konecta

ISO 9001
BUREAU VERITAS
Certification

INFORME DE SERVIDOR CENTRALIZADO DE AUTENTICACIÓN Y ORQUESTADOR DE SERVICIOS

CONTRATO DE PRÉSTAMO BID N° 4526 PC-PR - PROGRAMA DE GESTION DE RIESGO EN SANIDAD ANIMAL (PR-L1148)
SERVICIO DE DIGITALIZACION DE TRAMITES

ABRIL 2023

SENACSA

Índice

Índice 1
Introducción 3
Objetivos del proyecto 3
Servidor de Autenticación Centralizado 4
Actividades 4
¿Qué es el autenticador? Alcance. 4
¿Qué es el Keycloak? 4
¿Qué es OpenID Connect? 4
Esquema de Despliegue 4
Infraestructura como código 5
docker-compose.yml 6
Versionado 7
Orquestador de Servicios Web 8
Funcionalidades del Orquestador de Servicios Web 10
Actividades 10
Resultados parciales 11
Pila (stack) tecnológica 11
Adaptación de trámites 12
Conjunto de datos: Personas físicas y Jurídicas 12
Descripción de adaptaciones 12
Conjunto de datos: Establecimientos Ganaderos 13
Descripción de adaptaciones 13
Conjunto de datos: Marcas 13
Descripción de adaptaciones 13
Conjunto de datos: Casas Expendedoras 14
Descripción de adaptaciones 14
Conjunto de datos: Centro de Distribución 14
Descripción de adaptaciones 14
Conjunto de datos: Establecimiento Registro 14
Descripción de adaptaciones 14
Conjunto de datos: Sucursales FUNDASSA 14
Descripción de adaptaciones 14
Capturas de las adaptaciones y modificaciones 15
ANEXO 1: Manual técnico - Autenticador Único 21
Sistema de Administración del Keycloak 22
Realm Settings 22
Login 22
Email 23
Themes 24
Tokens 24
Clients 25

Client adapters 26
OpenID Connect 26
Java Adapters 26
JBoss EAP/WildFly Adapter 26
Add Client 26
Editar Client 27
User Federation 29
User 30
Referencias 31

Objetivos del proyecto

Este proyecto tiene por objetivo principal fortalecer el objetivo inicial del proyecto de Digitalización de Trámites que enuncia *"Implementar la digitalización de trámites que el SENACSA brinda a sus usuarios"*. Este fortalecimiento se basa en los objetivos específicos de:.

- *Centralizar la gestión de identidad de los sistemas de SENACSA.*
    - Implementar una plataforma centralizada de gestión de identidad, de manera a estandarizar los eventos de autenticación de usuarios de sistemas de SENACSA.
- *Implementar una plataforma de orquestación de servicios para la interacción de sistemas.*
    - Ejecutar iniciativas alineadas con políticas de gobierno de datos, implementando mecanismos estándares para el adecuado intercambio de información entre sistemas.

De manera a capitalizar el conocimiento adquirido por el equipo técnico de Konecta en la primera fase del proyecto, los principales hitos de las iniciativas enmarcadas dentro del presente proyecto son:

- **Análisis de brecha para adaptaciones:** Los trámites digitalizados dentro del alcance del proyecto de Digitalización de Trámites, serán adaptados para su interacción con el sistema SIGOR. Se deberá establecer de manera detallada y específica las acciones a realizar en el marco de adaptaciones de los trámites construidos.
- **Configuración:** Existen componentes estandarizados que serán implementados y así también, los sistemas actuales serán evolucionados para construir capas configurables que les permita una implementación escalable de las soluciones a implementar en cuanto a autenticación e integración de servicios web.
- **Adaptación:** Una vez identificadas y documentadas las adaptaciones, el equipo de desarrollo deberá implementar adaptaciones a los paquetes de software generados, para interactuar con el sistema SIGOR a través del módulo de orquestación de servicios.
- **Integración:** Los diferentes conjuntos de datos deberán ser diseñados de manera a que sean compatibles con los diferentes usos que los sistemas podrán dar.
- **Implementación:** El equipo técnico acompañará la implementación de los productos en los diferentes ambientes.
- **Capacitación:** El equipo de UTIC será debidamente capacitado para la operación, evolución y soporte de los diferentes paquetes de software a ser implementados.

Servidor de Autenticación Centralizado

Actividades

- Identificación de necesidades de SENACSA para la gestión centralizada de identidad de sistemas internos.
- Instalación y configuración del servidor KeyCloak en infraestructura de SENACSA en ambientes de desarrollo, homologación y producción, en función a las necesidades identificadas.
- Implementación de funcionalidades como autenticación, cambio de contraseña y creación de usuarios.
- Configuración de políticas de contraseñas.

- Documentación técnica de administración del servidor.

¿Qué es el autenticador? Alcance

El autenticador es un software especializado en la centralización de la gestión del acceso a múltiples sistemas independientes.
En cuanto al alcance, la plataforma solo se encargará de la autenticación de los sistemas, el control de acceso deberá ser gestionado por cada sistema en base a sus reglas de acceso.
En base a las especificaciones técnicas del proyecto, se decidió utilizar un software muy popular en el área conocido como Keycloak.

¿Qué es el Keycloak?

El keycloak es un software open source que ofrece varios servicios relacionados a aspectos de seguridad necesarios en cualquier sistema web. El mismo tiene soporte para ser utilizado con los gestores de base de datos más utilizados, e implementa un conjunto amplio de servicios referentes a requisitos básicos de seguridad.

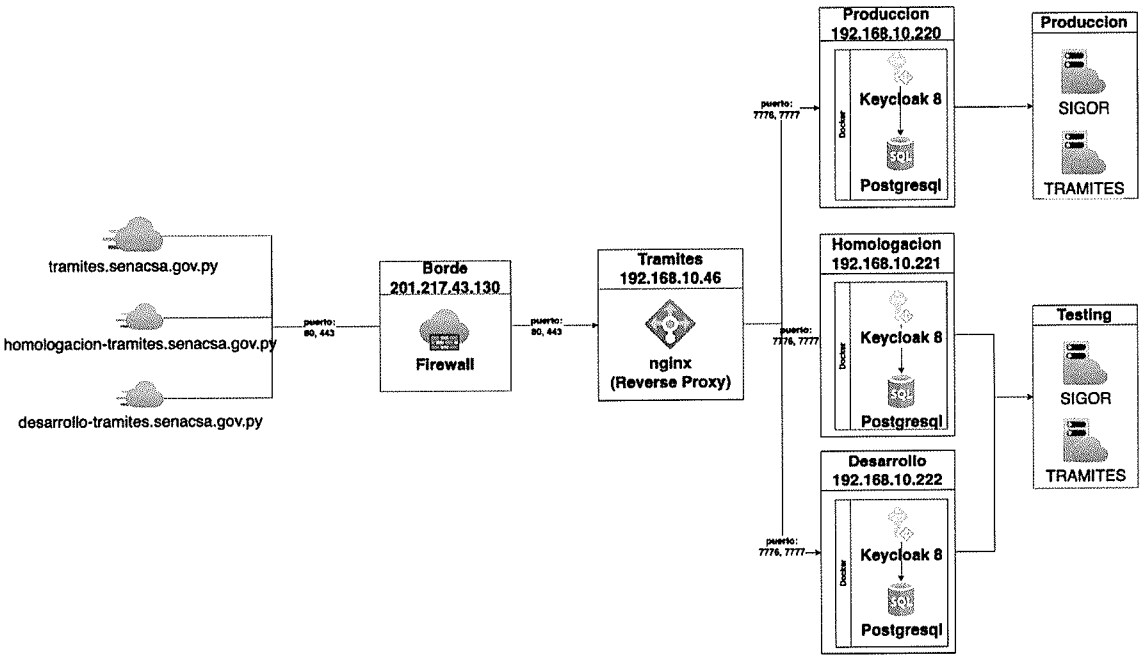
¿Qué es OpenID Connect?

Es un protocolo de autenticación y autorización basado en OAuth 2.0, le añade una capa adicional de seguridad, mediante la inclusión de información adicional del usuario y la utilización de tokens JWT (JSON Web Tokens).
Es uno de los protocolos ofrecidos por Keycloak para proveer los servicios de autenticación y autorización.
Este protocolo es el seleccionado para este proyecto para proveer el servicio de autenticación, pero no para el servicio de autorización, puesto esto quedará a cargo de cada sistema que se desee integrar al autenticador.

Esquema de Despliegue

Para el despliegue del autenticador hemos utilizado un esquema de contenedores, puesto que teníamos que mantener 3 entornos totalmente independientes. Un entorno de producción, uno de homologación y uno para desarrollo. Cada entorno debe contar con su propia base de datos y sus configuraciones totalmente independientes.

Para la gestión de contenedores hemos decidido utilizar Docker.



Infraestructura como código

La Infraestructura como Código es el proceso de gestionar y provisionar recursos de infraestructura de TI mediante código, en lugar de realizarlo manualmente, lo que permite una mayor eficiencia, consistencia y automatización en la gestión de la infraestructura.
Para codificar la infraestructura como código hemos decidido utilizar docker-compose. El autenticador se encuentra instalado en el directorio "/opt/kc8-sigor", teniendo la siguiente estructura de directorios.

```
[admin@AutenticadorProduccion kc8-sigor]$ ll
total 8
-rw-r--r--.  1 root    root 1765 Mar 24 11:[illegible] docker-compose.yml
drwxr-xr-x.  3 root    root   92 Mar 24 11:[illegible] etc
drwxr-xr-x.  2 root    root   40 Feb  3 11:33 jdbc
drwx------. 19 polkitd root 4096 Mar 24 11:25 pg_data
drwxr-xr-x.  4 root    root   32 Feb  3 11:33 senacsa
```

1. docker-compose.yml: Archivo donde se encuentra codificada toda la infraestructura necesaria para que corra el autenticador.
2. etc: Directorio donde se guardan algunos archivos de configuración específicos para nuestros proyectos.
3. jdbc: Carpeta que tiene la librería que el keycloak necesita para conectarse a la base de datos. En este caso se utiliza una base de datos PostgreSQL.
4. pg_data: Carpeta donde se persisten los datos del PostgreSQL. En esta carpeta se guardan todos los datos de la base de datos. Un posible procedimiento de backup podría

ser cada cierto tiempo guardar un comprimido de esta carpeta en algún dispositivo externo.

5. senacsa: Carpeta donde se guarda todo lo referente a la apariencia del login y otras pantallas vistas por el usuario. En el futuro si se desea cambiar la apariencia del login, habría que entrar a modificar los archivos en esta carpeta.

docker-compose.yml

Este es el archivo en formato yaml donde se define todas las especificaciones que tendrá la infraestructura que desplegará el sistema. El mapeo de puerto, la configuración de la base de datos, orden de despliegue de los servicios, mantener siempre arriba el servicio en caso de reinicio del sistema operativo, etc.

```
version: '3'

services:
  postgres:
    image: postgres
    restart: always
    volumes:
      - ./pg_data:/var/lib/postgresql/data
      - ./etc/init.sh:/docker-entrypoint-initdb.d/init.sh
    environment:
      POSTGRES_DB: keycloak
      POSTGRES_USER: [redacted]
      POSTGRES_PASSWORD: [redacted]
      TZ: America/Asuncion
    ports:
      - 5432:5432
  keycloak:
    image: jboss/keycloak:8.0.1
    restart: always
    environment:
      DB_VENDOR: POSTGRES
      DB_ADDR: postgres
      DB_DATABASE: keycloak
      DB_USER: [redacted]
      DB_SCHEMA: public
      DB_PASSWORD: [redacted]
      KEYCLOAK_USER: [redacted]
      KEYCLOAK_PASSWORD: [redacted]
      server-config: standalone.xml
      start-mode: normal
      PROXY_ADDRESS_FORWARDING: "true"
      TZ: America/Asuncion
      SIGOR35_URL: http://vader.sigor.gov.py:8580/Sigor-Seguridad-WS/rest/v1/
      SIGOR35_USER: [redacted]
      SIGOR35_PW: [redacted]
      USER_TELEF_COD: USER_NRO_TELEF
    volumes:
      - ./etc/standalone/configuration/application-roles.properties:/opt/jboss/keycloak/standalone/configuration/application-roles.properties
      - ./etc/standalone/configuration/application-users.properties:/opt/jboss/keycloak/standalone/configuration/application-users.properties
      - ./etc/standalone/configuration/standalone-senacsa.xml:/opt/jboss/keycloak/standalone/configuration/standalone.xml
      - ./etc/standalone/deployments/Sigor-SPI-WAR.war:/opt/jboss/keycloak/standalone/deployments/Sigor-SPI-WAR.war
      - ./jdbc:/opt/jboss/keycloak/modules/system/layers/base/com/oracle/jdbc/main/driver
      - ./senacsa:/opt/jboss/keycloak/themes/senacsa
    command: ["--start-mode","normal","-c","standalone.xml"]
    ports:
      - 7777:8443
      - 7778:8080
      - 7779:8009
    depends_on:
      - postgres
```

1. **Base de datos**: Se define la configuración inicial para el despliegue del servicio desde el arranque. En nuestro caso elegimos como base de datos PostgreSQL 15 en su última versión.
    1. **volumes**: se define el lugar en el sistema de archivo del sistema operativo anfitrión donde se guardarán todos los archivos referentes a los datos de la base de datos. Es donde se define que en la carpeta *pg_data* se guardaran los datos. También se define un script para la generación automática de la estructura de base datos

necesaria para correr un demonio que actualizará datos de forma automática en el SIGOR.

2. **environment**: Se definen variables de entornos que son utilizados por la imagen del contenedor para inicializar el servicio.

2. **Autenticador**: Se define la configuración inicial para el despliegue del servicio desde el arranque. Por cuestiones de compatibilidad con el SIGOR 3.5, se eligió el Keycloak 8.0.1.
    1. **volumes**: Esta versión del Keycloak corre utilizando como base el servidor de aplicaciones Wildfly, por lo que la estructura de directorios como los archivos de configuración son los mismos que tiene el servidor de aplicaciones. En esta configuración se definen el lugar en el sistema de archivo del sistema operativo anfitrión donde se guardaran los principales archivos de configuración del Keycloak. A continuación detallamos el contenido de los principales archivos:
        1. ***Sigor-SPI-WAR.war***: Plugin del Keycloak desarrollado a medida del SIGOR, para soportar compatibilidad hacia atrás en la autenticación. Este plugin hace que sea transparente para el usuario final el cambio de procedimiento de autenticación. Anteriormente las credenciales se guardaban en la base de datos del SIGOR, actualmente se guardarán en la base de datos del autenticador. Este módulo también cuenta con el manejo de eventos dentro del Keycloak referentes al cambios de datos que puedan ser relevantes al sistema de terceros. Actualmente, en caso que cambie el correo, se tiene preparado para invocar un Web Service del SIGOR, pero se podría ampliar esto para publicar en una cola de datos que cualquier sistema se podría suscribir para gestionar los eventos de forma particular.
        2. ***standalone-senacsa.xml***: Archivo de configuración propio del Wildfly. Donde se definen todas las configuraciones del servidor de aplicaciones.
        3. ***senacsa***: carpeta donde se guarda el código referente a la apariencia de la página de login que es mostrado por keycloak.
    2. **environment**: Se definen las credenciales que el keycloak utilizará para conectarse a la base de datos, como también otras variables de entornos que son utilizadas para la correcta interacción con el SIGOR.

Versionado

El tener la infraestructura como código, nos permite tener un versionado de los cambios en la infraestructura. Para esto hemos utilizado Git, y toda la estructura del directorio se encuentra versionado, a excepción de la carpeta *pg_data*, puesto que ahí se guardan datos sensibles y además el tamaño podría aumentar considerablemente.

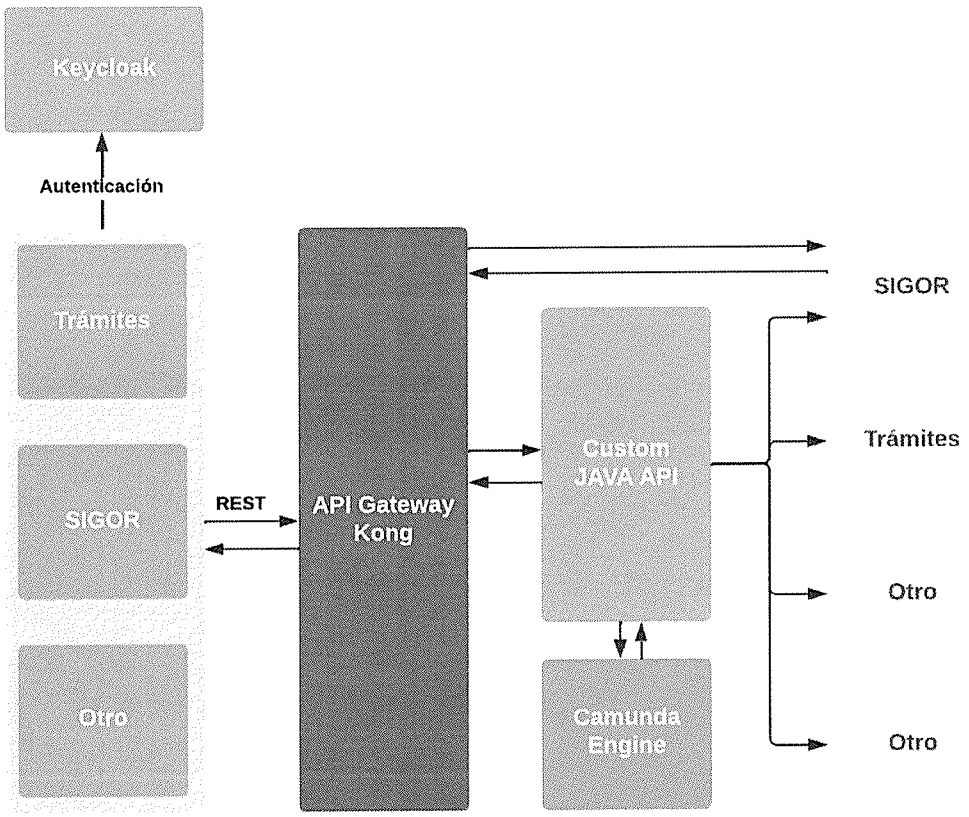
En los tres entornos se encuentra versionado la estructura de directorio.

Orquestador de Servicios Web

Para realizar la integración con los servicios externos se implementó una arquitectura que permita una fácil escalabilidad a futuro, la misma está integrada por diferentes capas comprendidas por:

Cliente: El cliente que realiza la petición inicial.

API Gateway: Un API Gateway que resuelva funcionalidades genéricas tales como autenticación, autorización y auditoría.
Keycloak: Es un autenticador centralizado que permite a los clientes mantener la información de credenciales en un único lugar, es utilizado por los clientes para autenticar a los usuarios..
Custom API: Una aplicación Java Spring Boot que personaliza las invocaciones recibidas por el API Gateway y se comunica con el Camunda Engine para ejecutar las integraciones de sistemas como procesos, de manera a brindar traza, control de reintentos y métricas de rendimiento. Provee la capacidad de paralelizar invocaciones de manera a aumentar el rendimiento y escalabilidad de la integración entre sistemas.
Camunda Engine: El complemento Camunda que actúa como el Workflow Engine y el Service Bus. Recibe las peticiones del Custom API, ejecuta los flujos asociados y dispara eventos que son gestionados por el Custom API.
Servicios: Los diferentes servicios de sistemas internos a interconectar (el alcance de esta fase del proyecto es la integración entre el SIGOR y trámites digitales) que son invocados por el Camunda Engine.



API Gateway (Puerta de Enlace de API)

Es un componente de software que actúa como punto de entrada para una colección de servicios web y/o microservicios. Esencialmente, el API Gateway es una capa de abstracción que se sitúa entre el cliente que consume la API y los servicios que proporcionan la funcionalidad.

El API Gateway proporciona una serie de beneficios, incluyendo la gestión centralizada de las peticiones de los clientes, la protección de los servicios subyacentes de posibles ataques externos, y la implementación de políticas de seguridad, autenticación y autorización. Además, también puede ofrecer funcionalidades de enrutamiento, transformación y composición de datos para simplificar el acceso a los servicios y mejorar el rendimiento.

Entre las funciones típicas que puede proporcionar un API Gateway se incluyen el enrutamiento de las solicitudes a los servicios correspondientes, la autenticación y autorización de los usuarios, el manejo de la memoria caché para reducir la carga de los servicios subyacentes, la agregación y transformación de los datos y la monitorización del tráfico y el rendimiento.

En este proyecto el API Gateway es utilizado para realizar las consultas a los servicios de SIGOR, aprovechando todos los beneficios comentados anteriormente. En algunas consultas se usa exclusivamente esta capa para consultas.

Para esta función se ha seleccionado Kong API Gateway que es una plataforma de gestión de API y microservicios de código abierto.

Kong ofrece una amplia gama de plug-ins para personalizar y ampliar la funcionalidad del API Gateway. Estos plugins incluyen capacidades de autenticación y autorización, como el uso de tokens de acceso y la integración con proveedores de identidad externos, así como la transformación y manipulación de datos,

Orquestador de servicios

Es un componente de software que coordina y gestiona la interacción entre varios servicios web para proporcionar una herramienta de gobierno sobre los mismos y consecuentemente, sobre la interacción entre los sistemas informáticos. La comunicación está basada en diferentes tecnologías web service (Rest, SOAP, etc) y transportadas sobre protocolo HTTP/HTTPS.

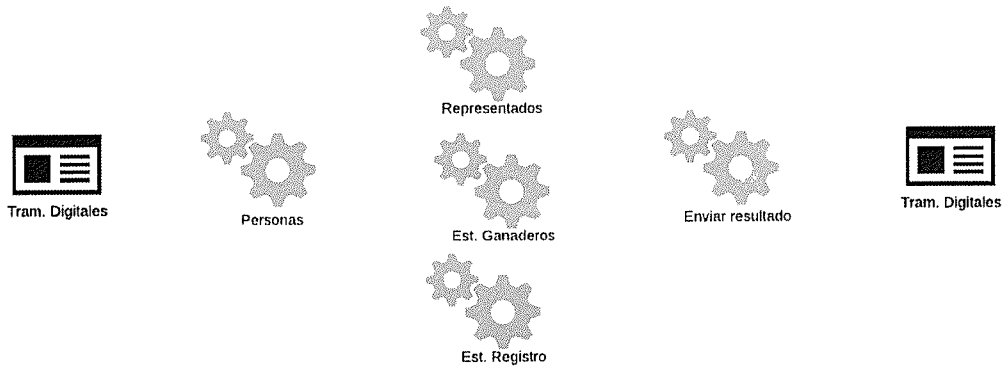
El orquestador de servicios web actúa como un intermediario entre los servicios, coordinando sus interacciones y asegurando que se cumplan los objetivos deseados. En lugar de interactuar directamente con cada servicio, los clientes interactúan con el orquestador, que a su vez interactúa con los servicios necesarios.

El alcance de la utilización del orquestador en este proyecto es el de automatizar la interacción entre los sistemas SIGOR y trámites digitales, sobre un grupo de "conjunto de datos" previamente definidos en el Informe 2 de este proyecto, y cuya documentación continúa siendo extendida en correspondencia con la construcción de las interacciones.

La Orquestación de servicios se ha implementado con Camunda que es una plataforma de automatización de procesos que ocupa con solvencia el rol de orquestación de servicios. Con su

motor de flujo de trabajo, motor de reglas de negocio, herramientas de monitoreo y análisis, y capacidad de personalización y extensión, Camunda es una opción sólida para los usuarios que buscan orquestar servicios en un entorno empresarial.

En la orquestación de servicios se ha implementado el patrón de desarrollo denominado *"Aggregation pattern"* que consiste en que el orquestador de servicios envía solicitudes a varios servicios secundarios y luego recopila y agrega las respuestas en una única respuesta para el cliente. Esto puede mejorar el rendimiento y la eficiencia en los sistemas distribuidos, ya que se pueden realizar varias solicitudes simultáneamente en lugar de una por una.



Este patrón se utiliza para obtener los datos de la persona, datos de sus representados y sus establecimientos del sistema SIGOR una vez que un usuario inicia sesión en Trámites Digitales. Esto se hace con el fin de recopilar estas informaciones y utilizarlas en los diferentes trámites disponibles en el sistema. Al utilizar este patrón, se garantiza que la información se obtenga y gestione de manera adecuada para su posterior uso en los trámites requeridos.

Funcionalidades del Orquestador de Servicios Web

- La solución está basada en tecnología Open Source y libre de costos de licencia.
- El orquestador de servicios expone un API de tipo REST a las aplicaciones (consumidoras) que deseen invocar servicios de otros sistemas a través del orquestador.
- Desde el orquestador de servicios será posible integrar a aplicaciones (productoras) mediante servicios web de tipo REST y SOAP.
- El API expuesto por el orquestador hacia las aplicaciones consumidoras está securizado por protocolos de seguridad de tipo Access Token.
- Desde el orquestador es posible invocar a servicios web de aplicaciones productoras que requieran de autenticación para invocar a su API.
- El orquestador soporta invocaciones a servicios web de forma asíncrona, para las peticiones síncronas se utiliza el API Gateway directamente.
- La capa de aplicación el orquestador soporta un modelo de deployment redundante de manera a garantizar la alta disponibilidad.
- La solución de orquestador no requiere de licencia de terceros para su óptimo funcionamiento.

Actividades

- Investigación y desarrollo sobre estado de arte de las principales técnicas, herramientas y componentes para interacción de micro servicios con arquitectura escalable.
- Diseño, pruebas de concepto, pruebas de laboratorio, adaptaciones y desarrollo de todos los componentes relevantes para la construcción de un orquestador de servicios web, implementable en SENACSA.
- Desarrollo de capas de servicios intermedias para recepción de solicitudes de sistemas desplegados en la infraestructura de SENACSA.
- Sesiones de trabajo con el equipo técnico de SIGOR y equipo técnico de trámites digitales.
- Sesiones de demostración de funcionamiento de trámite plenamente integrado al equipo UTIC.
- Conexión vía capa de servicios con el sistema SIGOR para la obtención de datos de dicho sistema.
- Instalación y configuración del orquestador de servicios en los ambientes de desarrollo, homologación y producción de SENACSA.
- Elaboración de documentación técnica parcial.

Resultados parciales

Entregable según plan de trabajo	Descripción
Documentación de estructuras de datos	Presentado en el informe 2.
Servidor instalado y configurado	El servidor centralizado se encuentra instalado y configurado en los ambientes de desarrollo, homologación y producción. Los sistemas SIGOR y trámites digitales se autentican mediante el servidor centralizado de autenticación.
Orquestador de Servicios Web	El orquestador de servicios se encuentra instalado y configurado en los ambientes desarrollo, homologación y producción.
Integración unidireccional con sistema SIGOR	El "Trámite 09: Solicitud de permisos a módulos de SIGOR" ha sido implementado con integración automática al orquestador de servicios.

Pila (stack) tecnológica

Actualmente los responsables de UTIC se encuentran elaborando una guía de pila tecnológica como parte de la estrategia de gobierno de TIC; sin embargo, se han relevado los siguientes tecnologías aprobadas:

- **Base de datos:** SQL Server, MySQL y PostgreSQL.

- **Lenguajes de programación:** Java y PHP.
- **Versionado de código:** No implementado.

En función a lo anterior, Konecta propone una pila tecnológica compatible y que pueda contribuir para la elaboración del documento interno de UTIC.

Tecnología seleccionada	Características y justificación
Java	Es uno de los lenguajes más utilizados mundialmente y el más adoptado para soluciones empresariales. En el país contamos con muchos profesionales capacitados y con experiencia en este lenguaje. El ecosistema de librerías, frameworks, etc es abundante y con opciones pagas y open source.
CAMUNDA	Es el mejor motor de BPM (Business Process Management) open source existente. Es una solución madura, muy robusta y con una comunidad de usuarios amplia.
PostgreSQL	Es la base de datos open source más robusta, es ampliamente difundida, madura y en constante evolución. Nuestra empresa cuenta en el país con experiencias de éxito en escenarios de uso muy demandantes.
WildFly	Es el servidor de aplicaciones Java Enterprise open source más difundido y maduro. Ofrece a las aplicaciones servicios de nivel empresarial para abstraer el manejo de transacciones de base de datos, cómputo concurrente, cómputo asíncrono, comunicación entre procesos y mucho más.
KEYCLOAK	Es una herramienta para gestión del acceso e identidad a las aplicaciones. Basado en licencias open source provee funcionalidades de federación, strong authentication, gestión de usuarios y autorización.
Swagger Supported by SMARTBEAR	Herramienta para promover la eficiencia en el desarrollo y documentación de API.
spring boot	Herramienta que brinda capacidad de construir módulos java stand-alone que brindan desacoplamiento y un entorno eficiente de construcción de microservicios.

Adaptación de trámites

Conjunto de datos: Personas físicas y Jurídicas

Descripción de adaptaciones

En función al número de documento de la persona solicitante, se consulta en el SIGOR las empresas (personas jurídicas) que tiene vinculadas en la base de datos de SIGOR.

Trámites que utilizan el conjunto de datos

1. TR01
2. TR03
3. TR04
4. TR05
5. TR08
6. TR09
7. TR10
8. TR11
9. TR14
10. TR15
11. TR18
12. TR19
13. TR24

Observación: En el trámite 09, en caso que este campo no retorne valores, se habilitó el campo **"Otra"** que permite a ingresar un número de RUC válido y el SIGOR retorna los datos de la empresa que está registrada en su base de datos, con dicha denominación y así se utiliza esta información en la solicitud.

Conjunto de datos: Establecimientos Ganaderos

Descripción de adaptaciones

En función al número de documento de la persona solicitante, se consulta en el SIGOR las personas físicas y jurídicas representadas por el mismo, luego se consultan los establecimientos ganaderos que tienen vinculadas éstas en la base de datos de SIGOR.

Trámites que utilizan el conjunto de datos

1. TR01
2. TR02
3. TR04
4. TR05
5. TR10
6. TR11
7. TR14
8. TR19
9. TR24

Conjunto de datos: Marcas

Descripción de adaptaciones

En función del número de boleta ingresado por el solicitante se consulta los datos relacionados en la base de datos de SIGOR.

Trámites que utilizan el conjunto de datos

1. TR18

Conjunto de datos: Casas Expendedoras

Descripción de adaptaciones

En función del número de habilitación de casa expendedora ingresado por el solicitante se consulta los datos de la misma en la base de datos de SIGOR.

Trámites que utilizan el conjunto de datos

1. TR09

Conjunto de datos: Centro de Distribución

Descripción de adaptaciones

En función del número de habilitación del centro de distribución ingresado por el solicitante se consulta los datos del mismo en la base de datos de SIGOR.

Trámites que utilizan el conjunto de datos

1. TR09

Conjunto de datos: Establecimiento Registro

Descripción de adaptaciones

En función al número de documento de la persona solicitante, se consulta en el SIGOR las personas físicas y jurídicas representadas por el solicitante, luego se consulta los establecimientos registro que tienen vinculadas éstas en la base de datos de SIGOR.

Trámites que utilizan el conjunto de datos

1. TR08
2. TR19

Conjunto de datos: Sucursales FUNDASSA

Descripción de adaptaciones

Se realiza una consulta del servicio que devuelve todas las sucursales de FUNDASSA en la base de datos de SIGOR..

Trámites que utilizan el conjunto de datos

1. TR09

Capturas de las adaptaciones y modificaciones

TR01 - Orden de trabajo para colecta de muestras de enfermedades y tuberculinización

En este trámite se utilizan los conjuntos de datos de Establecimientos Ganaderos y Personas físicas y jurídicas

1 - Orden de trabajo para colecta de muestras de enfermedades y tuberculinización.

Antes de realizar el pago de los diagnósticos, favor comunicarse al siguiente número (+595 21) 729 0015 para verificar la disponibilidad de los insumos.

Datos del establecimiento — Establecimientos Ganaderos

Establecimiento * | Departamento *

Distrito * | Localidad *

Código SIGOR *

Datos del propietario o solicitante — Datos de Personas físicas / jurídicas

Nombre * | Documento de identidad *

TR03 - Autorización para Exportación de Animales Vivos y Material Genético

En este trámite se utilizan los conjuntos de datos de Establecimientos Ganaderos y Personas físicas y jurídicas

3 - Autorización para exportación de animales vivos y material genético(embrión y semen).

Tipo de persona *

Datos del propietario — Datos de Personas físicas / jurídicas

Nombres * | Apellidos *

Cédula de identidad * | Departamento *

Distrito * | Localidad *

Dirección *

Teléfono/Fax * | Correo electrónico *

Tipo de envío * | Envío de carácter *

Procedencia

Establecimiento * | Código SIGOR — Establecimientos Ganaderos

TR04 - Habilitación de Establecimientos de Productos y Subproductos de Origen Animal / Registro de Empresa / Registro de Firma

En este trámite se utilizan los conjuntos de datos de Establecimientos Ganaderos y Personas físicas y jurídicas

4 - Habilitación de establecimientos de productos y subproductos de origen animal

Datos del establecimiento — Establecimientos Ganaderos

Establecimiento * | Departamento *

Distrito * | Localidad *

Código SIGOR *

Datos del propietario o solicitante — Datos de Personas físicas / jurídicas

Nombre * | Documento de identidad *

TR05 - Habilitación de Establecimientos Mataderos y Frigoríficos

En este trámite se utilizan los conjuntos de datos de Establecimientos Ganaderos y Personas físicas y jurídicas

5 - Habilitación de establecimientos mataderos y frigoríficos.

Tipo de persona *

Datos del propietario — Datos de Personas físicas / jurídicas

Nombres * | Apellidos *

Cédula de identidad * | Departamento *

Distrito * | Localidad *

Dirección *

Teléfono/Fax * | Correo electrónico *

Datos del establecimiento — Establecimientos Ganaderos

Establecimiento *

Departamento * | Distrito *

TR08 - Renovación de habilitación de Clínica, Peluquería, Consultorio Veterinario, Hospital Veterinario y Expendedoras de Productos Veterinarios

En este trámite se utilizan los conjuntos de datos de Establecimientos Registro y Personas físicas y jurídicas

8 - Renovación de habilitación de Clínica, Peluquería, Consultorio Veterinario, Hospital Veterinario y Expendedoras de Productos Veterinarios

Datos del establecimiento — Establecimientos Registro

Establecimiento *
Departamento *
Rubros del Establecimiento:
Distrito *
Localidad *
Telefono
Correo
Dirección *

TR09 - Solicitud de acceso a módulos del Sigor

En este trámite se utilizan los conjuntos de datos de Personas físicas y jurídicas, Datos de Casas Expendedoras y Datos de Centros de Distribución.

9 - Solicitud de acceso a módulos del Sigor

Datos Generales

Tipo de Acceso: *
[illegible]

Seleccione módulo:
[illegible]

Para solicitar Guia/Ceta Digital debe tener primero usuario en Guia Electronica o debe solicitar nuevos Guia Electronica y Guia/Ceta Digital

Nro. Habilitación Casa Expendedora * — Descripción Casa Expendedora * — Datos de Casa Expendedora

Nro. Habilitacion Centro Distribución * — Descripción Centro de Distribución — Datos de Centro de Distribución

Otros:

Datos de la empresa — Datos de Personas físicas / jurídicas

Empresa: *
RUC:
Representante Legal o vinculado: *
[illegible]
C.I Nro. Representante Legal o vinculado: *
[illegible]

TR10 - Habilitación de Local de Cuarentena

En este trámite se utilizan los conjuntos de datos de Establecimientos Ganaderos y Personas físicas y jurídicas

10 - Habilitacion de local de cuarentena.

Tipo Persona *

Datos del solicitante — Datos de Personas físicas / jurídicas

Nombre *

Documento de identidad *

Local Cuarentenario — Establecimientos Ganaderos

Nombre del establecimiento *

País *

Departamento *

Distrito *

Localidad *

Dirección

Unidad Zonal *

TR11 - Habilitación y Baja de establecimientos ganaderos para la exportación a la UE

En este trámite se utilizan los conjuntos de datos de Establecimientos Ganaderos y Personas físicas y jurídicas

11 - Habilitación y Baja de establecimientos ganaderos para la exportación a la UE

Tipo de solicitud *

DECLARACIÓN JURADA DE ESTABLECIMIENTO / PROPIETARIO - SITRAP

Datos del propietario — Datos de Personas físicas / jurídicas

Nombre

Documento de identidad

Nacionalidad

Dirección

Teléfono

Correo electrónico

Siglas *

Nro. de boleta de marca *

Socio ARP Nro. *

Regional *

Datos del establecimiento — Establecimientos Ganaderos

Establecimiento *

Código SIGOR

Siglas *

Departamento *

Distrito *

Localidad *

TR14 - Habilitación de Centros Genéticos

En este trámite se utilizan los conjuntos de datos de Establecimientos Ganaderos y Personas físicas y jurídicas

14 - Habilitación de Cabañas y Centros Genéticos para importación y exportación

Datos de la orden

Seleccione el tipo de habilitación a solicitar *

- Primera vez
- Rehabilitación
- Renovación

Datos del centro genético

Tipo de propietario del centro genético *

- Persona física
- Establecimiento
- Empresa sin establecimiento
- Empresa con establecimiento

Nombre *

Correo electrónico * Teléfono *

Datos del establecimiento — Establecimientos Ganaderos

Establecimiento * Departamento

Distrito Localidad

Datos del propietario o solicitante — Datos de Personas físicas / jurídicas

Nombre Documento de identidad

Longitud * Tipo Centro Genético * Material genético *

TR15 - Habilitación de Casas Expendedoras de Productos Biológicos y/o Centros de Distribución de Vacunas (CDV) de la Comisión de Salud Animal (CSA)

En este trámite se utilizan los conjuntos de datos de Personas físicas y jurídicas

15 - Habilitacion de Casas Expendedoras y/o Centros de Distribución de Vacunas de la Comisión de Salud Animal

Tipo de solicitud *

Habilitación para *

Tipo *

Datos del propietario o solicitante — Datos de Personas físicas / jurídicas

Nombre * Documento de identidad *

Dirección *

TR18 - Actualización de marcas de propietarios de ganado

En este trámite se utilizan los conjuntos de datos de Personas físicas y jurídicas y marcas.

18 - Actualización de marcas de propietarios de ganado

Tipo Persona *

Datos del propietario

Nombres y Apellidos *

C.I. o R.U.C. del propietario *

Datos de Personas físicas / jurídicas

Seleccione el tipo de solicitud *

Marcas

Marcas a incorporar

Nro. de Boleta actual *

Datos de Marcas

+ Agregar otro

TR19 - Volumen de producción de alimentos con destino a la alimentación animal

En este trámite se utilizan los conjuntos de datos de Personas físicas y jurídicas y Establecimientos ganaderos.

19 - Volumen de producción de alimentos con destino a la alimentación animal

Los datos ingresados al formulario y los modificados posteriormente, son entera responsabilidad del usuario solicitante, teniendo en cuenta lo establecido en la Resolución Nro. 901/2013.

Tipo Solicitud *

Ruc *

Establecimiento *

Establecimientos Ganaderos

Dirección *

N° de Habilitación *

Nombre del Propietario y/o Representante Legal *

N° Líneas de producción *

Asesor Técnico

N° Registro Profesional Veterinario *

Datos de Personas físicas / jurídicas

Trimestre *

TR24 - Registro Nacional de Cabañas y Centros Genéticos de Bovinos para los programas sanitarios

En este trámite se utilizan los conjuntos de datos de Personas físicas y jurídicas y Establecimientos ganaderos

24 - Registro Nacional de Cabañas y Centros Genéticos para los Programas Sanitarios

Recuerde actualizar los datos de su Cabaña o Centro Genético en el plazo máximo de 1 año a partir del Registro inicial, o, en caso de alguna modificación de los mismos

Tipo de registro

Seleccione tipo de registro *

- (•) Registro inicial
- ( ) Actualización

Datos de la empresa

Empresa

[ ] Buscar Establecimientos asociados a la empresa

Datos del establecimiento

Establecimiento *

Código SIGOR *

Establecimientos Ganaderos

Domicilio

Teléfono

Latitud

Longitud

Departamento *

Distrito *

Localidad *

Datos del propietario o solicitante

Nombre *

Documento de identidad *

Datos de Personas físicas / jurídicas

Correo para contacto *

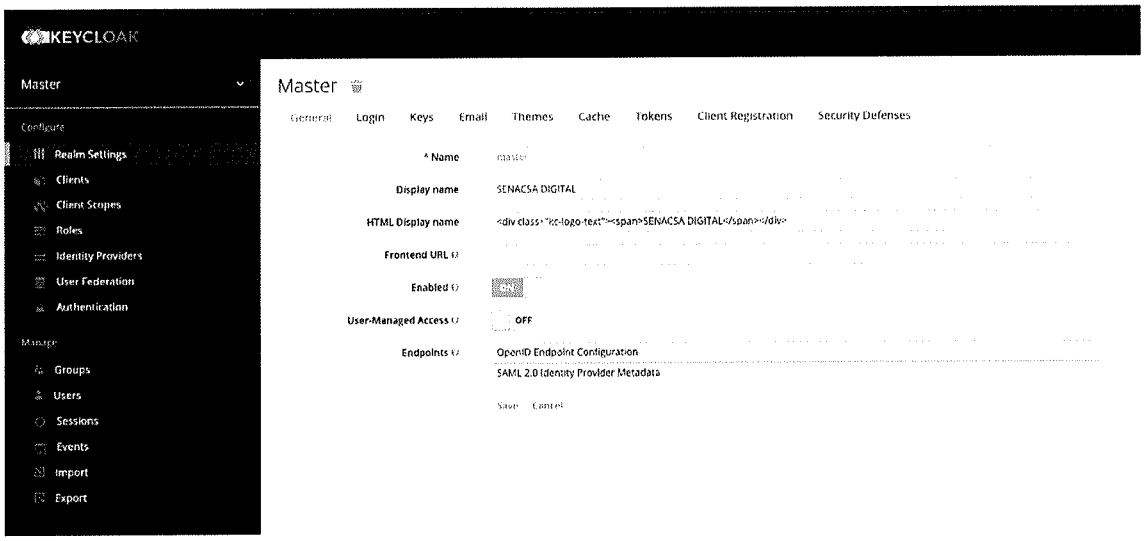
ANEXO 1: Manual técnico - Autenticador Único

Versión	Descripción	Fecha de publicación	Autor
1.0	Creación del documento	19/04/2023	Arturo Ferreira

Sistema de Administración del Keycloak

El Keycloak cuenta con un sistema de administración, el cual se encuentra en un entorno WEB. Si bien el producto cuenta con muchas configuraciones, solo tocaremos las relevantes para la implementación del servicio de autenticación. Para más detalle el sistema cuenta con una detallada documentación en línea y con una activa comunidad que está siempre predispuesta a ayudar.

Realm Settings

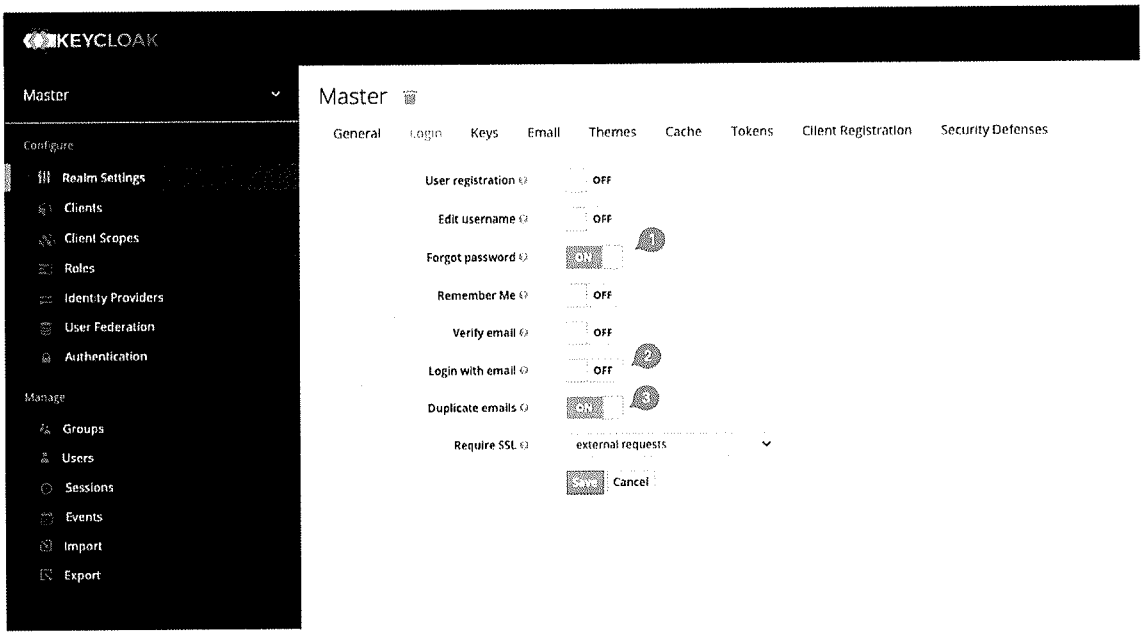


Un realm es un conjunto de configuraciones relevantes a una específica política de seguridad que deseamos que administre el Keycloak. El realm que viene por defecto es el Master, y en se encuentra configurado lo básico para administrar el Keycloak mismo.

Login

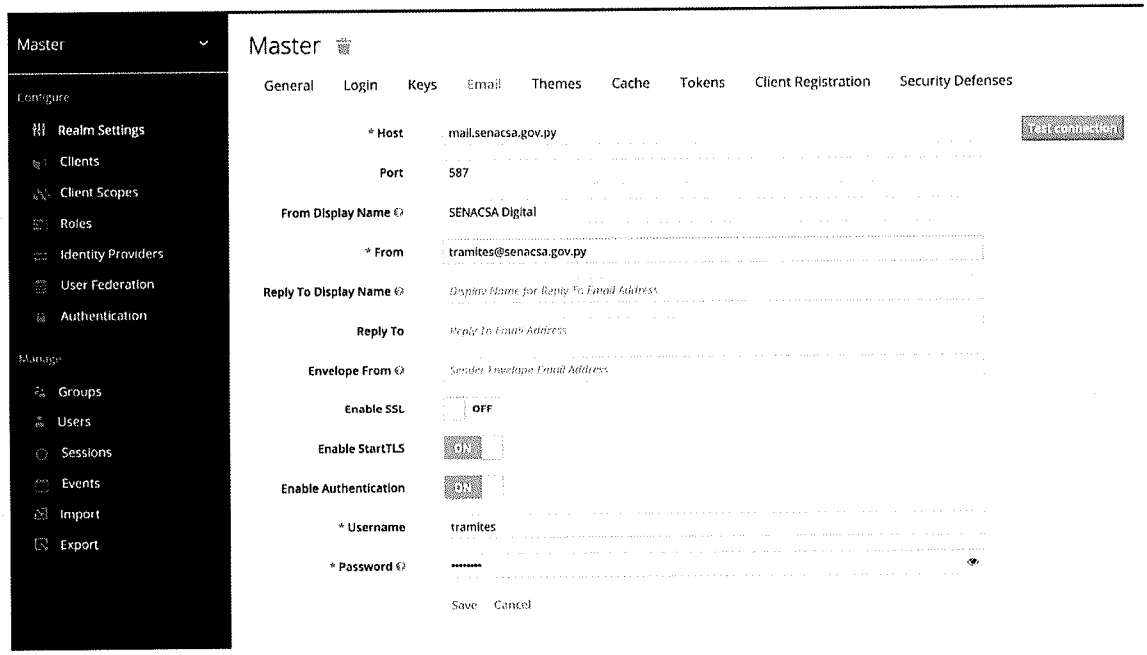
Configuración relacionada a la página de login publicada por el Keycloak.

1. Es para dar soporte a la funcionalidad de *Olvide mi contraseña.* Habilita el link correspondiente en la página de login, para que el usuario ingrese su nombre de usuario y se le envíe el correo electrónico correspondiente.
2. Desactivamos el login con dirección de correo, porque el SIGOR existe más de un usuario con el mismo correo.
3. Activamos que se acepten las direcciones de correo duplicadas.



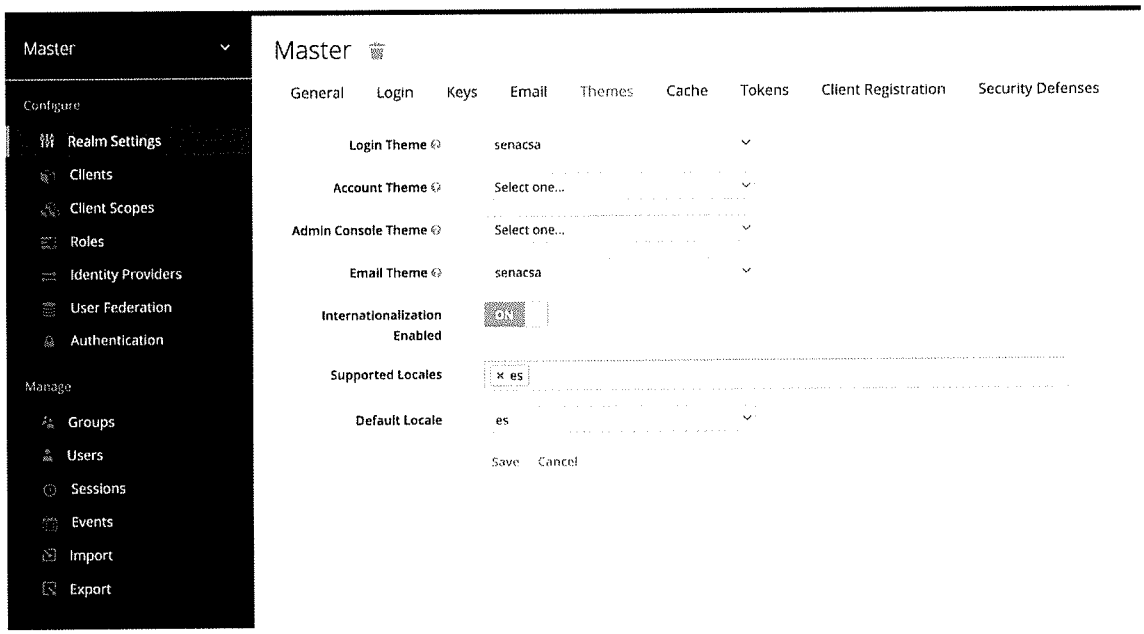
Email

Es el lugar donde se configuran las credenciales para el envío de correo electrónico por parte del Keycloak. Para poder testear la conexión, el usuario con el cual nos encontramos logueados debe contar con un correo electrónico configurado.



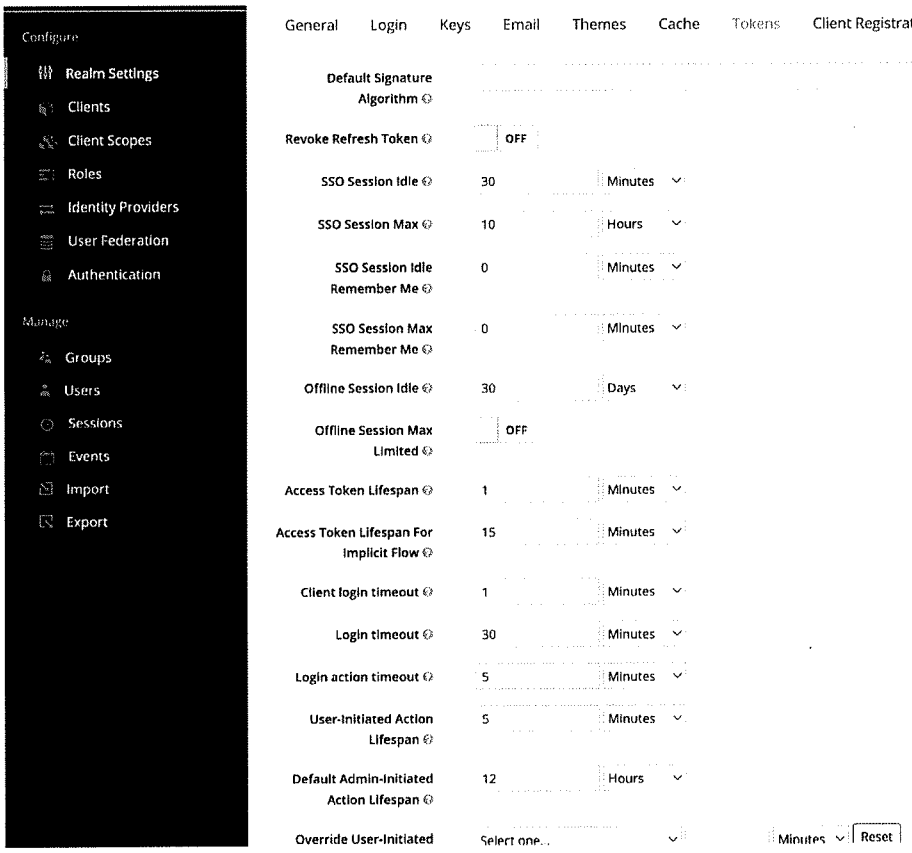
Themes

Se define qué tema se utilizará como apariencia para cada escenario en particular. Nosotros solo utilizamos dos escenarios. En el login y al enviar un correo electrónico. Cada escenario tiene su propio tema que puede ser personalizado en la carpeta senacsa que se encuentra en el directorio de instalación del sistema.



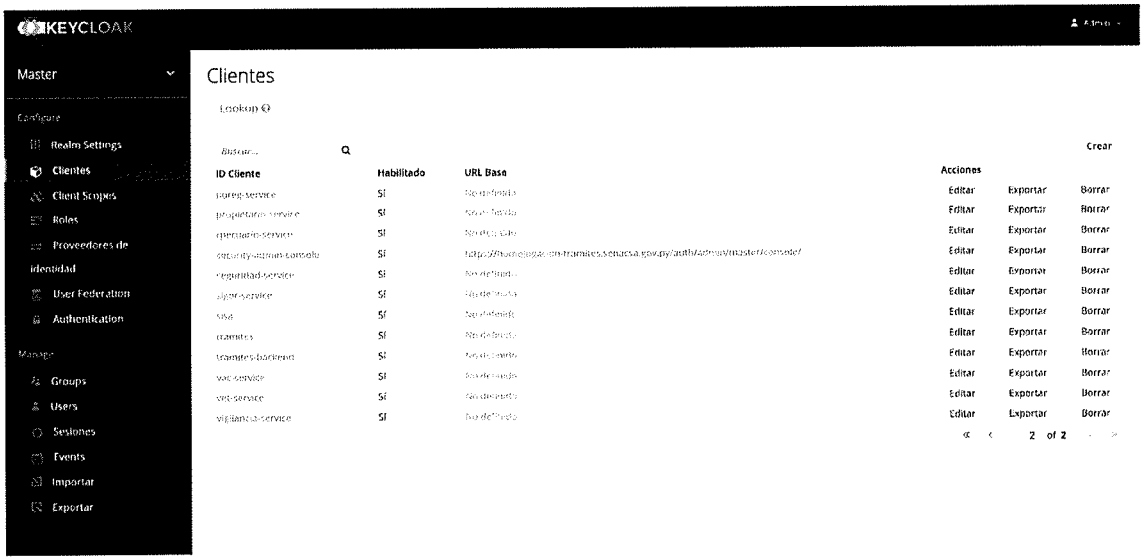
Tokens

En esta sección se maneja la configuración de los diferentes tipos de tokens que utiliza el keycloak. Como habíamos comentado anteriormente, el protocolo OpenID Connect se basa en el control de manejo de sesiones utilizando tokens como JWT. Entonces, para gestionar cuánto será el tiempo máximo que durará una sesión, se debe definir en este apartado.



Clients

Los clientes son aplicaciones WEB de confianza o servicios web de un dominio en particular. Estos clientes pueden solicitar un inicio de sesión.



Client adapters

Los Keycloak Client Adapter son librerías que facilitan la integración de cualquier aplicación WEB. Se les llama adaptadores y no solo librerías, porque están pensados para ser utilizados en plataformas o frameworks en un alto nivel, buscando escribir la menor cantidad de código posible, orientandonos más en la configuración que en la codificación de la integración. [1]

OpenID Connect

Java Adapters

Keycloak tiene una amplia gama de diferentes adaptadores para aplicaciones JAVA. Seleccionar el correcto adaptador solo depende de la plataforma con la cual trabajamos. Existen adaptadores para JBoss, Wildfly, Spring Boot, Tomcat, etc.

JBoss EAP/WildFly Adapter

Para asegurar una aplicación desplegada como un WAR en un JBoss EAP/Wildfy, debemos instalar y configurar el adaptador del Keycloak que viene como un subsistema del servidor de aplicaciones. Tenemos dos opciones para asegurar el WAR.

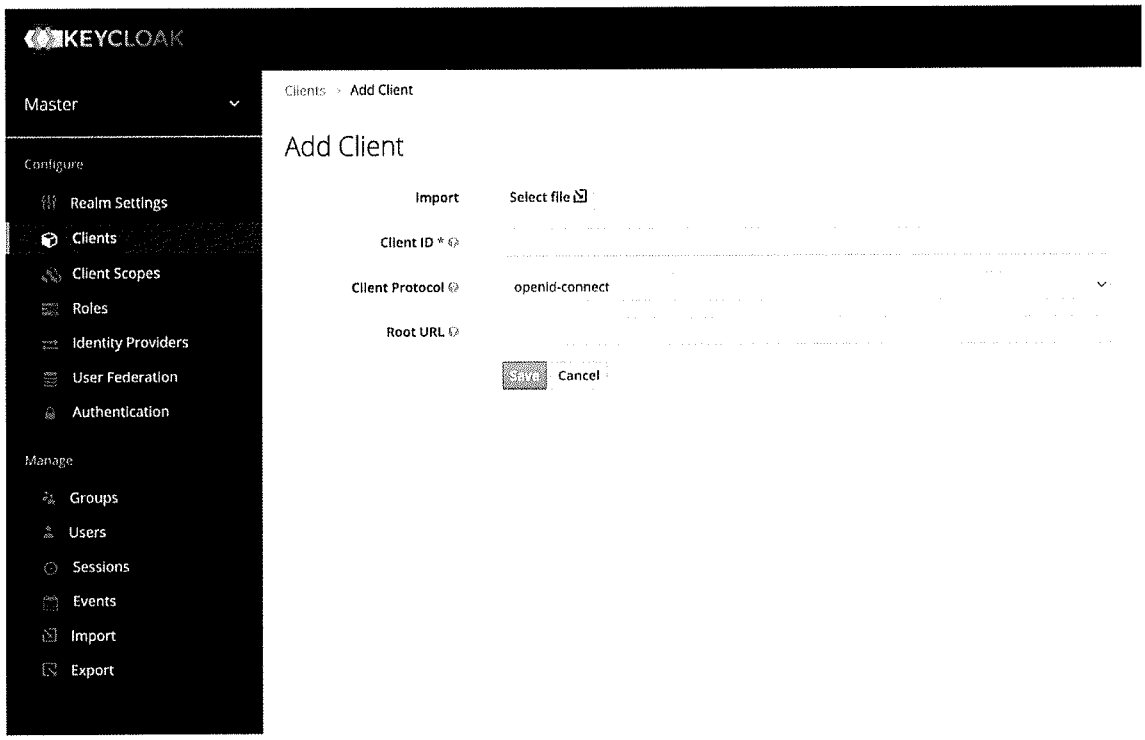
Es posible proveer un archivo de configuración para el adaptador en el WAR y cambiar el *auth-method* a KEYCLOAK dentro del web.xml.

Alternativamente, sin necesidad de modificar el WAR y es posible securizar via configuración del subsistema de adaptador de Keycloak en el archivo de configuración, por ejemplo standalone.xml.

Ambos métodos se tratan en detalle en la documentación oficial del producto Keycloak en su versión OpenSource.

Add Client

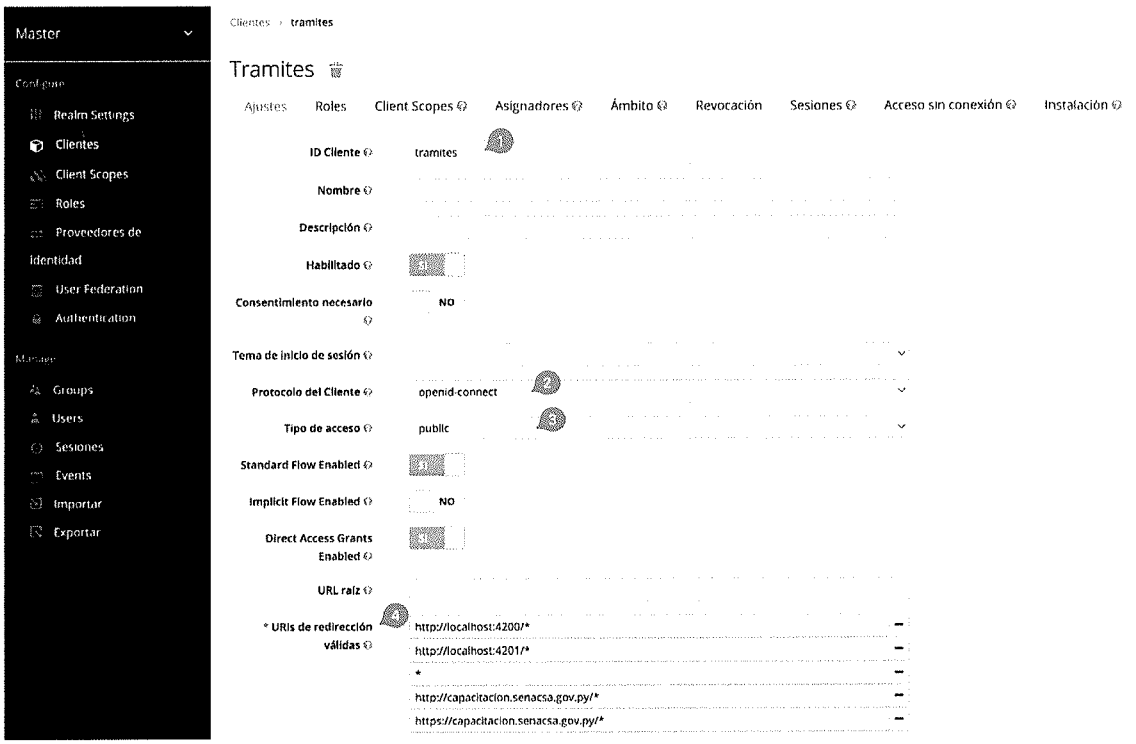
Al momento para agregar un cliente la configuración más importante y obligatoria es el Client ID, es un identificador para el sistema que desea que se le gestione el inicio de sesión. En el Client Protocol, preferimos utilizar el openid connect, pero existen otras alternativas.



Editar Client

Una vez que hemos agregado el cliente nuevo, podemos ingresar en el mismo para definir en más detalle la configuración de interacción con el mismo.

A continuación detallamos los puntos más importante de configuración:



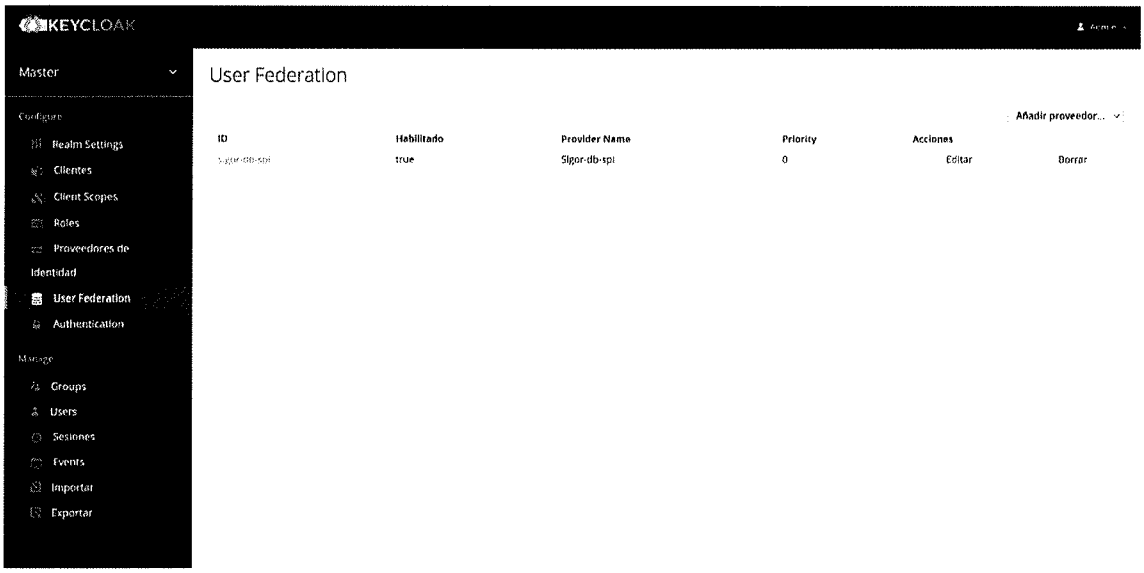
1. ID Cliente: Identificador único del cliente. Utilizado por el sistema externo para identificarse.
2. Protocolo Cliente: Por defecto utilizaremos el protocolo openID Connect.
3. Tipo de Acceso: Existen tres tipos de acceso:
    1. Confidential: necesitan una clave secreta para iniciar el protocolo de identificación.
    2. Public: No requiere que se defina la clave secreta.
    3. Bearer-only: Son servicios web que nunca inician un login.
4. URIs de Redirección válidas: Se definen cuales van a ser la uris válidas desde la cuales se puede solicitar un inicio de sesión y en el caso exitoso, se realizará una redirección a esa URI.

En el caso que en Tipo de Acceso seleccionamos el tipo Confidential, aparecerá la pestaña Credenciales y se puede regenerar la clave secreta que será compartida a los administradores del sistema externo.

User Federation

En esta sección se puede registrar el plugin de Keycloak hecho a medida para gestionar de forma externa la autenticación, en caso que sea necesario realizarlo en una base de datos externa a la base de datos del Keycloak.

En nuestro caso, usamos esta funcionalidad para dar soporte a usuarios antiguos del SIGOR que su contraseña todavía no se encuentra gestionada por el Keycloak. Utilizamos esta alternativa para hacer transparente para el usuario final la utilización del autenticador, por que en caso contrario debíamos pedir a todos los usuarios del SIGOR que cambien su contraseña al momento de implementar este nuevo componente. A medida que vayan venciendo las contraseña de los usuarios del SIGOR, se irán migrando de a poco los usuarios y su gestión de contraseña.



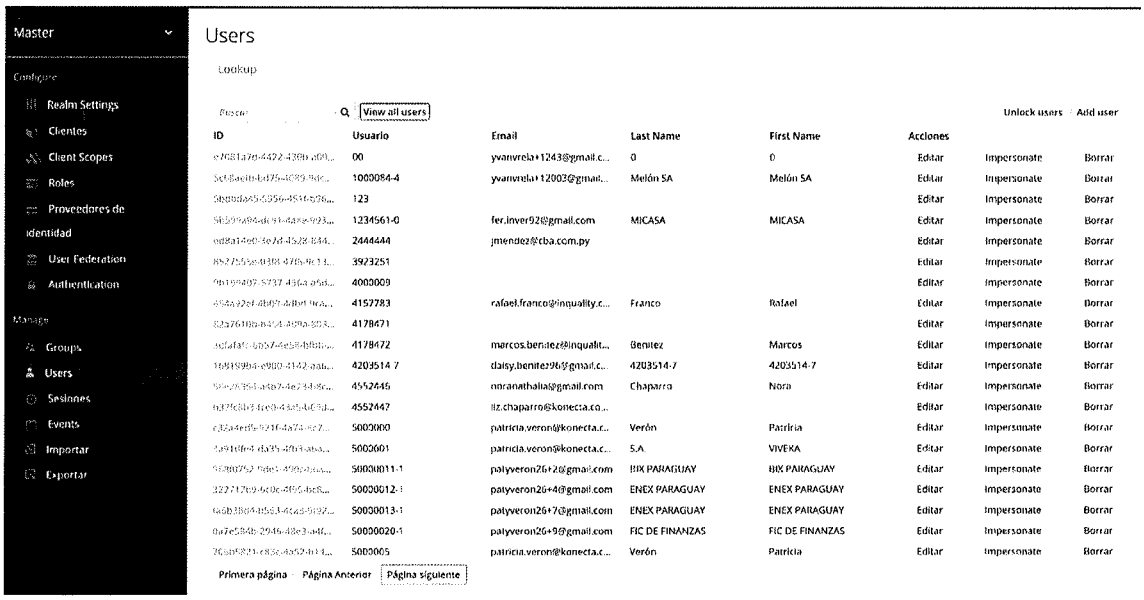
User

Es la sección donde se tienen todas las operaciones para gestionar todos los usuarios que se tiene registrado en el Keycloak. Desde este único portal se pueden realizar las principales operaciones sobre un usuario en particular.

- Agregar un usuario nuevo.
- Editar datos de usuario: En especial los relacionados a la autenticación, como la contraseña y el correo electrónico.
- Editar datos personales del usuario.
- Bloquear un usuario de forma general, para que no pueda acceder a ningún sistema.
- Iniciar sesión en nombre de un usuario en particular.

Todas estas operaciones básicas y más, pueden realizar desde esta sección, que solo se encuentra disponible para un super usuario que administrara el Keycloak. Para más detalle sugerimos consultar la documentación oficial del Keycloak.

Un gran poder, implica una gran responsabilidad.



Referencias

1. Client Adapters Keycloak [https://www.keycloak.org/docs/latest/securing_apps/index.html#client-adapters]