

CONSTRUCCIÓN WEB SERVICE SMARTSUPERVISION

**SEPTIEMBRE 2024**

**OBJETIVO**

Explicar la funcionalidad de los Recursos REST que se expondrá a las entidades vigiladas para mantener su información de quejas o reclamos para su respectiva gestión al día y disponible cuando la Superintendencia Financiera de Colombia lo requiera.

Estos recursos REST deben ser consumidos por cada una de las entidades sometidas a vigilancia verificando los lineamientos de este documento suministrados por la Superintendencia Financiera de Colombia.

**ASPECTOS TECNOLÓGICOS**

# DEFINICIONES

* + **REST (Representational State Transfer o Transferencia de estados representacional):** Estilo de arquitectura de comunicación entre un cliente y un servidor, comúnmente entre una URI (servidor) y un cliente (cliente) en donde el tipo de mensajes puede ser JSON o XML entre los más comunes. Es combinado generalmente con el protocolo de transporte HTTP para la interoperabilidad entre sistemas de información.
  + **JSON (JavaScript Object Notation o Notación de Objetos JavaScript):** Formato de intercambio ligero de datos. La gran propiedad es que es legible y entendible por humanos y de la misma forma es fácil para los sistemas su generación e interpretación.
  + **JWT:** es un estándar abierto basado en JSON propuesto por IETF (RFC 7519) para la creación de tokens de acceso que permiten la propagación de identidad y privilegios. El token está compuesto por tres partes header (identifica qué algoritmo fue usado para generar la firma), payload (contiene información básica del usuario y el tiempo de expiración del token), signature (es la firma de la información del token creada a través de la llave del servidor).
  + **HMAC:** Es una construcción específica para calcular un código de autentificación de mensaje (MAC) que implica una función hash criptográfica en combinación con una llave criptográfica secreta. Como cualquier MAC, puede ser utilizado para verificar simultáneamente la integridad de los datos y la autentificación de un mensaje.
  + **Recurso REST:** Elemento expuesto que cumple la especificación REST mediante una URI (Identificador Uniforme de Recurso) a través de HTTP para intercambiar representaciones (tramas) de información. Este recurso está expuesto para el consumo de conectores que reciben y procesan la información.
  + **Endpoint:** Dirección completa que incluye una URL base más los parámetros necesarios (obligatorios u opcionales) para su ejecución.
  + **URL Base:** Dirección raíz para el consumo del REST.

# Estructura canónica

**Request**

**{**

**"Header":{**

**“Authorization”: “<Token>”, “Cache-Control”: ”no-cache”, “accept”: “aplication/json”, “content-type”: “aplication/json”,**

**“Accept-Language”: “[<es> or <en>]”, “X-SFC-Signature”: “<Signature>”**

**},**

**"Body":{**

**}**

**}**

**"Entity":"<Estructura de datos JSON>"**

**Response:**

**{**

**"status\_code":"<S: Success | E: Error>",**

**"messages": ["<Mensaje ‘Transacción exitosa’ o el mensaje de error>"]**

**}**

# Definición de la exposición del servicio

La exposición del recurso estará sujeta a las siguientes características:

* + La implementación del recurso REST deberá seguir lo/s lineamientos tecnológicos descritos por el estándar REST y JSON. Por consiguiente, no se permitirá la implementación de Web Services tipo SOAP ni de otra tecnología.
  + El método HTTPS usado para la comunicación entre el recurso REST y el cliente será GET, POST y PUT.
  + El recurso GET debe solamente enviar peticiones tipo JSON y en la propiedad Content-Type del encabezado HTTPS debe ser application/json.
  + Dentro de las cabeceras de cada petición deberá ir el atributo X-SFC-Signature con la firma de los datos que viajan dentro de la petición. Para las peticiones GET se debe utilizar la url completa (con los query params) con el fin de generar la firma de forma correcta. Para peticiones POST, PUT se debe usar todo el cuerpo de la petición (JSON) convertidos en una cadena de texto.
  + Para las firmas se debe usar el algoritmo de cifrado HMAC-SHA256 y firmarlos con el secret asignado a cada entidad vigilada.
  + Cada ejecución de un Endpoint, entrega: Un código de resultado: RESPONSE
    - El RESPONSE, es un código que representa el resultado de la ejecución:
      * 200: resultado satisfactorio
      * 400: problema en la ejecución
      * 500: problema en el servicio (interno)

# Definición de campos del archivo

Una vez definido el archivo de integración, primero, se explica mediante un ejemplo cómo funciona POST para autenticación en los servicios:

*“https://UrlBase/api/login/”*

Después de autenticarse exitosamente, el servidor retorna dos token’s, el primero como token de acceso (access token) que tendrá una duración de **30 minutos** y el segundo (refresh token) token servirá para actualizar el token de acceso, este tendrá una vigencia de **12 horas**. Pasado este tiempo la sesión expira y es necesario autenticarse nuevamente para obtener un nuevo par de token’s (access token y refresh token). En caso de ingresar datos de autenticación incorrectos el método retornará error.

Es necesario que se cuente con la siguiente información para autenticarse:

* + username: Es el usuario asignado, con el cual se va a autenticar.
  + password: Es la contraseña asignada al usuario.
  + secret key: Es la llave secreta que se utiliza para firmar las peticiones

Dicha identificación les permitirá a las Entidades vigiladas generar un token de acceso para conectarse a la Superintendencia Financiera de Colombia para envío o disposición de información.

# MOMENTO 1

***Las entidades vigiladas deberán capturar la información por medio de API REST de las quejas o reclamos interpuestos por los consumidores financieros a través del portal SmartSupervisión de la Superintendencia Financiera de Colombia.***

* + *La Superintendencia Financiera de Colombia pone a disposición del consumidor financiero un formulario para la interposición de quejas o reclamos para el diligenciamiento de la información por parte del mismo.*
  + *El consumidor financiero requiere interponer una queja o reclamo dentro del portal web de la Superintendencia Financiera de Colombia o punto de servicio al ciudadano.*
* *La información recolectada de dicho formulario será guardada en SmartSupervision dentro de nuestra nube pública.*
* *La información, después de estar alojada en nuestra nube pública, será recolectada por la entidad vigilada ante la cual el consumidor financiero está interponiendo la queja o reclamo.*
* *La Entidad vigilada hace el llamado al servicio de inicio de sesión enviando los parámetros requeridos y obtiene los token’s como respuesta del servicio de inicio de sesión.*
* *Una vez se logra la autenticación y manteniendo la sesión por medio del access token, se pueden realizar peticiones para obtener recursos.*
* *La entidad vigilada consumirá la información por medio del API REST que será expuesto por parte de la Superintendencia Financiera de Colombia mediante el método (GET) donde se podrá realizar peticiones para obtener recursos que estarán agrupados en cierto número de páginas (vbgr páginas de 100 recursos, de un total de 1000 que nos darán 10 páginas o de la petición:*
  + URI: https://UrlBase/api/queja/
  + Tipo: GET
  + Encabezados requeridos:
    - Content-Type: application/json
    - Authorization: <token>
    - X-SFC-Signature: <signature>

**Actualización de endpoint para Control de cambios Fraude**

**Para este endpoint que permite obtener el listado de quejas con sus respectivos atributos y/o parámetros necesarios se agregan los campos fraude\_tipologia, fraude\_modalidad, monto\_reclamado y monto\_reconocido, en la respuesta dentro del parámetro de salida.**

* *A continuación, se muestra la descripción de los campos que se envían a la entidad vigilada haciendo uso del método:*

|  |  |  |  |
| --- | --- | --- | --- |
| ***Nombre*** | ***Campo*** | ***Tipo*** | ***Longitud*** |
| **Tipo de Entidad** | tipo\_entidad | Numérico | 3 |
| **Código de Entidad** | entidad\_cod | Numérico | 5 |
| **Fecha y hora de creación** | fecha\_creacion | Fecha | YYYY-MM-DD THH:MM:SS |
| **Código de la queja** | codigo\_queja | Texto | 30 |
| **Código País** | codigo\_pais | Alfanumérico | 3 |
| **Departamento** | departamento\_cod | Alfanumérico | 3 |
| **Municipio** | municipio\_cod | Alfanumérico | 5 |
| **Nombre o razón social del consumidor financiero** | Nombres | Texto | 50 |
| **Tipo identificación del consumidor financiero** | tipo\_id\_CF | Numérico | 2 |
| **Número de identificación del consumidor financiero** | numero\_id\_CF | Texto | **15** |
| **Teléfono** | Teléfono | Texto | 15 |
| **Correo electrónico** | Correo | Texto | 50 |
| **Dirección** | Dirección | Texto | 250 |
| **Tipo de persona** | tipo\_persona | Numérico | 1 |
| **Sexo** | Sexo | Numérico | 2 |
| **LGBTIQ+** | Lgbtiq | Numérico | 1 |
| **Canal** | canal\_cod | Numérico | 2 |
| **Condición especial** | condicion\_especial | Numérico | 2 |
| **Producto** | producto\_cod | Numérico | 5 |
| **Detalle del producto** | producto\_nombre | Texto | 100 |
| **Motivo** | macro\_motivo\_cod | Numérico | 5 |
| **Texto de la queja** | texto\_queja | Texto | **4500** |
| **Anexos de la queja** | anexo\_queja | Booleano |  |
| **Tutela** | Tutela | Numérico | 2 |
| **Ente de control** | ente\_control | Numérico | 2 |
| **Escalamiento al defensor del consumidor financiero** | escalamiento\_DCF | Numérico | 2 |
| **Réplica** | Replica | Numérico | 2 |
| **Argumento réplica** | argumento\_replica | Texto | 1000 |
| **Desistimiento** | desistimiento\_queja | Numérico | 2 |
| **Queja Exprés** | queja\_expres | Numérico | 2 |
| **¡TIpología de fraude** | **fraude\_tipologia** | **Id**  **(entero)** | **3** |
| **¡Modalidad de fraude** | **fraude\_modalidad** | **Id**  **(entero)** | **3** |
| **¡Monto reclamado** | **monto\_reclamado** | **Numérico (Double)** | **No aplica** |
| **¡Monto reconicido** | **monto\_reconocido** | **Numérico (Double)** | **No aplica** |



# Estructura JSON expuesta por la SFC (Momento 1)

**Request: GET**

**{**

**"Headers":{**

**“Authorization”: “<Token>”, “Cache-Control”: ”no-cache”, “Accept”: “aplication/json”, “Content-type”: “aplication/json”,**

**“Accept-Language”: “[<es> or <en>]”, “X-SFC-Signature”: “<Signature>”**

**}**

**}**

**Response: 200 OK**

**{**

**"Headers":{**

**“Content-type”: “aplication/json”, “Content-Language”: “[<es> or <en-us>]”**

**},**

**"Response":{**

**“count”: ””,**

**“pages”: “”,**

**“current\_page”: “”,**

**“next”: “”,**

**“previous”: “”, “results“:[**

**{**

**"tipo\_entidad ":"",**

**"entidad\_cod”:””, “fecha\_creacion”: ””, “codigo\_queja”: ””,**

**“codigo\_pais”: ””; “departamento\_cod” :””, “municipio\_cod” :””,**

**“nombres” :””,**

**“tipo\_id\_CF” :””,**

**“numero\_id\_CF” :””;**

**“telefono” :””;**

**“correo” :””;**

**“tipo\_persona” :””,**

**“sexo”:” ”;**

**“lgbtiq” :””;**

**“canal\_cod”:””, “condicion\_especial” :””, “producto\_cod” :””, “producto\_nombre” :””, “macro\_motivo\_cod” :””,**

**“texto\_queja”:””,**

**“anexo\_queja”:””,**

**“tutela”:””,**

**“ente\_control”:””, “escalamiento\_DCF ”:””, “replica ”:””, “argumento\_replica”:””, “desistimiento\_queja”:””, “queja\_expres”:””**

**“fraud\_typology”:1,**

**“fraud\_modality”:1,"**

**“monto\_reclamado”: 2000,**



**“monto\_reconocido”:2000**

**}**

**]**

**}**

**}**

*O Una vez sincronizadas las quejas o reclamos, la entidad vigilada tiene la obligación de informar el recibido a satisfacción de las mismas, consumiendo el endpoint api/complaint/ack/; allí el servicio esperará un array de no más de 100 registros con los códigos de las quejas o reclamos sincronizados y procederá a realizar la marcación para cada una de estas y así no presentarlas en la siguiente consulta de la entidad vigilada. Una vez visualizada la queja o reclamo se tendrá un máximo de 48 horas para informar el recibido, de lo contrario el sistema generará la marcación de forma automática.*

# Momento 1 - ACK

* + *Detalles de la petición:*
    - URI: https://UrlBase/api/complaint/ack/
    - Tipo: POST
    - Longitud campo prqs :únicamente se realizará el ack de los primeros 100 registros enviados en el el vector ***pqrs.***
    - Encabezados requeridos:
      * Content-Type: application/json
      * Authorization: <Token>
      * X-SFC-Signature: <Signature>
* *A continuación, se muestra la descripción de los campos que se retornan a la entidad vigilada haciendo el consumo del método:*

|  |  |  |  |
| --- | --- | --- | --- |
| ***Nombre*** | ***Campo*** | ***Tipo*** | ***Longitud*** |
| **mensaje** | **Message** | Texto | N/A |
| **quejas fallidas** | **pqrs\_error** | Lista | 100 |

* *A continuación, se muestra la descripción de los campos que envían las entidades vigiladas haciendo uso del servicio expuesto por la Superintendencia Financiera de Colombia para el envío de la información:*

|  |  |  |  |
| --- | --- | --- | --- |
| ***Nombre*** | ***Campo*** | ***Tipo*** | ***Longitud*** |
| **quejas** | **Pqrs** | Lista | max. 100 |

# Estructura JSON expuesta por la SFC (Momento 1 ACK)

**Request: POST**

**{**

**"Headers":{**

**“Authorization”: “<Token>”,**

**},**

**"body":{**

**“Cache-Control”: ”no-cache”, “Accept”: “aplication/json”, “Content-type”: “aplication/json”,**

**“Accept-Language”: “[<es> or <en>]”, “X-SFC-Signature”: “<Signature>”**

**“pqrs”: [**

**“ID\_QUEJA\_1”, “ID\_QUEJA\_2”, “ID\_QUEJA\_3”,**

**…………………. “ID\_QUEJA\_n”,**

**]**

**}**

**}**

**Response: 200 OK**

**{**

**"Headers":{**

**“Content-type”: “aplication/json”, “Content-Language”: “[<es> or <en-us>]”**

**},**

**"Response":{**

**“message”;”Código actualizado”, “pqrs\_error”: []**

**}**

**}**

# Momento 1 - Transferencia de archivos

* + *Los archivos cargados al sistema son validados por un antivirus en tiempo real, el cual genera las alertas pertinentes, y los envía dentro de la zona de cuarentena para cada uno de los archivos que se consideren sospechosos. (Las entidades vigiladas pueden realizar de forma voluntaria una validación externa si así lo desea).*
  + *El valor del campo* ***referencia*** *se retorna en la respuesta que devuelve el servicio al momento de ser consumido, corresponde con los siguientes valores:*

*{*

1. *: ‘queja’,*
2. *: ‘apoderado’,*
3. *: ‘replica’,*
4. *: ‘escalonamiento’, 5 : ‘anexo nuevo’,*
5. *: ‘gestion’*
6. *: ‘respuesta’*

*}*

*Nota: La entidad recibirá el ID de la referencia del anexo.*

* + *Detalles de la petición:*
    - URI:

https://UrlBase/api/storage/?codigo\_queja codigo\_queja=<codigo\_queja>

* + - Tipo: GET
    - Encabezados requeridos:
      * Content-Type: application/json
      * Authorization: <Token>
      * X-SFC-Signature: <Signature>
* *A continuación, se muestra la descripción de los campos que se retornan a la entidad vigilada haciendo el consumo del método:*

|  |  |  |  |
| --- | --- | --- | --- |
| **Nombre** | **Campo** | **Tipo** | **Longitud** |
| **Identificador** | Id | Numérico(Long) | - |
| **Archivo(URL)** | File | File | 30 MB // Nombre archivo -> máximo 150 caracteres |
| **Tipo de Archivo** | Type | Texto | 100 |
| **Estado del archivo** | State | Numérico | 1 |
| **Código de la Queja** | codigo\_queja | Numérico | 30 |
| **Referencia** | Reference | Numérico | 1 |

# Estructura JSON expuesta por la SFC (Momento 1 - transferencia de archivos)

**Request: GET**

**{**

**"Headers":{**

**“Authorization”: “<Token>”, “Cache-Control”: ”no-cache”, “Accept”: “aplication/json”, “Content-type”: “aplication/json”,**

**“Accept-Language”: “[<es> or <en>]”, “X-SFC-Signature”: “<Signature>”**

**},**

**“Query Params”: [?codigo\_queja codigo\_queja=<codigo\_queja>]**

**}**

**Response: 200 OK**

**{**

**"Headers":{**

**“Content-type”: “aplication/json”, “Content-Language”: “[<es> or <en-us>]**

**},**

**"Response":{**

**“count”: ””,**

**“pages”: “”,**

**“current\_page”: “”,**

**“next”: “”,**

**“previous”: “”,**

**"results":"[**

**{**

**}**

**“id”: “”,**

**“file”: “”**

**“type”: “”,**

**“state”: “”,**

**“codigo\_queja”: “”,**

**“reference”:””,**

**]**

**}**

**}**

# MOMENTO 2

***La Superintendencia Financiera de Colombia recibirá información de la interposición de quejas o reclamos de los consumidores financieros ante las entidades vigiladas.***

* + *La entidad vigilada recolecta la información la cual debe ser enviada al servicio expuesto por la Superintendencia Financiera de Colombia.*
* *La Superintendencia Financiera de Colombia tendrá el servicio expuesto para el envío de la información recolectada. Para ello se hace uso del método del api/queja/ enviando la información de encabezado y cuerpo de petición.*

**Actualización de endpoint para Control de cambios Fraude**

**Para este endpoint que permite obtener el listado de quejas con sus respectivos atributos y/o parámetros necesarios se agregan los ¡campos fraude\_tipologia, fraude\_modalidad, monto\_reclamado y monto\_reconocido, en la respuesta de entrada y salida..**

* *Detalles de la petición:*
  + URI: https://UrlBase/api/queja/
  + Tipo: POST
  + Encabezados requeridos:
    - Content-Type: application/json
    - Authorization: <Token>
    - X-SFC-Signature: <Signature>
* *A continuación, se muestra la descripción de los campos que envían las entidades vigiladas haciendo uso del servicio expuesto por la Superintendencia Financiera de Colombia para el consumo de la información:*



|  |  |  |  |
| --- | --- | --- | --- |
| ***Nombre*** | ***Campo*** | ***Tipo*** | ***Longitud*** |
| **Código de la queja o reclamo** | codigo\_queja | Texto | 30 |
| **Código País** | codigo\_pais | Alfanumérico | 3 |
| **Departamento** | departamento\_cod | Alfanumérico | 3 |
| **Municipio** | municipio\_cod | Alfanumérico | 5 |
| **Canal** | canal\_cod | Numérico | 2 |
| **Producto** | producto\_cod | Numérico | 5 |
| **Motivo** | macro\_motivo\_cod | Numérico | 5 |
| **Fecha y hora de creación** | fecha\_creacion | Fecha | YYYY-MM-DDTH H:MM:SS |
| **Nombre o razón social del consumidor financiero** | Nombres | Texto | 50 |
| **Tipo identificación del consumidor financiero** | tipo\_id\_CF | Numérico | 2 |
| **Número de identificación del consumidor financiero** | numero\_id\_CF | Texto | **15** |
| **Tipo de persona** | tipo\_persona | Numérico | 1 |
| **Instancia de recepción** | insta\_recepcion | Numérico | 2 |
| **Punto de recepción** | punto\_recepcion | Numérico | 2 |
| **Admisión** | admision | Numérico | 2 |
| **Texto de la queja o reclamo** | texto\_queja | Texto | **4500** |
| **Anexos de la queja o reclamo** | anexo\_queja | Booleano | N/A |
| **Ente de control** | ente\_control | Numérico | 2 |
| **¡TIpología de fraude** | **fraude\_tipologia** | **Id**  **(entero)** | **3** |
| **¡Modalidad de fraude** | **fraude\_modalidad** | **Id**  **(entero)** | **3** |
| **¡Monto reclamado** | **monto\_reclamado** | **Numérico (Double)** | **No aplica** |
| **¡Monto reconicido** | **monto\_reconocido** | **Numérico (Double)** | **No aplica** |



# Estructura JSON expuesta por la SFC (Momento 2)

**Request: POST**

**{**

**"Headers":{**

**“Authorization”: “<Token>”, “Cache-Control”: ”no-cache”, “Accept”: “aplication/json”, “Content-type”: “aplication/json”,**

**“Accept-Language”: “[<es> or <en>]”, “X-SFC-Signature”: “<Signature>”**

**},**

**"Body":{**

**}**

**}**

**“codigo\_queja” :””,**

**“codigo\_pais” :””, “departamento\_cod” :””, “municipio\_cod” :””,**

**“canal\_cod” :””,**

**“producto\_cod” :””, “macro\_motivo\_cod” :””, “fecha\_creación” :””, “nombres”:””,**

**“tipo\_id\_CF” :””,**

**“numero\_id\_CF” :””,**

**“tipo\_Persona” :””, “insta\_recepcion” :””, “punto\_recepcion” :””, “admision” :””,**

**“texto\_queja”:””,**

**“anexo\_queja”:””, “ente\_control”:””**

**Response: 201 CREATED**

**{**

**"Headers":{**

**“Content-type”: “aplication/json”, “Content-Language”: “[<es> or <en-us>]”**

**},**

**"Response":{**

**“codigo\_queja” :””,**

**“codigo\_pais” :””, “departamento\_cod” :””, “municipio\_cod” :””,**

**“canal\_cod” :””,**

**“producto\_cod” :””, “macro\_motivo\_cod” :””, “fecha\_creación” :””, “nombres”:””,**

**“tipo\_id\_CF” :””,**

**“numero\_id\_CF” :””,**

**“tipo\_Persona” :””,**

**“insta\_recepcion” :””, “punto\_recepcion” :””, “admision” :””;,**

**“texto\_queja”:””,**

**“anexo\_queja”:””, “ente\_control”:””**

**“fraud\_typology”:1,**

**“fraud\_modality”:1,**

**“monto\_reclamado”: 2000,**



**“monto\_reconocido”:2000**

**}**

**}**

***NOTA: ES IMPORTANTE QUE EN EL CODIGO\_QUEJA, TODAS LAS ENTIDADES ENVÍEN EL TIPO DE ENTIDAD Y CÓDIGO DE ENTIDAD ANTEPUESTO AL CÓDIGO DE LA QUEJA EN EL MOMENTO 2.***

***Ejemplo:***

Tipo de entidad: 1  
Código de entidad: 423  
Código de queja:16551509974606  
Resultado: 142316551509974606

# Momento 2 - Transferencia de archivos

* + *Se deberán enviar los anexos que se hayan generado en el seguimiento de quejas o reclamos por parte de la entidad vigilada.*
    - *Los archivos cargados al sistema deberán ser validados por las entidades vigiladas, garantizando que no habrá vulnerabilidad por parte de archivos maliciosos. El sistema (antivirus) elegido por cada entidad vigilada para realizar este proceso es de libre elección siempre y cuando se pueda garantizar lo anteriormente mencionado.*

*La firma correspondiente para este servicio se realiza con los campos*

*<codigo\_queja> y <type>, por ende, se debe omitir el campo <file>.*

* *Detalles de la petición:*
  + URI: https://UrlBase/api/storage/
  + Tipo: POST
  + Encabezados requeridos:
    - Content-Type: multipart/form-data
    - Authorization: <Token>
    - X-SFC-Signature: <Signature>
* *A continuación, se muestra la descripción de los campos que envían las entidades vigiladas haciendo uso del servicio expuesto por la Superintendencia Financiera de Colombia para el envío de la información:*

|  |  |  |  |
| --- | --- | --- | --- |
| **Nombre** | **Campo** | **Tipo** | **Longitud** |
| **Archivo** | File | File | 30 MB // Nombre archivo -> máximo 150 caracteres |
| **Código de la queja** | codigo\_queja | Numérico | 30 |
| **Tipo de Archivo** | Type | Texto | 100 |

# Estructura JSON expuesta por la SFC (Momento 2 - transferencia de archivos)

**Request: POST**

**{**

**"Headers":{**

**“Authorization”: “<Token>”, “Cache-Control”: ”no-cache”, “Accept”: “\*/\*”,**

**“Content-type”: “multipart/form-data”, “Accept-Language”: “[<es> or <en>]”, “X-SFC-Signature”: “<Signature>”**

**},**

**"Body":{**

**}**

**}**

**“file” :””,**

**“codigo\_queja”:””,**

**“type”: ””**

**Response: 201 CREATED**

**{**

**"Headers":{**

**“Content-type”: “aplication/json”, “Content-Language”: “[<es> or <en-us>]”**

**},**

**"Response":{**

**“id” :””;**

**“file”:””,**

**“type”:””,**

**“state”: ””, “codigo\_queja”: ””**

**}**

**}**

# MOMENTO 3

***La Superintendencia Financiera de Colombia recibirá la información derivada del proceso de gestión de las quejas o reclamos, llevado a cabo por parte de las entidades vigiladas.***

* + *Después de la recolección de información, esta será enviada por la entidad vigilada, para ser almacenada en la base de datos dentro de smartsupervision, que está alojada en la nube pública de la Superintendencia Financiera de Colombia.*
* *Las entidades vigiladas, utilizarán el servicio expuesto por la Superintendencia Financiera de Colombia, donde enviarán la información derivada de la gestión suministrada por la propia entidad vigilada para ello se hace uso del método del api api/queja/<codigo queja>/ enviando la información de encabezado y cuerpo de petición.*
* *Se deben verificar las restricciones de gestión de cierre de quejas con respecto a los documentos de respuesta final definidas en la siguiente sección* ***Momento 3 - Transferencia de archivos***

**Actualización de endpoint para Control de cambios Fraude**

**Para este endpoint que permite obtener el listado de quejas con sus respectivos atributos y/o parámetros necesarios se agregan los campos ¡fraude\_tipologia, fraude\_modalidad, monto\_reclamado y monto\_reconocido, en la respuesta de entrada y salida.**

* *Detalles de la petición:*
  + URI: https://UrlBase/api/queja/<codigo\_queja>/
  + Tipo: PUT/PATCH
  + Encabezados requeridos:
    - Content-Type: application/json
    - Authorization: <Token>
    - X-SFC-Signature: <Signature>
* *A continuación, se muestra la descripción de los campos que envían las entidades vigiladas haciendo uso del servicio expuesto por la Superintendencia Financiera de Colombia para el consumo de la información:*

|  |  |  |  |
| --- | --- | --- | --- |
| **Nombre** | **Campo** | **Tipo** | **Longitud** |
| **Código de la queja o reclamo** | codigo\_queja | Texto | 30 |
| **Sexo** | Sexo | Numérico | 2 |
| **LGBTIQ+** | Lgbtiq | Numérico | 1 |
| **Condición especial** | condicion\_especial | Numérico | 2 |
| **Canal** | canal\_cod | Numérico | 2 |
| **Producto** | producto\_cod | Numérico | 5 |
| **Motivo** | macro\_motivo\_cod | Numérico | 5 |
| **Estado de la queja o reclamo** | estado\_cod | Numérico | 2 |
| **Fecha de actualización** | fecha\_actualizacion | Fecha | YYYY-MM-DDTHH:MM: SS |
| **Producto digital** | producto\_digital | Numérico | 1 |
| **Favorabilidad** | a\_favor\_de | Numérico | 2 |
| **Aceptación** | aceptacion\_queja | Numérico | 2 |
| **Rectificación** | rectificacion\_queja | Numérico | 2 |
| **Desistimiento** | desistimiento\_queja | Numérico | 2 |
| **Prórroga** | prorroga\_queja | Numérico | 2 |
| **Admisión** | Admisión | Numérico | 2 |
| **Documentación de respuesta final** | documentacion\_rta\_final | Booleano |  |
| **Anexos a la respuesta final** | anexo\_queja | Booleano |  |
| **Fecha de cierre** | fecha\_cierre | Fecha | YYYY-MM-DDTHH:MM: SS |
| **Tutela** | Tutela | Numérico | 2 |
| **Ente de control** | ente\_control | Numérico | 2 |
| **Marcación** | Marcación | Numérico | 2 |
| **Queja Exprés** | queja\_expres | Numérico | 2 |
| **¡TIpología de fraude** | **fraude\_tipologia** | **Id**  **(entero)** | **3** |
| **¡Modalidad de fraude** | **fraude\_modalidad** | **Id**  **(entero)** | **3** |
| **¡Monto reclamado** | **monto\_reclamado** | **Numérico (Double)** | **No aplica** |
| **¡Monto reconicido** | **monto\_reconocido** | **Numérico (Double)** | **No aplica** |



# Estructura JSON expuesta por la SFC (Momento 3)

**Request: PUT/PATCH**

**{**

**"Headers":{**

**“Authorization”: “<Token>”, “Cache-Control”: ”no-cache”, “Accept”: “aplication/json”, “Content-type”: “aplication/json”,**

**“Accept-Language”: “[<es> or <en>]”, “X-SFC-Signature”: “<Signature>”},**

**"Body":{“codigo\_queja” :””,**

**“sexo”:””,**

**“lgbtiq” :””, “condicion\_especial” :””, “canal\_cod” :””,**

**“producto\_cod” :””, “macro\_motivo\_cod”:””,**

**“estado\_cod”:””, “fecha\_actualizacion”:””, “producto\_digital”:””, “a\_favor\_de”:””, “aceptacion\_queja”:””, “rectificacion\_queja”:””, “desistimiento\_queja”:””, “prorroga\_queja”:””, “admision” :””, “documentacion\_rta\_final”:””, “anexo\_queja”:””,**

**“fecha\_cierre”:””,**

**“tutela”:””,**

**“ente\_control”:””,**

**“marcacion”:””, “queja\_expres”:””**

**“fraud\_typology”:1,**

**“fraud\_modality”:1,"**



**“monto\_reclamado”: 2000,**

**“monto\_reconocido”:2000**

**}**

**}**

**Response: 200 OK**

**{**

**"Headers":{**

**“Content-type”: “aplication/json”, “Content-Language”: “[<es> or <en-us>]”**

**},**

**"Response":{**

**“codigo\_queja” :””,**

**“sexo”:” ”,**

**“lgbtiq” :””, “condicion\_especial” :””, “canal\_cod” :””,**

**“producto\_cod” :””, “macro\_motivo\_cod”:””, “estado\_cod”:””, “fecha\_actualizacion”:””, “producto\_digital”:””, “a\_favor\_de”:””, “aceptacion\_queja”:””, “rectificacion\_queja”:””, “desistimiento\_queja”:””, “prorroga\_queja”:””, “admision” :””, “documentacion\_rta\_final”:””, “anexo\_queja”:””,**

**“fecha\_cierre”:””,**

**“tutela”:””,**

**“ente\_control”:””,**

**“marcacion”:””, “queja\_expres”:””**

**}**

**}**

# Momento 3 - Transferencia de archivos

* + *Se deberán enviar los anexos que se hayan generado en el seguimiento de la queja o reclamos por parte de la entidad vigilada.*
    - *Los archivos cargados al sistema deberán ser validados por las entidades vigiladas, garantizando que no habrá vulnerabilidad por parte de archivos maliciosos. El sistema (antivirus) elegido por cada entidad vigilada para realizar este proceso es de libre elección siempre y cuando se pueda garantizar lo anteriormente mencionado.*

*La firma correspondiente para este servicio se realiza con los campos*

*<codigo\_queja> y <type>, por ende se debe omitir el campo <file>.*

* *Detalles de la petición:*
  + URI: https://UrlBase/api/storage/
  + Tipo: POST
  + Encabezados requeridos:
    - Content-Type: multipart/form-data
    - Authorization: <Token>
    - X-SFC-Signature: <Signature>
* El primer paso que deben realizar las entidades vigiladas para realizar gestiones por Momento 3 es enviar los documentos anexos, posteriormente realizar las gestiones pertinentes.
* En caso tal que se desee realizar una gestión de cierre, la entidad debe enviar previamente un documento de respuesta final el cual debe contener en el afijo1 de su nombre la siguiente nomenclatura definida por la SFC: **RESP\_FINAL\_SFC**, tal como se indica en el siguiente ejemplo**.**

***“nombre\_de\_archivo\_ejemplo\_RESP\_FINAL\_SFC\_1.docx”***

* Consideraciones a tener en cuenta para la gestión de cierre de quejas*:*
  + Si la queja se gestiona con el valor 4 en el campo estado\_cod y existe un documento con la nomenclatura definida en su nombre, se cierra la queja.
  + Si la queja se gestiona con el valor 4 en el campo estado\_cod y NO existe un documento con la nomenclatura definida en su nombre, NO se cierra la queja.
  + Si la queja se gestiona con un valor diferente de 4 en el campo estado\_cod y existe un documento con la nomenclatura definida en su nombre, se genera alerta y no se permite la gestión.
  + Si la queja se gestiona con un valor diferente de 4 en el campo **estado\_cod** y NO existe un documento con la nomenclatura definida en su nombre, se permite la gestión.
* En caso tal que se desee realizar una gestión de fraude, la entidad debe enviar previamente un documento de fraude el cual debe contener en el sufijo2 de su nombre la siguiente nomenclatura definida por la SFC: **INV\_FRAUDE\_SFC**, tal como se indica en el siguiente ejemplo**.**

***“nombre\_de\_archivo\_ejemplo\_INV\_FRAUDE\_SFC\_1.docx”***

* Consideraciones a tener en cuenta para gestión de fraude en las quejas*:*
* Si un documento tiene los dos sufijos, se rechaza la gestión y se indica que se deben enviar los documentos por separado.
* Si llegan dos documentos: Cierre “RESP\_FINAL\_SFC” e investigación “INV\_FRAUDE\_SFC”:
  + Se toma el documento de investigación y se hacen las validaciones necesarias:
    - Que la queja tenga un motivo de fraude.
    - Si no tiene motivo fraude se indica que no puede realizar la gestión.
    - Si tiene motivo fraude, se permite la gestión.

1 Afijo que se añade al final de una palabra o de su raíz para formar una palabra derivada.

* + Se toma el documento de cierre y se hacen las validaciones de cierre, indicadas en el ítem anterior.
* Si se tiene un cierre de la queja previo a la gestión, solo se podrá hacer gestión de investigación por fraude.
* Si no se tiene cierre, se evalúa la gestión: Se toma el documento de investigación y se hacen las validaciones necesarias:
  + Que la queja tenga un motivo de fraude.
  + Si no tiene motivo fraude se indica que no puede realizar la gestión.
  + Si tiene motivo fraude, se permite la gestión.
* *A continuación, se muestra la descripción de los campos que envía la entidad vigilada haciendo uso del método:*

|  |  |  |  |
| --- | --- | --- | --- |
| **Nombre** | **Campo** | **Tipo** | **Longitud** |
| **Archivo(s)** | File | File | 30 MB // Nombre archivo -> máximo 150 caracteres |
| **Código de la queja** | codigo\_queja | Numérico | 30 |
| **Tipo de Archivo** | Type | Texto | 100 |

2 Sufijo que se añade al final de una palabra o de su raíz para formar una palabra derivada.

# Estructura JSON expuesta por la SFC (Momento 3 - transferencia de archivos)

**Request: POST**

**{**

**"Headers":{**

**“Authorization”: “<Token>”, “Cache-Control”: ”no-cache”, “Accept”: “\*/\*”,**

**“Content-type”: “multipart/form-data”, “Accept-Language”: “[<es> or <en>]”, “X-SFC-Signature”: “<Signature>”**

**},**

**"Body":{**

**}**

**}**

**“file” :””;**

**“codigo\_queja”:””,**

**“type”: ””**

**Response: 201 CREATED**

**{**

**"Headers":{**

**“Content-type”: “aplication/json”, “Content-Language”: “[<es> or <en-us>]”**

**},**

**"Response":{**

**“id” :””,**

**“file”:””,**

**“type”:””,**

**“state”: ””, “codigo\_queja”: ””**

**}**

**}**

# MOMENTO 4

***Las entidades vigiladas deberán capturar la información por medio de API REST de información actualizada de usuarios consumidores financieros a través del portal SmartSupervisión de la Superintendencia Financiera de Colombia.***

* + *La Superintendencia Financiera de Colombia pone a disposición del consumidor financiero un formulario para la edición de la información por parte del mismo.*
  + *El consumidor financiero requiere editar sus datos personales dentro del portal web de la Superintendencia Financiera de Colombia o punto de servicio al ciudadano.*
* *La información recolectada de dicho formulario será guardada en SmartSupervision dentro de nuestra nube pública.*
* *La información, después de estar alojada en nuestra nube pública, será recolectada por la entidad vigilada ante la cual el consumidor financiero ha interpuesto quejas o reclamos.*
* *La Entidad vigilada hace el llamado al servicio de inicio de sesión enviando los parámetros requeridos y obtiene los token’s como respuesta del servicio de inicio de sesión.*
* *Una vez se logra la autenticación y manteniendo la sesión por medio del access token, se pueden realizar peticiones para obtener recursos.*
* *La entidad vigilada consumirá la información por medio del API REST que será expuesto por parte de la Superintendencia Financiera de Colombia mediante el método (GET) donde se podrá realizar peticiones para obtener recursos que estarán agrupados en cierto número de páginas (páginas de 100 recursos, de un total de 1000 que nos darán 10 páginas o grupos) según la cantidad total que tenga pendiente por sincronizar la entidad vigilada.*
* *Consumir el servicio, para ello se hace uso del método del endpoint api/usuarios/info/, enviando la información de encabezado y cuerpo de petición correspondiente.*
* *Dentro de la petición se retorna el total de recursos disponibles, número de páginas a consultar, página actual, dos URL que nos permitirá consumir la información de la página anterior o de la página siguiente y un vector que contiene la información actualizada de los usuarios*
* *Detalles de la petición:*
  + URI: https://UrlBase/api/usuarios/info/
  + Tipo: GET
  + Encabezados requeridos:
    - Content-Type: application/json
    - Authorization: <token>
    - X-SFC-Signature: <signature>
* *A continuación, se muestra la descripción de los campos que se envían a la entidad vigilada haciendo uso del método:*

|  |  |  |  |
| --- | --- | --- | --- |
| **Nombre** | **Campo** | **Tipo** | **Longitud** |
| **Número de identificación del consumidor financiero** | numero\_id\_CF | Texto | **15** |
| **Tipo identificación del consumidor financiero** | tipo\_id\_CF | Numérico | 2 |
| **Nombres del consumidor financiero** | Nombres | Texto | 25 |
| **Apellidos del consumidor financiero** | Apellidos | Texto | 25 |
| **Fecha de nacimiento** | fecha\_nacimiento | Fecha | YYYY-MM-DDTHH:MM:SS |
| **Correo electrónico** | Correo | Texto | 50 |
| **Teléfono** | Teléfono | Texto | 15 |
| **Razón social - persona jurídica** | razon\_social | Texto | 50 |
| **Dirección** | Dirección | Texto | 250 |
| **Departamento** | departamento\_cod | Alfanumérico | 3 |
| **Municipio** | municipio\_cod | Alfanumérico | 5 |

# Estructura JSON expuesta por la SFC (Momento 4)

**Request: GET**

**{**

**"Headers":{**

**“Authorization”: “<Token>”, “Cache-Control”: ”no-cache”, “Accept”: “aplication/json”, “Content-type”: “aplication/json”,**

**“Accept-Language”: “[<es> or <en>]”, “X-SFC-Signature”: “<Signature>”**

**}**

**}**

**Response: 200 OK**

**{**

**"Headers":{**

**“Content-type”: “aplication/json”, “Content-Language”: “[<es> or <en-us>]”**

**},**

**"Response":{**

**“numero\_id\_CF“:““,**

**“tipo\_id\_CF“:““,**

**“nombre“:““,**

**“apellido“:““, “fecha\_nacimiento“:““, “correo“:““,**

**“telefono“:““,**

**“razon\_social“:““,**

**“direccion“:““, “departamento\_cod“:““, “municipio\_cod“:““**

**}**

**}**

# Momento 4 - ACK

* + *Detalles de la petición:*
    - URI: https://UrlBase/api/usuarios/ack/
    - Tipo: POST
    - Encabezados requeridos:
      * Content-Type: application/json
      * Authorization: <Token>
      * X-SFC-Signature: <Signature>
* *A continuación, se muestra la descripción de los campos que se envían a la entidad vigilada haciendo uso del método:*

|  |  |  |  |
| --- | --- | --- | --- |
| ***Nombre*** | ***Campo*** | ***Tipo*** | ***Longitud*** |
| **mensaje** | **Message** | Texto | N/A |
| **quejas fallidas** | numero\_id\_CF\_error | Lista | N/A |

# Estructura JSON expuesta por la SFC (Momento 4 ACK)

**Request: POST**

**{**

**"Headers":{**

**“Authorization”: “<Token>”, “Cache-Control”: ”no-cache”,**

**},**

**"body":{**

**“Accept”: “aplication/json”, “Content-type”: “aplication/json”,**

**“Accept-Language”: “[<es> or <en>]”, “X-SFC-Signature”: “<Signature>”**

**“numero\_id\_CF”: [ “numero\_id\_CF\_1”, “numero\_id\_CF\_2”, “numero\_id\_CF\_3”,**

**…………………. “numero\_id\_CF\_n”**

**]**

**}**

**}**

**Response: 200 OK**

**{**

**"Headers":{**

**“Content-type”: “aplication/json”, “Content-Language”: “[<es> or <en-us>]”**

**},**

**"Response":{**

**“message”;”ID CF actualizado”, “numero\_id\_CF\_error”: []**

**}**

**}**

# Notas

* Se aclara que la entidad vigilada debe crear un desarrollo interno de implementación para el envío de la información***.***
* El servicio expuesto por la Superintendencia Financiera de Colombia debe ser consumido por las entidades vigiladas.
* La Superintendencia Financiera de Colombia tendrá el servicio activo siempre para que sea consumido por las entidades vigiladas.
* El momento 2 hace referencia a la proforma F.0000-165 (formato 410) “Smartsupervisión-Interposición de la queja o reclamo” suministrado por la Superintendencia Financiera de Colombia con sus respectivos lineamientos.
* El momento 3 hace referencia a la proforma F.0000-166 (formato 411) “Smartsupervision-Gestión de la queja o reclamo” suministrado por la Superintendencia Financiera de Colombia con sus respectivos lineamientos.
* En caso en que la información solicitada no aplique para la queja o reclamo del consumidor financiero reportado, el campo deberá ser reportado vacío o con los valores por defecto que correspondan al campo.

# Definiciones de condiciones de desempeño

Se define que el producto final SmartSupervision estará acorde a las condiciones de infraestructura en términos de capacidad, conectividad y desempeño, que permiten que el sistema tenga confiabilidad, integridad, disponibilidad y confidencialidad. El sistema cumplirá con las condiciones de réplica de la información en diferentes ambientes y redundancia en hardware y software que permitan contar con la información en términos de desempeño y disponibilidad superior a 99.7%.

# Definición del uso de los mecanismos de integración entidad vigilada

* + Se define que el mecanismo de integración que debe tener el sistema para la comunicación hacia y desde la Superintendencia Financiera de Colombia a las entidades vigiladas es por medio de API Rest
  + Las entidades vigiladas deben, a través de los mecanismos de integración:
* Recoger la información de las quejas o reclamos radicados en la Superintendencia Financiera de Colombia, para ser atendida y resuelta por la entidad vigilada o para el Defensor del consumidor financiero (DCF).
* Enviar las quejas o reclamos nuevos radicados en la entidad vigilada o el DCF
* Enviar las respuestas a las quejas o reclamos creados en Superintendencia Financiera de Colombia, entidad vigilada o el DCF
  + En cuanto a los archivos anexos se define que:
* Al recoger las quejas o reclamos radicados en la Superintendencia Financiera de Colombia también se deben llevar los archivos anexos colocados por el Consumidor Financiero como soportes de la queja o reclamo.
* Al transmitir la respuesta de la queja o reclamo la entidad vigilada debe anexar toda la información que soporte dicha respuesta y sus actualizaciones.

# Códigos de estado http

En el momento en que las diferentes entidades vigiladas obtienen el respectivo reporte o información, las entidades vigiladas recibirán, en sus respuestas HTTP, el código de estado (status code) más adecuado y acorde a la situación presentada. Los siguientes enlaces de internet se toman como referencia para establecer los códigos de estado:

The Internet Engineering Task Force <https://www.ietf.org/assignments/http-status-codes/http-status-codes.xml>

The World Wide Web Consortium <https://www.w3.org/Protocols/HTTP/HTRESP.html>

Mozilla Developer Network <https://developer.mozilla.org/es/docs/Web/HTTP/Status>

**REST** hace uso de los métodos que ofrece el protocolo HTTP, estos métodos son:

* POST Se usa para crear un recurso en el servidor.
* GET Se usa para obtener un recurso.
* PUT se usa para cambiar el estado de un recurso o actualizarlo.

A continuación, presentamos alguno de los códigos de estado que se deben de usar al momento de dar respuesta a un evento en las operaciones de captura de información y respuesta:

|  |  |  |
| --- | --- | --- |
| **POST** | **Creación de un recurso en el servidor** | |
| **Código de estado** | **Descripción** | **Evento** |
| 200 OK | El recurso se ha obtenido y se transmite en el cuerpo del mensaje | Cuando se obtiene de forma satisfactoria el informe solicitado |
| 201 Created | El recurso se ha creado y se transmite en el cuerpo del mensaje | Cuando se obtiene de forma satisfactoria la creación solicitada |
| 401  Unauthorized | El recurso requiere una autorización | Cuando las credenciales de autenticación con la entidad vigilada no se envían o no son correctas, esto solo aplica para los mecanismos de seguridad de API Key y OAuth |
| 404 Not Found | El servidor no encuentra el recurso solicitado | Cuando el informe solicitado no se encuentre disponible para ser capturado por la petición enviada. |
| **GET** | **Obtener recurso del servidor** | |
| 204 Not  Content | La petición se procesó de forma correcta pero no hay cuerpo de mensaje en la respuesta. | Cuando la entidad vigilada recibe de forma satisfactoria la respuesta enviada por la Superintendencia Financiera de Colombia a un informe capturado con anterioridad. |

|  |  |  |
| --- | --- | --- |
| 401  Unauthorized | El recurso requiere una autorización | Cuando las credenciales de autenticación con la entidad vigilada no se envían o no son correctas, esto solo aplica para los mecanismos de seguridad de API Key y OAuth |
| 500 Internal Server Error | El servidor ha encontrado una situación que no sabe cómo manejarla | Cuando las estructuras JSON del cuerpo de mensaje de la respuesta no coinciden con la definición del servidor, o en cualquier caso que se asemeja la situación. |

# Seguridad

Las comunicaciones se efectuarán sobre protocolo TLS versión 1.2 (TLSv1.2). Los recursos REST deberán estar expuestos mediante uno de los mecanismos de seguridad descritos en los numerales 9.1, 9.2 o 9.3 de este documento, ó, la combinación de la Autenticación (numeral 9.1) con Api Key (numeral 9.2) o OAuth (9.3). Se debe asegurar que el recurso REST sea expuesto EXCLUSIVAMENTE a esta Superintendencia Financiera de Colombia ya que la información transmitida no debe ser accedida por ningún motivo por otras entidades vigiladas.

# Autenticación TLS

La autenticación en el protocolo TLS v1.2 consiste en la validación en doble vía de los servidores que se están comunicando, esta doble validación se realizará a través de certificados digitales SSL. El proceso de validación inicia al momento de iniciar las conexiones entre los dos servidores y se conoce como el handshake el cual consiste en cuatro etapas (acá una breve descripción):

* + El cliente envía un mensaje ClientHello al servidor para establecer comunicación.
  + El cliente, recibe un registro ServerHello, junto con los certificados del servidor
  + El cliente envía sus certificados y se realiza la negociación de cifrados.
  + Se aceptan condiciones y se establece el canal de comunicaciones.

Posterior al establecimiento del canal, el cliente hace envío de la petición al recurso. Para realizar la implementación de la autenticación a doble vía del protocolo TLS v1.2, es requerido que los dos actores, en este caso la Superintendencia Financiera de Colombia (cliente) y cada una de las entidades vigiladas realicen la respectiva autenticación.

# API Key

Es un mecanismo o identificador que sirve como medio de autenticación de un servidor cliente al que se le proporciona, de acuerdo con el rol que se le establezca, permisos de

uso sobre un recurso expuesto en la web. Este identificador es único por servidor cliente y es únicamente conocido por las dos partes (cliente - servidor).

Previo a cualquier petición sobre un recurso, el administrador del servidor entrega el api-key al cliente, al momento de realizar las peticiones el cliente inyecta en el contexto de la petición un header con el nombre designado (ej: x-api-key) y como valor de este header el identificador único asignado al cliente.

# Estandar OAuth

Es un estándar de autorización que permite, de forma limitada, acceso sobre 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). Aunque el flujo de autorización varía de acuerdo con su implementación.

En primera instancia, el cliente, previo al consumo del recurso web, hace una petición de autorización a través de un servicio web en el cual envía un identificador único del cliente (ClientID) y una palabra secreta (ClientSecret), los cuales pueden ser enviados en el cuerpo o como header de la petición. Si los datos son correctos el servicio de autenticación retornara un token el cual es usado por el cliente para solicitar el recurso. Posterior a esto, el cliente realiza una petición al recurso inyectando en el header de la misma, los datos de ClienID y del token obtenido previamente. Si los datos enviados son correctos se servirá el recurso solicitado.

# Condiciones para exponer el web service

Cuando se surtan las pruebas de comunicación y de conectividad entre la entidad vigilada y la Superintendencia Financiera de Colombia en ambientes de desarrollo y pruebas, la entidad vigilada deberá remitir a la Superintendencia Financiera de Colombia la dirección donde se encontrará el Web Service para consumir en ambiente productivo con el fin de adecuar y configurar los permisos de firewall/direccionamiento y de registro en el cliente desarrollado por la Superintendencia Financiera de Colombia para acceder al recurso.

No se contempla dentro de las condiciones para exponer el Web Service que se establezcan VPNs.

# ACTUALIZACIÓN DE BASE DE DATOS PARA CONTROL DE CAMBIOS FRAUDE

**De acuerdo con el control de cambios relacionado a fraude, se tienen previsto realizar cambios a nivel de base de datos, desde la creación de tablas y creación de llaves foráneas en tablas ya existentes, las cuales podrán relacionar directamente entre las tablas de fraude a incluir y las tablas ya existentes.**

**Por lo tanto, se crearán en la base de datos las tablas “Tipología de queja por fraude” y “Modalidad de fraude”. Asimismo, las llaves foráneas de estas tablas se relacionarán en la tabla de quejas (complaints\_queja), junto con los campos de Monto reclamado y Monto reconocido.**

A continuación, se muestran las tablas a detalle de como quedaran en base de datos:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***fraud\_typology*** | | | | |
| ***Nombre*** | ***Campo*** | ***Tipo*** | ***Longitud*** | ***\**** |
| **Código** | **id** | **Id** | **3** | **\*** |
| **Tipología queja fraude** | **name** | **Texto** | **No aplica** | **\*** |
| **Descripción** | **description** | **Texto** | **No aplica** | **\*** |



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***fraud\_modality*** | | | | |
| ***Nombre*** | ***Campo*** | ***Tipo*** | ***Longitud*** | ***\**** |
| **Código** | **id** | **Id** | **3** | **\*** |
| **Estado de la queja** | **name** | **Texto** | **No aplica** | **\*** |
| **Descripción** | **description** | **Texto** | **No aplica** | **\*** |

**En la tabla complaints\_queja, se agrega a la estructura existente los siguientes campos:**



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***complaints\_queja*** | | | | |
| ***Nombre*** | ***Campo*** | ***Tipo*** | ***Longitud*** | ***\**** |
| **TIpología de fraude** | **tipologia\_fraude\_id** | **Id** | **3** | **\*** |
| **Modalidad de fraude** | **modalidad\_fraude\_id** | **Id** | **3** | **\*** |
| **Monto reclamado** | **monto\_reclamado** | **Numérico (Double)** | **No aplica** | **\*** |
| **Monto reconicido** | **monto\_reconocido** | **Numérico (Double)** | **No aplica** | **\*** |

# ACTUALIZACIÓN EN BIGQUERY PARA CONTROL DE CAMBIOS FRAUDE

**De acuerdo con el control de cambios relacionado a fraude, se tienen previsto realizar cambios a nivel de bigquery, en relación a la adición de una serie de campos que representan la información de “Tipología de queja por fraude”, “Modalidad de fraude”,  Monto reclamado y Monto reconocido en el dataset audit.quejas**

**A continuación se muestran las columnas que se agregan al dataset existente:**

¡

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***audit.quejas*** | | | | |
| ***Nombre*** | ***Campo*** | ***Tipo*** | ***Longitud*** | ***\**** |
| **TIpología de fraude** | **tipologia\_fraude** | **String** | **No aplica** | **\*** |
| **Modalidad de fraude** | **modalidad\_fraude** | **String** | **No aplica** | **\*** |
| **Monto reclamado** | **monto\_reclamado** | **Numérico (Float)** | **No aplica** | **\*** |
| **Monto reconicido** | **monto\_reconocido** | **Numérico (Float)** | **No aplica** | **\*** |



## **Tablero de control (Dashboard) de fraude**

**Una vez la Superintendencia Financiera de Colombia recibe la información respecto al tema de fraude, datos de interés como: Total de quejas, Total de entidades, Total de usuarios, Tiempos totales de respuesta, Fraude interno, Fraude externo, Montos reclamados y Montos reconocidos, se brindaran estadísticas a manera de reporte en la cual se pueda entrega la información de interés en promedio y porcentajes. Esto mediante la implementación de un tablero de control o Dashboard con la información relacionada a fraudes.**

**La Superintendencia Financiera de Colombia dispondrá de un servicio expuesto para el envío de la información recolectada. Para ello se hace uso de API REST, cuyo servicio será definido como volumetry-fraud en la cual deberá enviarse la información de encabezado y cuerpo de la petición.**

**Esta información será almacenada en base de datos dentro de smartsupervision, la cual se encuentra alojada en la nube pública de la Superintendencia Financiera de Colombia.**

**Volumetry Fraud**

**Endpoint que permite obtener toda la información necesaria para el tablero de control o dashboard de fraude.**

#### **Creación de endpoint para Control de cambios Fraude**

**Para este endpoint que permite obtener toda la información necesaria para el tablero de control o dashboard de fraude se crearán todos los campos necesarios y expuestos a continuación en los parámetros de entrada y parámetros de salida respectivamente.**

**Generalidades**

|  |  |
| --- | --- |
| **URL** | **{{url base}}/api/dashboard/volumetry-fraud/** |
| **Metodo** | **POST** |
| **Autenticación requerida (Bearer token)** | **SI** |
| **Formato entrada** | **JSON** |
| **Formato salida** | **JSON** |

**Headers**

|  |  |  |
| --- | --- | --- |
| **Clave** | **Valor** | **Descripción** |
| **Content-Type** | **application/json** | **Indica el tipo de medio del recurso, es decir, el formato de los datos que se están enviando o recibiendo. Por ejemplo, text/html para HTML, application/json para JSON, etc** |
| **Authorization** | **<Token>** | **Este encabezado se utiliza para identificar y autenticar al usuario que realiza la solicitud a un servidor, en este caso es una credencial codificada como token.** |
| **X-SFC-Signature** | **<Signature>** | **Los encabezados que comienzan con ‘X-’ son personalizados. En este caso, se utiliza para enviar la firma digital que verifica la autenticidad de la solicitud o respuesta.** |

**Parámetros de entrada (body)**



|  |  |  |  |
| --- | --- | --- | --- |
| **Nombre** | **Campo** | **Tipo** | **Longitud** |
| **Modelo de filtro** | **filter\_model** | **Diccionario** | **No aplica** |
| **Fecha de creación** | **fecha\_creacion** | **Diccionario** | **No aplica** |
| **Tipo de filtro** | **filter\_type** | **Texto** | **No aplica** |
| **Operador** | **operator** | **Texto** | **No aplica** |
| **Condición Uno (1)** | **condition1** | **Diccionario** | **No aplica** |
| **Fecha desde (Condición Uno)** | **date\_from** | **Texto** | **No aplica** |
| **Fecha hasta (Condición Uno)** | **date\_to** | **Texto** | **No aplica** |
| **Tipo de filtro (Condición Uno)** | **filter\_type** | **Texto** | **No aplica** |
| **Tipo de operador (Condición Uno)** | **type** | **Texto** | **No aplica** |
| **Condición Dos (2)** | **condition2** | **Diccionario** | **No aplica** |
| **Fecha desde (Condición Dos)** | **date\_from** | **Texto** | **No aplica** |
| **Fecha hasta (Condición Dos)** | **date\_to** | **Texto** | **No aplica** |
| **Tipo de filtro (Condición Dos)** | **filter\_type** | **Texto** | **No aplica** |
| **Tipo de operador (Condición Dos)** | **type** | **Texto** | **No aplica** |

# Ejemplo de consumo del endpoint

**{**

**"Headers": {**

**“Authorization”: “<Token>”,**

**“Cache-Control”: ”no-cache”,**

**“Accept”: “aplication/json”,**

**“Content-type”: “aplication/json”,**

**“Accept-Language”: “[<es> or <en>]”,**

**“X-SFC-Signature”: “<Signature>”**

**},**

**"Body":{**

**"filter\_model": {**

**"fecha\_creacion": {**

**"filter\_type": "date",**

**"operator": "AND",**

**"condition1": {**

**"date\_from": "2024-07-24",**

**"date\_to": null,**

**"filter\_type": "date",**

**"type": "greaterThanOrEqual"**

**},**

**"condition2": {**

**"date\_from": "2024-07-31",**

**"date\_to": null,**

**"filter\_type": "date",**

**"type": "lessThanOrEqual"**

**}**

**}**

**}**

**}**

**Parámetros de salida (response)**

¡



|  |  |  |  |
| --- | --- | --- | --- |
| **Nombre** | **Campo** | **Tipo** | **Longitud** |
| **Total de quejas** | **total\_quejas** | **Numérico (entero)** | **6** |
| **Promedio de quejas** | **avg\_quejas** | **Numérico (Double)** | **No aplica** |
| **Porcentaje de quejas** | **percent\_quejas** | **Numérico (Double)** | **No aplica** |
| **Total de entidades** | **total\_entidades** | **Numérico (entero)** | **6** |
| **Promedio de entidades** | **avg\_entidades** | **Numérico (Double)** | **No aplica** |
| **Porcentaje de entidades** | **percent\_entidades** | **Numérico (Double)** | **No aplica** |
| **Total usuarios** | **total\_usuarios** | **Numérico (entero)** | **6** |
| **Promedio usuarios** | **avg\_usuarios** | **Numérico (Double)** | **No aplica** |
| **Porcentaje usuarios** | **percent\_usuarios** | **Numérico (Double)** | **No aplica** |
| **Tiempo total de respuesta** | **tiempo\_respuesta** | **Numérico (entero)** | **6** |
| **Promedio tiempo total de respuesta** | **avg\_tiempo\_respuesta** | **Numérico (Double)** | **No aplica** |
| **Porcentaje tiempo total de respuesta** | **percent\_tiempo\_respuesta** | **Numérico (Double)** | **No aplica** |
| **Fraude interno** | **total\_fraude\_interno** | **Numérico (entero)** | **6** |
| **Promedio fraude interno** | **avg\_fraude\_interno** | **Numérico (Double)** | **No aplica** |
| **Porcentaje fraude interno** | **percent\_fraude\_interno** | **Numérico (Double)** | **No aplica** |
| **Fraude externo** | **total\_fraude\_externo** | **Numérico (entero)** | **6** |
| **Promedio fraude externo** | **avg\_fraude\_externo** | **Numérico (Double)** | **No aplica** |
| **Porcentaje fraude externo** | **percent\_fraude\_externo** | **Numérico (Double)** | **No aplica** |
| **Monto reclamado** | **total\_monto\_reclamado** | **Numérico (entero)** | **6** |
| **Promedio monto reclamado** | **avg\_monto\_reclamado** | **Numérico (Double)** | **No aplica** |
| **Porcentaje monto reclamado** | **percent\_monto\_reclamado** | **Numérico (Double)** | **No aplica** |
| **Monto reconocido** | **total\_monto\_reconocido** | **Numérico (entero)** | **6** |
| **Promedio monto reconocido** | **avg\_promedio\_reconocido** | **Numérico (Double)** | **No aplica** |
| **Porcentaje monto reconocido** | **percent\_monto\_reconocido** | **Numérico (Double)** | **No aplica** |

# Ejemplo de respuesta del endpoint

**200 - OK - Volumetry Fraud**

**{**

**"total\_quejas": 378,**

**"avg\_quejas": 23747.50248756219,**

**"percent\_quejas": 404.0,**

**"total\_entidades": 378,**

**"avg\_entidades": 23747.50248756219,**

**"percent\_entidades": 404.0,**

**"total\_usuarios": 378,**

**"avg\_usuarios": 23747.50248756219,**

**"percent\_usuarios": 404.0,**

**"tiempo\_respuesta": 378,**

**"avg\_tiempo\_respuesta": 23747.50248756219,**

**"percent\_tiempo\_respuesta": 404.0,**

**"total\_fraude\_interno": 378,**

**"avg\_fraude\_interno": 23747.50248756219,**

**"percent\_fraude\_interno": 404.0,**

**"total\_fraude\_externo": 378,**

**"avg\_fraude\_externo": 23747.50248756219,**

**"percent\_fraude\_externo": 404.0,**

**"total\_monto\_reclamado": -378,**

**"avg\_monto\_reclamado": 23747.50248756219,**

**"percent\_monto\_reclamado": 404.0,**

**"total\_monto\_reconocido": 378,**

**"avg\_promedio\_reconocido": 23747.50248756219,**

**"percent\_monto\_reconocido": 404.0,**

**}**

**HISTORIAL DE CAMBIOS**

|  |  |  |
| --- | --- | --- |
| **Fecha** | **Versión** | **Cambios** |
| |  |  |  | | --- | --- | --- | | 27/05/2024 |  |  | | 1 | Inicio de versión |
| 10/09/2024 | 2 | Fraude |