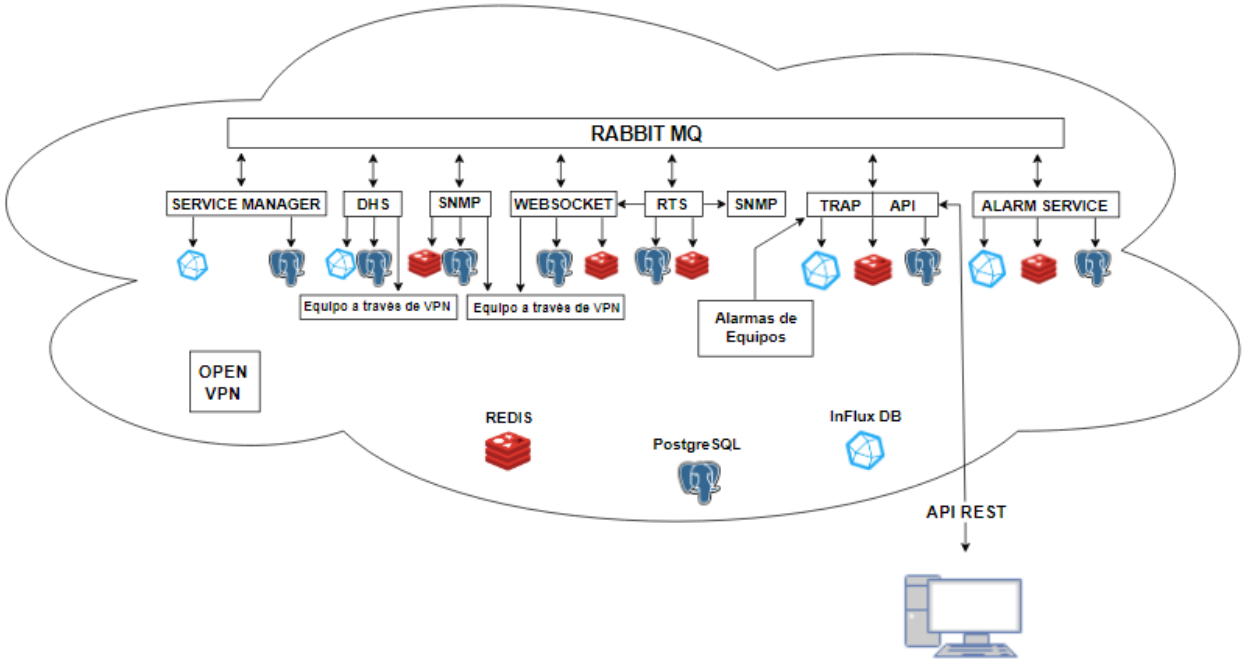
1. Introducción de Software

Nemesys® es una nueva generación de software de gestión de red desarrollado por TSDA para satisfacer las crecientes demandas y necesidades de sus clientes.

Una aplicación WEB basada en arquitectura SOA (Service Oriented Architectures) y tiene la característica de un sistema escalable.

2. Resumen del Sistema

La siguiente imagen presenta el sistema em general, mostrando su funcionalidade y operatividad.



CIFRA 1 – RESUMEN NEMESYS®

3. Detalles del Sistema

3.1. Bancos de Datos

El sistema utiliza três bases de datos, a saber, REDIS, PostgreSQL e InFlux DB. Cada base de datos se encarga de almacenar diferentes datos.

- **REDIS:** Se utiliza para almacenar en caché tokens y datos en tiempo real;
- **PostgreSQL:** Se utiliza para configurar usuarios, equipos, etc.;
- **InFlux DB:** Se utiliza para almacenar datos históricos, por ejemplo, métricas, historiales de alarmas, registros del sistema, etc.

3.2. RabbitMQ

RabbitMQ es un despachador de mensajes utilizado para la comunicación entre servicios. Es responsable de mediar todas las comunicaciones del sistema.

3.3. API Manager

El API Manager es una API Rest responsable de toda la comunicación con el usuario final, realiza toda la configuración de usuarios y equipos y también es una entrada para obtener datos métricos.

3.4. Service Manager

El Service Manager es responsable de controlar los otros servicios y escuchar los registros.

3.5. Alarm Service

El Alarm Service escucha los mensajes de alarma y validación de alarme a través de RabbitMQ y los procesa, notificando a los usuarios finales de acuerdo con la configuración del sistema.

3.6. DHS

El Data History Service (DHS) es responsable de obtener los datos históricos de todos los contenedores almacenándolos en la base de datos histórica.

3.7. RTS

El Real Time Services (RTS) se encargan de mantener actualizados en la memoria caché los datos en tiempo real del equipo durante el tiempo que sea necesario.

3.8. SNMP

El servicio SNMP es el encargado de comunicarse con los equipos mediante el protocolo SNMP, sirviendo como herramienta de comunicación para otros servicios.

3.9. Websocket

Es un servicio encargado de comunicarse con los equipos mediante Websocket, más concretamente con la nueva línea FLEX da TSDA.

3.10. Traps

Es una característica de SNMP que permite que los equipos administrados envíen información al servidor en situaciones de alarma previamente programadas.

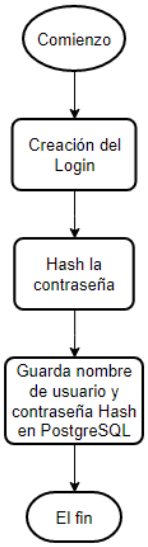
3.11. Open VPN

Para un acceso seguro y encriptado a su equipo, se utiliza Open VPN Client.

4. Sistema de Seguridad

La seguridad del sistema se presenta a continuación a través de diagramas de flujo.

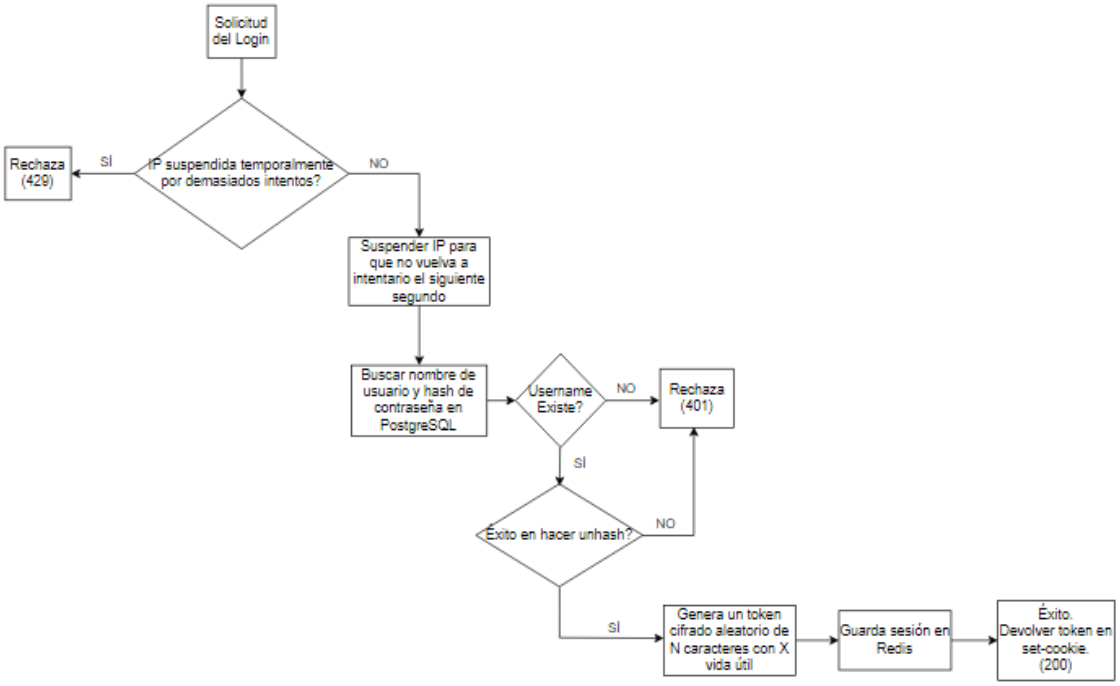
4.1. Creación del Login



CIFRA 2 – DIAGRAMA DE FLUJO DE CREACIÓN DEL LOGIN

Nota: La comunicación entre el cliente y la API se realiza mediante el protocolo HTTPS.

4.2. Solicitud del Login



CIFRA 3 – DIAGRAMA DE FLUJO DEL LOGIN

Notas:

- El tamaño y la duración del token se pueden configurar al iniciar el servidor. El valor predeterminado es 64 caracteres y una semana de vida;
- Si ya se guardó otra sesión, se sobrescribirá y su token dejará de ser válido.