COORDINADOR
ELÉCTRICO NACIONAL

USO DE APIS

Ingeniería de Software y Arquitectura
Gerencia de Tecnología y Sistemas

www.coordinador.cl

Tabla de contenido

1 Propósito 3

2 ¿A quién va dirigido? 3

3 Modelos de Seguridad 3

3.1 OAut 2.0 3

3.2 API Key 4

4 Registro en el Portal del Desarrollador 4

4.1 Apis de Servicios Públicos 6

4.1.1 Uso 6

4.2 Apis de Servicios Operacionales 7

4.2.1 Uso 8

1 Propósito

El presente documento tiene como propósito explicar el uso de apis que tienen el modelo de seguridad OAuth 2.0 y ApyKey.

2 ¿A quién va dirigido?

El documento va dirigido a equipos de desarrollo y personas que tengan conocimiento previo de uso de apis genéricas y con métodos de seguridad.

3 Modelos de Seguridad

La Subgerencia de Ingeniería de Software y Arquitectura se encuentra implementado mejoras en métodos de seguridad de sus APIS, lo anterior implica cambios en la forma de acceder a estas ya que se incorporan métodos como API Key (comúnmente usadas) y OAuth 2.0.

Por otra parte, todo acceso debe ser desde la plataforma de API Manager del Coordinador, lo cual implica un proceso de corto y mediano plazo para realizar los cambios de endpoint de los clientes que hoy consumen nuestras APIS. Lo anterior, será informado de forma paulatina a cada entidad que se vea afectada.

Finalmente, se han definido tipologías de uso de APIS:

1. Api de Servicios Públicos
    a. APIs de Servicio que no tienen impacto en operación y que están destinadas a consultar información al menos con un desface de 1 día. En esta categoría caen las APIS del Sistema de Información Pública (SIP).
    b. Su modelo de seguridad será mediante API Key y se deberá realizar el registro mediante el portal del desarrollador (https://portal.api.coordinador.cl). El uso no quedará sujeto a aprobación del Coordinador Eléctrico Nacional y quedará activo de forma inmediata.
2. Api de Servicios Operacionales
    a. APIs de Servicio que son parte de la operatoria de cada unidad y que prestan servicio a Coordinados. Estas impactan directamente a los sistemas.
    b. Su modelo de seguridad será mediante OAuth 2.0, y se deberá realizar el registro mediante el portal del desarrollador (https://portal.api.coordinador.cl). El uso quedará sujeto a aprobación del Coordinador Eléctrico Nacional.

3.1 OAut 2.0

OAuth 2.0 es un protocolo de autorización, OIDC es un protocolo de autenticación de identidad y puede utilizarse para verificar la identidad de un usuario ante un servicio de cliente, también llamado Parte de confianza.

OIDC utiliza JSON Web Tokens (JWT), flujos HTTP y evita compartir las credenciales del usuario con los servicios.

3.2 API Key

Una API key es una cadena alfanumérica (token) que los desarrolladores de API utilizan para controlar el acceso a sus API. Una API es un mecanismo de comunicación que permite el intercambio de datos entre dos módulos de software. La clave de API identifica el uso autorizado de la API para que pueda mantener, administrar y monetizar las API de forma más eficiente.

4 Registro en el Portal del Desarrollador

Todos aquellos que deseen utilizar las apis de Coordinador, deben inscribirse en el Portal del Desarrollador dispuesto en el sitio web del Coordinador sección Coordinados (https://www.coordinador.cl) o en su efecto ingresar directamente al portal (https://portal.api.coordinador.cl).

En el Portal del Desarrollador se encuentra una sección denominada "Planes", en donde encontrarán lo que se encuentra disponible a utilizar:

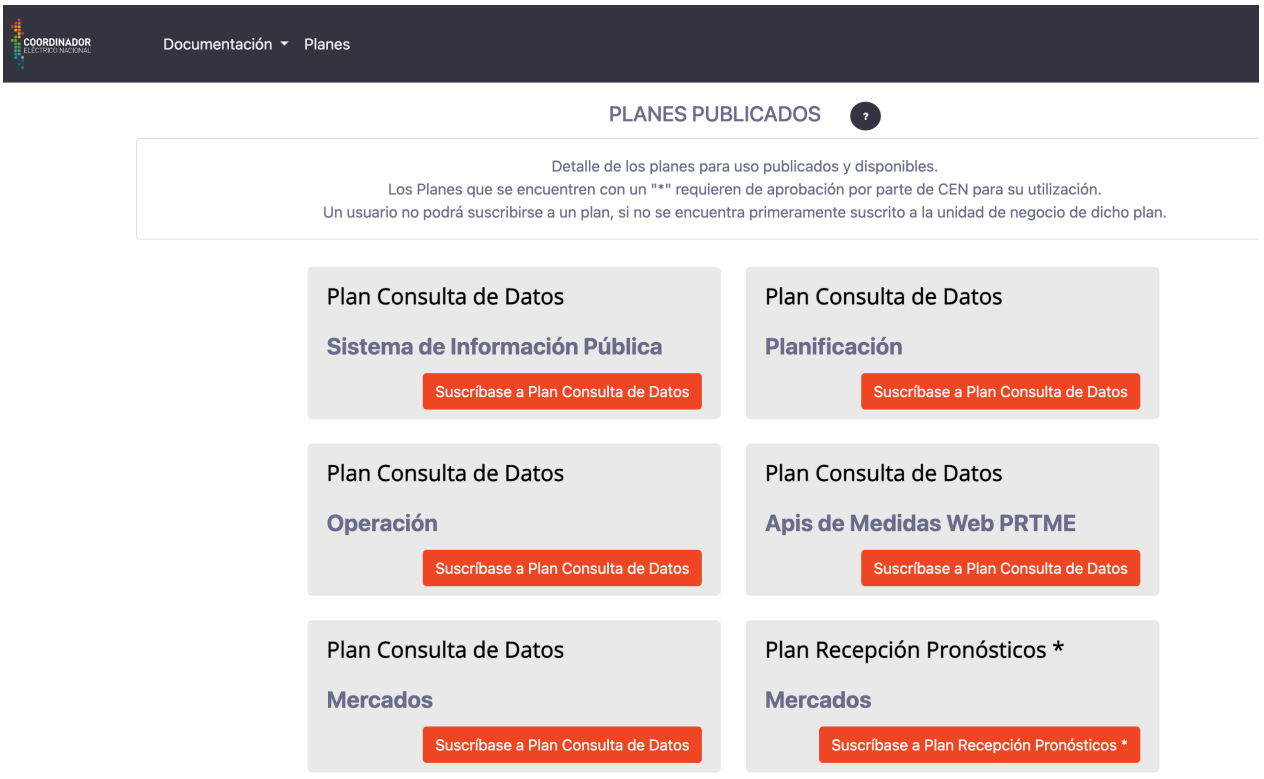

Figura 1 Planes Disponibles

Cada "Plan" hace referencia a un conjunto de APIS disponibles para uso, sin embargo, para poder comenzar a utilizarlos se debe realizar un registro previamente:

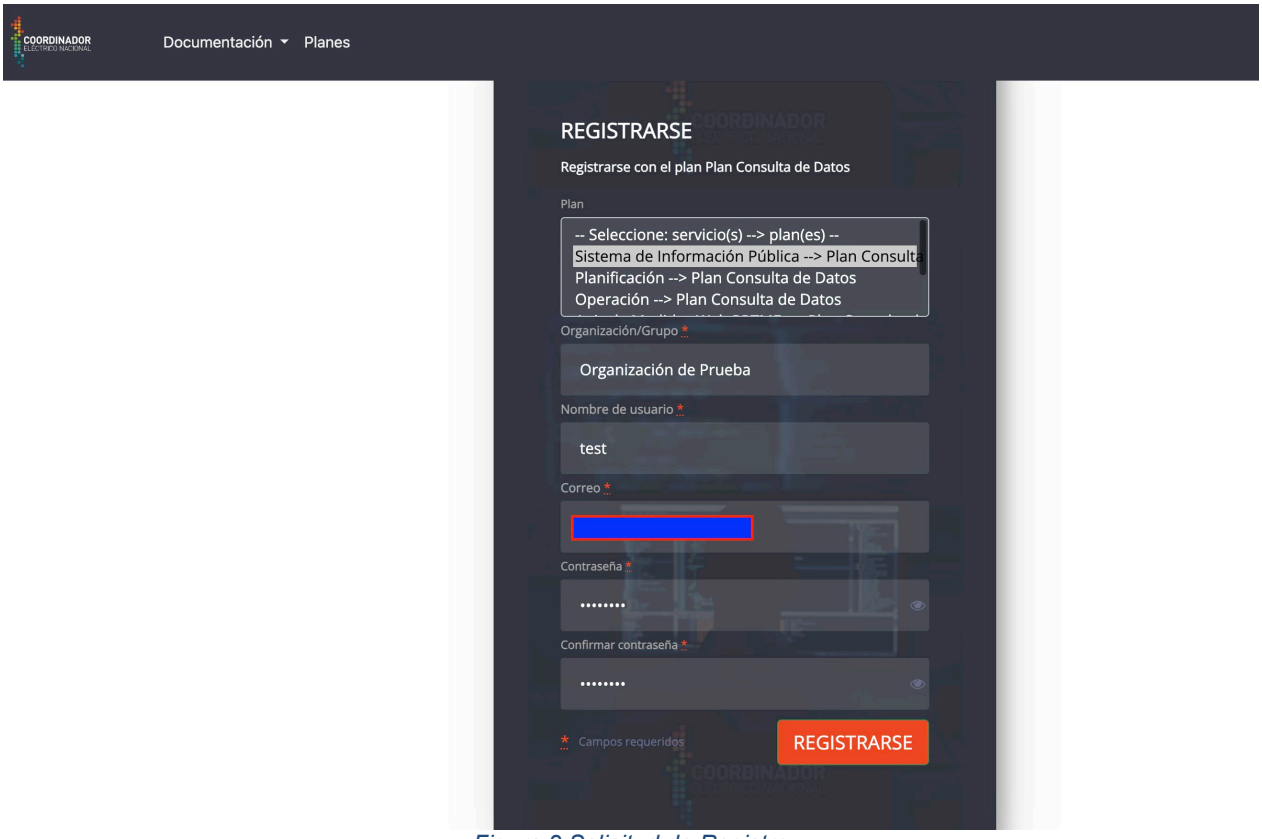

Figura 2 Solicitud de Registro

En esta solicitud se le pedirá ingresar los datos obligatorios para la identificación posterior, es importante tener en cuenta que el correo electrónico es fundamental para al menos la primera fase de registro.

Es obligatorio al menos registrarse la primera vez a un "Plan", si desea inscribir más de uno, esto se podrá realizar posterior al primer registro de la cuenta.

Una vez realizado el registro deberá realizar la confirmación de este mediante el correo electrónico ingresado.

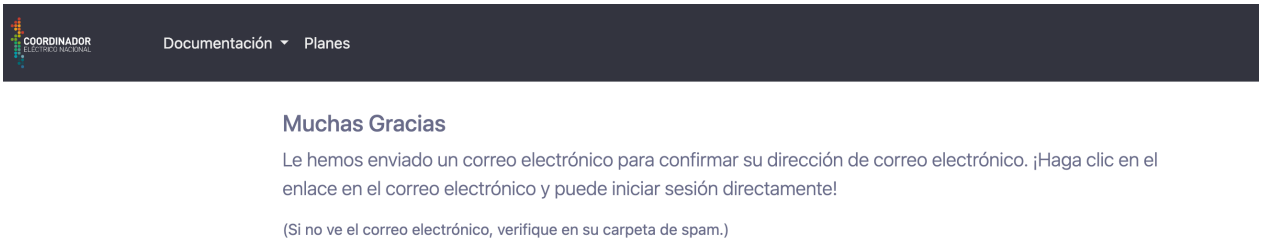

Figura 3 Confirmación de Registro

Una vez confirmado el registro, podrá acceder al portal en donde administrará sus credenciales y uso de las apis disponibles.

4.1 Apis de Servicios Públicos

Para el uso de "Planes" de uso público, en el apartado de "Aplicaciones" se dispondrá de todas aquellas aplicaciones con las cuales se ha suscrito a un "Plan", y aparecerán como "Activo", ya que no requieren de aprobación previa.

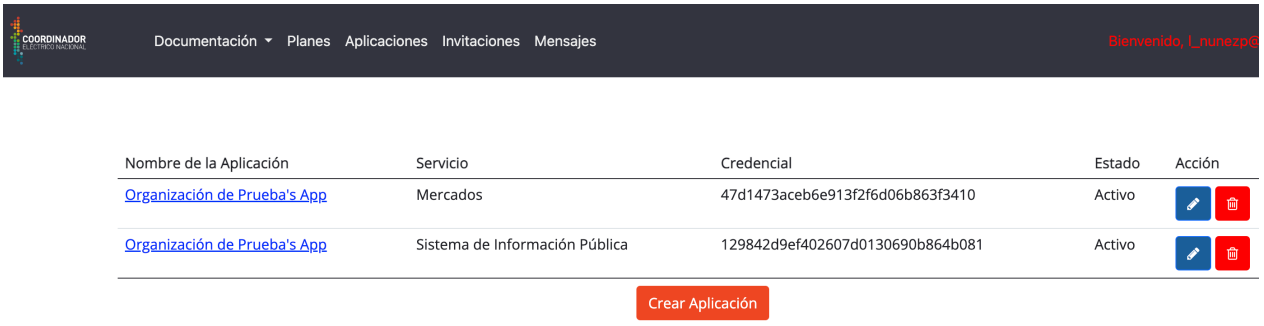

Figura 4 Lista de Aplicaciones

4.1.1 Uso

Para el uso, se debe seleccionar la aplicación de la lista en donde se desplegará el API Key con el cual se debe realizar la llamada.

Figura 5 Detalle de Aplicaciones

Para comprar el uso, se debe ingresar al menú de Documentación y seleccionar a que producto se ha suscrito, para el ejemplo seleccionamos "Sistema de Información Pública".

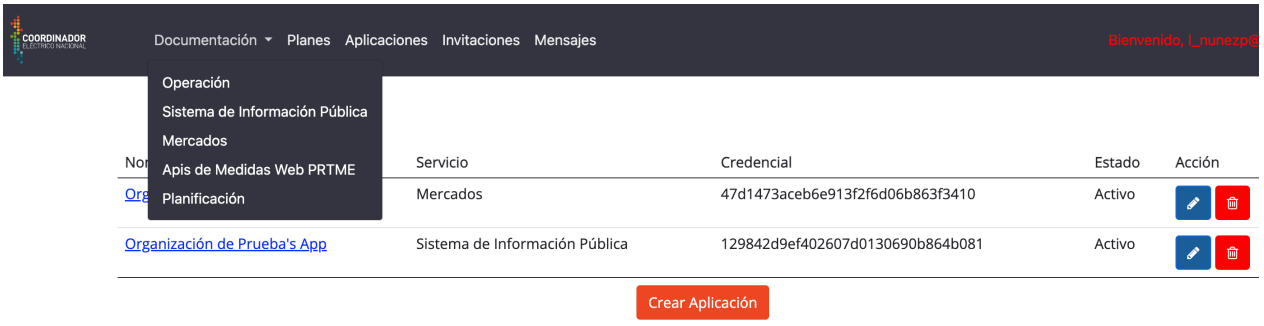

Figura 6 Ejemplo

Una vez en el la "Documentación", presionamos en el botón "Authorize" y agregamos el API key que tenemos.

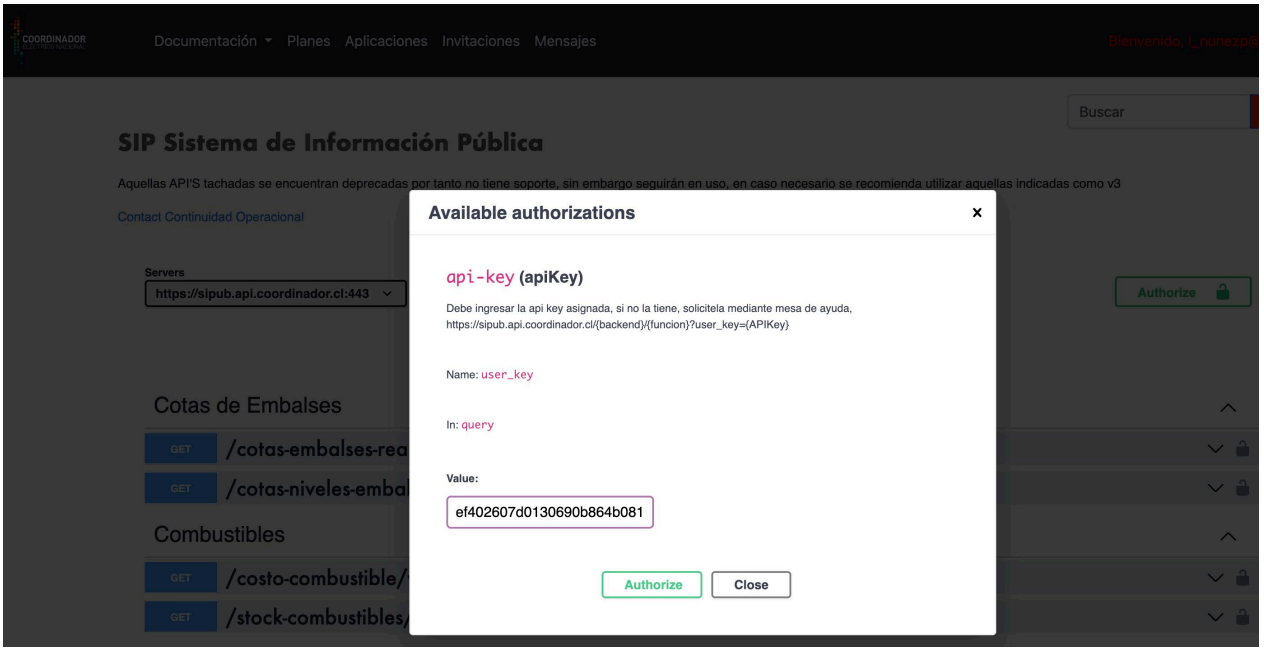

Figura 7 Autorización

Ya con esto podemos hacer uso de las apis disponibles.

Otro método es realizarlo mediante CURL

```
curl -X 'GET' \
  'https://sipub.api.coordinador.cl/cotas-embalses-reales/v3/findAll?startDate=2024-01-
01&endDate=2024-01-02&page=0&user_key=129842d9ef402607d0130690b864b081' \
     'accept: application/json'
```

4.2 Apis de Servicios Operacionales

Para el uso de "Planes" de uso restringido, en el apartado de "Aplicaciones" se dispondrá de todas aquellas aplicaciones con las cuales se ha suscrito a un "Plan", y aparecerá como "Pendiente", ya que requieren de aprobación previa.

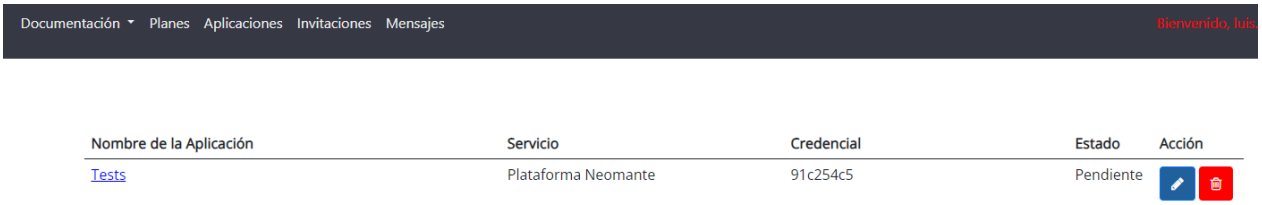

Figura 8 Aplicaciones pendientes de aprobación

Una vez que el administrador de Coordinador apruebe el uso, quedará en estado "Activo" y podrá comenzar a utilizar las apis.

4.2.1 Uso

A diferencia del apartado anterior (API Key) el uso de estas apis será restringido por el método de seguridad OAuth 2.0, por lo que requiere de unos pasos adicionales. Como paso previo también requiere de registro en el Portal del Desarrollador siguiendo los mismos pasos.

Una vez que ingrese con su usuario y clave al Portal del Desarrollador, aparecerá el detalle de su aplicación de forma diferente al que se muestra en el apartado anterior (API Key). Ahora dispone de dos atributos que son:

1. Client ID: Es el identificador único del cliente o aplicación que hará la comunicación.
2. Secret: Es la clave secreta de la aplicación.

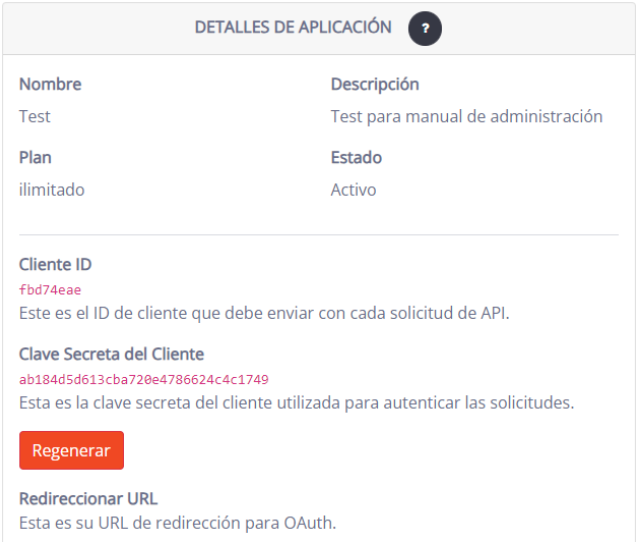

Figura 9 Detalle de la Aplicación para OAuth 2.0

Para comenzar a utilizar las apis se debe realizar los siguiente:

1. Solicitar la autorización de la siguiente forma:

   Hacer una llamada mediante método POST a la siguiente URL:
   https://security-access.api.coordinador.cl/auth/realms/API-MANAGER/protocol/openid-

connect/token
Agregando los parámetros:

a. client_id: Entregado al momento de crear la aplicación en el portal del desarrollador.

b. client_secret: Entregado al momento de crear la aplicación en el portal del desarrollador.

c. grant_type: client_credentials

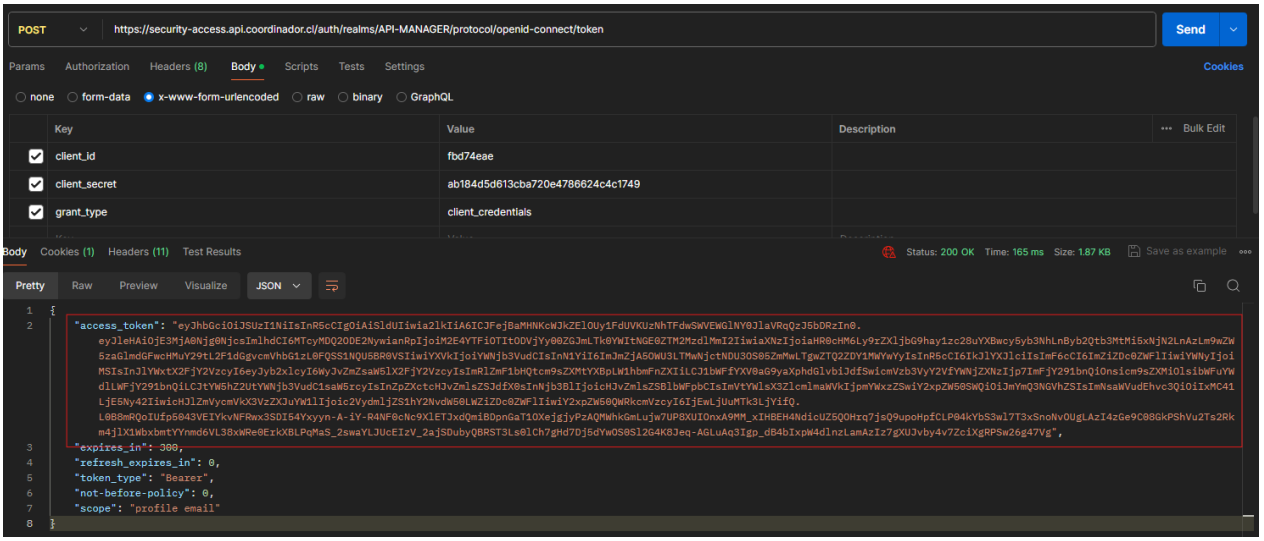

Figura 10 Ejemplo mediante Postman

El resultado será un token del tipo JWT, definido en el atributo "access_token".

2. Con este “access_token” se deberá realizar la llamada en la api correspondiente:

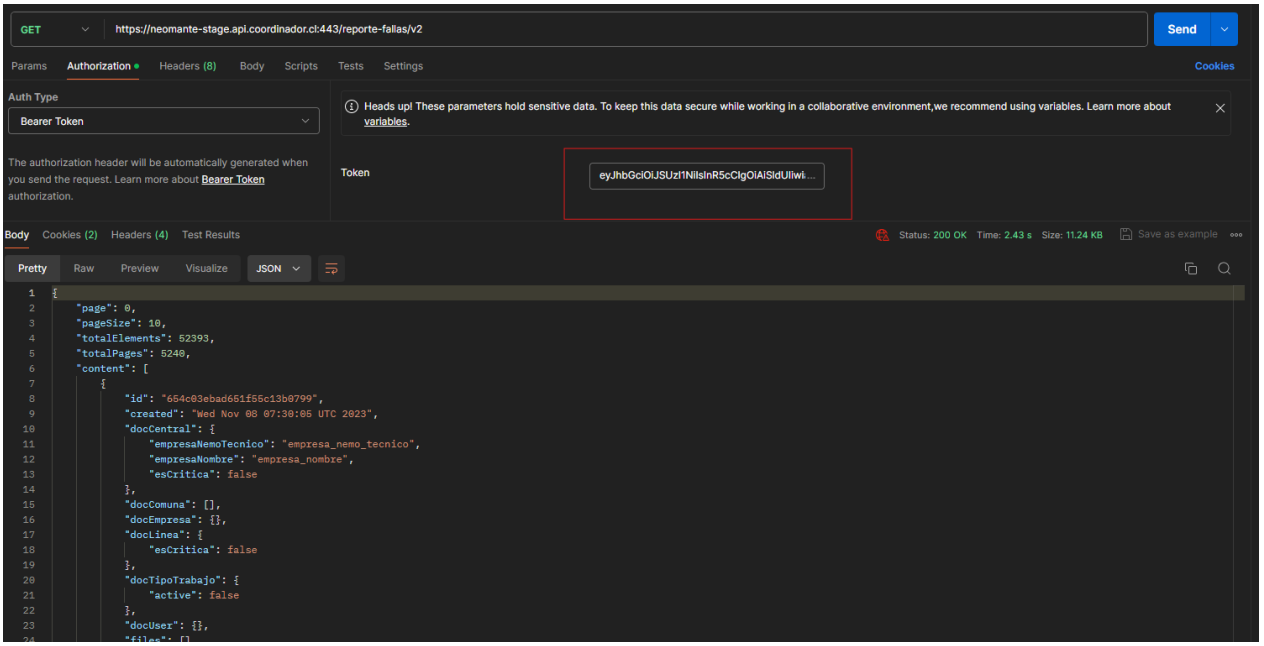

Figura 11 Llamada mediante JWT Token