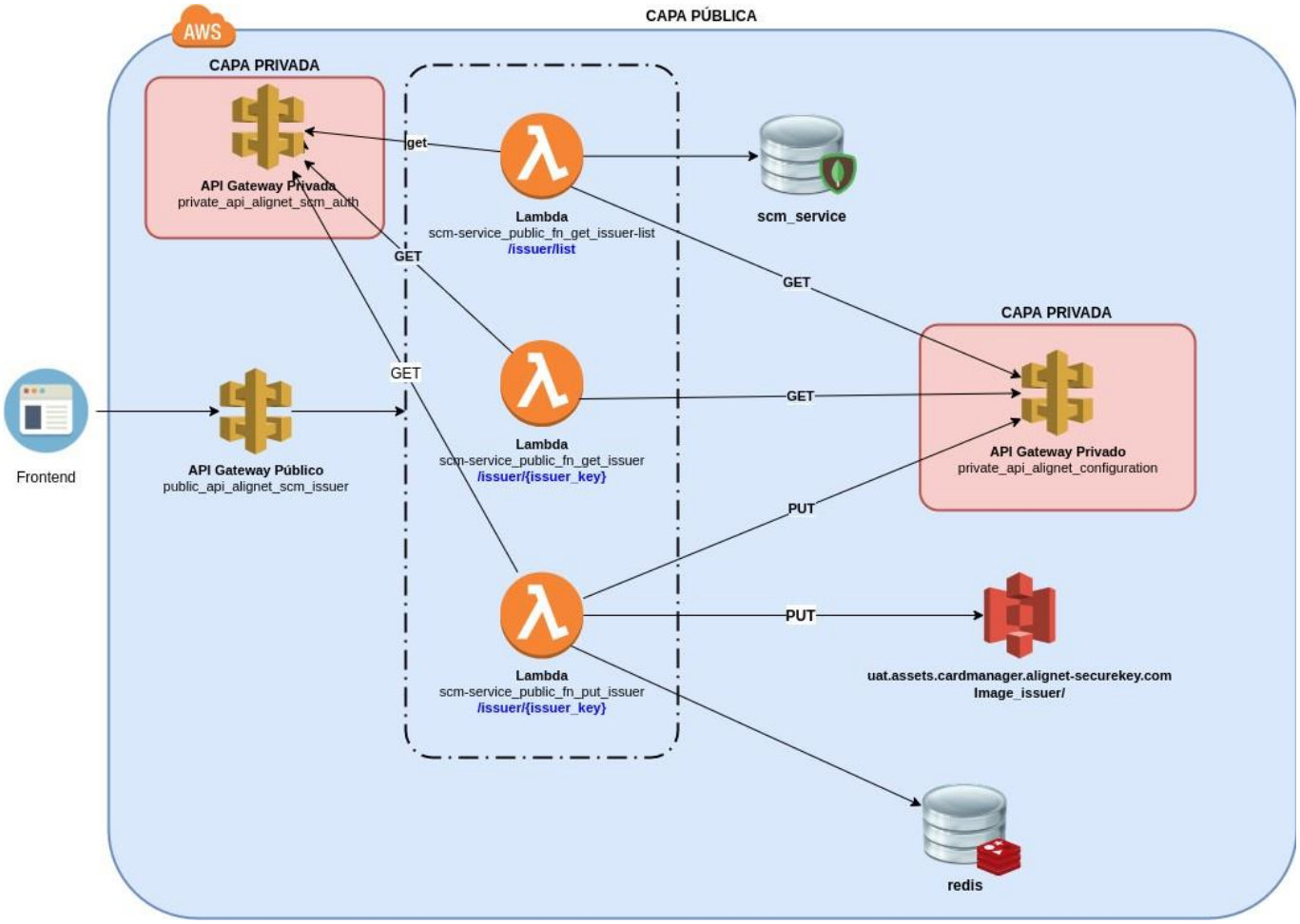


Componente	Tipo	Protocolo	Url	Descripción
public_api_alignet_scm_card	API GATEWAY	REST API	/card	Recurso en api gateway con protocolo rest
scm-service_public_fn_get_card-list	LAMBDA	REST - GET	/card/list	Lambda encargado de mostrar los datos correspondientes mediante un filtro específico de una lista de tarjetas.
scm-service_public_fn_get_card	LAMBDA	REST - GET	/card/{pan}	Lambda encargado de mostrar los datos correspondientes a una tarjeta.

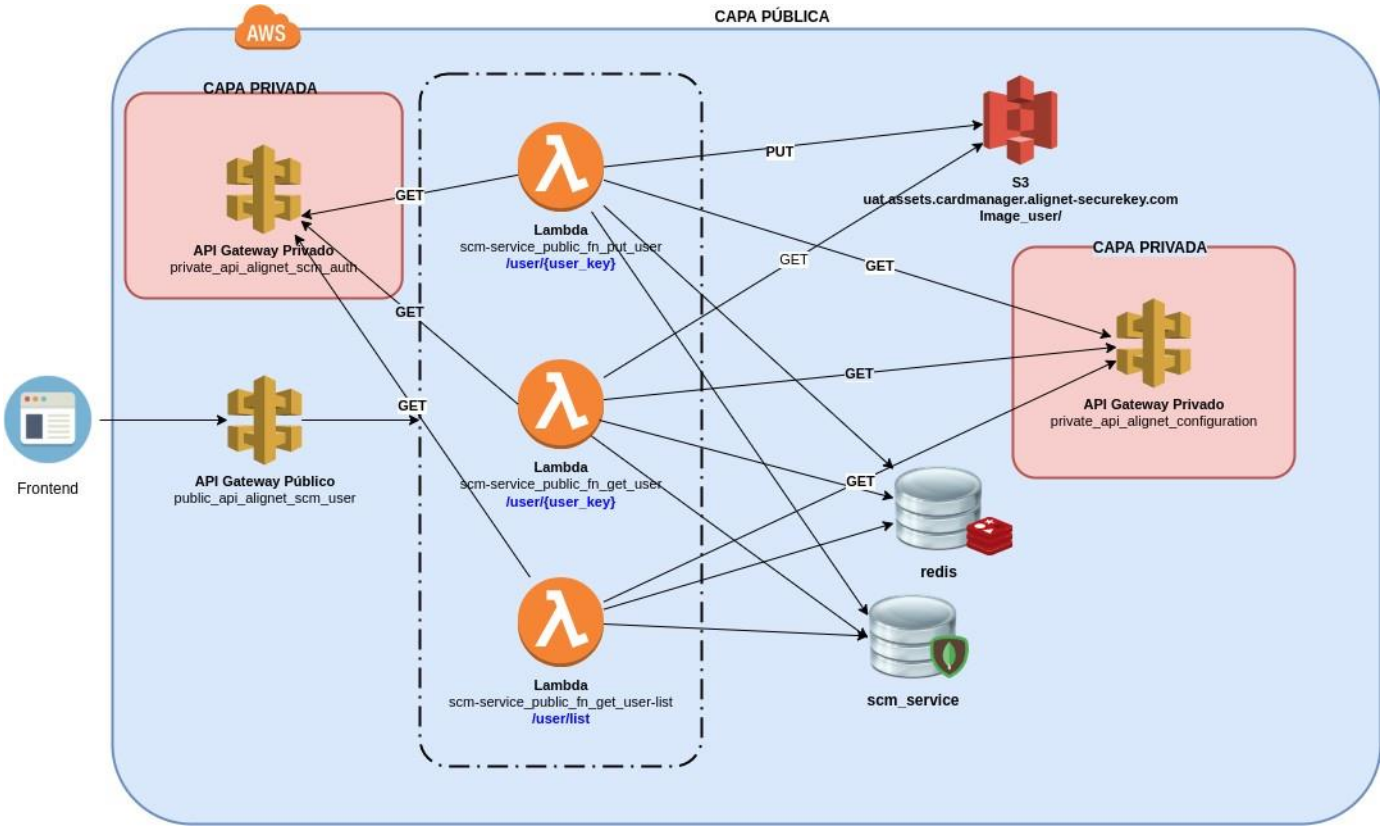
scm-service_public_fn_put_card	LAMBDA	REST - PUT	/card	Lambda encargado de actualizar los datos de una tarjeta.
scm-service_public_fn_post_ca rd	LAMBDA	REST - POST	/card	Lambda encargado de afiliar una tarjeta.
api-alignet-onboarding	API GATEWAY	REST - GET		Recurso en api gateway existente y realizado para un proyecto en paralelo que se reutilizará, el cual se encarga de comunicarse con la bd y devolver los datos de la tarjeta.
public_api_alignet_scm_operation	API GATEWAY	REST - POST		Recurso en api gateway existente encargado de enrolar una tarjeta.
private_api_alignet_scm_auth	API GATEWAY	REST - GET		Recurso en api gateway encargado de validar la sesión de usuario.

private_api_alignet_configuration	API GATEWAY	REST - GET		Recurso en api gateway encargado de deovolver los datos de datos de un emisor por medio de su id.
configuration-service_private_fn_get-currencies-networks-API	API GATEWAY	REST - GET		Recurso en api gateway encargado de devolver un listado con la descripción, simbolo y tipos de monedas.
ttps://search-token-audit-re4f2u6dnxi4b532n23tlvojpa.us-east-1.es.amazonaws.com	API GATEWAY	REST - GET	cardmanager_cards/_search	Recurso usado por el lambda “scm-service_public_fn_get_card-list“ para consultar las tarjetas a travez de filtros.

RFC 063 - Emisor

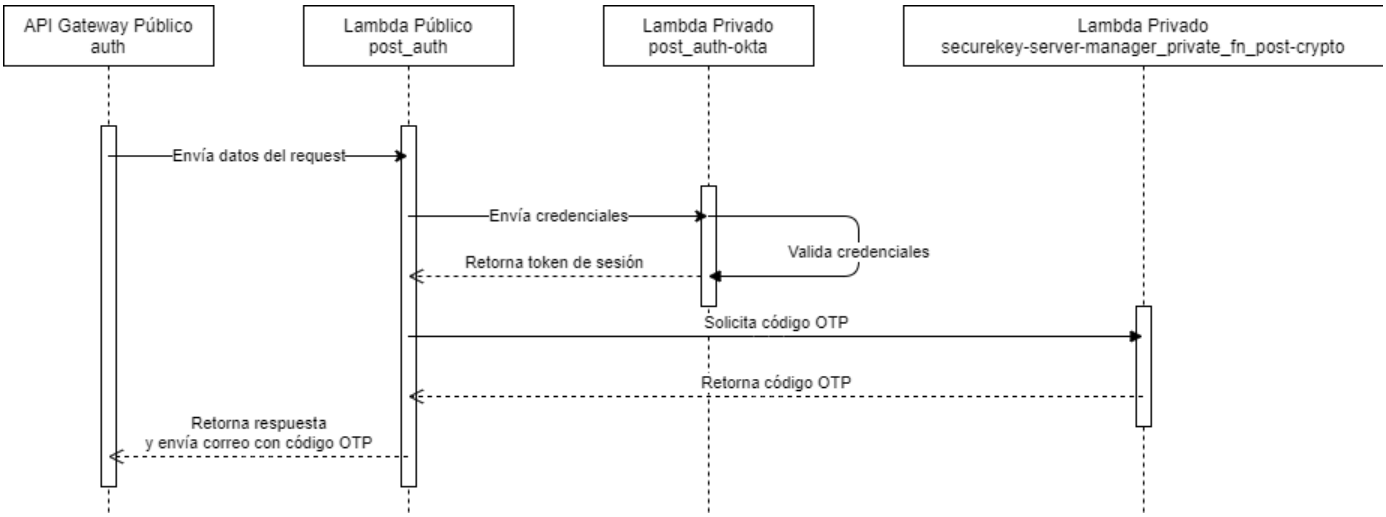


RFC 063 - Usuario

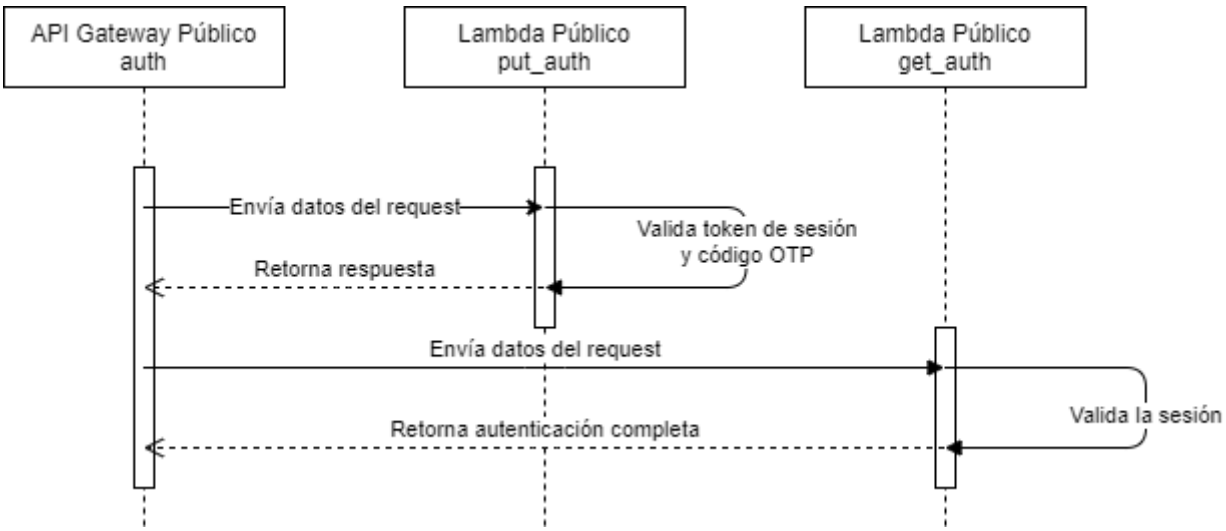


Inicio de sesión

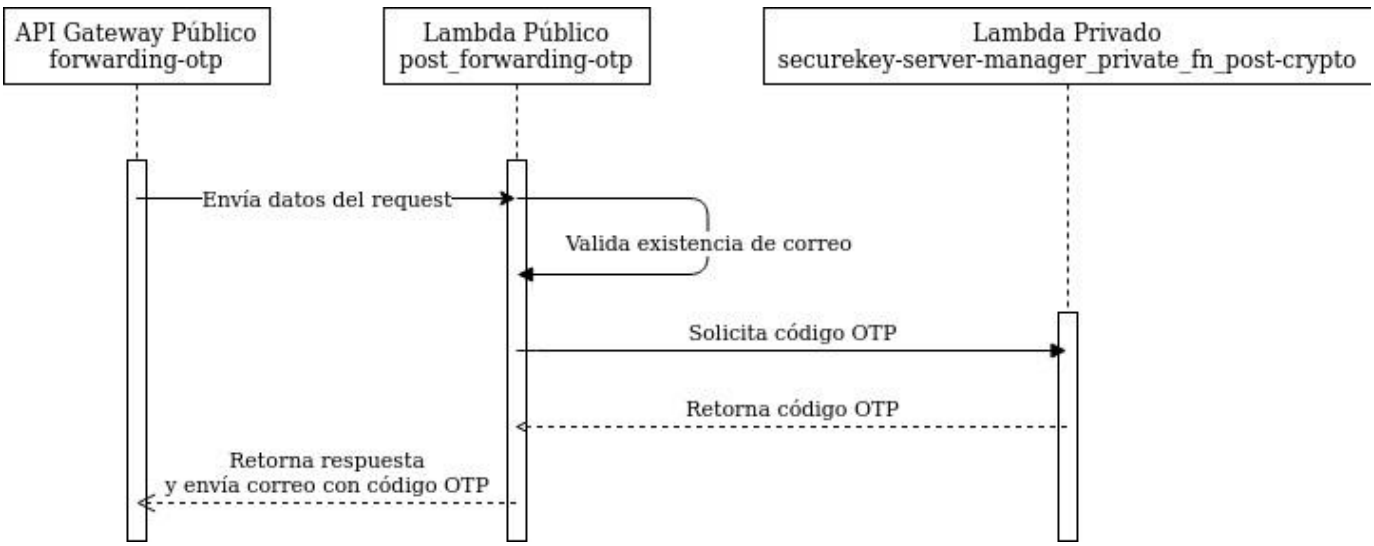
Primera autenticación



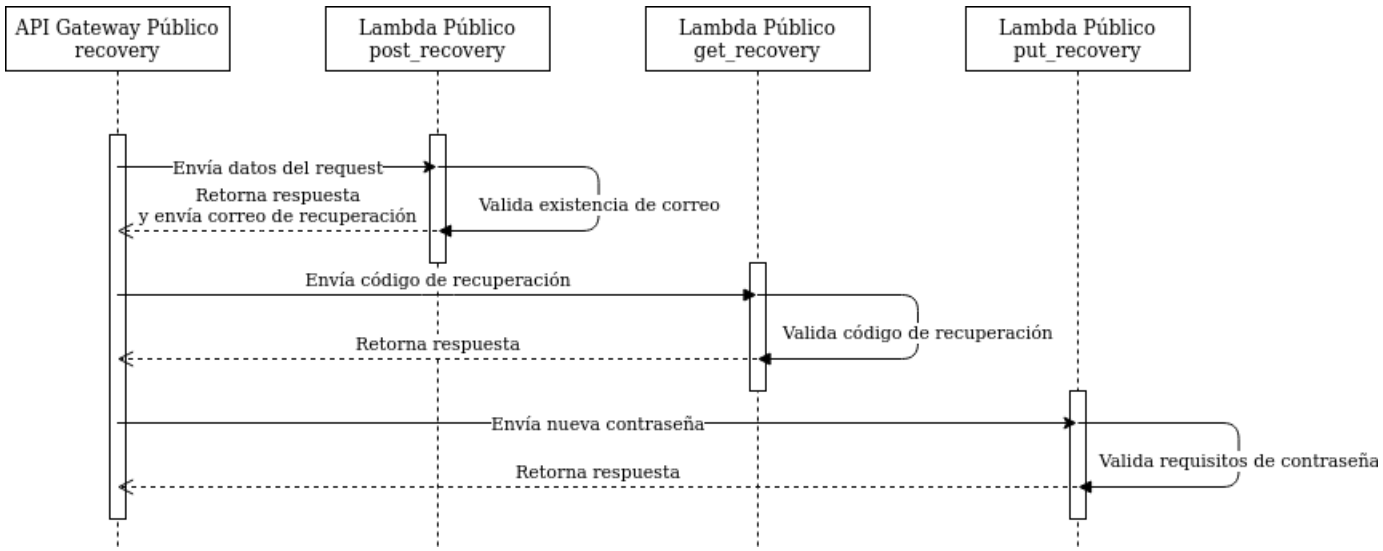
Segunda autenticación



Reenvío de código OTP

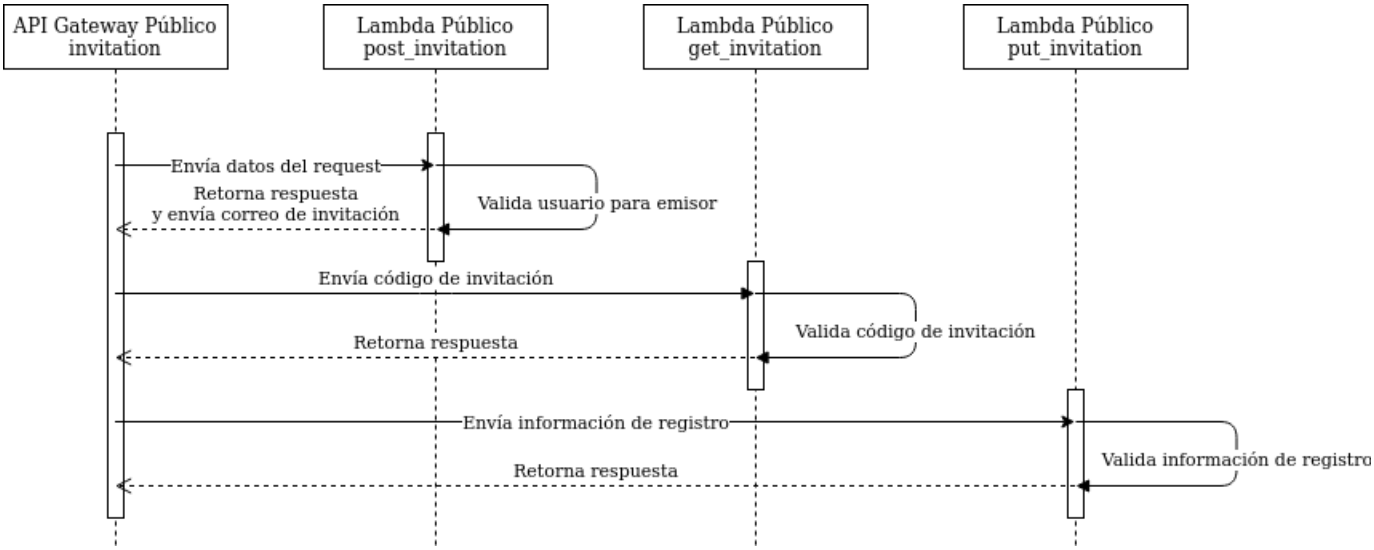


Recuperación de contraseña

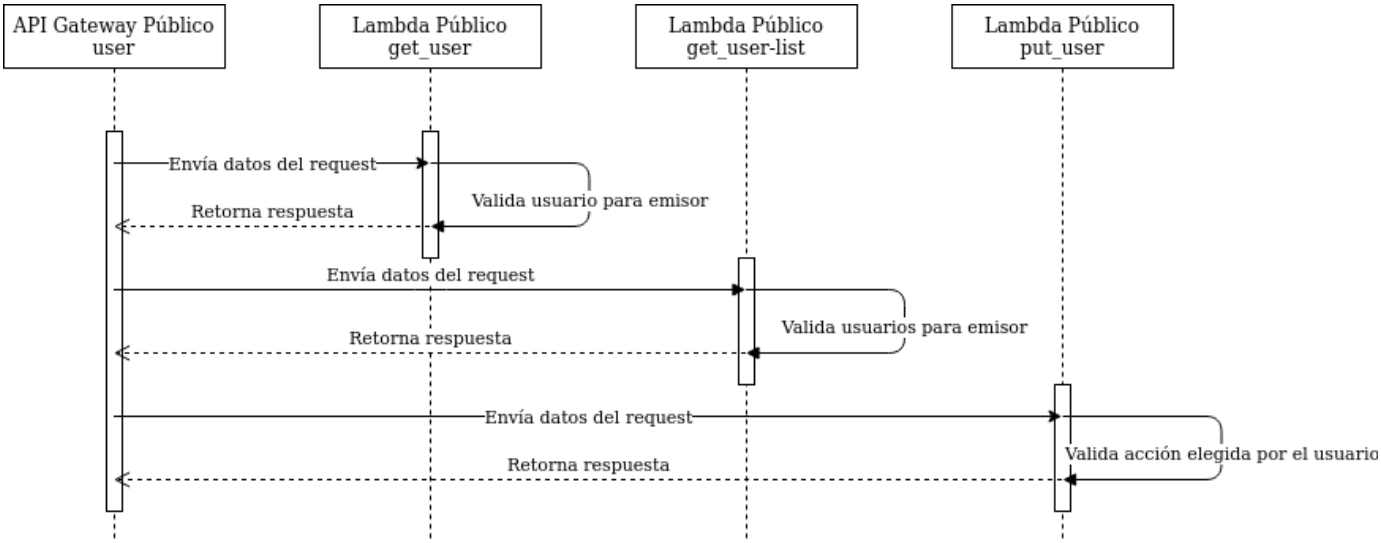

API Gateway Público
recovery
Lambda Público
post_recovery
Lambda Público
get_recovery
Lambda Público
put_recovery
Envía datos del request
Retorna respuesta
y envía correo de recuperación
Valida existencia de correo
Envía código de recuperación
Valida código de recuperación
Retorna respuesta
Envía nueva contraseña
Valida requisitos de contraseña
Retorna respuesta

Gestión de usuarios

Invitar usuario

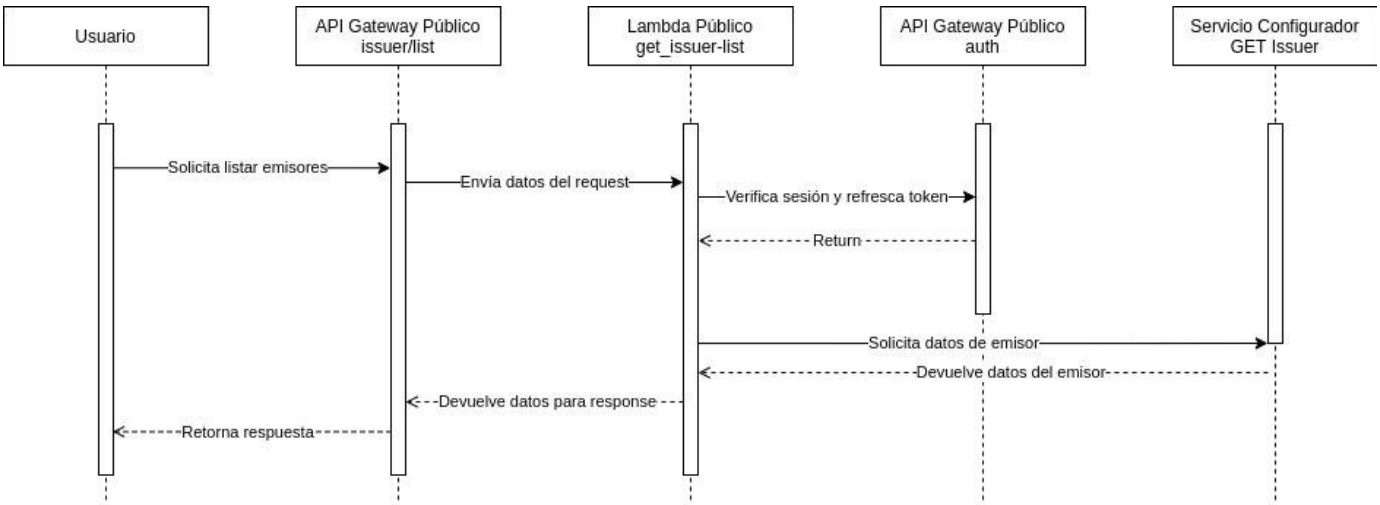


Usuarios



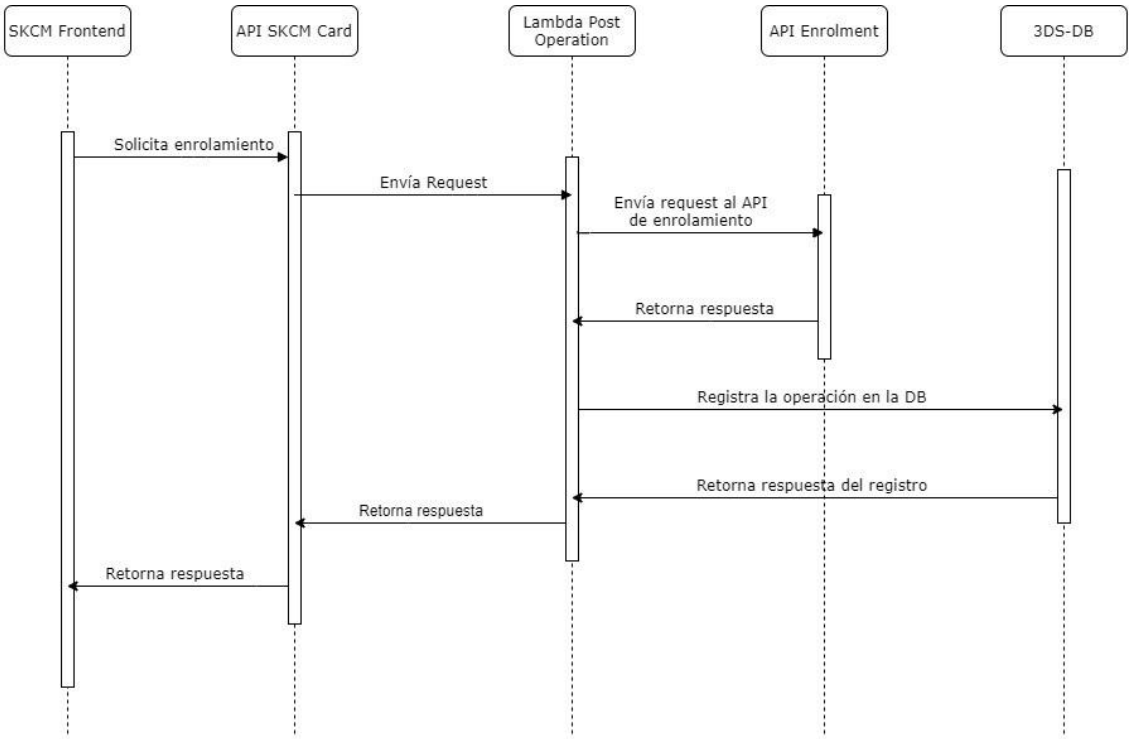
Emisores

Obtener datos del Emisor

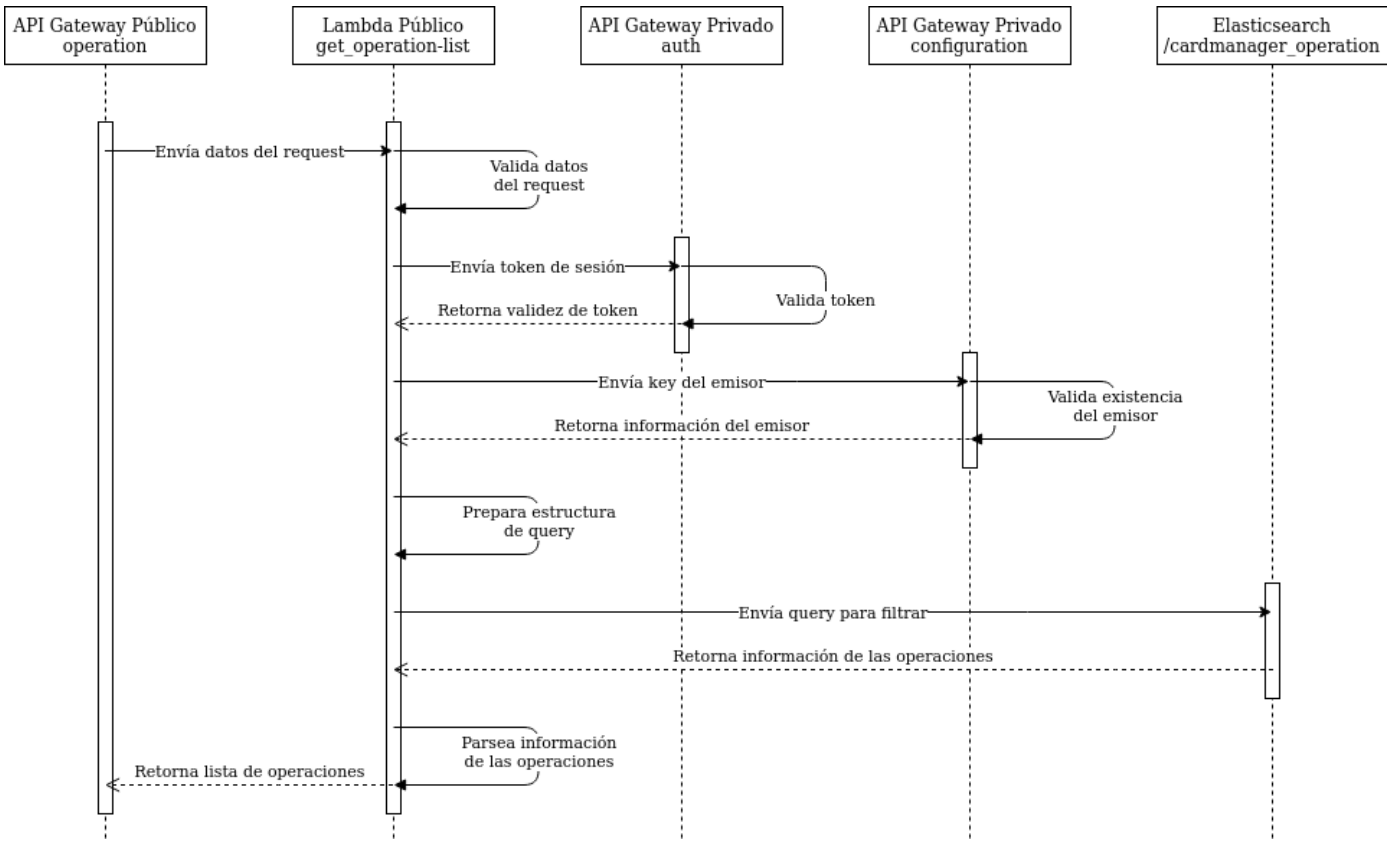


Operaciones

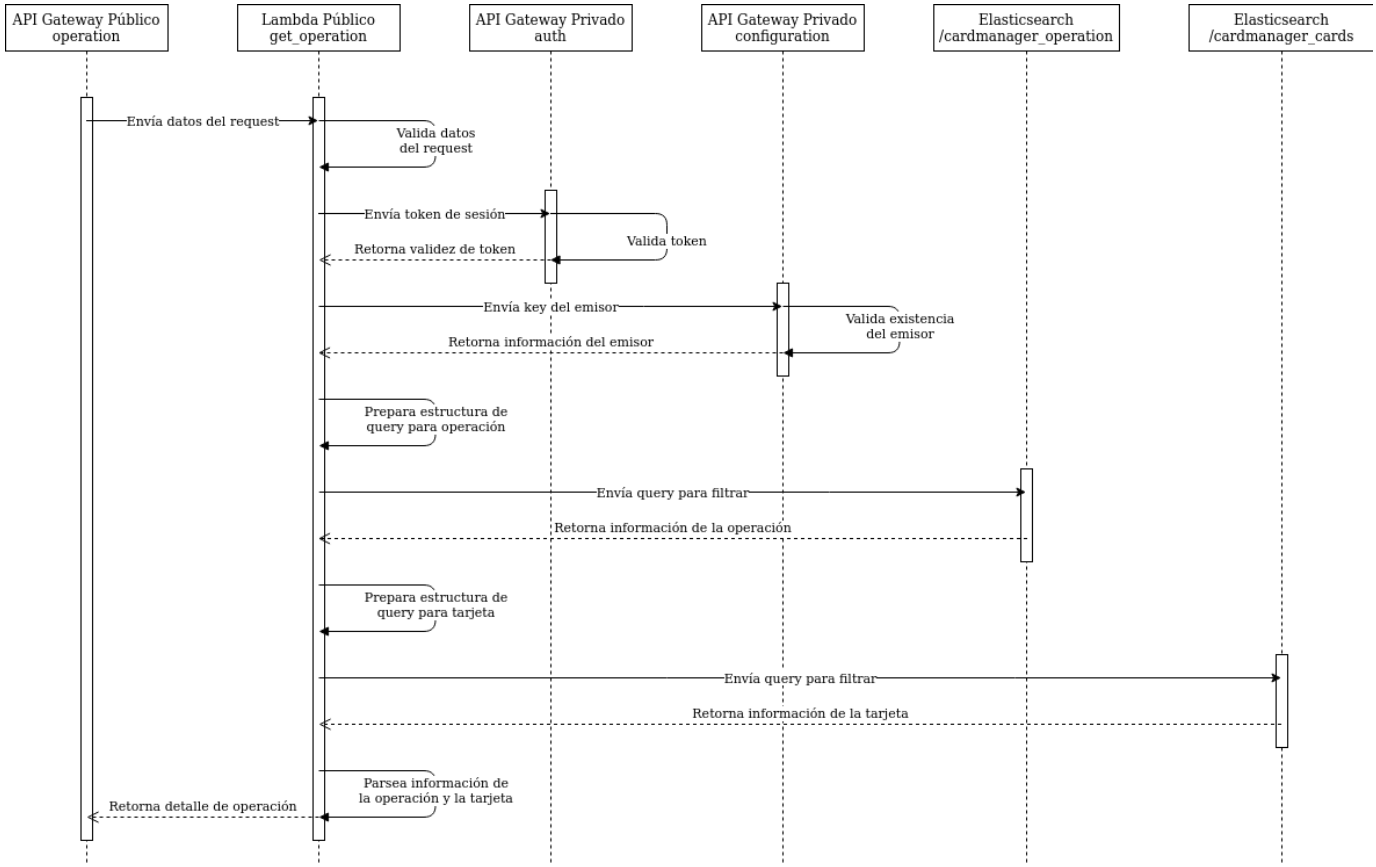
Registrar Operaciones



Obtener lista de Operaciones

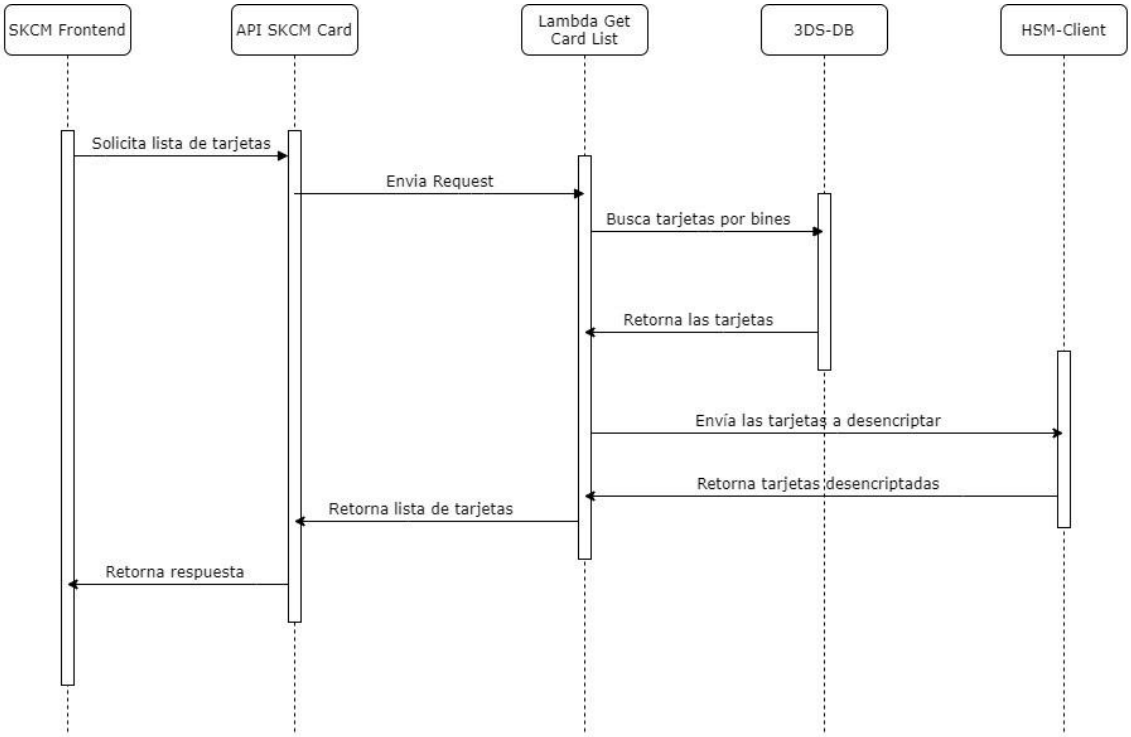


Obtener datos de Operación

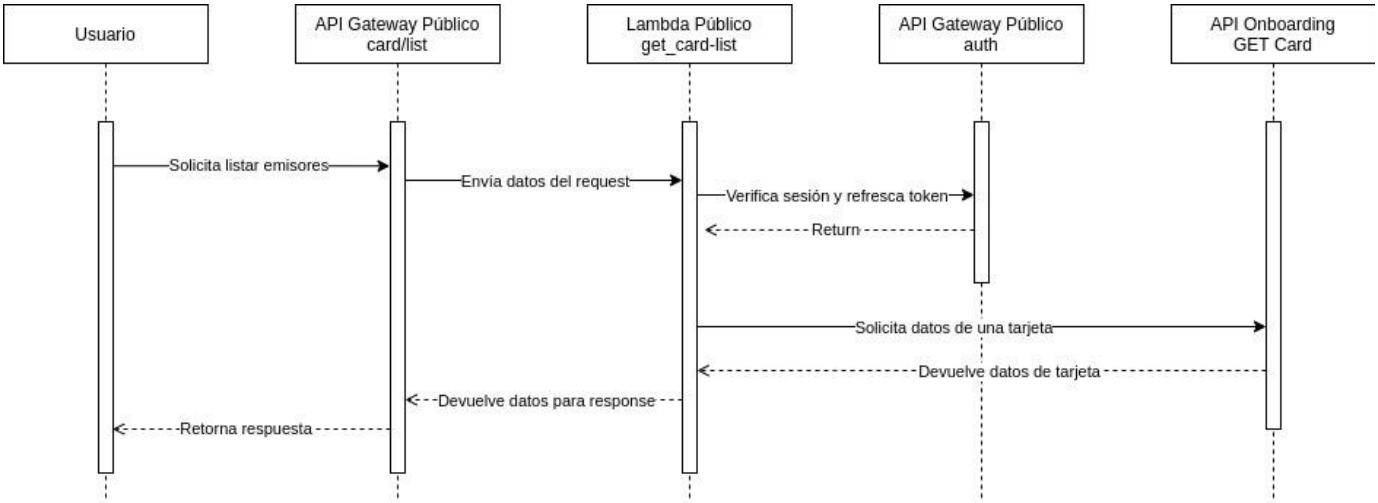

API Gateway Público
operation
Lambda Público
get_operation
API Gateway Privado
auth
API Gateway Privado
configuration
Elasticsearch
/cardmanager_operation
Elasticsearch
/cardmanager_cards
Envía datos del request
Valida datos
del request
Envía token de sesión
Valida token
Retorna validez de token
Envía key del emisor
Valida existencia
del emisor
Retorna información del emisor
Prepara estructura de
query para operación
Envía query para filtrar
Retorna información de la operación
Prepara estructura de
query para tarjeta
Envía query para filtrar
Retorna información de la tarjeta
Parsea información de
la operación y la tarjeta
Retorna detalle de operación

Tarjeta

Obtener lista de tarjetas

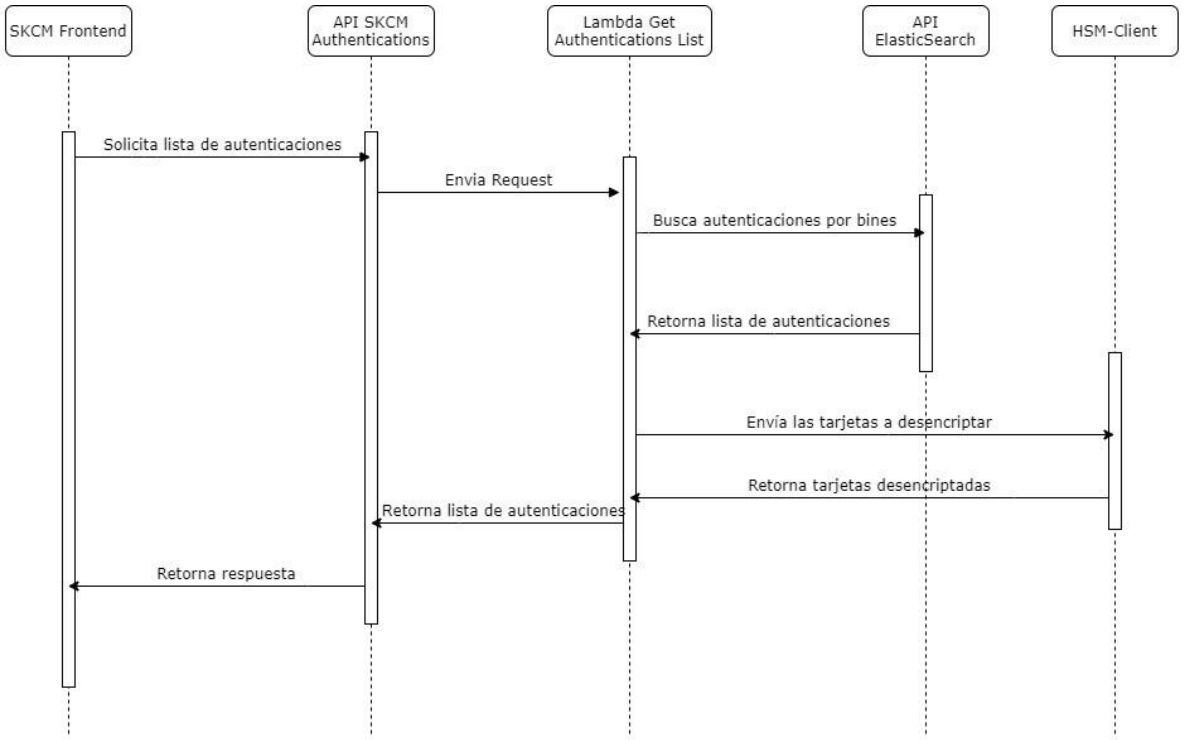


Obtener datos de tarjeta

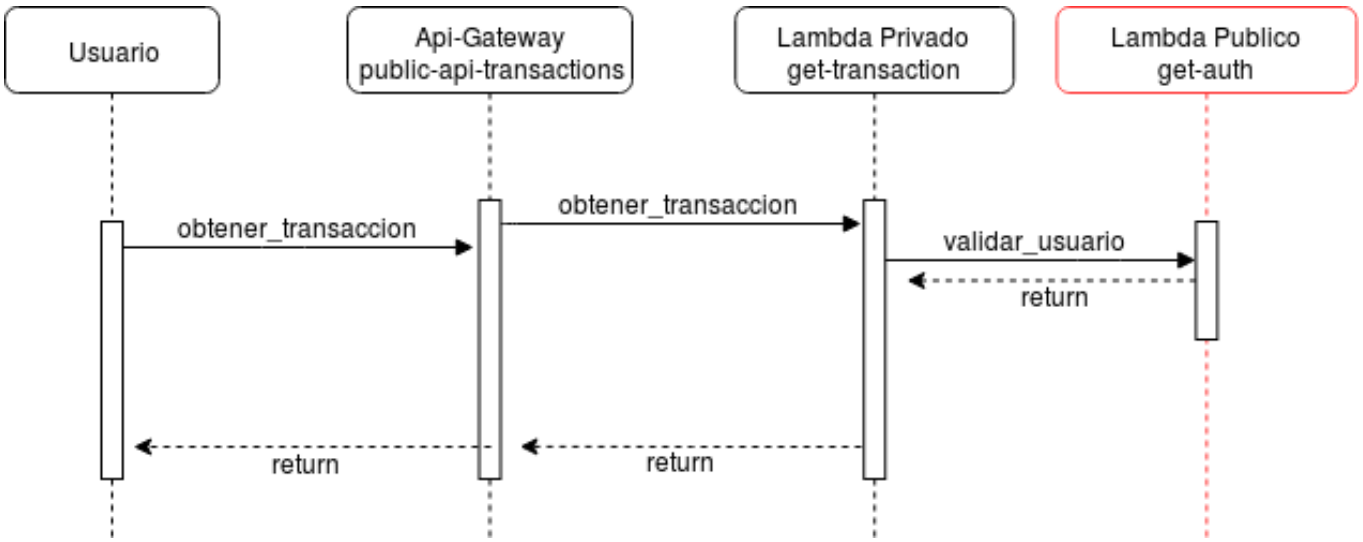

Usuario
API Gateway Público
card/list
Lambda Público
get_card-list
API Gateway Público
auth
API Onboarding
GET Card
Solicita listar emisores
Envía datos del request
Verifica sesión y refresca token
Return
Solicita datos de una tarjeta
Devuelve datos de tarjeta
Devuelve datos para response
Retorna respuesta

Transacciones

Obtener lista de transacciones

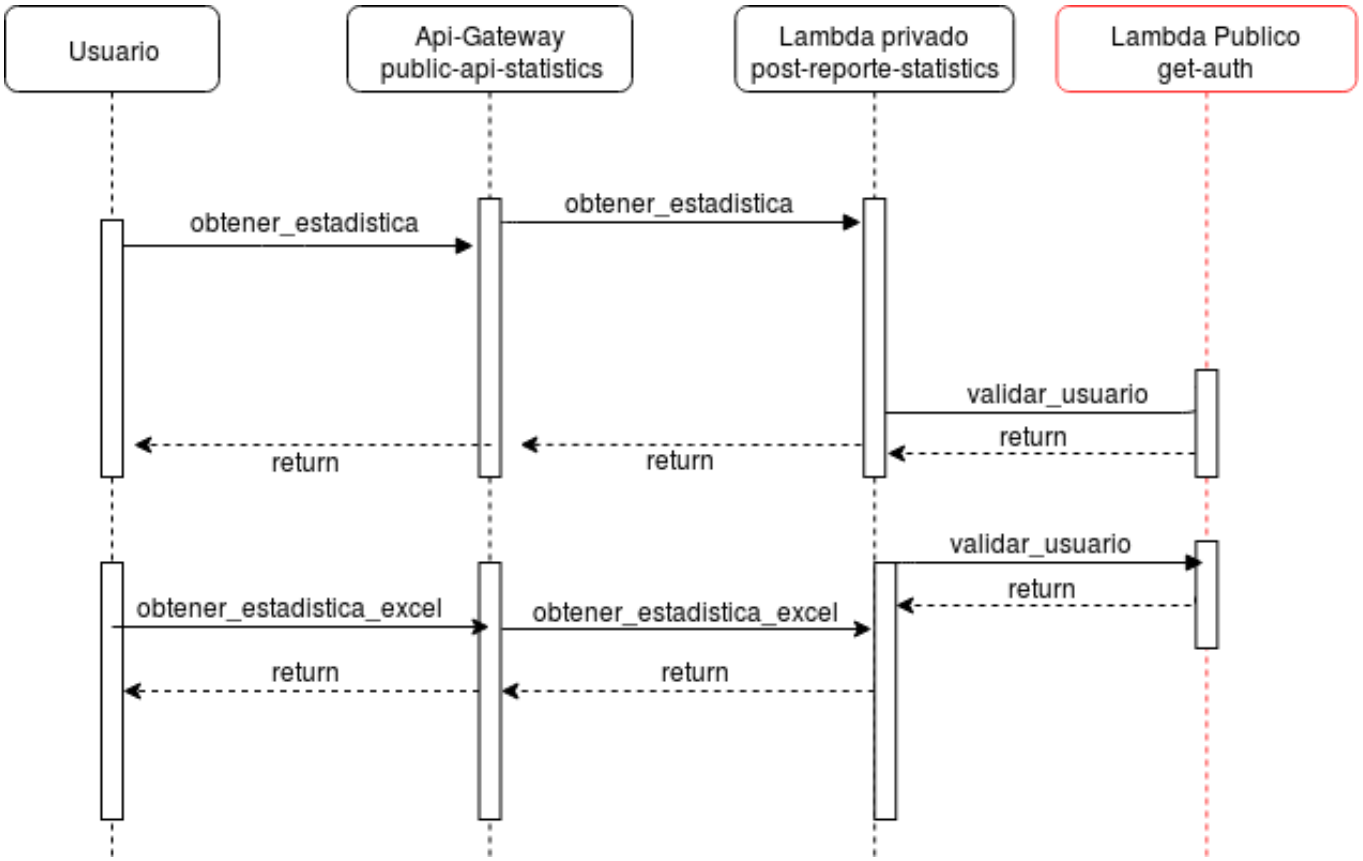


Obtener transaccion



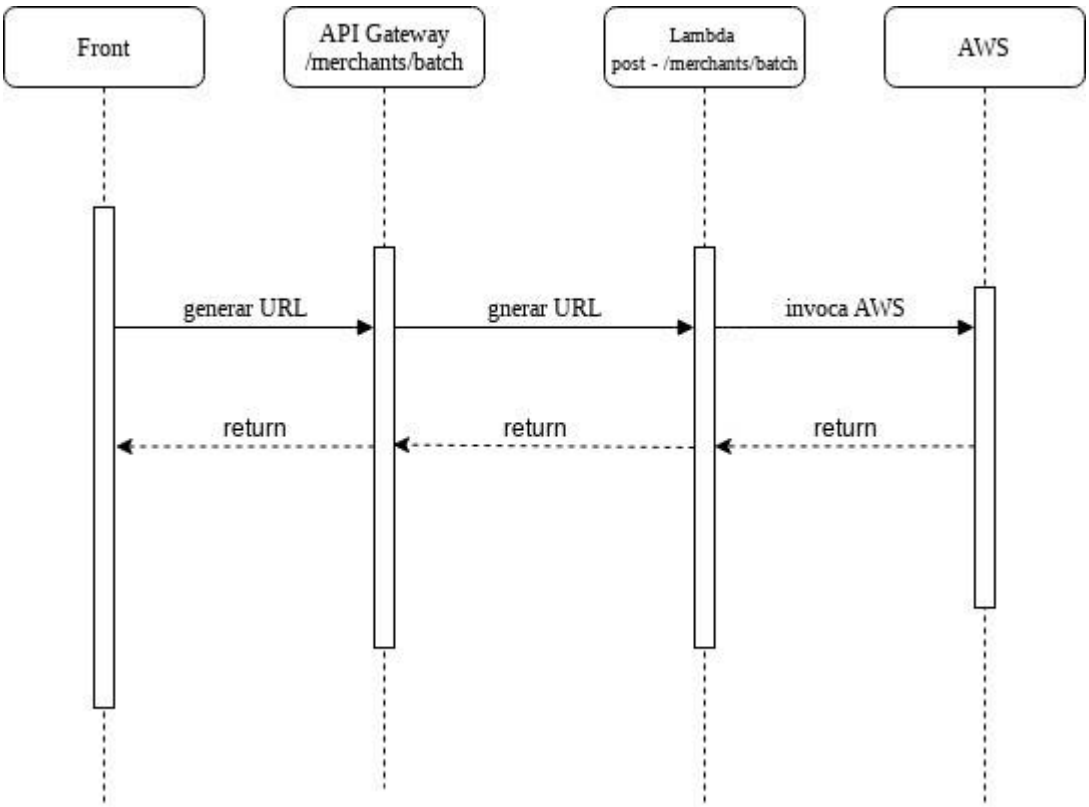
Estadisticas

Obtener estadística

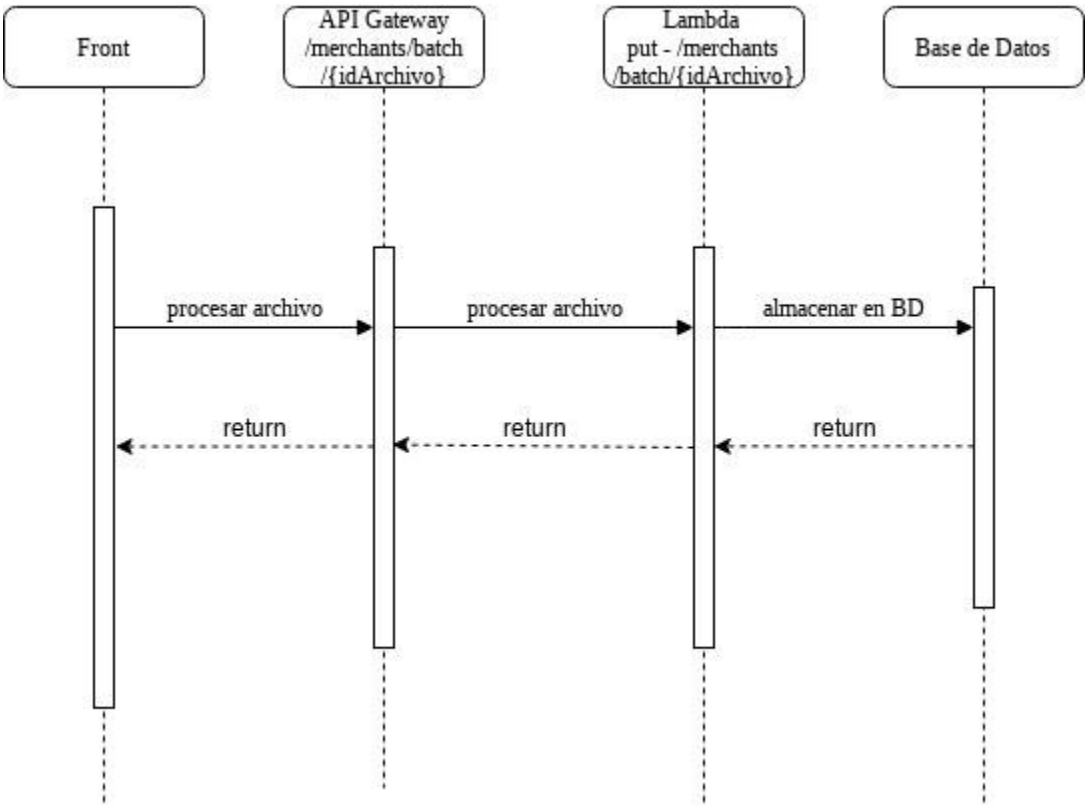


Registro para carga masiva

Generar URL



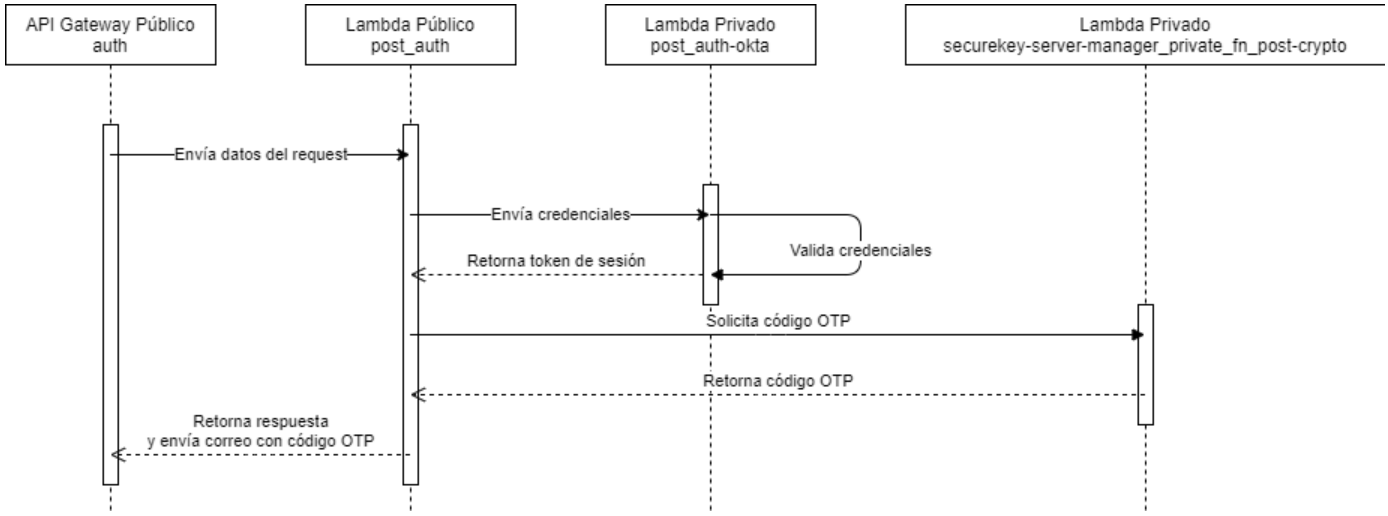
Procesar Archivo Cargado



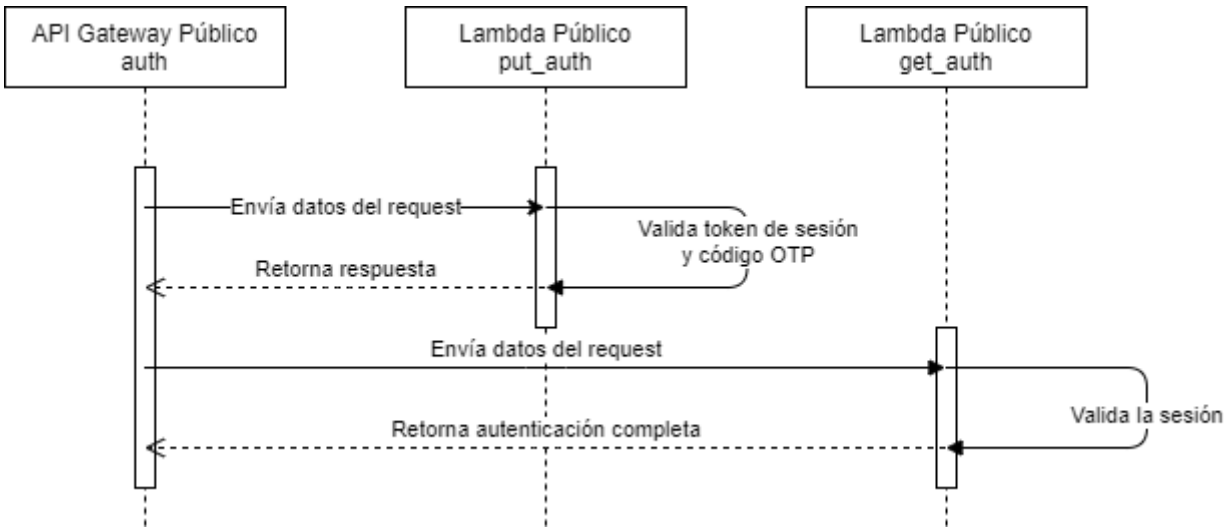
RFC 063 - Diagramas - Flujo

Inicio de sesión

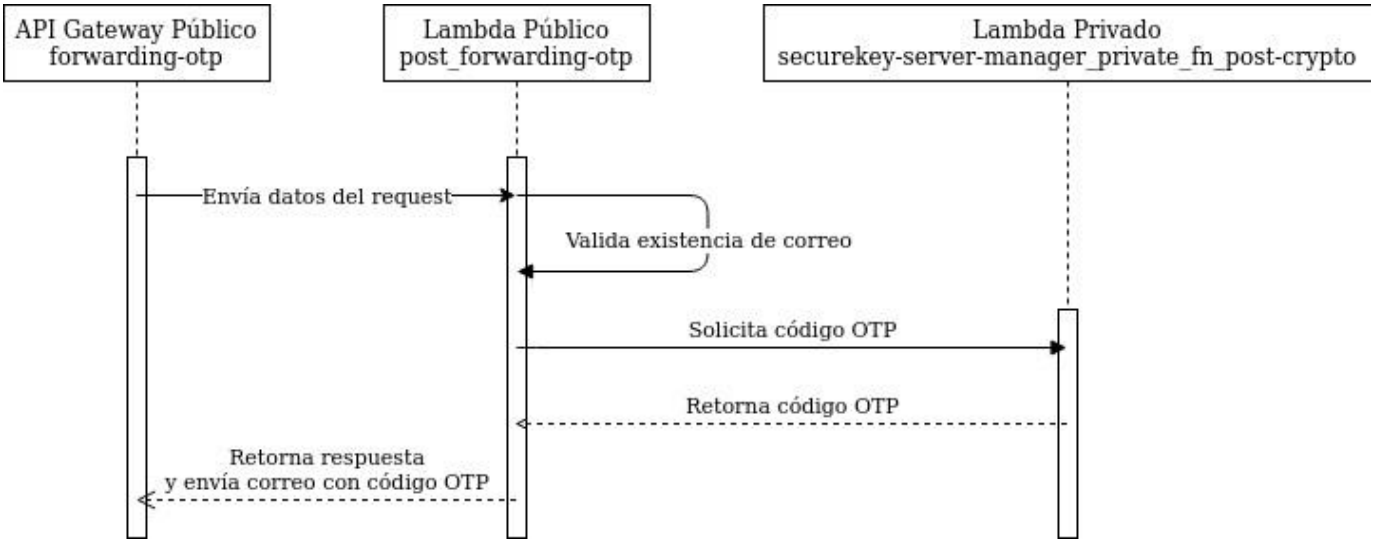
Primera autenticación



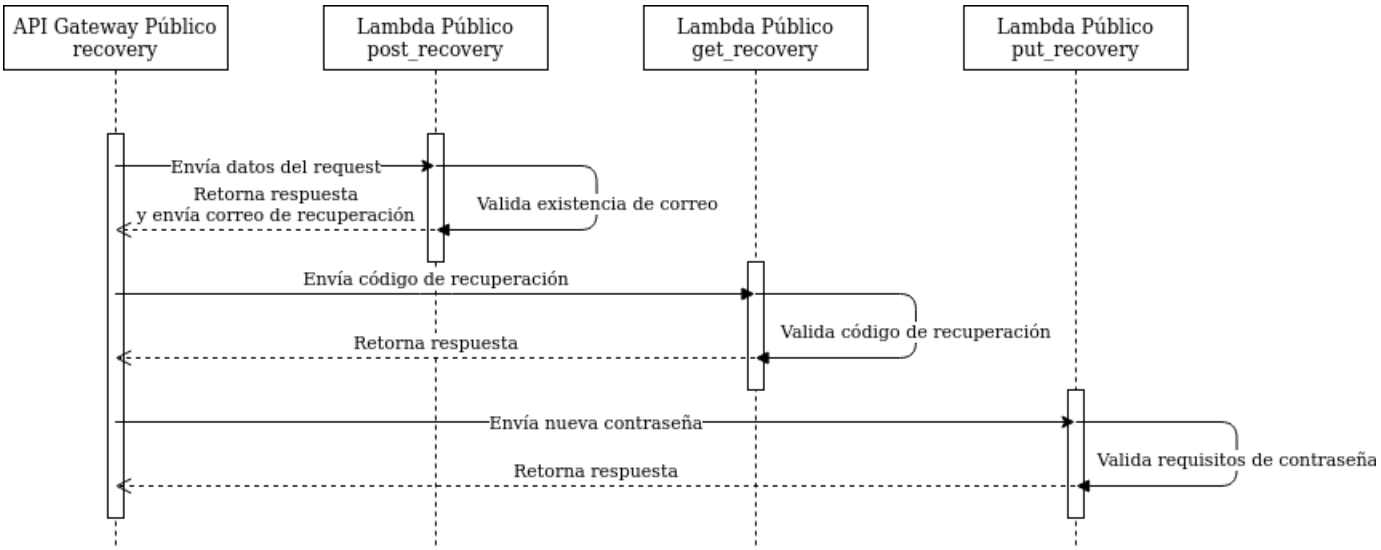
Segunda autenticación



Reenvío de código OTP

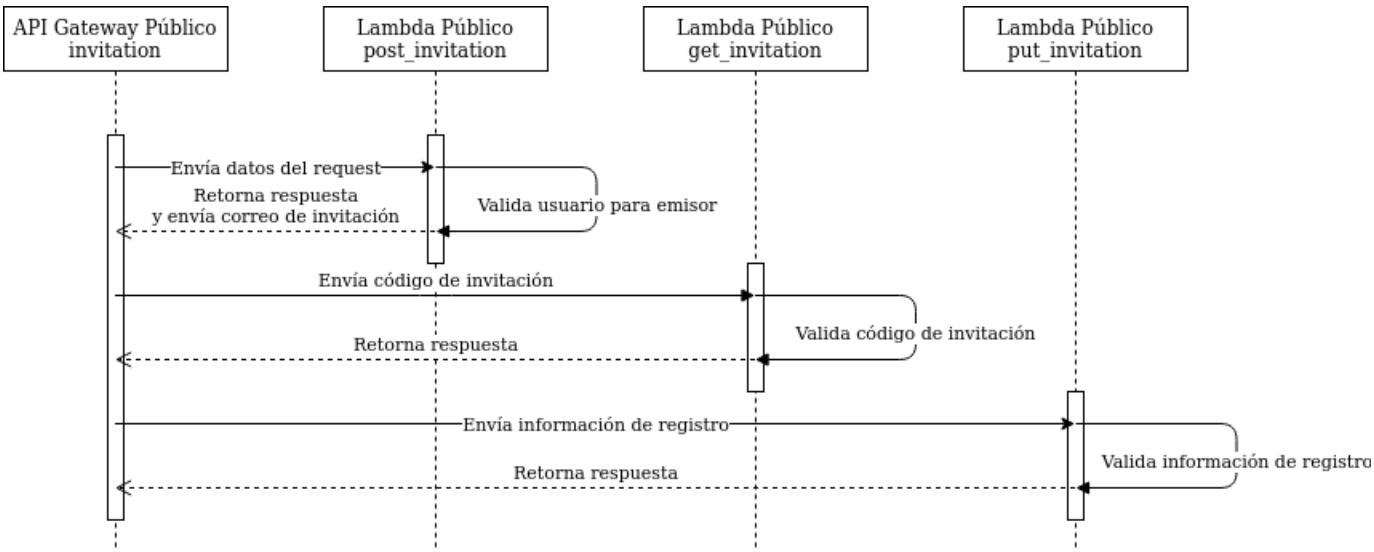


Recuperación de contraseña

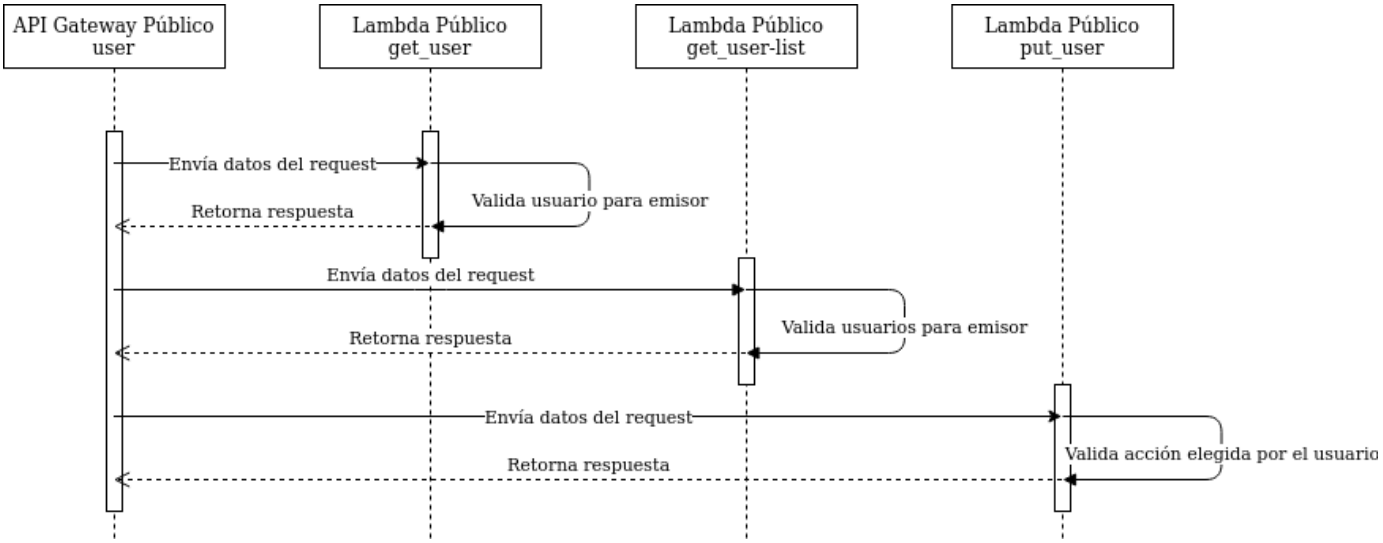


Gestión de usuarios

Invitar usuario

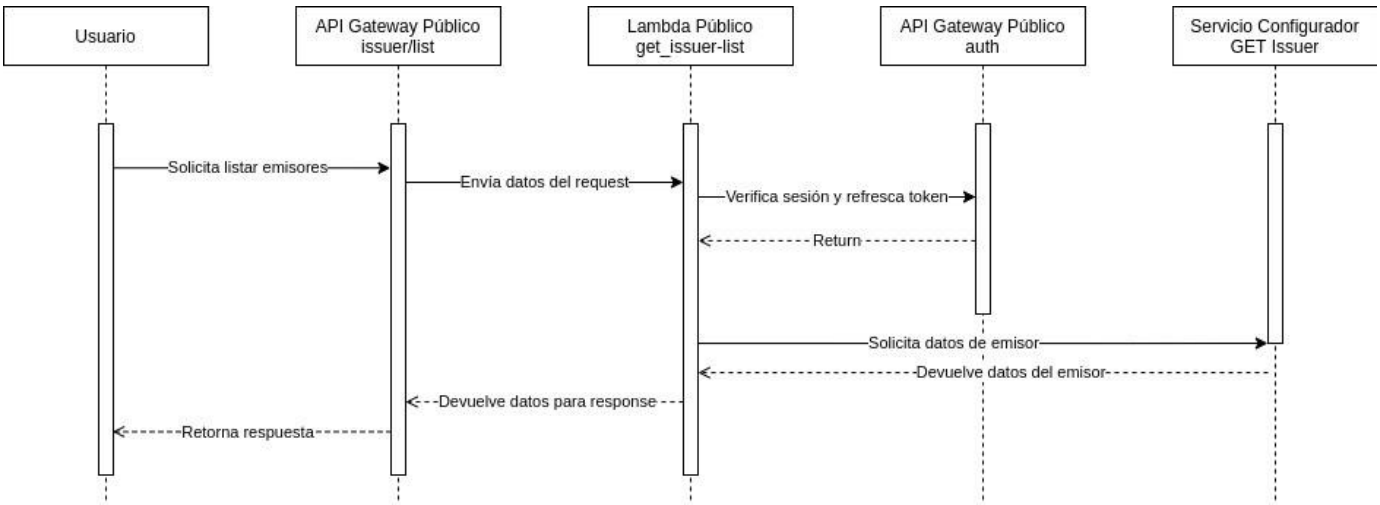


Usuarios



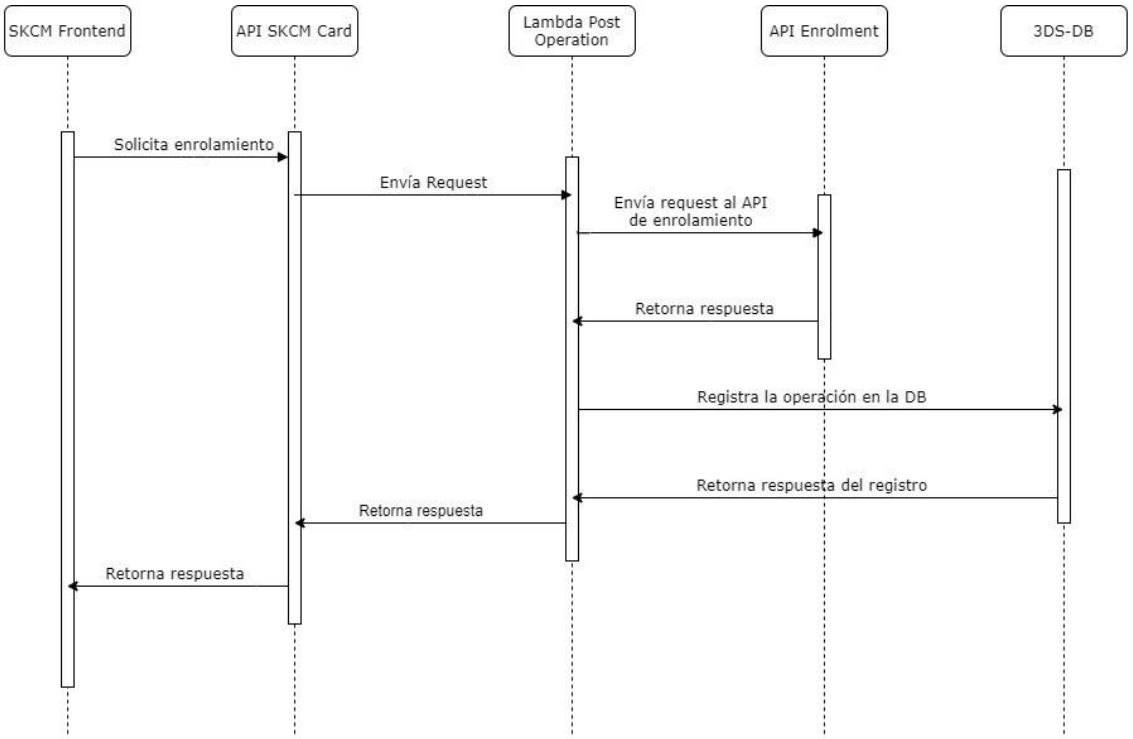
Emisores

Obtener datos del Emisor

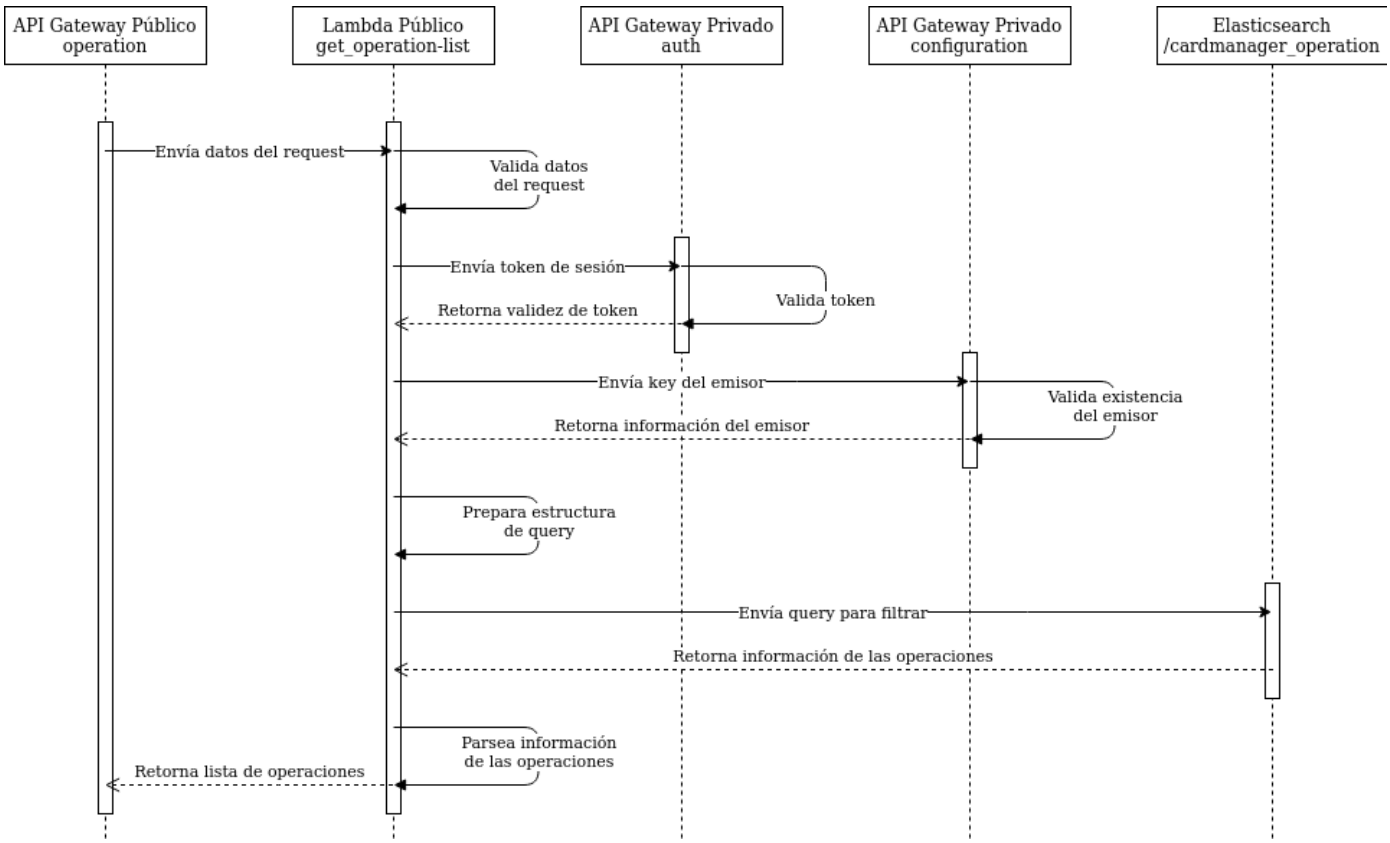


Operaciones

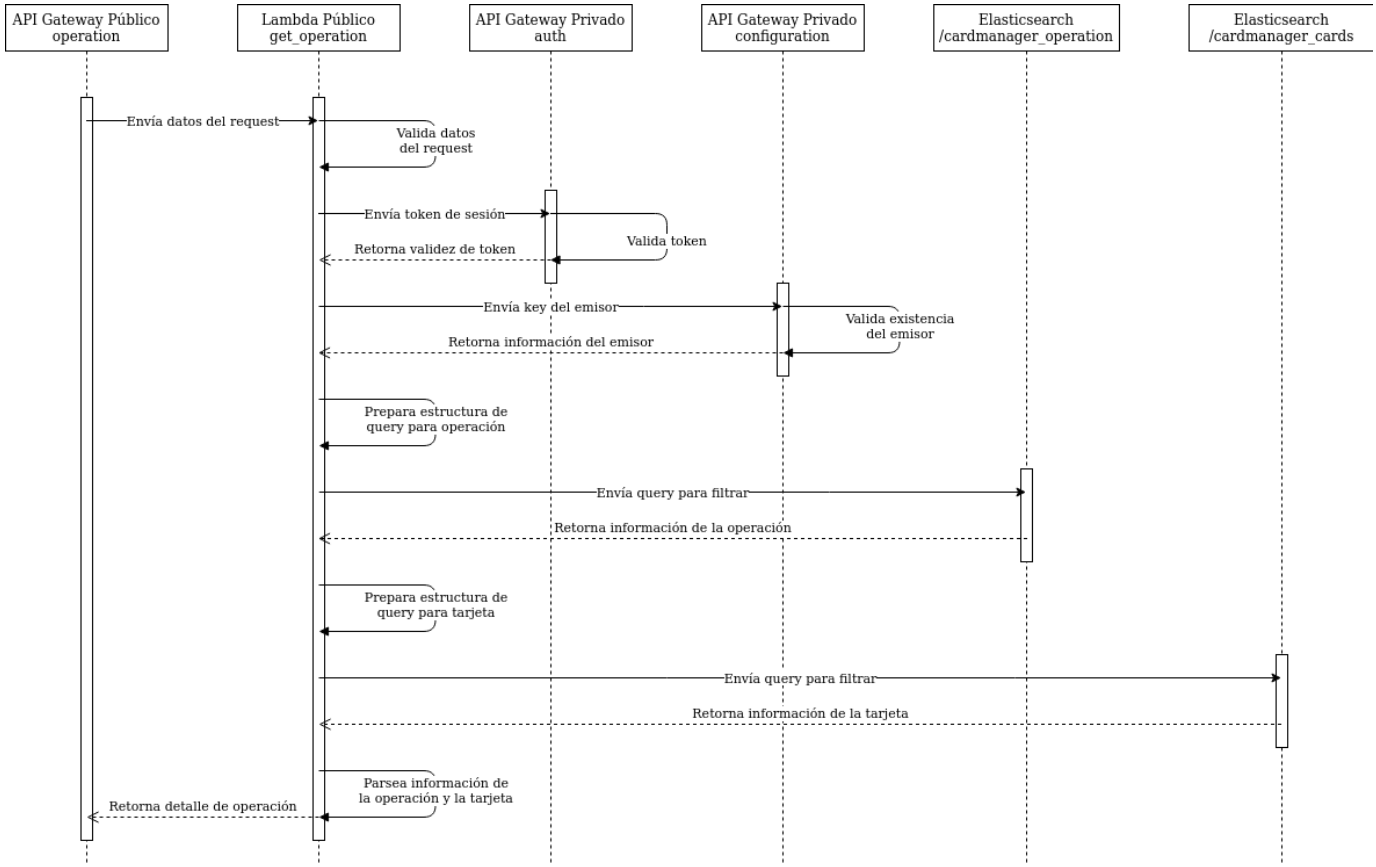
Registrar Operaciones



Obtener lista de Operaciones

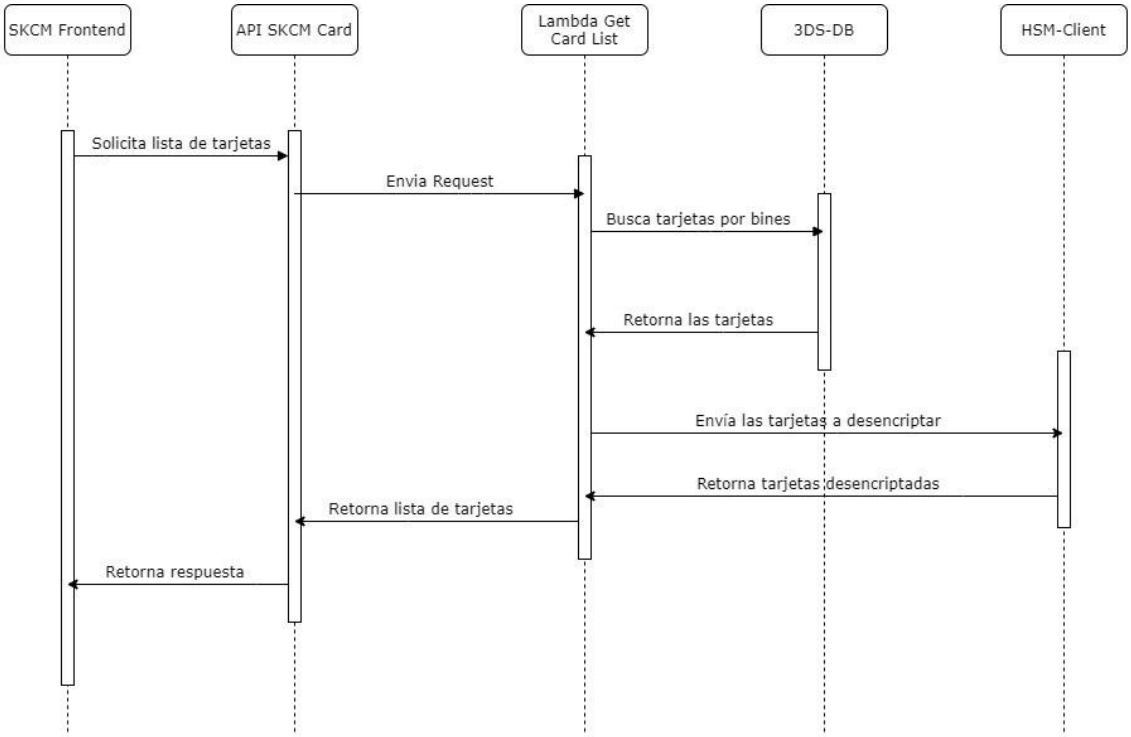


Obtener datos de Operación

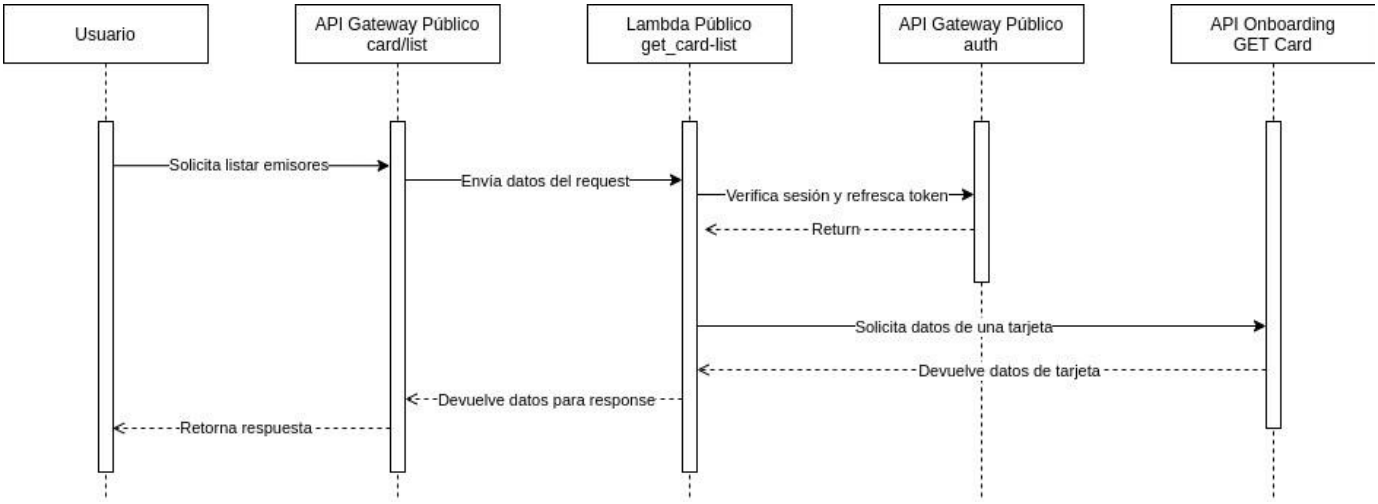

API Gateway Público
operation
Lambda Público
get_operation
API Gateway Privado
auth
API Gateway Privado
configuration
Elasticsearch
/cardmanager_operation
Elasticsearch
/cardmanager_cards
Envía datos del request
Valida datos
del request
Envía token de sesión
Valida token
Retorna validez de token
Envía key del emisor
Valida existencia
del emisor
Retorna información del emisor
Prepara estructura de
query para operación
Envía query para filtrar
Retorna información de la operación
Prepara estructura de
query para tarjeta
Envía query para filtrar
Retorna información de la tarjeta
Parsea información de
la operación y la tarjeta
Retorna detalle de operación

Tarjeta

Obtener lista de tarjetas

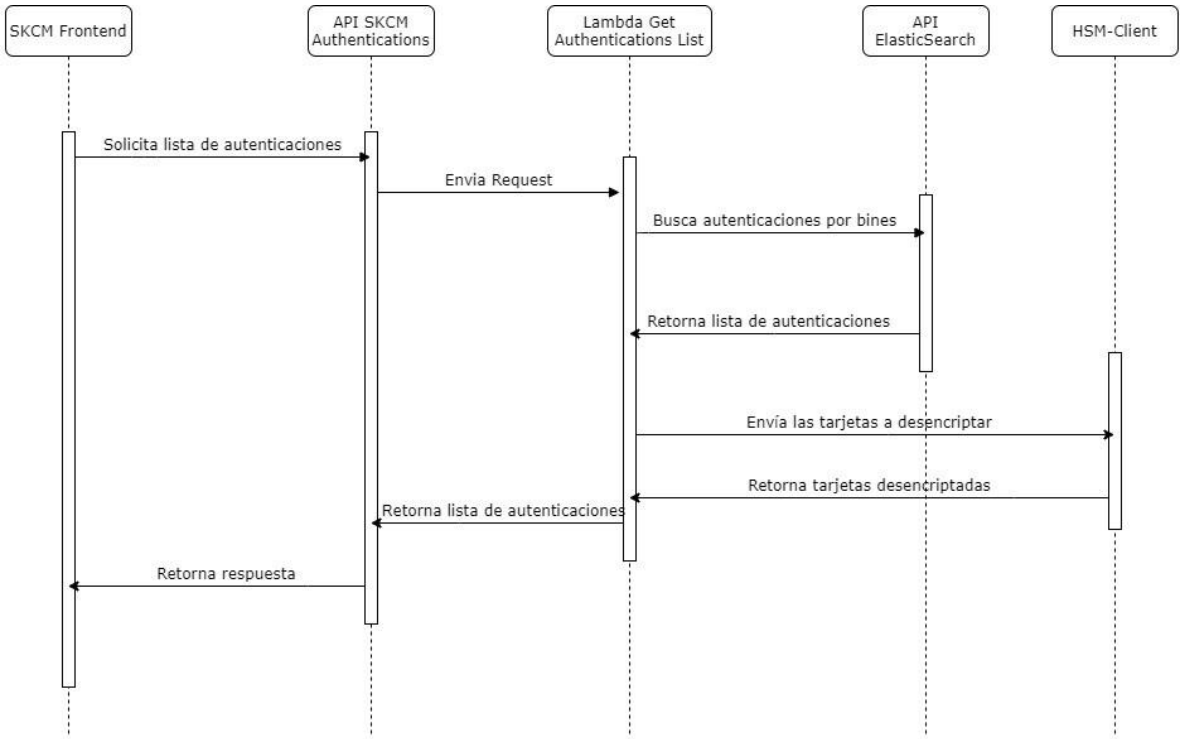


Obtener datos de tarjeta

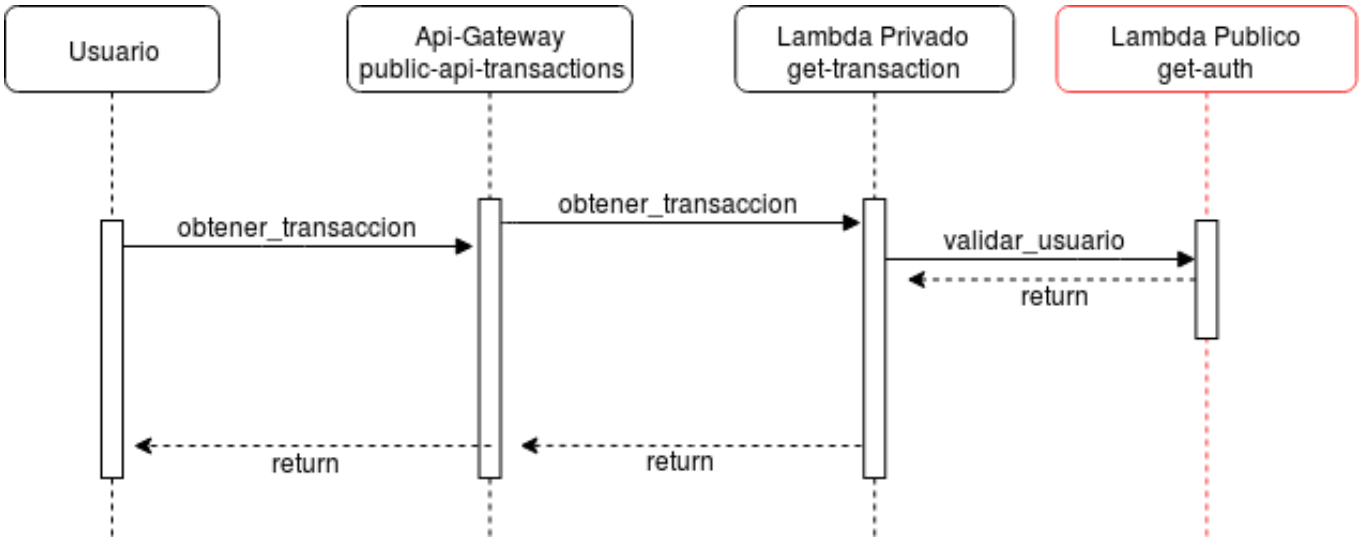


Transacciones

Obtener lista de transacciones

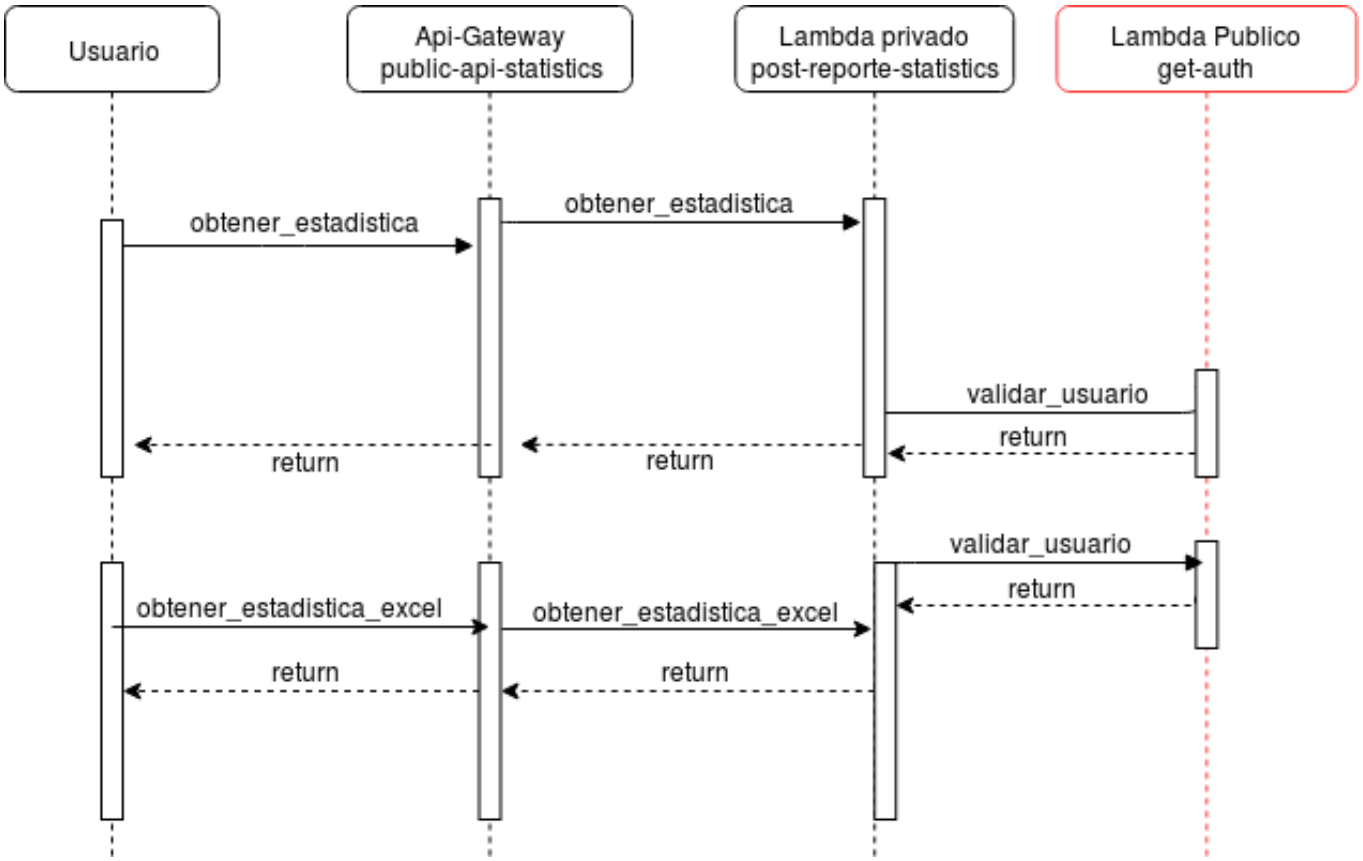


Obtener transaccion


Usuario
Api-Gateway
public-api-transactions
Lambda Privado
get-transaction
Lambda Publico
get-auth
obtener_transaccion
obtener_transaccion
validar_usuario
return
return
return

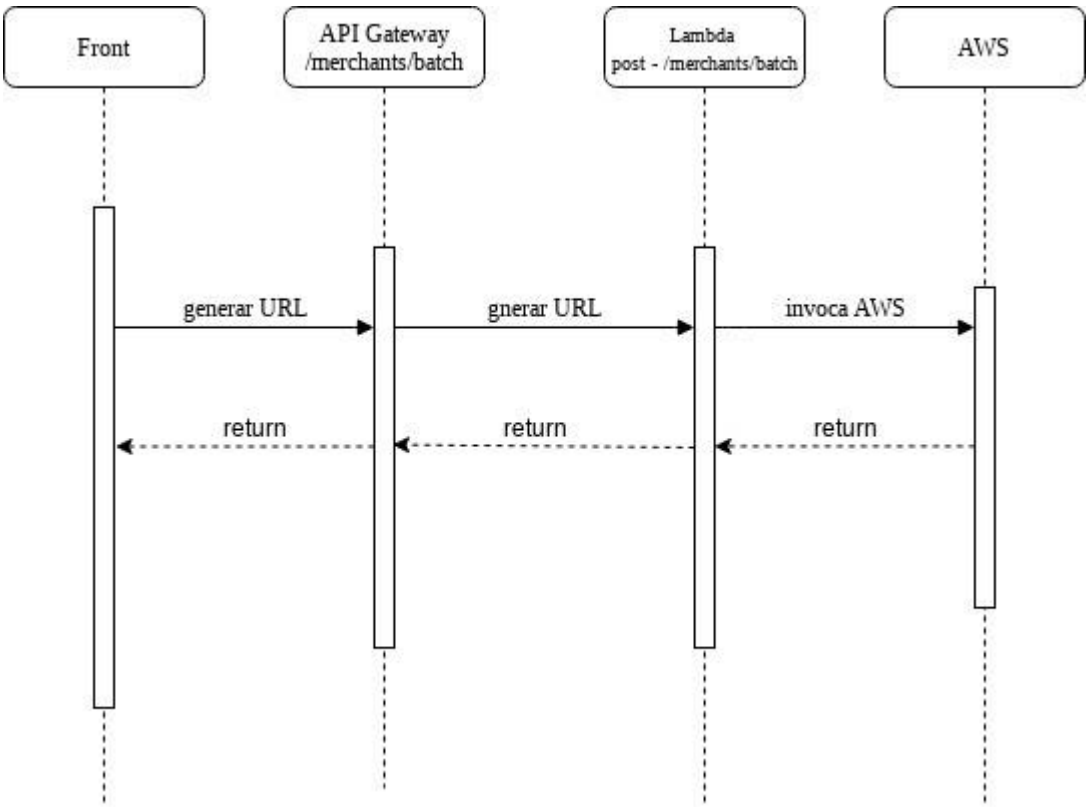
Estadisticas

Obtener estadística

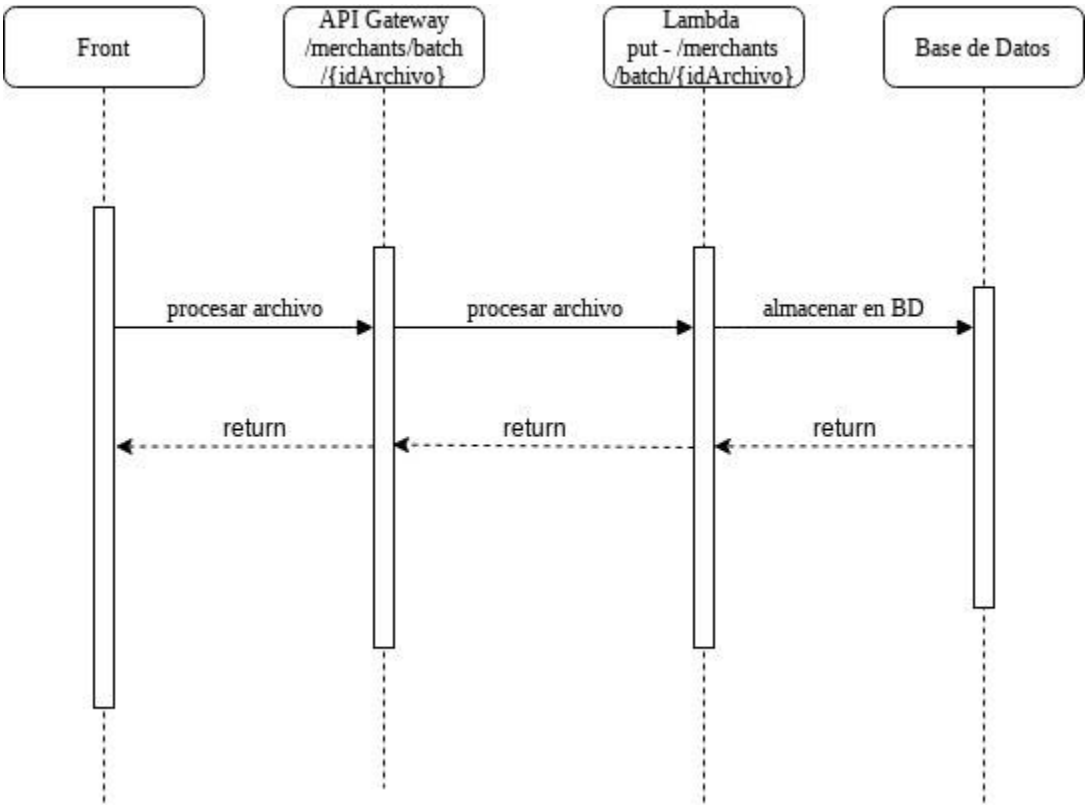


Registro para carga masiva

Generar URL



Procesar Archivo Cargado

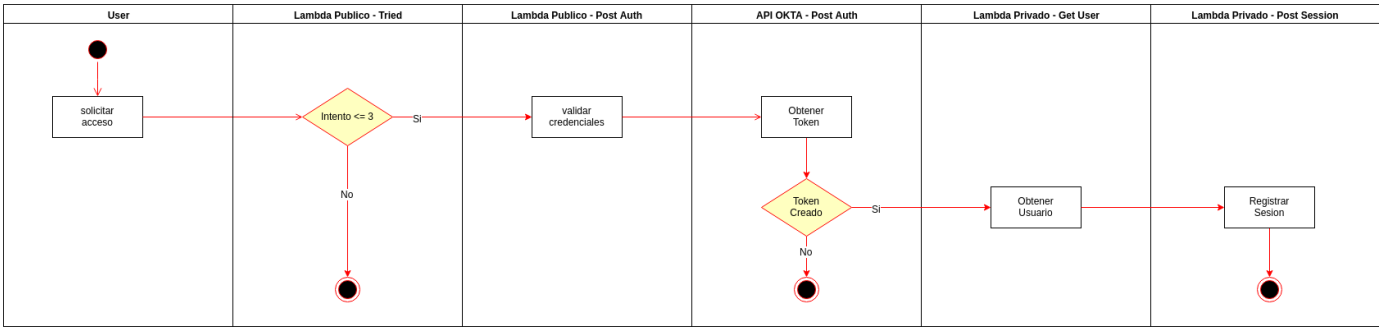


RFC 063 - Diagramas - Actividades

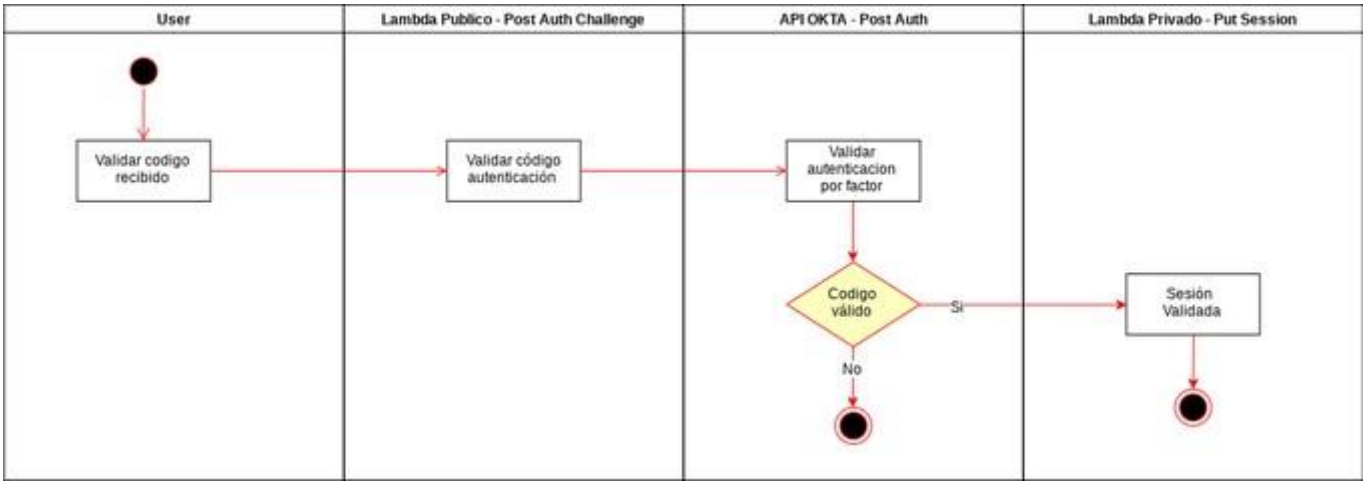
Primera Autenticación Segunda Autenticación

Login

Primera Autenticación

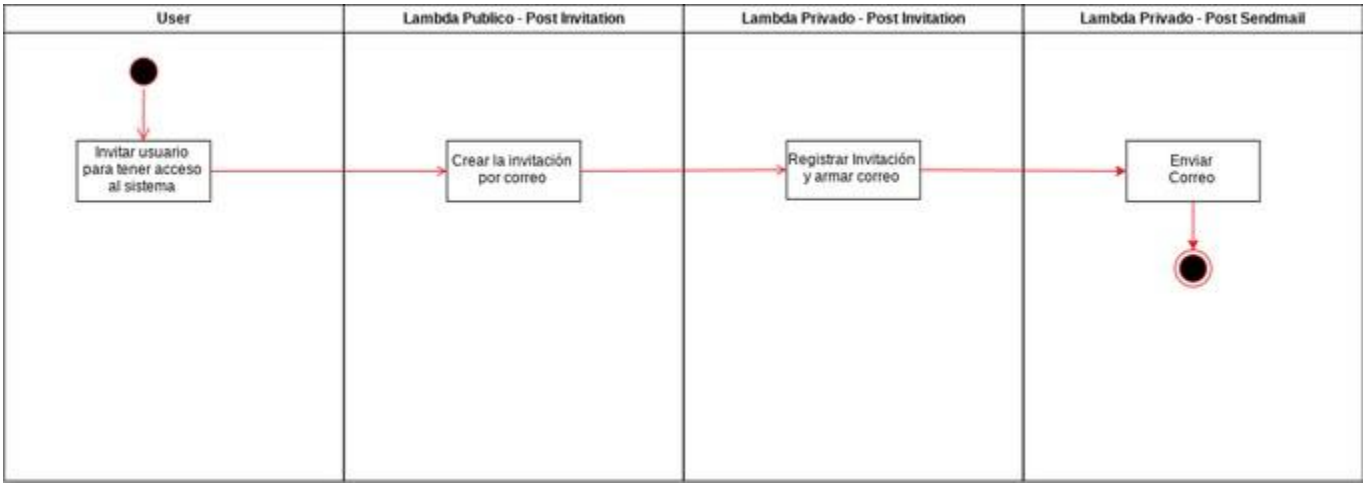


Segunda Autenticación

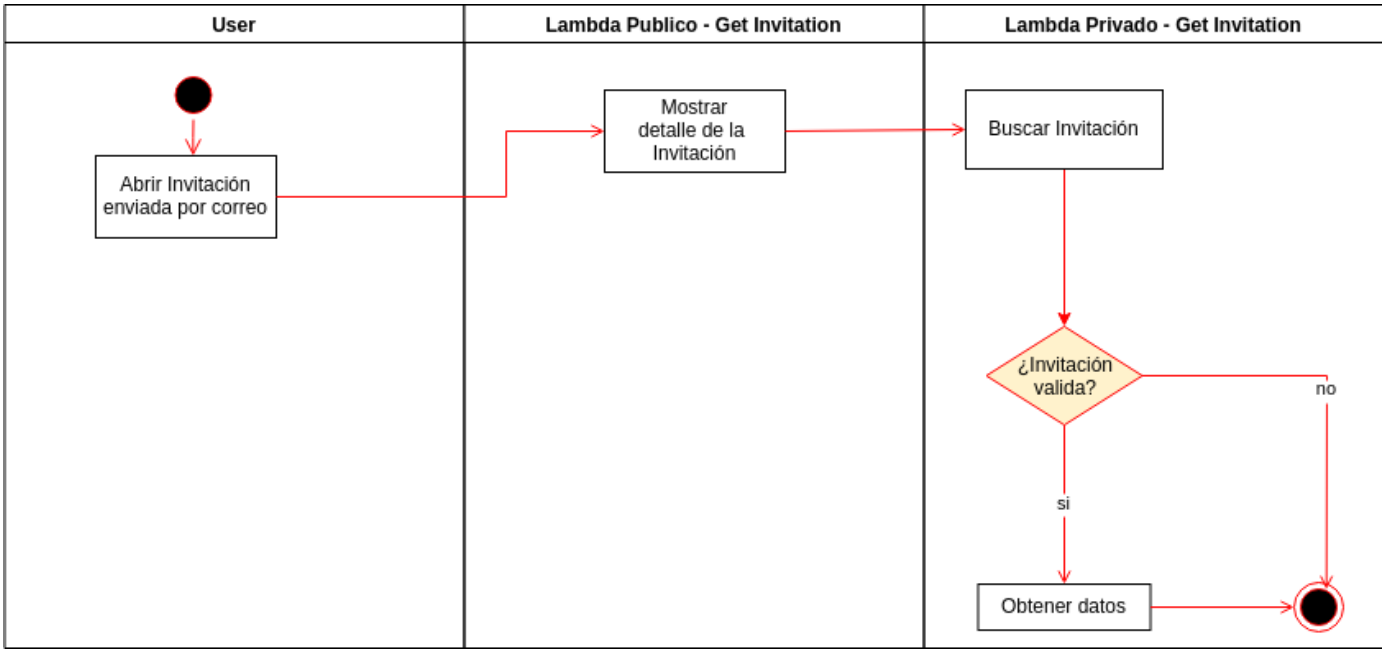


Invitaciones

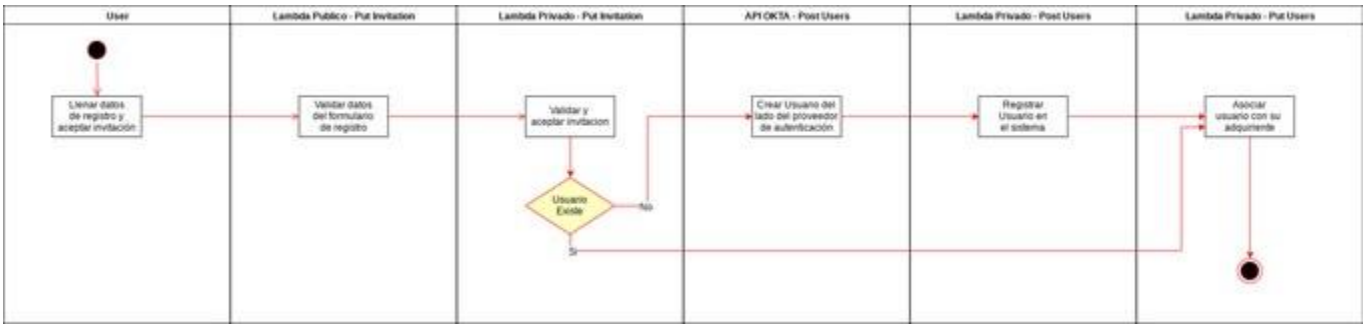
Invitar Usuario



Abrir Invitación

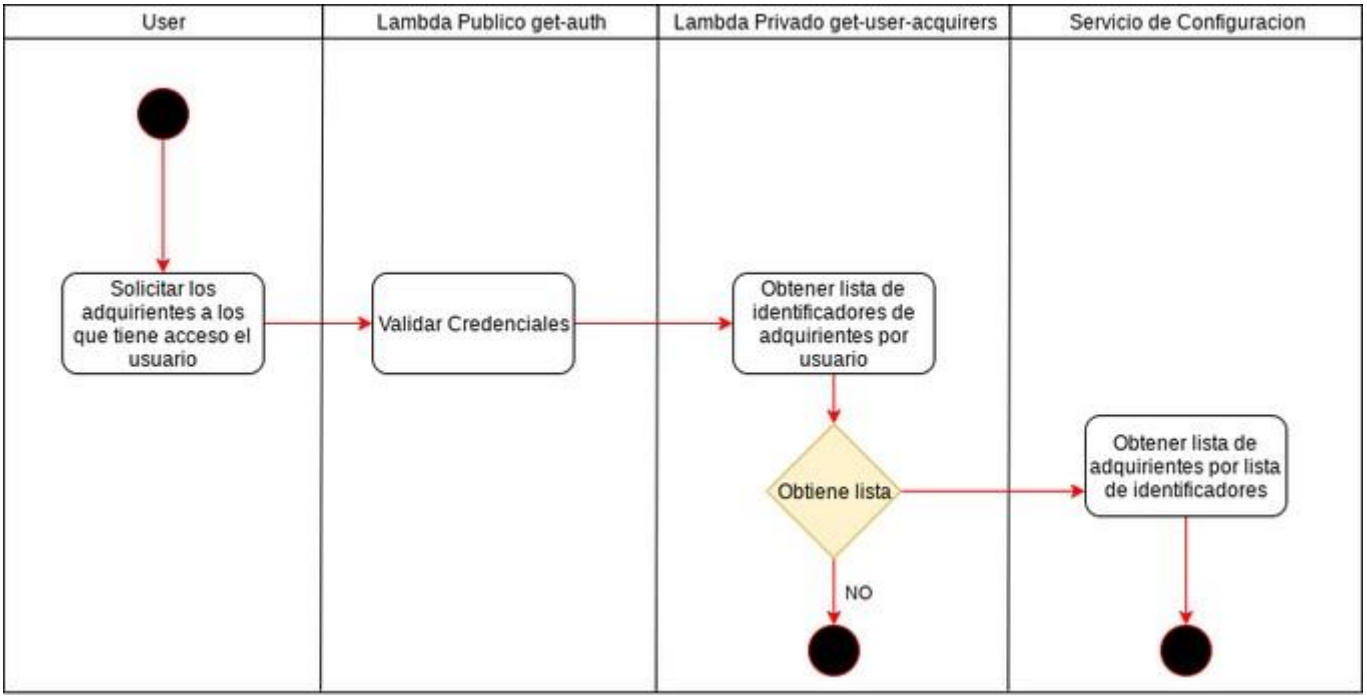


Aceptar Invitación

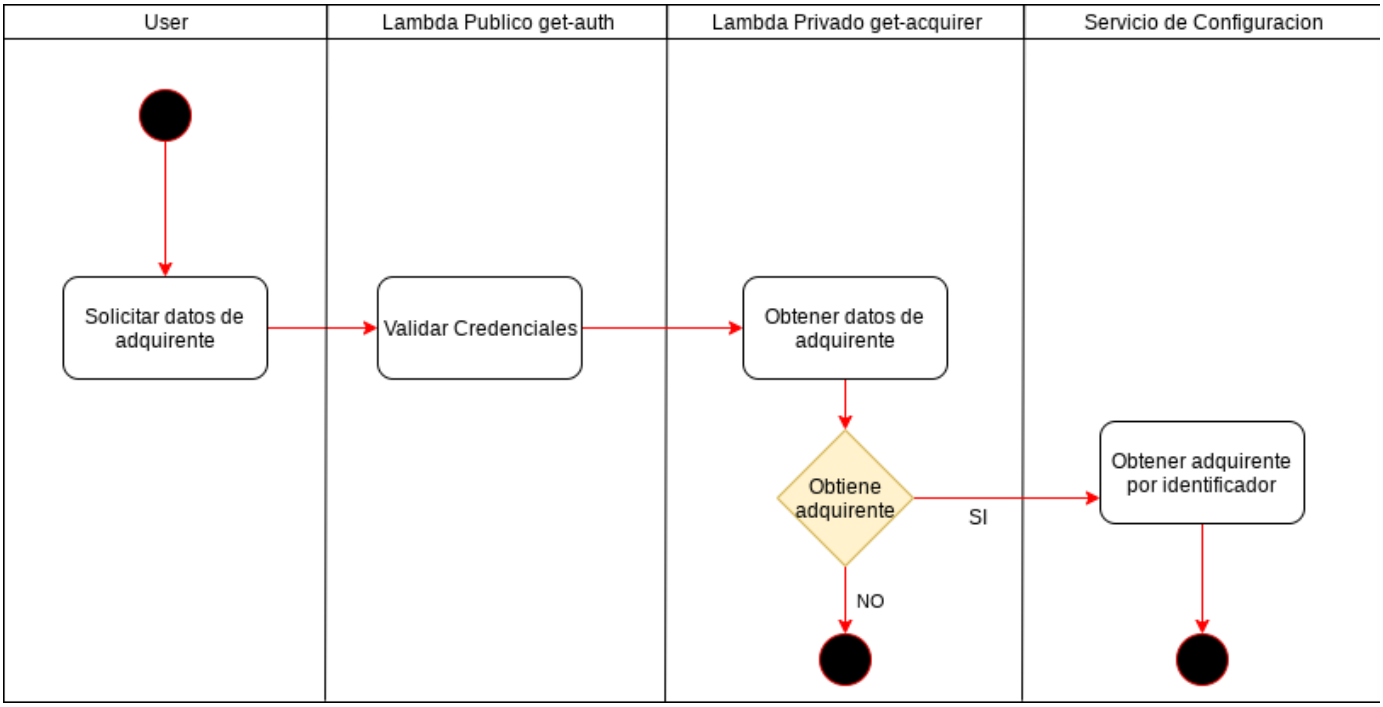


Adquiriente

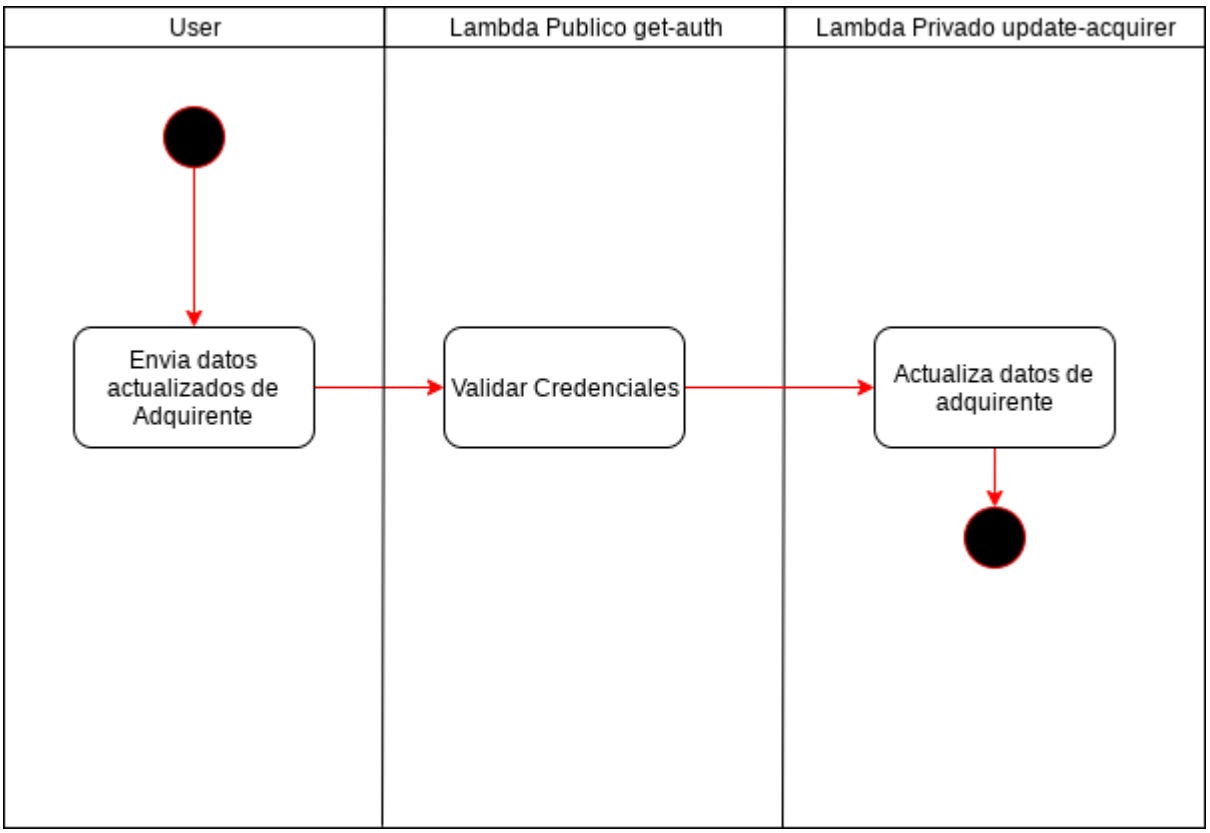
Obtener lista de adquirentes por usuario



Obtener datos de adquirente

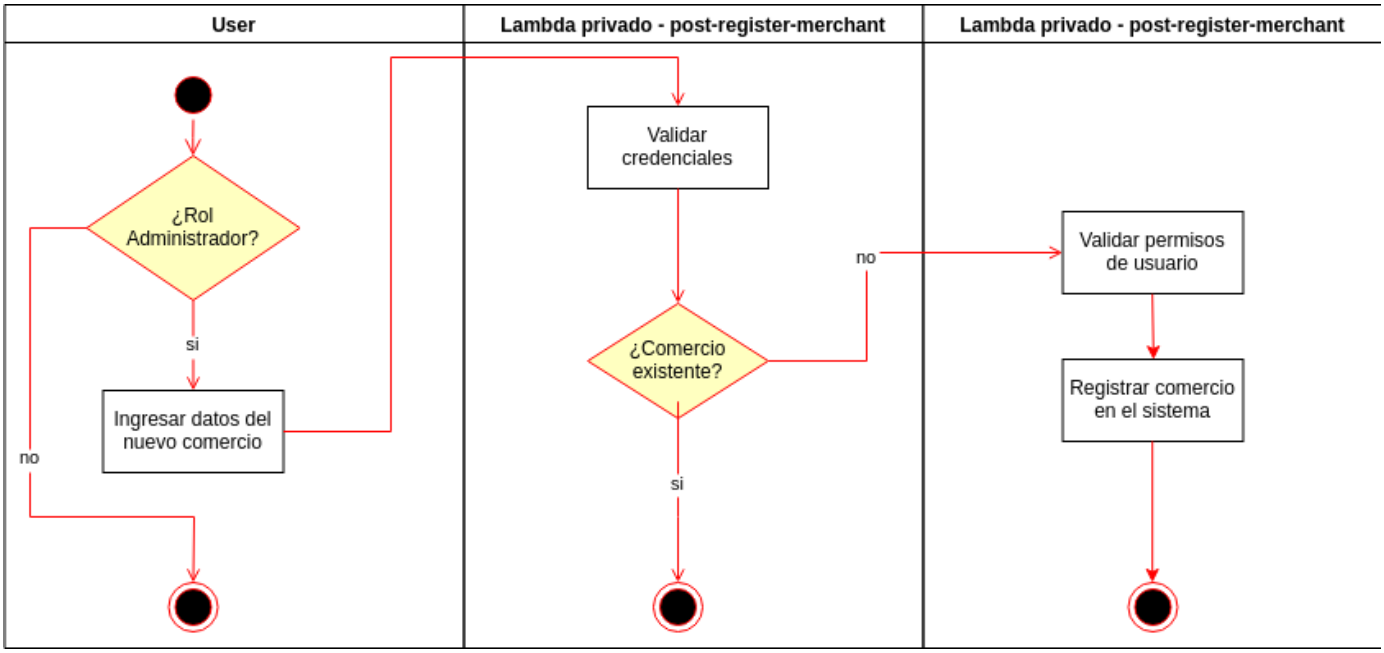


Actualizar adquirente

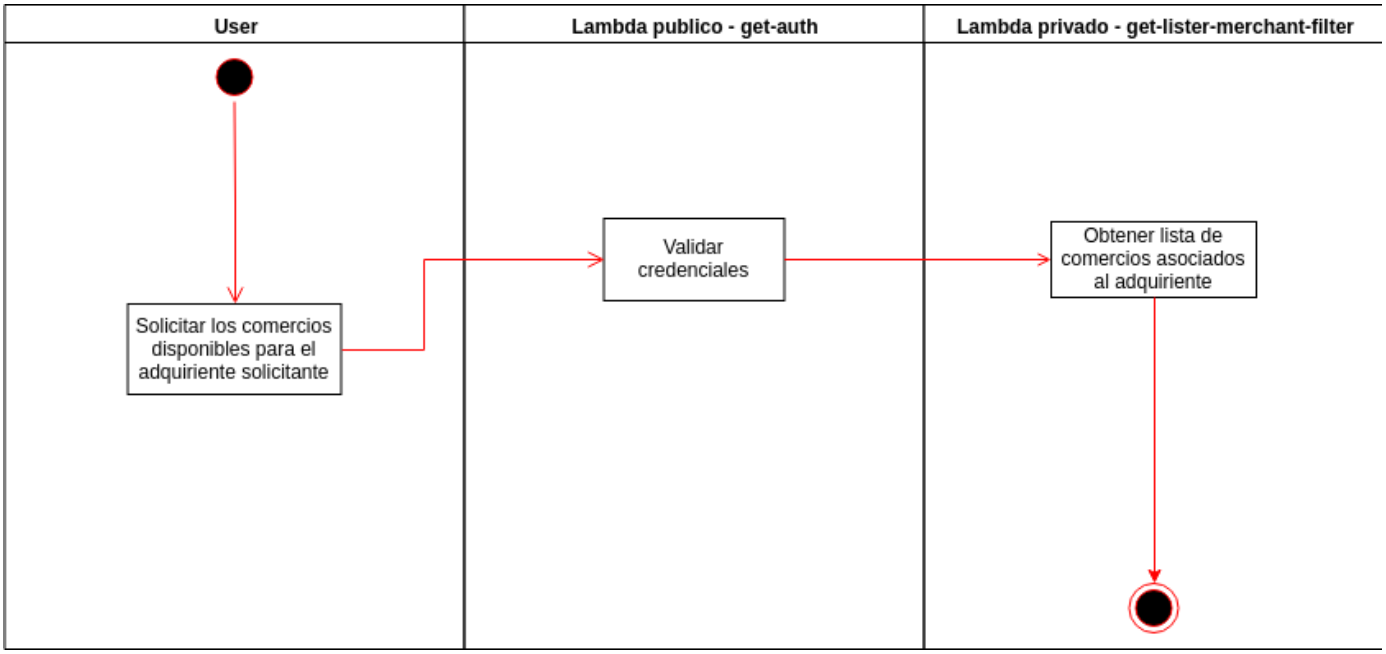


Comercio

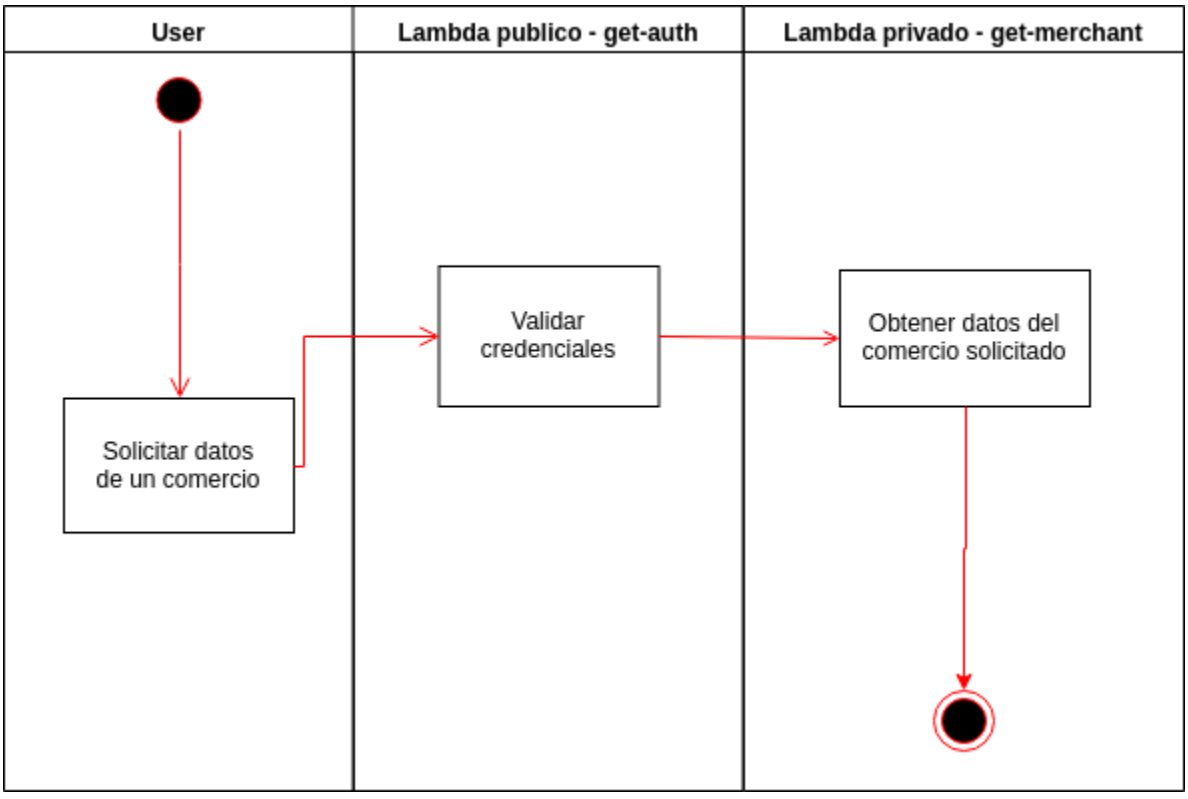
Registrar comercio



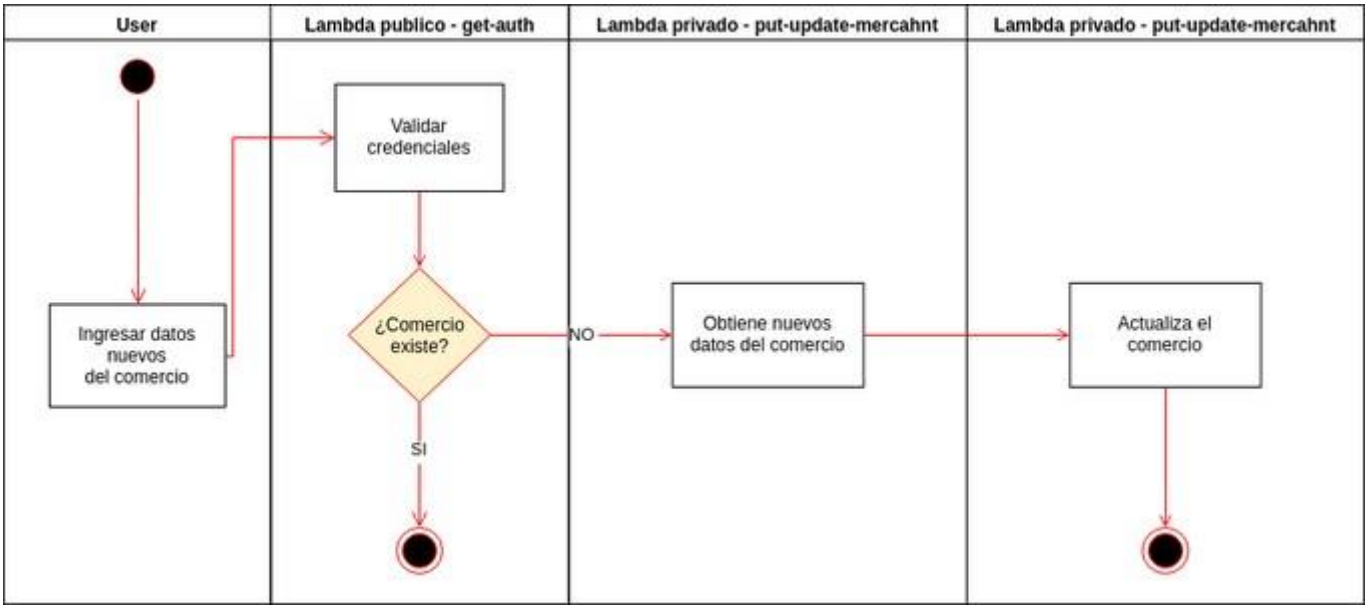
Listar comercio



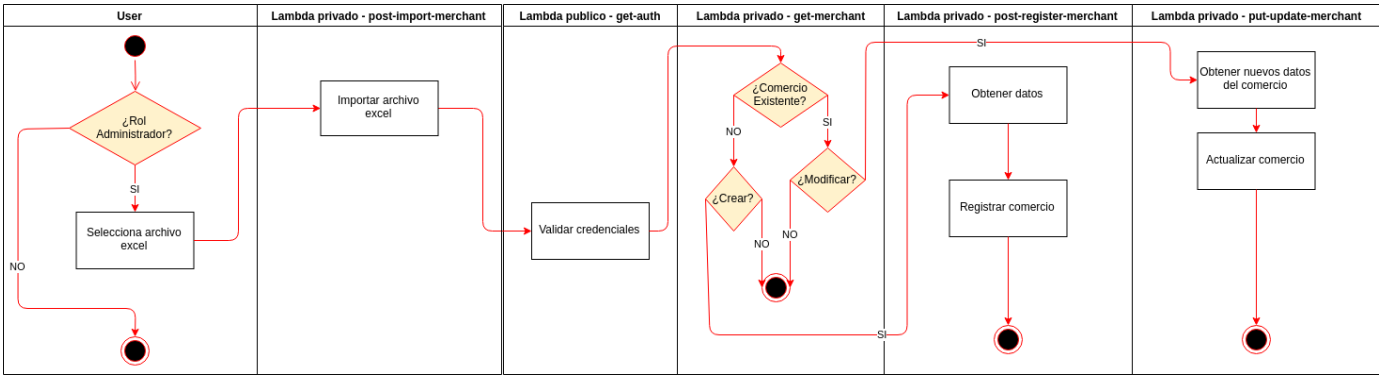
Obtener un comercio



Actualizar datos del comercio

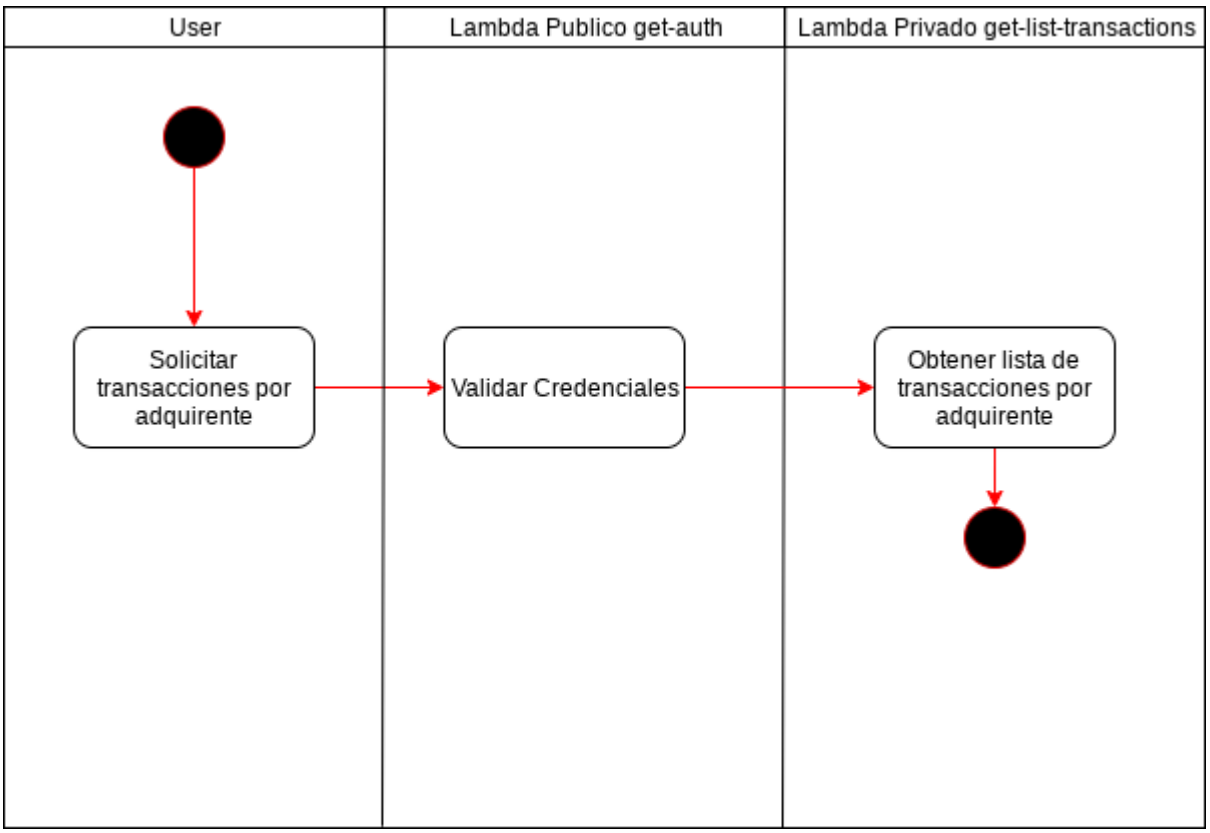


Carga masiva de comercios

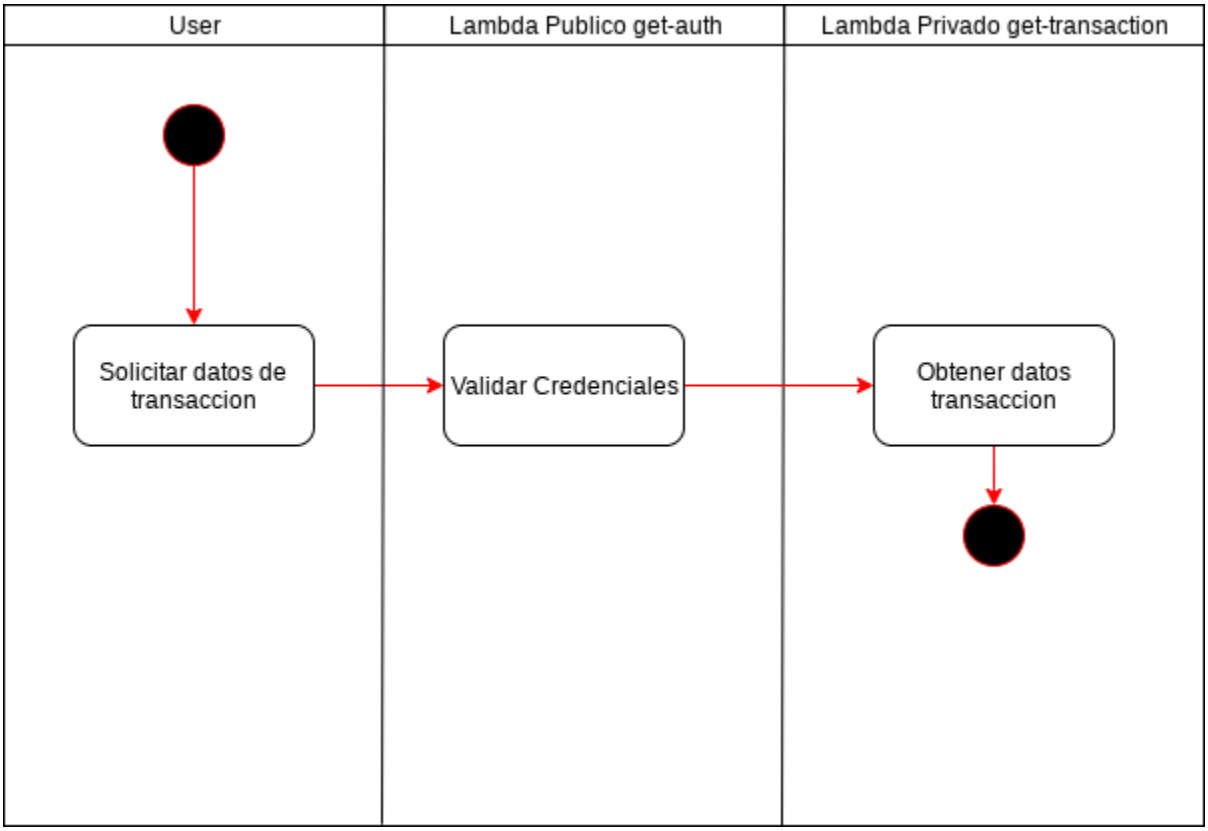


Transacciones

Obtener lista de transacciones por adquirente

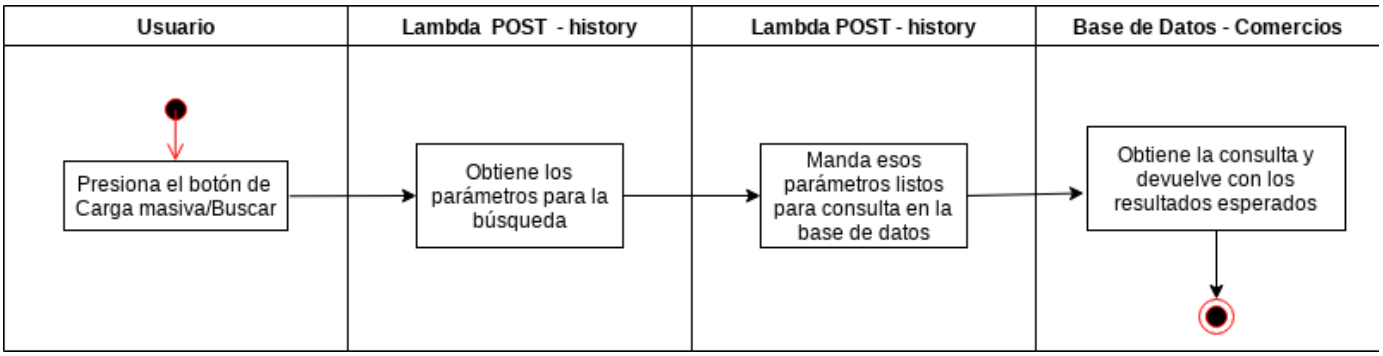


Obtener datos de transacción

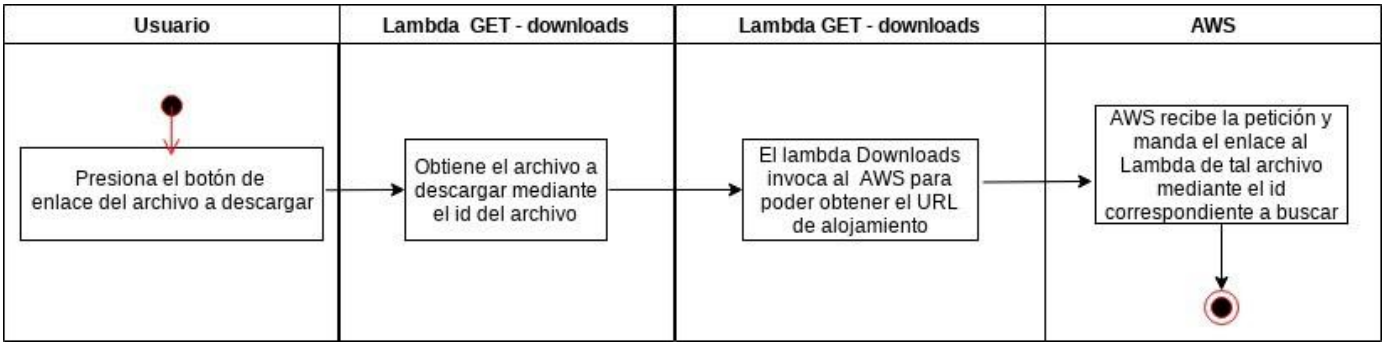

User
Lambda Publico get-auth
Lambda Privado get-transaction
Solicitar datos de transaccion
Validar Credenciales
Obtener datos transaccion

Historial

Listar/Buscar archivos

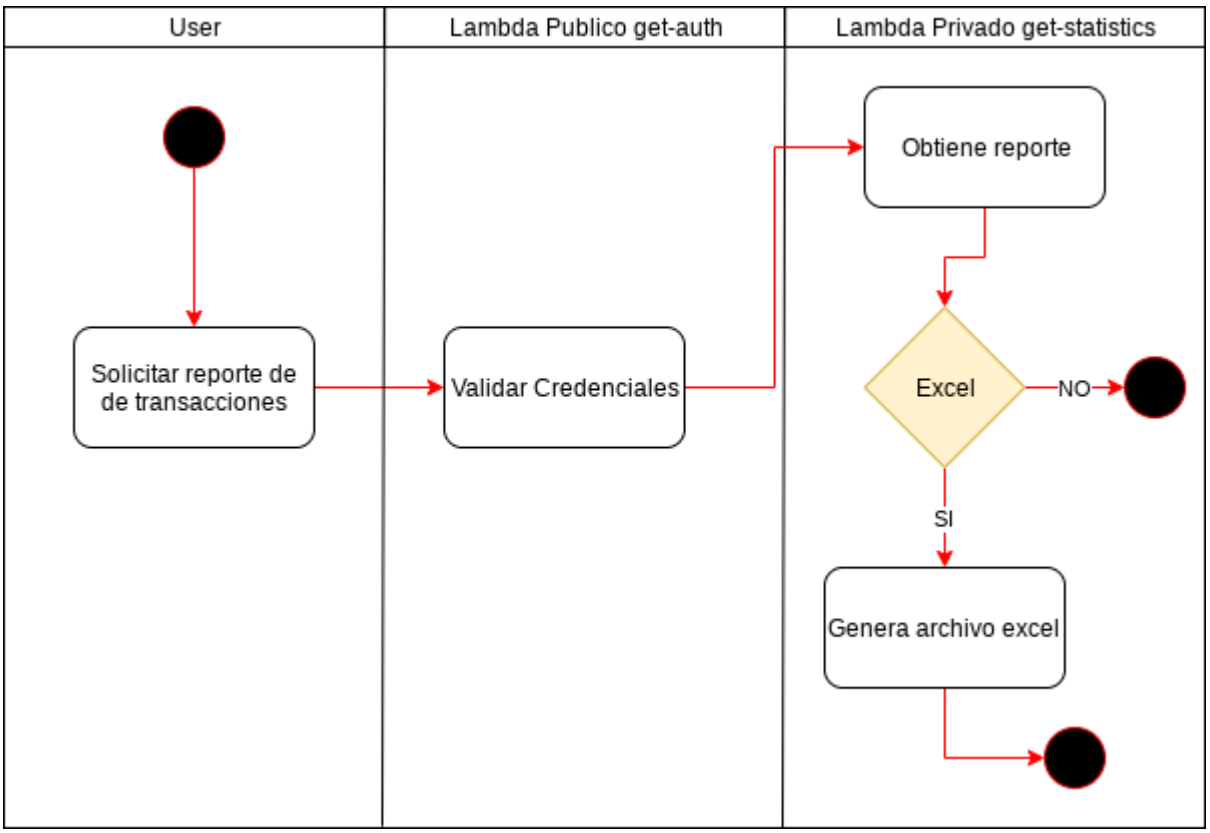


Descargar archivo



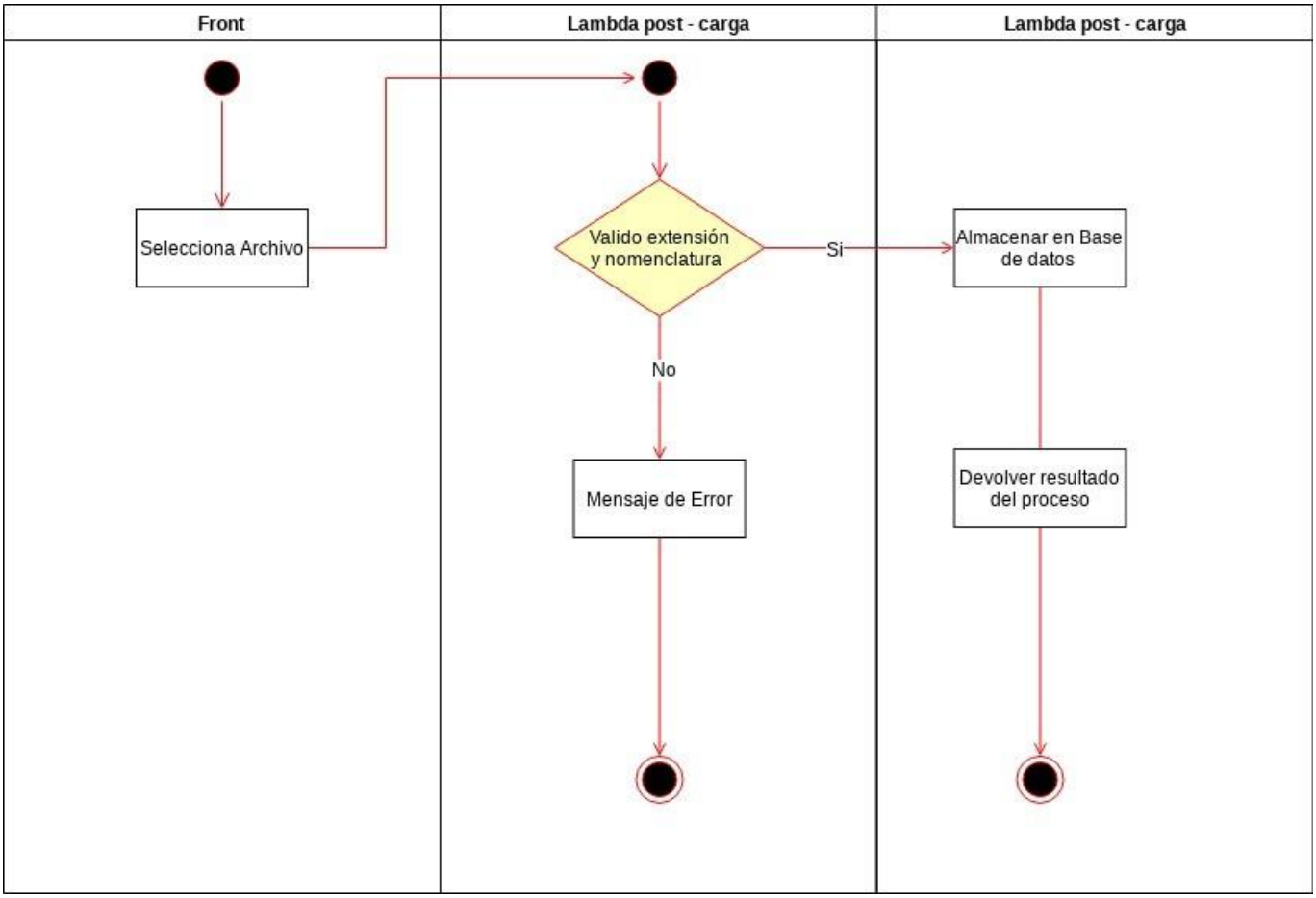
Estadísticas

Obtener reporte de transacciones



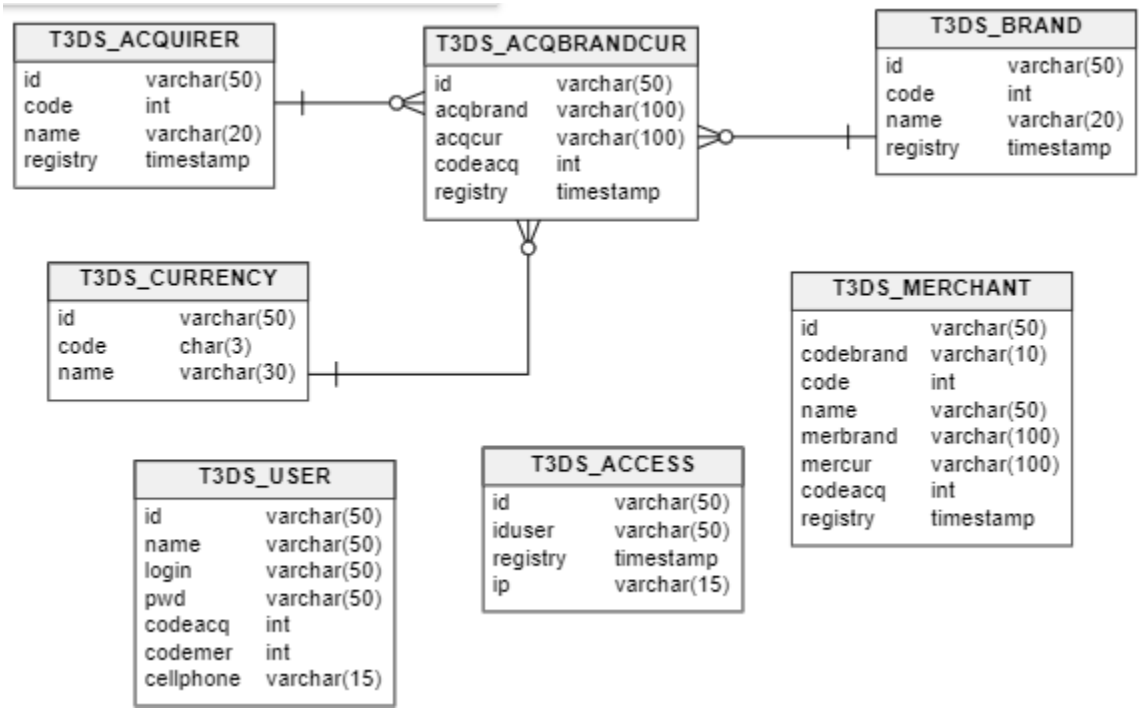
Registro

Cargar archivo


Front
Lambda post - carga
Lambda post - carga
Selecciona Archivo
Valido extensión y nomenclatura
Si
No
Mensaje de Error
Almacenar en Base de datos
Devolver resultado del proceso

RFC 063 - Modelo de Datos

La base de datos del SecureKey Server Manager estara conformada por data maestra y/o de configuraciones para las entidades como adquirentes y comercios.



Colecciones

T3DS_ACQUIRER

Adquirentes

Column name	Type	Properties	Description
id	varchar(50)		identificador del registro
code	int		codigo que identifica al adquirente
name	varchar(20)		

registry	timestamp		Fecha y tiempo en que se realiza el registro

T3DS_BRAND

Registra las marcas soportadas por el protocolo

Column name	Type	Properties	Description
id	varchar(50)		Identifica al registro
code	int		Identifcador de la marca
name	varchar(20)		Nombre de la marca
registry	timestamp		Fecha y tiempo en que se realiza el registro

T3DS_CURRENCY

Registra las monedas segun ISO

Column name	Type	Properties	Description
id	varchar(50)		Identificador del registro
code	char(3)		Codigo numerico ISO que identifica a la moneda
name	varchar(30)		Nombre de la moneda

T3DS_MERCHANT

Registra los coemrcios afiliados al protocolo

Column name	Type	Properties	Description
id	varchar(50)		Identificador del regsitro
codebrand	varchar(10)		codigo del comercio ante la marca
code	int		Codigo que identifica al comercio
name	varchar(50)		Nombre del comercio
merbrand	varchar(100)		Relacion de marcas asociadas al comercio
mercur	varchar(100)		Relaciona las monedas configuradas para el comercio
codeacq	int		Identifica al adquirente al que

			pertence el comercio
registry	timestamp		Fecha y tiempo en que se realiza el registro

T3DS_ACQBRANDCUR

Registra la relacion de los adquirentes con las marcas y monedas que tienen configurados

Column name	Type	Properties	Description
id	varchar(50)		Identificador del registro
acqbrand	varchar(100)		Relacion de marcas asociada a la marca
acqcur	varchar(100)		Relacion de monedas asocidas al adquirente
codeacq	int		Codigo que identifica al adquirente
registry	timestamp		Fecha y tiempo en que se realiza el registro

T3DS_USER

Registra los usuarios que tendran acceso al SKSM

Column name	Type	Properties	Description
id	varchar(50)		Identificador del resgistro
name	varchar(50)		Nombre del usuario
login	varchar(50)		Login de acceso al SKSM. Este valor debe corresponder con la cuenta de un mail
pwd	varchar(50)		Clave de acceso al SKSM
codeacq	int		Codigo que identifica a un adquirente al que pertenece el usuario
codemer	int		Codigo que identifica a un comercio al que pertenece el usuario
cellphone	varchar(15)		

T3DS_ACCESS

Registra los accesos realizados por el usuario al SKSM

Column name	Type	Properties	Description
id	varchar(50)		Identofocador
iduser	varchar(50)		
registry	timestamp		Fecha y tiempo en que se realizo el acceso
ip	varchar(15)		Direccion IP desde

			donde se accede

RFC 063 - Modelo de datos del sac

Base de Datos SCM_Service Colección User

- Colección Recovery Colección Invitation Colección Factors Colección Blocking Colección Attempts Colección Issuer_User

Base de Datos SCM_Service

Colección User

Se registra información sobre el usuario.

Nombre de campo	Tipo de dato	Descripción
email	String	Email del usuario.
id_user	String	Identificador del usuario que se registra en Okta.
firstName	String	Nombre del usuario.
lastName	String	Apellido del usuario.
type_country	String	Código telefónico de la región.
country	String	País del usuario.
phone	String	Número de celular del usuario.
state	String	Estado del usuario, si esta habilitado o deshabilitado.
audit_attributes	Object	Campos de auditoría.
audit_attributes.created_at	Double	Fecha de creación del usuario.
audit_attributes.updated_at	Double	Fecha de modificación de los datos del usuario.
audit_attributes.edited_by	String	Autor de la modificación de los datos del usuario.
image_url	String	Enlace de la imagen de perfil del usuario.
image	String	Imagen de perfil del usuario codificada en Base64.
created_at	Double	Fecha de creación del usuario.

edited_by	String	Autor de la modificación de los datos del usuario.
updated_at	Double	Fecha de modificación de los datos del usuario.

Colección Recovery

Se registra información cuando el usuario olvida o quiere recuperar su contraseña.

Nombre de campo	Tipo de dato	Descripción
action	String	Nombre de la acción que se realiza.
recovery_code	String	Código autogenerado para el permiso de cambio de contraseña.
email	String	Email del usuario.
expiration_date	Double	Fecha de expiración del código de recuperación de contraseña.
state	String	Estado del código de recuperación de contraseña.

Colección Invitation

Se registra información sobre las invitaciones que realiza el usuario a otros usuarios.

Nombre de campo	Tipo de dato	Descripción
id_user	String	Identificador del usuario que fue registrado en Okta y que realiza la invitación.
invitation_code	String	Código autogenerado para el permiso de registro de usuario.
email	String	Email del usuario.
issuer-key	String	Código identificador del emisor.
role	String	Rol que se le asignará al usuario.
invitation_date	Double	Fecha de la invitación.
expiration_date	Double	Fecha de expiración de la invitación.
cancellation_date	Double	Fecha de cancelación de la invitación.
association_date	Double	Fecha de asociación entre el usuario y el emisor.
state	String	Estado de la invitación.

Colección Factors

Se registra información sobre el segundo factor de autenticación (OTP).

Nombre de campo	Tipo de dato	Descripción
tokensesion	String	Token de la sesión del usuario.
code	String	Código OTP de seis dígitos.
expiry_date	String	Fecha de expiración del código OTP.
type_send	String	Medio por el que se envía el

		código OTP.
email	String	Email donde se envía el código OTP.
phone	String	Número de celular donde se envía el código OTP.

Colección Blocking

Se registra información sobre los usuarios bloqueados por exceder los intentos permitidos.

Nombre de campo	Tipo de dato	Descripción
username	String	Email del usuario bloqueado.
time	Double	Fecha que el usuario fue bloqueado.

Colección Attempts

Se registra información de los intentos de inicio de sesión que realizó el usuario.

Nombre de campo	Tipo de dato	Descripción
username	String	Email del usuario que intentó iniciar sesión.
password	String	Contraseña que se usó para intentar iniciar sesión.
options	Object	
options.multiOptionalFactorEnroll	Boolean	
options.warnBeforePasswordExpired	Boolean	

Colección Issuer_User

Se registra información de la relación que existe entre el emisor y el usuario.

Nombre de campo	Tipo de dato	Descripción
id_user	String	Identificador del usuario que fue registrado en Okta.
issuer-key	String	Código identificador del emisor.
role	String	Rol que se le asigna al usuario.
state	String	Estado del usuario ante el emisor.