CONSTRUCCIÓN WEB SERVICE SMARTSUPERVISION

Junio de 2022

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

1. 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.

2. *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>"]
}
```

3. *Definición de la exposición del servicio*

La exposición del recurso estará sujeta a las siguientes características:

- La implementación del recurso REST deberá seguir los 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)

4. *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 el secret que deberán utilizar 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 por medio de POST y manteniendo la sesión por medio del access token, se puede realizar peticiones para obtener un recurso.*
- *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 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/queja/ enviando la información de encabezado y cuerpo de petición.*
- *Dentro de la petición se retorna la URL que nos permitirá consumir la información de la página anterior o de la página siguiente, el número de páginas a consultar y el total de recursos que se devolverán entre todas las páginas.*
- *Detalles de la petición:*
  - URI: https://UrlBase/api/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 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-DDTHH: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	14
Teléfono	telefono	Texto	15
Correo electrónico	correo	Texto	50
Dirección	direccion	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	1000
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

- ***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":""
                }
            ]
        }
}
```

- *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 con los códigos de las quejas o reclamos sincronizados y procederá a realizar la marcación para cada una de estas y asi 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
    - 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	**pqrs_error**	Lista	N/A

- ***Estructura JSON expuesta por la SFC (Momento 1 ACK)***

```
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":{
                "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',
      6 : 'gestion'
      }

      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 envían a la entidad vigilada haciendo uso del método:*

Nombre	Campo	Tipo	Longitud
Identificador	id	Numérico(Long)	-
Archivo(URL)	file	File	30 MB
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.*
  - *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-DDTHH: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	14
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	1000
Anexos de la queja o reclamo	anexo_queja	Booleano	N/A
Ente de control	ente_control	Numérico	2

- ***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”:””;
            }
}
```

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.

- ***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 envía la entidad vigilada haciendo uso del método:*

Nombre	Campo	Tipo	Longitud
Archivo	file	File	30 MB
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, utilizaran 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.*
  - *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 envía la entidad vigilada haciendo uso del método:*

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	admision	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	marcacion	Numérico	2
Queja Exprés	queja_expres	Numérico	2

- ***Estructura JSON expuesta por la SFC (Momento 3)***

Request: PUT/PATCH

```
{
        "Headers":{
                “Authorization”: “<Token>”,
                “Cache-Control”: ”no-cache”,
                “Accept”: “*/*”,
                “Content-type”: “multipart/form-data”,
                “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”:””
        }
}

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>
    - *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
Código de la queja	codigo_queja	Numérico	30
Tipo de Archivo	type	Texto	100

- ***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”: ””
        }
}
```

5. 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.

6. 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%.

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.

8. 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.

9. 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.

9.1 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.

9.2 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.

9.3 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 a 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.

10. 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.