A close-up of a white background

Description automatically generated

DOCUMENTO TECNICO *SERVICIO CAPTURA INFORMACIÓN MURIC*

**Octubre 2025**

**Tabla de contenido**

[1. Introducción 3](#_Toc208236532)

[2. Servicios para la recepción de información 3](#_Toc208236533)

[**API REST Transmisión de Archivos** 5](#_Toc208236534)

[Superfinanciera Archivos (Canal Alterno) 11](#_Toc208236535)

[3. Anexos 12](#_Toc208236536)

[4. Historial de cambios 12](#_Toc208236537)

# 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 módulo para la recepción de datos. Este módulo cuenta con varios servicios para la transmisión de información: API REST, Superfinanciera-Archivos y SFTP. Este módulo permite la recepción y procesamiento de la información de las operaciones relacionadas en el numeral 2 de las reglas generales de diligenciamiento del documento funcional y sus respectivos movimientos mensuales.

Este documento define el proceso de consumo de los servicios de intercambio de información.

Proceso necesario para activar la contingencia SFTP.

Diagrama

El contenido generado por IA puede ser incorrecto.

MTA: Método de transmisión de archivos

API: Método de transmisión REST (Transferencia de Estado Representacional)

Es importante resaltar que se debe usar un solo método de transmisión al momento de enviar la información requerida.

# Servicios para la recepción de información

**API REST**

# 

La exposición del servicio estará sujeta a las siguientes características:

Dirección (URL) base expuesta por la SFC para ambiente de desarrollo, el cual estará disponible para las entidades en los eventos en que se requiera realizar pruebas

<https://apidev.superfinanciera.gov.co/v2/services/>

Dirección (URL) base expuesta por la SFC para ambiente de producción, el cual estará disponible para las entidades para realizar la transmisión periódica:

<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>

**API REST Autenticación**

Obtención de token JWT mediante autenticación de usuario y contraseña, las credenciales deben obtenerse por medio del proceso de Autogestión de usuarios de cada entidad, que se encuentra en la página web de la Superintendencia Financiera en la sección trámites en línea y remisión de información.

Descripción:

El servicio será expuesto en la dirección (URL)

<https://apim-sfc-prod-cross.azure-api.net/api/auth/>

**Método:** POST

**Headers:** Content-Type: application/json; charset=utf-8

**Body** (JSON): parámetros de entrada **exactos**: ***usuario***, ***contrasena***, ***nombreModulo*** (sin tildes).

Parámetros de entrada:

|  |  |  |
| --- | --- | --- |
| **Nombre** | **Descripción** | **Obligatorio** |
| ***usuario*** | Usuario que intentará iniciar sesión. | Si |
| ***contrasena*** | Contraseña del usuario que intentará iniciar sesión. (codificado en base64) | Si |
| ***nombreModulo*** | Debe ser exactamente "MURIC". | Si |

## 

Ejemplo JSON de consumo

Solicitud (JSON):

{  
 "usuario": "<usuario\_asignado>",  
 "contrasena": "<base64(password\_en\_plano)>",  
 "nombreModulo": "MURIC"  
}

Parámetros de salida:

En caso de ser exitosa la autenticación del usuario, se recibirá el token basado en el estándar JWT, este token tiene un período de vigencia de 15 minutos (<https://jwt.io>)

Ejemplo Respuesta (200 OK, JSON):

{  
 "mensaje": "Autenticado",  
 "token": " *eyJhbGciOiJIUzUxMiJ9.eyJpYXQiOjE1NjAyMDM2MjcsImlzcyI6Im0wdmlpcmVkLXN1cGVyIiwic3ViIjoibTB2aWlyZWQtc3VwZXIiLCJleHAiOjE1NjAyMDM2ODd9.hDvgkg53wd5naF0uhuDh47MtAPZvTqg7hEXEHmFGaqEKPmDCXLE4h1WW-BQzQe\_8HFy1UTPeqQHLUdxaH3WgiQ*"  
}

Errores comunes:

401 no Autenticado (credenciales inválidas o clave/entorno incorrecto).

400 solicitud incorrecta (Falta un parámetro obligatorio).

Nota: El proceso de autenticación emite un token JWT que deberá incluirse en el encabezado “Authorization“ en el servicio de envío y consulta de transmisión.

### **API REST Transmisión de Archivos**

Permite a las entidades transmitir archivos firmados digitalmente (extensión esperada.avro.p7z) por el representante legal al módulo MURIC, además se deberá realizar la compresión de los archivos con el proceso Snappy. Si el tamaño es <= 100 MB, se envía en una sola solicitud (single). Si es > 100 MB, se debe enviar en múltiples partes (multipart) secuenciales.

Convención de nombre de archivo (nombre base)

El nombre base del archivo (antes de la extensión) debe cumplir:

T<tipoentidad>\_C<codigoentidad>\_muric\_<PeriodoATransmitir>

T<tipoentidad>: prefijo T + código de tipo de entidad (numérico).

C<codigoentidad>: prefijo C + código de entidad (numérico).

muric: literal en minúsculas.

<PeriodoATransmitir>: fecha del periodo en formato DDMMAAAA.

Ejemplos válidos *single*

T1\_C57\_muric\_30042025.avro.p7z

T22\_C1\_muric\_01052025.avro.p7z

Multipart: cada fragmento usa el mismo nombre + sufijo .partN:

T1\_C57\_muric\_30042025.avro.p7z.part1, ...part2, …, ...partN.

Descripción:

El servicio será expuesto en la dirección (URL)

<https://apim-sfc-prod-cross.azure-api.net/api/muric>.

Método: POST

Headers:

|  |  |  |  |
| --- | --- | --- | --- |
| **Nombre** | **Descripción** | **Ejemplo** | **Obligatorio** |
| Authorization | Token JWT obtenido en el servicio de autenticación | Bearer <jwt> | Si |
| checksum\_original | SHA-256 (hex) del archivo firmado completo (.avro.p7z). | df9b7699ad33af0eb41a1d | Si |
| part\_number | Número de parte (1...N). En single debe ser "1". | 1 | Si |
| total\_parts | Total, de partes (N). En single debe ser "1". | 1 | Si |

**API REST Transmisión de Archivos**

Body: (multipart/form-data):

|  |  |  |
| --- | --- | --- |
| **Nombre** | **Descripción** | **Obligatorio** |
| *file* | Archivo por transmitir. En *single*: T... \_C.. \_muric\_...avro.p7z. En *multipart*: ....avro.p7z.partN. | Si |

Parámetros de entrada (resumen)

Single (<=100MB):

part\_number=1, total\_parts=1.

file: T<tipoentidad>\_C<codigoentidad>\_muric\_<PeriodoATransmitir>.avro.p7z.

Multipart (>100MB):

Enviar N solicitudes (una por parte) en orden 1..N.

file: ... .avro.p7z.partN.

Las partes se deben enviar secuencialmente.

Parámetros de salida:

Single: acuse de recibo del archivo.

Ejemplo — Respuesta

Éxito (última parte, 200 OK):

{

   "status": "Exitoso",

   "response": "Fragmento 1 de 1 recibido y guardado correctamente",

   "error": {

        "tipo\_entidad": < tipo\_entidad >,

        "codigo\_entidad": < codigo\_entidad >,

        "nombre\_modulo": "muric",

        "fecha\_corte": "2025-04-30",

        "fecha\_transmision": "2025-09-02"

    },

   "timestamp": null,

   "status\_code": 200,

   "nombre\_proceso": null,

   "id\_transmision": "50292581"

}

Parámetros de salida:

Multipart: acuse de cada parte.

En la última parte (N de N), la respuesta incluirá id\_transmision cuando la recepción sea exitosa y consistente.

Ejemplo — Respuesta

Éxito (última parte, 200 OK):

{

"status": "Exitoso",

"response": "Fragmento 6 de 6 recibido y guardado correctamente",

"error": {

"tipo\_entidad": < tipo\_entidad >,

"codigo\_entidad": < codigo\_entidad >,

"nombre\_modulo": "muric",

"fecha\_corte": "2023-08-31",

"fecha\_transmision": "2025-08-29"

},

"timestamp": null,

"status\_code": 200,

"nombre\_proceso": null,

"id\_transmision": "19374938"

}

Errores comunes:

400 Bad Request:

El token o el nombre del archivo no es válido

Diferencia entre checksum recibido y checksum calculado.

Ventana de transmisión no habilitada para el periodo solicitado.

5xx Errores del servidor: reintentos con backoff.

Nota: El proceso de trasmisión devuelve en la última parte (o en single), el “id\_transmision” que deberá incluirse en el cuerpo “idTx\_values“ del servicio de consulta de transmisión.

**API REST Consulta de Estado de la Transmisión**

Permite consultar la respuesta asociada a una transmisión previamente registrada.

Descripción:

El servicio será expuesto en la dirección (URL) https//apim-sfc-prod-cross.azure-api.net/salida/respuesta

Método: POST

Headers:

|  |  |  |  |
| --- | --- | --- | --- |
| **Nombre** | **Descripción** | **Ejemplo** | **Obligatorio** |
| Authorization | Token JWT obtenido en el servicio de autenticación | Bearer <jwt> | Si |

**API REST Consulta de Estado de la Transmisión**

Body: multipart/form-data.

|  |  |  |  |
| --- | --- | --- | --- |
| Nombre | Descripción | Ejemplo | Obligatorio |
| idTx\_values | Identificador <id\_transmision> de la transmisión obtenido del Servicio envío información  . | <id\_transmision> | Si |

Parámetros de salida

|  |  |  |  |
| --- | --- | --- | --- |
| **Nombre** | **Tipo** | **Descripción** | **Ejemplo** |
| status | String | Estado textual de la operación (p. ej., OK, Aprobado, error, Error).. | Aprobado / error |
| response | String|Null | Mensaje adicional o null si no aplica. | Archivo de respuesta no encontrado... |
| error | Object|Null | Presente cuando hay error; incluye type, message y content. | { "type":"Error", ... } |
| error.type | String | Tipo o categoría del error. | Error |
| error.message | String | Mensaje de error legible. | Error en el esquema... |
| error.content | Object | Datos de contexto del error (transmisión, entidad, fechas, etc.). | { "id\_transmision":"19374938", ... } |
| timestamp | String | Fecha/hora de la respuesta del servicio. | 2025-09-03T14:39:19.802966 |
| status\_code | String | Código de estado de negocio. No confundir con el código HTTP. | 99 / 400 |
| nombre\_proceso | String | Etapa/proceso que generó la respuesta. | VALIDACION\_ESQUEMA |
| Nombre Modulo | String | Módulo asociado | muric |
| Fecha Transmision | String | Fecha en que se transmitió. Formato puede variar (dd-mm-aaaa / yyyy-mm-dd). | 31-08-2023 / 2025-09-03 |
| Fecha Corte | String | Fecha de corte del contenido transmitido. | 2023-07-31 |

Ejemplos

Respuesta (200 OK, JSON):

{

"Tipo Entidad": "1",

"Codigo Entidad": "57",

"Fecha Corte": "2023-07-31",

"Nombre Modulo": "muric",

"Fecha Transmision": "2025-09-03",

"status": "Aprobado",

"response": null,

"error": null,

"timestamp": "2025-09-03 14:50:54",

"status\_code": "99",

"nombre\_proceso": "VALIDACION DE REGLAS DE NEGOCIO"

}

**API REST Consulta de Estado de la Transmisión**

Respuesta (200 con errores en el contenido transmitido como esquema incorrectos o información que no corresponde a lo reportado en cuentas contables, JSON):

{

    "status": "error",

    "response": null,

    "error": {

        "type": "Error",

        "message": "Error en el esquema del archivo no coinciden con el esquema original",

        "content": {

            "id\_transmision": "19374938",

            "Tipo\_entidad": "1",

            "codigo\_entidad": "57",

            "nombre\_modulo": "muric",

            "fecha\_transmision": "31-08-2023"

        }

    },

    "timestamp": "2025-09-03T14:39:19.802966",

    "status\_code": 400,

    "nombre\_proceso": "VALIDACION\_ESQUEMA"

}

Respuesta (400 Error, JSON):

{

"status": "Error",

"response": "El token no es válido"

}

Errores comunes:

|  |  |
| --- | --- |
| Códigos transmisión bajo estándar HTTP | |
|  |  |
| Código HTTP | Descripción |
| 200 | Archivo transmitido correctamente |
| 400 | No se pudo realizar la transmisión de la información |
| 401 | Token de autorización no válido para el envío de la información |
| 403 | La entidad no tiene permiso para remitir esta información |
| 404 | El endpoint al que se realizó la petición no existe |
| 500 | Se presentó un error interno dentro del proceso de recepción de información |
|  |  |
|  |  |
| **API REST Consulta de Estado de la Transmisión**  Códigos internos / de negocio | |
|  |  |
| Código HTTP | Descripción |
|  |  |
| 413 | Tamaño del archivo es cero |
| 510 | La cantidad de chunks recibidos no coincide con la cantidad de chunks transmitidos |
| 511 | El checksum transmitido por la entidad es diferente al checksum calculado al reconstruir el archivo |
| 512 | Se presentó un error al reconstruir el archivo enviado |
| 513 | El archivo fue reconstruido de forma exitosa |
| 121 | Transmisión por validar (previo a reglas de lógica y de negocio) |
| 300 | Validación de información correcta |
| 301 | Validación de información errada |
| 303 | Información recibida validación pendiente |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

## Superfinanciera Archivos (Canal Alterno)

Este canal alterno se aplica para las entidades que soliciten transmisión por este método o en casos en los que el servicio de API no esté disponible.

Tramite Superfinanciera archivos:

En caso de estar interesado en usar este canal, podrán hacer la solicitud siguiendo las instrucciones del manual de usuario A-DT-GTI-001 ubicado en la sección documentos técnicos de la página de la Superintendencia Financiera.

**Notas y recomendaciones**

Trazabilidad: Conservar el código de identificación de transmisión (CIDT) como soporte.

Retransmisión: se debe hacer por este mismo canal, evitando enviar el mismo archivo por múltiples canales.

Formato de archivo: Se deben reportar los mismos formatos AVRO firmados y la misma nomenclatura usada en la transmisión usando API REST.

Estructura y nomenclatura: Subir un único archivo completo (no por partes)  
 T<tipoentidad>\_C<codigoentidad>\_muric\_<ddmmaaaa>.avro.p7z

**Superfinanciera SFTP (Canal de Contingencia)**

Canal de contingencia para transmisión del mismo archivo AVRO firmado que se reporta por API REST o Superfinanciera Archivos, usando SFTP (SSH2). Los parámetros operativos (host, puerto, usuario, llave pública/huella y rutas) serán comunicados por la SFC.

Parámetros operativos (definidos por SFC)

Host: <sftp.host.sfc.gov.co>

Puerto: 22 (salvo indicación distinta)

Usuario: <asignado\_por\_SFC>

Autenticación: Llave pública (ed25519 o RSA-2048/4096). No se habilita acceso shell.

Estructura y nomenclatura

Subir un único archivo completo (no por partes):

T<tipoentidad>\_C<codigoentidad>\_muric\_<ddmmaaaa>.avro.p7z

**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.

**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.

**Canales de comunicación para la atención técnica**

Mesa de servicio SFC: [www.superfinanciera.gov.co](https://www.superfinanciera.gov.co)

[https://www.superfinanciera.gov.co/publicaciones/10100576/industrias-supervisadasinteres-del-vigila…](https://www.superfinanciera.gov.co/publicaciones/10100576/industrias-supervisadasinteres-del-vigiladotramitestramites-en-linea-y-remision-de-informacion-10100576/)

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

El contenido generado por IA puede ser incorrecto.

Hacer clic sobre la opción de chat

# 3. Anexos

# 4. Historial de cambios

|  |  |  |
| --- | --- | --- |
| **Fecha** | **Versión** | **Cambios** |
| 18/02/2025 | 1 | Versión inicial |
| 08/09/2025 | 2 | Versión inicial 1.1 |