A close-up of a white background

Description automatically generated

DOCUMENTO TECNICO *SERVICIO CAPTURA INFORMACIÓN MURIC*

**Febrero 2024**

**Tabla de contenido**

[1. Introducción 3](#_Toc190872785)

[2. Objetivos 3](#_Toc190872786)

[3. Beneficios de la implementación del API REST 3](#_Toc190872787)

[4. Desarrollo 3](#_Toc190872788)

[4.1 Exposición del servicio 3](#_Toc190872789)

[4.2 Servicios expuestos 3](#_Toc190872790)

[4.2.1 Servicio *login* 3](#_Toc190872791)

[a. Parámetros de entrada 4](#_Toc190872792)

[b. Parámetros de salida 4](#_Toc190872793)

[c. Ejemplo de consumo/respuesta 4](#_Toc190872794)

[4.2.2 Servicio envío información 4](#_Toc190872795)

[a. Objeto JSON: Objeto JSON-AVRO de ejemplo para el envío de información. 5](#_Toc190872796)

[b. Datos de salida 5](#_Toc190872797)

[4.3 Seguridad 5](#_Toc190872798)

[4.3.1 Estándar OAuth 6](#_Toc190872799)

[4.4 Condiciones para consumir el servicio 6](#_Toc190872800)

[5. Anexos 6](#_Toc190872801)

[6. Historial de cambios 6](#_Toc190872802)

# Introducción

En el marco del proyecto estratégico de supervisión digital en el que está trabajando la Superintendencia Financiera de Colombia (SFC), y con el objetivo de mejorar la granularidad y oportunidad de la información de cartera, se ha desarrollado un servicio (API REST) que permite la recepción y procesamiento de la información de los deudores, los créditos y sus respectivos movimientos mensuales, con el fin de obtener información con una visión completa de cada operación crediticia. Esta nueva infraestructura no solo optimiza el flujo de datos, sino que también mejora la capacidad de respuesta ante datos atípicos, beneficiando a todas las partes involucradas en el proceso.

Este documento técnico tiene como propósito definir el proceso de consumo del servicio expuesto. A continuación, se detallarán los componentes requeridos para el envío de información.

# Objetivos

* Describir la estructura y funcionamiento del API REST diseñado para recibir información relacionada con la cartera de crédito.
* Establecer las directrices de seguridad, autenticación y manejo de datos dentro del servicio.

# Beneficios de la implementación del API REST

* Interoperabilidad y flexibilidad:los API REST facilitan la integración con diferentes sistemas y aplicaciones, permitiendo mayor flexibilidad en la gestión y uso de la información.

# Desarrollo

## Exposición del servicio

La exposición del servicio estará sujeta a las siguientes características:

Dirección (URL) base expuesto por la SFC para ambiente de desarrollo: <https://apidev.superfinanciera.gov.co/v2/services/>

Dirección (URL) base expuesto por la SFC para ambiente de producción: <https://api.superfinanciera.gov.co/v2/services/>

* + - La implementación del servicio deberá seguir los lineamientos tecnológicos descritos por el estándar REST y JSON.
    - El método HTTP usado para el intercambio de información entre el servicio y el cliente será POST, únicamente.
    - Las respuestas de los servicios expuestos por la SFC estarán basadas en el estándar de respuestas HTTP <https://developer.mozilla.org/es/docs/Web/HTTP/Status>

## Servicios expuestos

Los servicios expuestos serán los siguientes:

## Servicio *login*

Permite a los clientes obtener un token de inicio de sesión mediante autenticación de usuario y contraseña provistos por la SFC.

El servicio será expuesto mediante la dirección (URI) [base]/auth y responderá únicamente bajo el método POST.

La invocación correcta se entenderá cuando al invocar el servicio, este retorne el código HTTP 200.

## Parámetros de entrada

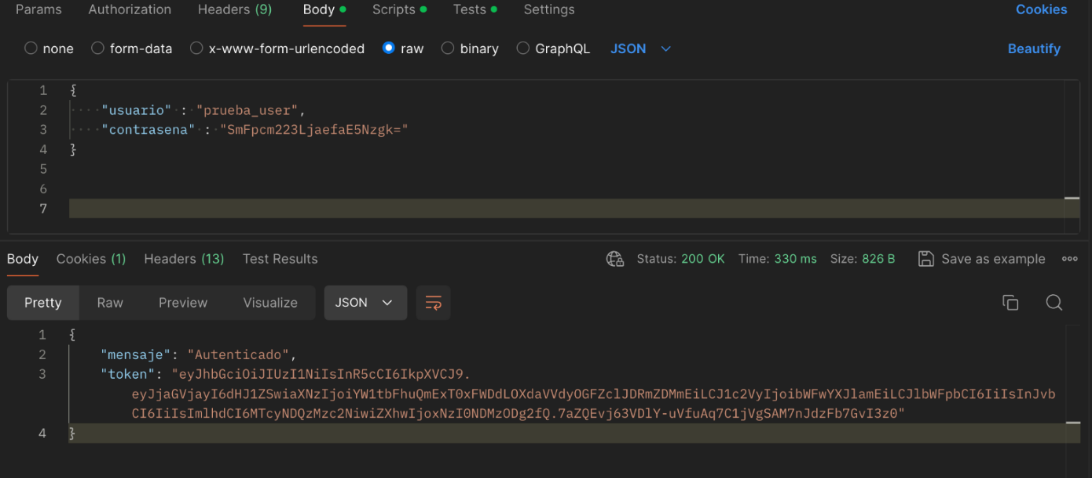
|  |  |  |  |
| --- | --- | --- | --- |
| **Nombre** | **Descripción** | **Tipo Dato** | **Obligatorio** |
| **Usuario** | Usuario que intentará iniciar sesión. | String[250] | Si |
| **contraseña** | Contraseña del usuario que intentará iniciar sesión. (codificado en base64) | String[250] | Si |

## Parámetros de salida

En caso de ser exitosa la autenticación del usuario, se recibirá el token basado en el estándar JWT (<https://jwt.io>)

authorization →Bearer eyJhbGciOiJIUzUxMiJ9.eyJpYXQiOjE1NjAyMDM2MjcsImlzcyI6Im0wdmlpcmVkLXN1cGVyIiwic3ViIjoibTB2aWlyZWQtc3VwZXIiLCJleHAiOjE1NjAyMDM2ODd9.hDvgkg53wd5naF0uhuDh47MtAPZvTqg7hEXEHmFGaqEKPmDCXLE4h1WW-BQzQe\_8HFy1UTPeqQHLUdxaH3WgiQ

## Ejemplo de consumo/respuesta



## Servicio envío información

El servicio será expuesto mediante la URI **[base]/muric** y responderá únicamente bajo el método POST.

1. Firmar el archivo AVRO completo digitalmente con la cantidad de firmas requeridas. En este caso, deberá ser firmado por el representante legal.
2. Generar el archivo .AVRO. Si este tiene un peso de más de 100MB, se debe dividir el archivo en segmentos de 100MB, los cuales deben ser enviados al API que recibe dichos segmentos.

En los encabezados (headers) de la petición se debe enviar el token obtenido del servicio de autenticación.

|  |  |  |  |
| --- | --- | --- | --- |
| Llave (key) | Valor (value) | Descripción | Ejemplo |
| Authorization | Bearer <token> | Token obtenido en el servicio de autenticación | ayJhdbd.aeEerjOi.juissefer |
| checksum\_file | Cadena Alfanumérica | Checksum del archivo original, es decir, el cálculo del archivo con todas las partes | df9b7699ad33af0eb41a1d |
| segment | X | Identificador de cada segmento del archivo original particionado acorde con la descripción posterior | 4 |
| total\_segments | YYY | Cantidad total de segmentos en los que se ha dividido el archivo | 500 |

El nombre de cada segmento se debe generar bajo la siguiente estructura:

**T<tipoentidad>\_C<codigoentidad>\_D<fecha>\_avro.part4**

Ejemplo del nombre del segmento: T1\_C14\_20240830\_avro.part4, donde el número 4 debe concordar con el header segment relacionado en la tabla anterior.

## Objeto JSON: Objeto JSON-AVRO de ejemplo para el envío de información.

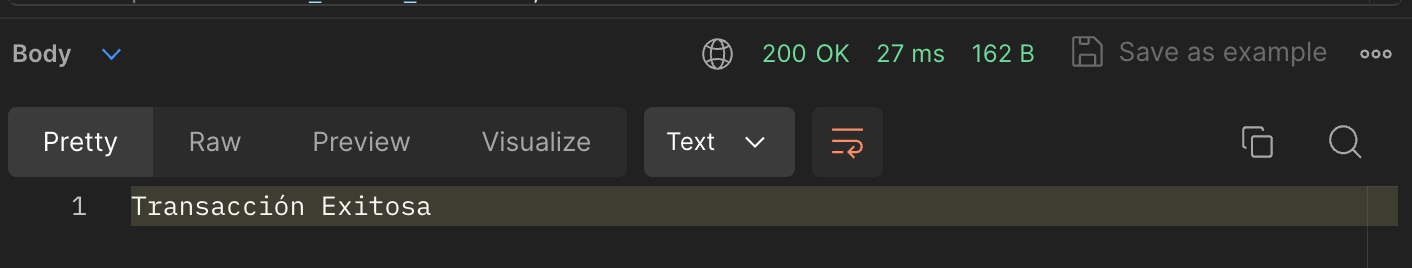
Interfaz de usuario gráfica, Aplicación, Teams

El contenido generado por IA puede ser incorrecto.

## Datos de salida

Una vez se recibe la información y la información es validada, el servicio responderá con el código HTTP 200 OK y el mensaje de “Transacción Exitosa”

Ejemplo:



Si se genera un error en la validación, se indicará qué campo está generando el error.

## Seguridad

Los servicios estarán protegidos mediante protocolos de encriptación, lo que garantiza la confidencialidad e integridad de las comunicaciones. La autenticación para acceder a estos servicios se realizará mediante la combinación usuario - contraseña, y utilizando adicionalmente el esquema de autenticación mediante token definido por la SFC. Además, se implementarán medidas de seguridad adicionales según los estándares y mejores prácticas técnicas, asegurando un acceso seguro y controlado a los servicios.

* + 1. **Estándar OAuth**

Es un estándar de autorización que permite, de forma limitada, el acceso a recursos expuestos sobre HTTP. Este mecanismo refuerza la funcionalidad del API Key y la mezcla con la generación de un doble factor de autenticación equivalente al JWT (JSON Web Token) por sus siglas en inglés.

En primera instancia, el cliente, previo al consumo del recurso web, realiza una petición de autorización a través de un servicio en el cual envía un identificador único del cliente (en este caso el usuario y la contraseña al servicio Oauth enviados en el body de la petición). Si los datos son correctos, el servicio de autenticación retornara un token el cual es usado por el cliente para invocar el recurso. Posterior a esto, el cliente realiza una petición al recurso (el endpoint de cierres) inyectando en el *HTTP Header* de la misma, los datos del token obtenido previamente. Si los datos enviados son correctos se ejecutará y procesará la solicitud recibida. En otro caso, se rechazará.

## Condiciones para consumir el servicio

Para poder consumir el servicio, los usuarios deben cumplir con los requisitos de autenticación y autorización establecidos por la SFC. Esto incluye la posesión de credenciales válidas (usuario y contraseña) y/o la utilización de otros mecanismos de autenticación aprobados. Los usuarios deberán seguir las políticas de uso aceptable y las directrices de seguridad vigentes, asegurándose de proteger sus credenciales y mantener la integridad de las comunicaciones. Además, cualquier acceso al servicio estará sujeto a monitoreo y auditoría para garantizar el cumplimiento de las normativas de seguridad.

# 5. Anexos

# 6. Historial de cambios

|  |  |  |
| --- | --- | --- |
| **Fecha** | **Versión** | **Cambios** |
| 18/02/2025 | 1 | Versión inicial |