



ANEXO TÉCNICO CUN

Requerimientos para la implementación de la asignación del CUN, Consulta de PQR y Reporte de Apelaciones por medios electrónicos.

2022.

CONTROL DE CAMBIOS

Versión	Descripción	Autor	Fecha
1.0	Versión Inicial	Diego Pedroza	
1.0	Revisión versión inicial	Jaroslav López y Leydi Peña	
1.0	Aprobación versión inicial	Oscar Asprilla	
1.1	Ajuste para incluir manejo de WS-Security en el Web Service de Apelaciones	Pablo Andrés Rodas	21/09/2017
1.1	Ajuste a validación de los campos del formulario de apelaciones para indicar cantidad, tipo y tamaño de los archivos permitidos	Norberto Villegas Pablo Rodas	22/09/2017
1.2	Cambios en el servicio de radicación de apelaciones. Eliminación de la secuencia de port-knocking. Actualización de precios de referencia.	Sebastián Montes	14/08/2019
1.3	Adición del campo observaciones y respuesta queja	Norberto Villegas	27/07/2020
1.4	Adición estructura respuesta sin resultados servicio operador y tramas de ejemplo para el consumo del servicio de consulta de pqr del operador y apelaciones de la SIC.	Norberto Villegas	19/03/2021
1.5	Detalle del tipo y uso de cada uno de los campos utilizados durante el intercambio de información en el punto de radicación y consulta de la apelación.	Norberto Villegas	08/11/2021
1.6	Actualización de requerimientos de hardware sugerido a los operadores.	Norberto Villegas	11/11/2021
1.7	Actualización del protocolo (https) utilizado para exponer el contrato de servicio consultaCUN, y precisión a nivel de seguridad en la dinámica de conexión al servidor SSH del operador.	Norberto Villegas	23/11/2021

TABLA DE CONTENIDO

1	INTRODUCCIÓN	5
1.1	ÁMBITO DE APLICACIÓN	5
1.2	PROPÓSITO.....	5
1.3	ALCANCE	5
1.4	IMPLEMENTACIÓN DEL MECANISMO DE SEGUIMIENTO Y ESTADO DE PQR´s Y SOLICITUDES DE INDEMNIZACIÓN (CUN)	6
2	ASPECTOS TÉCNICOS Y FUNCIONALES QUE DEBE CUMPLIR LA IMPLEMENTACIÓN DEL CUN	9
3	OBLIGACIONES GENERALES	9
3.1	SEGURIDAD Y CALIDAD	10
3.2	DOCUMENTACIÓN.....	11
3.3	DIVULGACIÓN DE LA INFORMACIÓN	13
4	ETAPA I – ASIGNACIÓN DEL CUN	13
4.1	DEFINICIONES DE CRITERIOS DE SEGURIDAD Y CALIDAD.	13
4.1.1	CRITERIOS DE SEGURIDAD	13
4.1.2	CRITERIOS DE CALIDAD.....	15
5	ETAPA II – CONSULTA INTERACTIVA	15
5.1	DEFINICIONES DE CRITERIOS DE SEGURIDAD Y CALIDAD	15
5.1.1	CRITERIOS DE SEGURIDAD	15
5.1.2	CRITERIOS DE CALIDAD.....	17
5.2	ESPECIFICACIONES TÉCNICAS.....	17
5.2.1	Escenario de consulta 1. La PQR o solicitud de indemnización se encuentra en trámite o resuelta ante el operador y el usuario ingresa a la página web de éste	19
5.2.2	Escenario de consulta 2. La PQR o solicitud de indemnización se encuentra en trámite o resuelta ante el operador y el usuario ingresa a la página web de la SIC	19
5.2.3	Escenario de consulta 3. La apelación se encuentra en trámite o resuelta ante la SIC y el usuario ingresa a la página web del operador	20
5.2.4	Escenario de consulta 4. La apelación se encuentra en trámite o resuelta ante la SIC y el usuario ingresa a la página web de la SIC.	21
5.2.5	Diagrama de Interacción entre Operadores y SIC	22
5.2.6	CONTRATOS DE SERVICIO	23
6	ETAPA III – ENVÍO DE EXPEDIENTES DE APELACIÓN A LA SIC POR MEDIOS ELECTRÓNICOS	31
6.1	DEFINICIONES DE CRITERIOS DE SEGURIDAD Y CALIDAD	31
6.1.1	CRITERIOS DE SEGURIDAD	31
6.2	ESPECÍFICACIONES TÉCNICAS	33
6.2.1	FORMULARIO WEB.....	33
6.2.2	WEB SERVICE.....	39
7	CONFIGURACIÓN SERVIDOR DE ARCHIVOS EN LINUX	54
7.1	REQUERIMIENTOS DE HARDWARE Y SOFTWARE	54
7.1.1	HARDWARE	55

7.1.2	SOFTWARE	55
7.1.3	COSTOS APROXIMADOS.....	55
7.2	INSTALACIÓN Y CONFIGURACIÓN DE SSH.....	56
8	CONFIGURACIÓN SERVIDOR DE ARCHIVOS EN WINDOWS.....	58
8.1	REQUERIMIENTOS DE HARDWARE Y SOFTWARE	58
8.1.1	HARDWARE	59
8.1.2	SOFTWARE	59
8.1.3	COSTOS APROXIMADOS.....	59
8.2	INSTALACIÓN Y CONFIGURACIÓN DE SSH.....	60
9	INFORMES	74
10	VALORES DE REFERENCIA.....	75
11	ACUERDO DE NIVEL DE SERVICIO.....	77
12	GLOSARIO DE TERMINOS	78

1 INTRODUCCIÓN

1.1 ÁMBITO DE APLICACIÓN

Las instrucciones y requerimientos que contiene el presente anexo técnico deben ser adoptadas e implementadas por todos los operadores de servicios de comunicaciones y servicios postales sujetos a los correspondientes Regímenes de Protección de los Derechos de los Usuarios de los Servicios de Comunicaciones y Postales, en concordancia con lo establecido en el Capítulo Tercero del Título III de la Circular Única de esta Superintendencia y en los plazos previstos por esta Entidad.

En todo caso, los vigilados destinatarios de las instrucciones contenidas en este documento deben implementar, en los plazos previstos, la totalidad de los requerimientos de carácter obligatorio aquí exigidos.

1.2 PROPÓSITO

Definir las especificaciones técnicas que deben cumplir los operadores de servicios de comunicaciones y postales, tanto para la asignación del Código Único Numérico –CUN- a las Peticiones, Quejas, Recursos (en adelante PQR's) y a las solicitudes de indemnización que así lo requieren, como para el reporte de expedientes que contienen recursos de apelación interpuestos en sede de empresa, para ser resueltos por parte de la Superintendencia de Industria y Comercio.

Indicar la técnica del método de consulta y datos resultantes que se originan desde la Superintendencia de Industria y Comercio frente al estado del trámite de las PQRs o solicitudes de indemnización presentadas ante los operadores de servicios de comunicaciones y postales.

Presentar y explicar el método de consumo del web service de la Superintendencia de Industria y Comercio cuando la consulta de las PQR's o las solicitudes de indemnización se origina desde el portal web del operador de servicios de comunicaciones o postal.

1.3 ALCANCE

Describir las actividades que deben ser desarrolladas tanto por los operadores de servicios de comunicaciones y postales, como por la Superintendencia de Industria y Comercio, con miras a llevar a cabo la implementación de la asignación, consulta de CUN y reportes de expedientes con recursos de apelaciones en sede de empresa para ser resueltos por la Superintendencia de Industria y Comercio.

Para el efecto este anexo técnico incluye la forma en que los operadores de servicios de comunicaciones y postales deben atender los requerimientos técnicos con el fin de implementar el CUN al interior de sus organizaciones.

Asimismo, contiene las especificaciones para el reporte de expedientes que contengan recursos de apelación interpuestos en sede de empresa que deben ser resueltos por la Superintendencia de Industria y Comercio y el mecanismo de consulta de las PQRs o solicitudes de indemnización presentadas por los usuarios, ya sea desde el portal de los operadores de servicios de comunicaciones y postales, o desde el portal de la SIC.

1.4 IMPLEMENTACIÓN DEL MECANISMO DE SEGUIMIENTO Y ESTADO DE PQR´s Y SOLICITUDES DE INDEMNIZACIÓN (CUN)

Con la finalidad de implementar la asignación del Código Único Numérico, la consulta interactiva de PQR's y las solicitudes de indemnización y el envío de expedientes que contienen recursos de apelación a través de servicios Web, se han previsto las siguientes etapas de desarrollo e implementación:

- 1) Asignación del CUN y seguimiento del estado de la PQR's o solicitud de indemnización en los sistemas de gestión del operador.

La asignación de CUN se puede solicitar a través del **Sistema Código Único Numérico - CUN**, realizando los siguientes pasos:

- Ingresar a la URL <https://serviciolinea.sic.gov.co/cun/index.xhtml>.
- Hacer clic en el botón "Solicitar CUN".
- Diligenciar la información de la sección "Datos del operador".
- Diligenciar la información de la sección "Datos del representante legal".
- Adjuntar los documentos solicitados en la sección "Carga de documentos".
- Ingresar la información del captcha.
- Aceptar términos y condiciones.
- Hacer clic en el botón "Solicitar".

Nota: En el manual de usuario en la sección **8.2.1 Solicitud de Asignación de CUN**, podrá encontrar más detalle del proceso mencionado anteriormente.

- 2) Implementación para los mecanismos de consulta interactiva entre los sistemas del operador y los sistemas de la Superintendencia de Industria y Comercio, para facilitar la consulta del estado del trámite (independientemente de la ubicación del mismo).
- 3) Implementación de los medios electrónicos de transferencia de expedientes desde el operador hacia la Superintendencia de Industria y Comercio.

Para la primera etapa, siempre y cuando se trate de vigilados que aún se encuentren en proceso de cumplir con este requisito, las actividades que se deben desarrollar son las siguientes:

- 1) Se deben realizar mesas de trabajo con las empresas vigiladas, así como brindar soporte a través del correo electrónico soportecun@sic.gov.co, con el fin de verificar las condiciones de asignación del CUN y el seguimiento del estado de las PQRs y solicitudes de indemnización en los sistemas de gestión.

- 2) Los vigilados deben llevar a cabo pruebas piloto internas de asignación del CUN y seguimiento del estado de las PQRs y solicitudes de indemnización en los sistemas de gestión. Las pruebas deben obedecer a un plan de pruebas establecidos por el operador.
- 3) Los operadores deben presentar un informe, que refleje los resultados de las pruebas piloto, al correo electrónico soportecun@sic.gov.co, el cual debe contener como mínimo la siguiente información:
 - a. Fecha de realización de la Prueba.
 - b. Casos a probar.
 - c. Parámetros. (Parámetros de entrada requeridos para realizar la prueba)
 - d. Persona(s) que realiza(n) la Prueba.
 - e. Datos del ambiente de Pruebas (motor base de datos, sistema operativo del servidor de aplicación y del servidor de base de datos).
 - f. Resultado de la Prueba (Exitoso/No exitoso).
 - g. Nombre y versión del sistema a probar. (Ej. Sistema PQR v.1.0)
- 4) Los operadores deben efectuar los ajustes resultantes de los incidentes detectados por ellos durante las pruebas piloto.
- 5) Una vez realizados, verificados y aprobados los anteriores pasos por la Superintendencia de Industria y Comercio, se dará el aval para poner en producción final el desarrollo expuesto en el presente numeral.
- 6) Las sociedades vigiladas, deberán llevar a cabo el proceso de puesta en producción final de los sistemas de asignación de CUN y seguimiento del estado de las PQR's y/o solicitudes de indemnización en sus sistemas de gestión, en un periodo de tiempo que no puede exceder un término máximo de un (1) mes.

Para la segunda etapa, los operadores deben llevar a cabo las siguientes actividades:

- 1) Implementar los mecanismos de consulta interactiva entre sus sistemas y los sistemas de la Superintendencia de Industria y Comercio.
 - a. Consulta de estado de PQRs o solicitudes de indemnización desde el portal del operador.
 - b. Servicio Web expuesto por el operador para consulta de estado de PQRs o solicitudes de indemnización desde el portal Web de la SIC.
 - c. Consumo del servicio Web expuesto por la SIC para consulta del estado de una apelación.
- 2) Presentar informes de avance sobre la ejecución de las actividades técnicas destinadas a implementar los mecanismos de consulta interactiva. Dichos informes, como mínimo, deben contener la siguiente información:
 - a. Fecha generación del informe.
 - b. Fecha inicial y final del periodo a reportar.

- c. Cronograma de actividades (actividad, descripción, fecha inicial, fecha final, porcentaje avance, resultado de la actividad).
- 3) Realizar mesas de trabajo y/o reuniones presenciales o virtuales programadas por la SIC o solicitadas por parte de las empresas vigiladas, a través del correo electrónico soportecun@sic.gov.co, para verificar la implementación del mecanismo de envío de expedientes y realizar la configuración de los parámetros de seguridad del operador en el sistema de la SIC.
- 4) Realizar pruebas piloto de los mecanismos de consulta interactiva entre los sistemas de los operadores y los sistemas de la Superintendencia de Industria y Comercio. Para ello, se coordinarán las fechas y la temática concreta de dichas pruebas piloto.
- 5) Presentar un informe de los resultados de cada una de las pruebas piloto efectuadas respecto de los mecanismos de consulta interactiva que trata esta segunda etapa. Dicho informe debe contener como mínimo la siguiente información:
 - a. Fecha de realización de la Prueba.
 - b. Casos a probar.
 - c. Parámetros. (Parámetros de entrada requeridos para realizar la prueba)
 - d. Persona(s) que realiza(n) la Prueba.
 - a. Datos del ambiente de Pruebas. (motor base de datos, sistema operativo del servidor de aplicación y del servidor de base de datos).
 - e. Resultado de la Prueba (Exitoso/No exitoso).
 - b. Nombre y versión del sistema a probar. (Ej. Consulta PQR v.1.0)
- 6) Realizar los ajustes resultantes de los incidentes detectados por los operadores durante las pruebas piloto.
- 7) Una vez realizados, verificados y aprobados los anteriores pasos por los la Superintendencia de Industria y Comercio, se dará el aval para poner en producción final el desarrollo expuesto en el presente numeral.
- 8) Llevar a cabo el proceso de puesta en producción final de los sistemas de asignación de CUN y seguimiento del estado de las PQR's y/o solicitudes de indemnización en sus sistemas de gestión, en un periodo de tiempo que no puede exceder un término máximo de un (1) mes.

Para el desarrollo de la segunda etapa de implementación, los operadores deben llevar a cabo las siguientes actividades:

- 1) Implementar el cliente del servicio Web para transferencia de expedientes expuesto por la SIC, siguiendo las indicaciones técnicas que se describen en este documento.
- 2) Realizar mesas de trabajo y/o reuniones presenciales o virtuales programadas por la SIC o solicitadas por parte de las empresas vigiladas, a través del correo electrónico soportecun@sic.gov.co, para verificar la implementación del mecanismo

de envío de expedientes y realizar la configuración de los parámetros de seguridad del operador en el sistema de la SIC.

- 3) Realizar pruebas piloto de los mecanismos de reporte de expedientes de apelaciones ante la SIC. Para ello se deberá coordinar con esta Entidad, la fecha de realización de dichas pruebas.
- 4) Presentar un informe de los resultados de las pruebas piloto de los mecanismos de reporte de expedientes de apelaciones ante la SIC, el cual debe contener como mínimo la siguiente información:
 - a. Fecha de realización de la Prueba.
 - b. Casos a probar.
 - c. Parámetros. (Parámetros de entrada requeridos para realizar la prueba)
 - d. Persona(s) que realiza(n) la Prueba.
 - e. Datos del ambiente de Pruebas. (motor base de datos, sistema operativo del servidor de aplicación y del servidor de base de datos).
 - f. Resultado de la Prueba. (Exitoso/No exitoso).
 - g. Nombre y versión del sistema a probar. (Ej. Consulta PQR v.1.0)
- 5) Realizar los ajustes resultantes de los incidentes detectados durante las pruebas piloto.
- 6) Una vez realizados, verificados y aprobados los anteriores pasos por parte de la Superintendencia de Industria y Comercio, se dará el aval para poner en producción final el desarrollo expuesto en el presente numeral.
- 7) Culminada exitosamente la etapa de pruebas, y previa habilitación por parte de esta Entidad, se deberá efectuar la puesta en producción final de los mecanismos electrónicos de reporte de expedientes de apelaciones ante la SIC.

2 ASPECTOS TÉCNICOS Y FUNCIONALES QUE DEBE CUMPLIR LA IMPLEMENTACIÓN DEL CUN

Con la finalidad de implementar de manera adecuada lo indicado en el numeral inmediatamente anterior, debe seguirse de manera estricta la estructura numérica y conceptual prevista en el Capítulo Tercero del Título III de la Circular Única de la Superintendencia de Industria y Comercio, en lo referente al Código Único Numérico (CUN).

3 OBLIGACIONES GENERALES

En desarrollo de lo dispuesto en el presente anexo técnico, los operadores deberán cumplir dentro de sus políticas y procedimientos relativos a la administración del CUN, con las siguientes obligaciones:

3.1 SEGURIDAD Y CALIDAD

En desarrollo de los criterios de seguridad y calidad, y considerando los canales para la asignación del CUN, los operadores deben cumplir, como mínimo, con los siguientes requerimientos:

- Disponer de la infraestructura tecnológica necesaria, así como de los procedimientos y controles requeridos, que permitan realizar la asignación del CUN y la gestión de la información conforme a las condiciones derivadas de los criterios de seguridad y calidad ya señalados.
- Velar porque la información que se encuentre disponible para consulta o que sea remitida a los usuarios esté libre de software malicioso.
- Tener en operación la infraestructura tecnológica y aspectos asociados (protocolos, servicios, aplicaciones, usuarios, equipos, entre otros) requeridos para el adecuado desarrollo de las actividades necesarias para la implementación y operación del CUN.
- El operador debe utilizar e implementar de acuerdo a su capacidad e infraestructura las mejores prácticas sobre los estándares mínimos de seguridad dispuestos en la norma Colombiana NTC-ISO/IEC 27001.

Para ello se sugiere, por ejemplo, mecanismos de monitoreo de disponibilidad de la base de datos que accede el servicio de asignación del CUN, mecanismos de monitoreo de disponibilidad del servidor de aplicaciones donde reside dicho servicio, mecanismos de monitoreo de disponibilidad del servidor de aplicaciones donde reside el servicio de consulta del CUN, entre otros.

- Disponer de planes de contingencia y continuidad debidamente documentados que garanticen la disponibilidad del servicio de asignación del CUN. Los planes de contingencia y continuidad deben tener al menos los siguientes componentes:
 - a. **Análisis y evaluación de riesgos:** Se trata de obtener un conocimiento de la plataforma tecnológica de la organización que soporta la asignación del CUN y de los procesos que se consideran críticos para el funcionamiento de este sistema. Una vez identificados los mismos, se debe analizar cuáles son los riesgos asociados, para identificar las causas potenciales que pueden llegar a interrumpir la asignación del CUN.
 - b. **Selección de estrategias:** El operador debe valorar las diferentes alternativas y estrategias de respaldo en función de los resultados obtenidos en la fase anterior, para seleccionar la estrategia más adecuada que garantice la disponibilidad del servicio, además, se deben corregir las vulnerabilidades detectadas en los procesos críticos identificadas en el análisis de riesgos.
 - c. **Desarrollo del plan:** Una vez que seleccionada la estrategia de respaldo hay que desarrollarla e implementarla para el sistema de generación del CUN. En esta fase

se desarrollan los procedimientos y planes de acción que permitan la ejecución del plan de contingencia.

Los tres componentes del plan de contingencia deben estar debidamente documentados y sustentados. Deben realizarse pruebas a este plan de contingencia cada 6 meses para demostrar su efectividad generando un informe con los resultados obtenidos.

El plan de contingencia debe revisarse y actualizarse por lo menos una vez al año, verificando nuevos riesgos en la plataforma tecnológica que soporta el sistema y tomando las acciones necesarias que permitan la continuidad y disponibilidad de la asignación del CUN.

3.2 DOCUMENTACIÓN

En materia de documentación, los operadores deben cumplir con los siguientes requerimientos:

- Un registro detallado de los códigos asignados, que debe contener como mínimo la siguiente información:
 - Número del CUN asignado.
 - Fecha y hora de radicación de la PQR o solicitud de indemnización.
 - Estado del trámite.
 - Datos básicos del quejoso que solicita el trámite. (Nombres y apellidos y número y tipo de identificación)
 - Datos Básicos del operador frente al cual se interpuso el trámite. (Razón social y Nit.)
- Procedimientos que describan la disponibilidad, mecanismo de asignación, control y registro de los números CUN asignados, para garantizar que se cumpla lo establecido en los criterios de seguridad y calidad ya indicados.
- Procedimientos que describan la disponibilidad de la consulta de CUN, para garantizar que se cumpla lo establecido en los criterios de seguridad y calidad ya indicados.

Mantener a disposición de la Superintendencia de Industria y Comercio, estadísticas anuales con corte a 31 de diciembre de cada año respecto de la asignación del CUN que contemplen: la bitácora de asignación del CUN, bitácora de anulación, bitácora del nivel de disponibilidad del servicio, Tipo de PQR. Esta información, debe ser conservada por un término mínimo de tres (3) años.

Asimismo, los operadores deben llevar estadísticas mensuales de acceso a la consulta del CUN indicando entre otros los siguientes datos: Número de consultas realizadas, Número de consultas exitosas, Número de consultas fallidas y Tiempo de respuesta promedio.

- En relación con los datos estadísticos, los datos que debe contener la bitácora de asignación son:
 - Operador: Código base (Identificador del Operador)
 - CUN: Número de CUN asignado
 - Fecha Asignación: Corresponde a la fecha de generación de CUN, en formato AAAA-MM-DD HH:MM:SS
 - Tipo de PQR: De acuerdo con la tipología de petición, queja, recurso y solicitud de indemnización establecida en el Régimen de Protección a Usuarios de Servicios de Comunicaciones y en el Título III de la Circular única (para el caso de postales)

- En relación con los datos estadísticos, los datos que debe contener la bitácora de anulados son:
 - Operador: Código base (Identificador del Operador)
 - CUN: Número de CUN asignado
 - Fecha Incidente: Corresponde a la fecha de ocurrencia de la incidencia, en formato AAAA-MM-DD HH:MM:SS
 - Motivo Incidencia: Corresponde al tipo de situación que generó la incidencia, la cual puede ser: Tipología exenta, Error de transcripción, entre otros.
 - Tipo y Número de Identificación: Asociado a la persona que registra el reporte del incidente
 - Nombre de la persona: Apellidos y nombres de la persona que registra el reporte del incidente
 - Fecha reporte: Fecha en que se reporta la incidencia en formato AAAA-MM-DD HH:MM:SS

- En relación los datos estadísticos, con incidentes que afecten la disponibilidad del módulo de asignación del CUN, así como la consulta del mismo, por motivos técnicos, deben ser registrados en una bitácora y la información que se debe consignar es:
 - Operador: Código base (Identificador del Operador)
 - Fecha y hora inicio Incidente: Corresponde a la fecha de ocurrencia de la incidencia, en formato AAAA-MM-DD HH:MM:SS
 - Fecha y hora recuperación del Incidente: Corresponde a la fecha en la que se logró recuperar de la incidencia, en formato AAAA-MM-DD HH:MM:SS
 - Motivo Incidencia: Corresponde al tipo de situación que generó la incidencia, la cual puede ser: Mantenimiento, Falla en servidor, Problemas de Fluído Eléctrico, Falla de Software, Otros
 - Tipo y Número de Identificación: Asociado a la persona que registra el reporte del incidente
 - Nombre de la persona: Apellidos y nombres de la persona que registrar el porte del incidente
 - Fecha reporte: Fecha en que se reporta la incidencia en formato AAAA-MM-DD HH:MM:SS

- En relación con los datos estadísticos asociados al tipo de PQR, se debe registrar tanto el tipo de PQR como la cantidad de solicitudes recibidas por el operador.

3.3 DIVULGACIÓN DE LA INFORMACIÓN

En materia de divulgación de información, los operadores deben cumplir, como mínimo, con los siguientes requerimientos:

- Suministrar a los usuarios, información clara, completa y oportuna sobre el CUN asignado, de conformidad con lo establecido en el numeral **3.4 “Mecanismos para informar o comunicar la asignación de un Código Único Numérico –CUN–”** del Capítulo Tercero del Título III de la Circular Única de esta Superintendencia.
- En el caso de servicios de comunicaciones empaquetados o interconectados, se deben tener en cuenta los procedimientos establecidos para asignación y reportes del CUN señalados en el Capítulo Tercero del Título III de la Circular Única.
- Cuando no se pueda realizar la asignación del CUN o no se pueda acceder a la consulta del mismo, se debe advertir previamente al usuario de esta situación, y debe seguirse el procedimiento señalado en el “*Procedimiento a seguir cuando el sistema no se encuentre disponible por fallas o mantenimientos*” del Capítulo Tercero del Título III de la Circular Única.
- Los operadores deben suministrar al usuario por cualquier medio idóneo la constancia de la presentación de la PQR o solicitud de indemnización, la cual contendrá como mínimo la siguiente información: fecha y hora, el CUN asignado y datos del solicitante (usuario).
- Informar y mantener debidamente actualizados, los procedimientos necesarios para atender de manera segura y eficiente a los usuarios en todo momento, en particular cuando se presenten situaciones especiales tales como: fallas en los sistemas, restricciones en los servicios o mantenimientos programados, entre otros.

4 ETAPA I – ASIGNACIÓN DEL CUN

4.1 DEFINICIONES DE CRITERIOS DE SEGURIDAD Y CALIDAD.

4.1.1 CRITERIOS DE SEGURIDAD

4.1.1.1 Confidencialidad

Los operadores deben garantizar la confidencialidad de la información, según las políticas de cada empresa, se sugiere que la información sea asegurada desde el origen de la solicitud hasta el destino donde se almacenará la información.

4.1.1.2 Integridad

La información asociada a la asignación del CUN debe ser precisa, coherente y completa. El sistema deberá tener los mecanismos que sean necesarios para garantizar la trazabilidad de los códigos asignados y que los mismos no puedan ser alterados posteriormente.

4.1.1.3 Disponibilidad

La información asociada a la asignación del CUN, deberá estar disponible en el momento que la SIC lo requiera, al igual que los recursos tecnológicos empleados por el operador.

Teniendo en cuenta que el módulo de asignación del CUN y el de su consulta son sistemas de alto impacto en la gestión de las PQRs y solicitudes de indemnización que realizan los usuarios ante los operadores, se debe garantizar la disponibilidad de tales servicios a efecto de que no se afecte la continuidad y la secuencia en la asignación del CUN.

Para ello cada operador debe disponer de las herramientas necesarias que le permitan alcanzar el nivel de disponibilidad del 98% +- 2%, de la infraestructura tecnológica que soporta el sistema de asignación del CUN

Los operadores deben tener disponibles los indicadores aquí señalados, con los cortes asociados a las metas establecidas. Los soportes de estos indicadores deben estar a disposición cuando la Superintendencia de Industria y Comercio así lo requiera. En todo caso, el informe del período deberá consolidarse dentro de los diez (10) días hábiles siguientes al vencimiento del mismo.

4.1.1.4 Auditoría

Es necesario dentro del esquema de seguridad, generar mecanismos de auditoría que permitan entender una cadena de eventos con los cuales se pueda determinar la causa de cualquier problema, por lo tanto, es obligatoria la generación de logs, que permitan la trazabilidad de objetos dentro de la aplicación, los accesos de usuario y los eventos propios del sistema.

Los logs de auditoría, asociados a la asignación del CUN, deben ser parte de cada uno de los aspectos de seguridad aquí tratados, con el fin de conocer los posibles aspectos de falla en los controles generados por las aplicaciones.

En el log se debe registrar como mínimo, lo siguiente:

- Número CUN asignado
- Fecha y hora de la asignación del CUN
- Identificación del usuario (Tipo y número de identificación)
- Resultado de la transacción (Éxito o Fallo)

El operador puede implementar mecanismos de auditoría adicionales.

4.1.2 CRITERIOS DE CALIDAD

4.1.2.1 Efectividad

El operador debe entregar al usuario el CUN asignado en el mismo momento de la presentación de la PQR o solicitud de indemnización, o a más tardar el día siguiente cuando la misma se haya presentado por la página web o red social, a través de cualquier medio idóneo.

4.1.2.2 Eficiencia

El operador deberá ajustar su infraestructura y medios disponibles para lograr la asignación del CUN, de forma tal que se eviten situaciones tales como reprocesos y demoras en la notificación del CUN que terminen afectando la atención al usuario.

4.1.2.3 Confiabilidad

El sistema debe garantizar que, para cada PQRs o solicitud de indemnización, el CUN asignado sea acorde con la estructura definida, asignado cronológicamente y sea único por cada asignación que realice el operador.

Para tal efecto, en relación con la fecha y hora de asignación del CUN, el mecanismo que se implemente para ello deberá estar sincronizado con el servidor de la hora legal para la República de Colombia, al cual podrá accederse a través del sitio web de la Superintendencia de Industria y Comercio.

5 ETAPA II – CONSULTA INTERACTIVA

5.1 DEFINICIONES DE CRITERIOS DE SEGURIDAD Y CALIDAD

5.1.1 CRITERIOS DE SEGURIDAD

5.1.1.1 Confidencialidad

Los operadores deben garantizar la confidencialidad de la información asociada a la consulta interactiva del CUN, proporcionando para ello mecanismos que permitan limitar la accesibilidad de dichos datos en su fase de transmisión, de manera exclusiva a los sistemas de información o personas destinatarias de la información.

Para asegurar la confidencialidad de la información a nivel de transporte para la consulta del CUN, los operadores deben implementar el protocolo TLS (**Transport Layer Security**) v 1.2 o superior (certificado de sitio seguro), en los canales de comunicación de los sistemas de información y aplicaciones que reciban o transmitan datos entre la infraestructura del operador y la SIC.

El certificado de sitio seguro debe ser un certificado válido (no autofirmado), de mínimo 256 bits, obtenido bajo la decisión y responsabilidad de cada una de las partes que por norma y política pública intervienen en esta implementación tecnológica, esta es una obligación tanto para esta entidad pública como para cada uno de los entes privados(Operador).

5.1.1.2 Integridad

La información asociada a la asignación del CUN debe ser precisa, coherente y completa. El sistema debe contar con los mecanismos que resulten necesarios para garantizar la trazabilidad de los códigos asignados y que los mismos no puedan ser alterados posteriormente.

5.1.1.3 Disponibilidad

En lo que corresponde a la disponibilidad en servicio del módulo de consulta interactiva, considerando que es un sistema de información de alto impacto en la gestión de las PQR's y solicitudes de indemnización que realizan los usuarios ante los operadores, éstos deben garantizar, la disponibilidad de los mencionados servicios, con la finalidad de evitar afectaciones que alteren la continuidad del servicio de consulta interactiva del CUN.

Para ello cada operador deberá disponer de las herramientas necesarias que le permitan alcanzar los niveles de disponibilidad del 98% +- 2%, de la infraestructura tecnológica que soporta la consulta del CUN (a través de los servicios web que sean implementados).

Los soportes de estos indicadores, deben mantenerse a disposición de la Superintendencia de Industria y Comercio, para cuando esta Entidad los requiera, durante un mínimo de tres (3) años. En todo caso, el informe de cada período deberá consolidarse dentro de los diez (10) días hábiles siguientes al vencimiento del mismo.

5.1.1.4 Auditoría

Es necesario dentro del esquema de seguridad, generar mecanismos de auditoría que permitan entender una cadena de eventos con los cuales se pueda determinar la causa de cualquier problema, por lo tanto, es obligatoria la generación de logs, que permitan la trazabilidad de objetos dentro de la aplicación, los accesos de usuario y los eventos propios del sistema.

Los logs de auditoría, asociados a la asignación del CUN, deben ser parte de cada uno de los aspectos de seguridad aquí tratados, con el fin de conocer los posibles aspectos de falla en los controles generados por las aplicaciones.

En el log se debe registrar como mínimo, lo siguiente:

- Número CUN asignado.
- Fecha y hora del consumo del servicio web.
- Identificación del usuario (Tipo y número de identificación).
- Resultado de la transacción (Éxito o Fallo).

El operador podrá implementar mecanismos de auditoría adicionales, como por ejemplo, llevar una bitácora de consultas efectuadas por los servicios web dispuestos por la SIC.

5.1.2 CRITERIOS DE CALIDAD

5.1.2.1 Efectividad

El operador debe entregar al usuario información exacta respecto a cada CUN consultado de forma instantánea, sin violar la ley de protección de datos personales cuando se realiza una consulta de forma pública (acceder a ella sin uso de usuario y clave personalizada).

5.1.2.2 Eficiencia

El operador debe ajustar su infraestructura y medios disponibles para lograr proveer al usuario la información del estado actual del CUN, de forma tal que se eviten situaciones tales como la desinformación del estado actual del trámite del usuario.

5.1.2.3 Confiabilidad

El operador debe entregar al usuario la información asociada a un CUN de forma íntegra, es decir, que esté implementada bajo un esquema que permita que la información sea exacta y completa.

5.2 ESPECIFICACIONES TÉCNICAS

Los operadores deben implementar el mecanismo que a continuación se especifica, el cual debe permitir la consulta interactiva del CUN, la cual debe estar accesible desde su página web.

Dicho mecanismo, debe permitir al usuario realizar una consulta sobre el estado actualizado de su PQR o solicitud de indemnización a través de la página web del operador, o desde la página web de la SIC (según aplique).

A continuación, se describen los cuatro escenarios en los que puede estar un usuario para obtener la información del estado actual de su PQR o solicitud de indemnización:

Escenario de consulta 1. La PQR o solicitud de indemnización se encuentra en trámite o resuelta ante el operador y el usuario ingresa a la página web de éste.

Escenario de consulta 2. La PQR o solicitud de indemnización se encuentra en trámite o resuelta ante el operador y el usuario ingresa a la página web de la SIC.

[Inicio](#) [Contáctenos](#) [Ayuda](#)

Consulta de peticiones, quejas, recursos y solicitudes de indemnización con código único numérico

Consulte aquí el estado de su trámite, utilizando para ello el Código Único Numérico que fue asignado por el proveedor de servicios de comunicaciones o el operador postal al momento de radicar su PQR

Peticiones, quejas, recursos o Solicitud de Indemnización
ante el operador o proveedor

Apelaciones
ante la SIC

Consulte esta opción si considera que su trámite se encuentra en la SIC. En esta consulta usted podrá realizar la consulta por alguno de los criterios que se muestran a continuación:

Opción de búsqueda:

BUSCAR POR EL CÓDIGO UNICO NUMÉRICO (CUN) ?

Operador o Proveedor *	Año *	Consecutivo *
<input type="text"/>	Elegir...	<input type="text"/>

Consultar
Limpiar

Para una mejor visualización de este sitio, utilice los navegadores Internet Explorer 9, Google Chrome 2.1, Mozilla Firefox 5 o Safari 6. Asegúrese que su navegador tenga habilitado la ejecución de scripts.

Escenario de consulta 3. La apelación se encuentra en trámite o resuelta ante la SIC y el usuario ingresa a la página web del operador.

Escenario de consulta 4. La apelación se encuentra en trámite o resuelta ante la SIC y el usuario ingresa a la página web de la SIC.

[Inicio](#) [Contáctenos](#) [Ayuda](#)

Consulta de peticiones, quejas, recursos y solicitudes de indemnización con código único numérico

Consulte aquí el estado de su trámite, utilizando para ello el Código Único Numérico que fue asignado por el proveedor de servicios de comunicaciones o el operador postal al momento de radicar su PQR

Peticiones, quejas, recursos o Solicitud de Indemnización
ante el operador o proveedor

Apelaciones
ante la SIC

Consulte esta opción si considera que su trámite se encuentra en la SIC. En esta consulta usted podrá realizar la consulta por alguno de los criterios que se muestran a continuación:

Opción de búsqueda:

BUSCAR POR EL CÓDIGO UNICO NUMÉRICO (CUN) ?

Operador o Proveedor *	Año *	Consecutivo *
<input type="text"/>	Elegir...	<input type="text"/>

Consultar
Limpiar

Para una mejor visualización de este sitio, utilice los navegadores Internet Explorer 9, Google Chrome 2.1, Mozilla Firefox 5 o Safari 6. Asegúrese que su navegador tenga habilitado la ejecución de scripts.

5.2.1 Escenario de consulta 1. La PQR o solicitud de indemnización se encuentra en trámite o resuelta ante el operador y el usuario ingresa a la página web de éste

El operador debe implementar una consulta en su página web. El usuario podrá acceder a esta mediante un enlace (link) en la página principal del portal web del operador, que lo lleve a un formulario donde el usuario tenga la opción de consultar su trámite con los siguientes parámetros:

- CUN asignado.
- Tipo de identificación y número de Identificación.

La información que se suministre al usuario debe contener como mínimo los siguientes parámetros:

Tabla 1. Resultado de consulta escenario 1

Nombre del Quejoso	Tipo de identificación	Número de identificación	Código Único Numérico (CUN)	Fecha asignación	Tipo de queja	Estado del trámite	Fecha de respuesta
--------------------	------------------------	--------------------------	-----------------------------	------------------	---------------	--------------------	--------------------

- Nombre del Quejoso: Debe visualizarse los nombres y apellidos completos del usuario.
- Código Único Numérico (CUN): Es el código único que identifica el trámite ante el operador y se debe mostrar al usuario con la máscara establecida en el numeral 3.1.1 **Estructura del Código Único Numérico – CUN**, del Título III de la Circular Única, de la SIC.
- Fecha de asignación: Es la fecha cuando se le asignó el CUN al usuario, esta fecha debe ser de tipo datetime (2012-10-28 09:03:55).
- Tipo de Queja: Es la tipología de petición, queja, recurso o solicitud de indemnización a la cual debe asignársele un código único numérico de acuerdo a las tipologías previstas en el RPU (en el caso de operadores de servicios de comunicaciones) y en el Título III de la Circular Única (en el caso de operadores postales).
- Estado del Trámite: Es el estado que describe en qué etapa del proceso está el trámite de la PQR o solicitud de indemnización ante el operador, estos estados son los que están previstos en el Capítulo III Título III de la Circular Única de esta Entidad.
- Fecha de respuesta: Esta fecha es de tipo date (2012-10-28) que informa al usuario la fecha que darán respuesta a su PQR o solicitud de indemnización.

5.2.2 Escenario de consulta 2. La PQR o solicitud de indemnización se encuentra en trámite o resuelta ante el operador y el usuario ingresa a la página web de la SIC

La SIC dispone de un esquema para la obtención de la información del operador, en el cual despliega un formulario en la página web de la SIC y requiere configurar un cliente de

servicio web para establecer comunicación con el operador, quien a su vez expone un servicio web que permite la consulta del estado de una PQR.

Los parámetros que serán remitidos al operador son los definidos en el numeral 5.2.6.1 Métodos Públicos Servicio Web Operador – consultaCUN – Parámetros de entrada.

Los Parámetros de retorno que debe devolver el operador a la SIC son los definidos en el numeral 5.2.6.1 Métodos Públicos Servicio Web Operador – consultaCUN – Parámetros de salida.

La información que se desplegará será la siguiente:

Tabla 2. Resultado de consulta escenario 2

Nombre del Quejoso	Tipo de identificación	Número de identificación	Código Único Numérico (CUN)	Fecha asignación	Tipo de queja	Estado del Trámite	Fecha de respuesta
--------------------	------------------------	--------------------------	-----------------------------	------------------	---------------	--------------------	--------------------



Consulta de peticiones, quejas, recursos y solicitudes de indemnización con código único numérico

Consulte aquí el estado de su CUN

Peticiones, quejas y recursos **Apelaciones**
 Indemnización ante el operador o proveedor **ante la SIC**

Resultados Consulta realizada Descargar PDF

2 ID operador/proveedor: 403 Año: 12 Consultiva: 00000000 Para ingresar, descargue este contenido en PDF Nueva consulta

Nombre: Norberto Villegas Castañeda
 Cédula de Ciudadanía: 321
 Operador/proveedor: NOMBRE OPERADOR 2

Fecha de consulta: 05/12/2012
 A continuación se presenta el resultado de su consulta. Este resultado fue obtenido del operador/proveedor: NOMBRE OPERADOR 2

CUN	Fecha asignación CUN	Fecha de respuesta	Estado del trámite	Tipo de queja
4436-12-0000000001	2012-01-01	2012-01-01	Esta es la queja	
4436-12-0000000001	2012-01-01	2012-01-01	Esta es la queja	

5.2.3 Escenario de consulta 3. La apelación se encuentra en trámite o resuelta ante la SIC y el usuario ingresa a la página web del operador

La SIC dispone de un servicio web para consulta del estado actual de una apelación (ver numeral 5.2.6.3 Servicio SIC). Los operadores deben implementar un mecanismo de consumo (cliente) del servicio web y generar un formulario web, que permita a sus usuarios consultar el estado actual de la apelación de su PQR o solicitud de indemnización.

Los parámetros que serán remitidos desde operador son los definidos en el numeral 5.2.6.2 Métodos Públicos Servicio Web SIC – consultaCUN – Parámetros de entrada.

Los Parámetros de retorno que debe devolver la SIC al operador son los definidos en el numeral 5.2.6.2 Métodos Públicos Servicio Web SIC – consultaCUN – Parámetros de salida.

Los parámetros de retorno se describen a continuación:

- Datos mínimos del usuario (Natural o jurídico según aplique).
- Código Único Numérico – CUN.
- Fecha de Asignación.
- Estado actual de trámite de su PQR.
- Tipo de queja.
- Link (Ver detalle): Este link será suministrado por la SIC para que el usuario cuando realice el evento de click sobre el enlace puede dirigirse a la página de la SIC para ver la trazabilidad de su trámite ante la Entidad.

Presentación de la Información:

“Resultado de información originada de la SIC”

Tabla 3. Parámetros de consulta escenario 3

Nombre del Quejoso	Tipo de identificación	Número de identificación	Código Único Numérico (CUN)	Fecha asignación	Tipo de queja	Estado del trámite	Ver detalle del trámite

5.2.4 Escenario de consulta 4. La apelación se encuentra en trámite o resuelta ante la SIC y el usuario ingresa a la página web de la SIC.

La SIC dispone de un formulario Web por medio del cual el usuario podrá realizar la consulta del estado de su trámite (apelación), ingresando para ello el CUN o tipo y número de identificación.

La presentación de la información por parte de la SIC, será de la siguiente manera:

Tabla 4. Parámetros de consulta escenario 4

Nombre del Quejoso	Tipo de identificación	Número de identificación	Código Único Numérico (CUN)	Fecha asignación	Estado del trámite	Tipo de queja	Ver detalle del trámite



5.2.5 Diagrama de Interacción entre Operadores y SIC

La integración por medio de servicios entre sistemas de información, requiere la definición del modelo de datos o estructura de datos a ser usada como paquete de transmisión tanto desde la SIC como desde el operador. Para tal efecto, se define a continuación un único esquema de transmisión, de tal manera que la integración de servicios sea transparente.

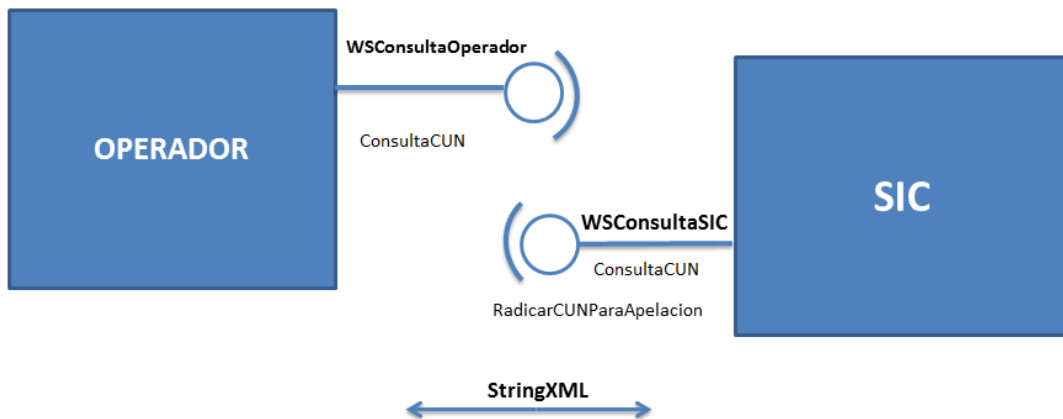


Imagen 1. Diagrama de interacción.

De acuerdo al diagrama anterior, se evidencia que tanto el operador como la SIC en la integración, deben realizar su función por medio de la exposición de Servicios WEB SOAP XML, lo cual implica una organización de interoperabilidad que requiere tanto contratos para los servicios como estructuras de información para el intercambio de los mensajes.

5.2.6 CONTRATOS DE SERVICIO

Los contratos de servicio definen la interfaz de comunicación entre servicios WEB, por lo tanto, describen las firmas de los métodos que se deben ejecutar para llevar a cabo las respuestas a las solicitudes o peticiones de servicios que se envían de un sistema a otro.

Para la integración de servicios entre la SIC y los Operadores se han definido dos servicios WEB que son implementados respectivamente.

La siguiente tabla describe los contratos de servicio, detallando los métodos, tipos de dato de retorno y los parámetros de entrada a ser implementados para lograr el objetivo de integración.

5.2.6.1 Métodos Públicos Servicio Web Operador

Tabla 5. Métodos Públicos Web Services Operador

NOMBRE	PARAMETROS DE ENTRADA	PARAMETROS DE SALIDA
consultaCUN	<ul style="list-style-type: none"> • CUN (cadena de caracteres) <ul style="list-style-type: none"> ○ IO (Identificador del Operador) ○ AA (Año actual del CR) ○ CR (Consecutivo de Radicación) • Tipo de Identificación (tipo identificación) • Número de Identificación (cadena de caracteres) 	Cadena de caracteres XML-String (ver esquema).

5.2.6.2 Métodos Públicos Servicio Web SIC

Tabla 6. Métodos Públicos Web Services SIC

NOMBRE	PARAMETROS DE ENTRADA	PARAMETROS DE SALIDA
consultaCUN	<ul style="list-style-type: none"> • CUN (cadena de caracteres) • Tipo de Identificación (tipo identificación) • Número de Identificación (cadena de caracteres) 	XML (ver esquema).

5.2.6.3 Servicio SIC

Corresponde al contrato de servicios que expone la SIC para que el operador lo consuma. Este servicio se encuentra publicado en la URL:

https://webcun.sic.gov.co/consultaCUN/SIC_1.0.0/WSConsultaSIC/WSConsultaSIC?wsdl

```

<wsdl:definitions xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
xmlns:wsaw="http://www.w3.org/2006/05/addressing/wsdl" xmlns:tns="http://ws.wso2.org/dataservice"
xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
xmlns:mime="http://schemas.xmlsoap.org/wsdl/mime/" xmlns:http="http://schemas.xmlsoap.org/wsdl/http/"
targetNamespace="http://ws.wso2.org/dataservice">
  <wsdl:types>
    <xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
xmlns:wsaw="http://www.w3.org/2006/05/addressing/wsdl" xmlns:tns="http://ws.wso2.org/dataservice"
xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
xmlns:mime="http://schemas.xmlsoap.org/wsdl/mime/" xmlns:http="http://schemas.xmlsoap.org/wsdl/http/"
attributeFormDefault="unqualified" elementFormDefault="qualified"
targetNamespace="http://ws.wso2.org/dataservice">
      <xs:element name="DataServiceFault" type="xs:string"/>
      <xs:element name="REQUEST_STATUS" type="xs:string"/>
      <xs:element name="DATA_SERVICE_RESPONSE">
        <xs:complexType>
          <xs:sequence>
            <xs:any minOccurs="0"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
      <xs:element name="consultaCUN">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="identificadorOperador" nillable="true" type="xs:integer"/>
            <xs:element name="anoRadicacionCun" nillable="true" type="xs:integer"/>
            <xs:element name="ConsecutivoRadCun" nillable="true" type="xs:integer"/>
            <xs:element name="numeroRadicacion" nillable="true" type="xs:integer"/>
            <xs:element name="anoRadicacion" nillable="true" type="xs:integer"/>
            <xs:element name="nombreOperador" nillable="true" type="xs:string"/>
            <xs:element name="tipoldIdentificacion" nillable="true" type="xs:string"/>
            <xs:element name="numeroIdentificacion" nillable="true" type="xs:integer"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
      <xs:element name="ArrayOfIntegracionCUN" type="tns:ArrayOfIntegracionCUN"/>
      <xs:complexType name="ArrayOfIntegracionCUN">
        <xs:sequence>
          <xs:element maxOccurs="unbounded" minOccurs="0" name="IntegracionCUN" type="tns:IntegracionCUN"/>
        </xs:sequence>
      </xs:complexType>
      <xs:complexType name="IntegracionCUN">
        <xs:sequence>
          <xs:element name="nomOperador" nillable="true" type="xs:string"/>
          <xs:element name="codigoUnicoNumerico" type="tns:codigoUnicoNumerico"/>
          <xs:element name="numRadicadoCun" type="tns:numRadicadoCun"/>
          <xs:element minOccurs="0" name="nomPersona" type="tns:nomPersona"/>
          <xs:element name="tipoldNacionalPersona" nillable="true" type="tns:tipoldNacionalPersona"/>
          <xs:element name="grupoNumeroIdentificacion" nillable="true" type="xs:string"/>
          <xs:element name="descripcionEstado" type="xs:string"/>
          <xs:element name="fechaEstRespuesta" type="xs:dateTime"/>
          <xs:element name="fechaAsignacion" type="xs:dateTime"/>
          <xs:element minOccurs="0" name="razonSocial" type="xs:string"/>
          <xs:element name="url" type="xs:string"/>
          <xs:element name="tipoQuejaSic" nillable="true" type="tns:tipoQuejaSic"/>
          <xs:element minOccurs="0" name="MensajeServicio" nillable="true" type="tns:MensajeServicio"/>
        </xs:sequence>
      </xs:complexType>
      <xs:complexType name="codigoUnicoNumerico">
        <xs:sequence>
          <xs:element name="identificadorOperador" type="xs:integer"/>
          <xs:element name="anoRadicacionCun" nillable="true" type="xs:integer"/>
          <xs:element name="ConsecutivoRadCun" type="xs:integer"/>
        </xs:sequence>
      </xs:complexType>
      <xs:complexType name="numRadicadoCun">
        <xs:sequence>

```



```

    <xs:element name="anoRadicacionCun" type="xs:integer"/>
    <xs:element name="numRadicacionCun" type="xs:integer"/>
    <xs:element name="controlRadicadoCun" type="xs:string"/>
    <xs:element name="consecutivoRadicacion" type="xs:integer"/>
  </xs:sequence>
</xs:complexType>
<xs:complexType name="nomPersona">
  <xs:sequence>
    <xs:element name="primerApellido" nillable="true" type="xs:string"/>
    <xs:element minOccurs="0" name="segundoApellido" nillable="true" type="xs:string"/>
    <xs:element name="primerNombre" nillable="true" type="xs:string"/>
    <xs:element minOccurs="0" name="segundoNombre" nillable="true" type="xs:string"/>
  </xs:sequence>
</xs:complexType>
<xs:complexType name="tipoldNacionalPersona">
  <xs:sequence>
    <xs:element name="codTipoldNacionalPersona" nillable="true" type="xs:string"/>
    <xs:element name="nomTipoidentificacionNacionalPersona" nillable="true" type="xs:string"/>
  </xs:sequence>
</xs:complexType>
<xs:complexType name="tipoQuejaSic">
  <xs:sequence>
    <xs:element name="nomtipoQuejaSic" nillable="true" type="xs:string"/>
    <xs:element minOccurs="0" name="codtipoQuejaSic" nillable="true" type="xs:string"/>
  </xs:sequence>
</xs:complexType>
<xs:complexType name="MensajeServicio">
  <xs:sequence>
    <xs:element name="CodigoError" nillable="true" type="xs:string"/>
    <xs:element name="Descripcion" nillable="true" type="xs:string"/>
    <xs:element minOccurs="0" name="Opcional" nillable="true" type="xs:string"/>
    <xs:element name="TimeStamp" type="xs:dateTime"/>
  </xs:sequence>
</xs:complexType>
</xs:schema>
</wsdl:types>
<wsdl:message name="DataServiceFault">
  <wsdl:part element="tns:DataServiceFault" name="parameters" />
</wsdl:message>
<wsdl:message name="consultaCUNRequest">
  <wsdl:part element="tns:consultaCUN" name="parameters" />
</wsdl:message>
<wsdl:message name="consultaCUNResponse">
  <wsdl:part element="tns:ArrayOfIntegracionCUN" name="parameters" />
</wsdl:message>
<wsdl:portType name="WSConsultaSICPortType">
  <wsdl:operation name="consultaCUN">
    <wsdl:input message="tns:consultaCUNRequest" wsaw:Action="urn:consultaCUN" />
    <wsdl:output message="tns:consultaCUNResponse" wsaw:Action="urn:consultaCUNResponse" />
    <wsdl:fault message="tns:DataServiceFault" name="DataServiceFault"
wsaw:Action="urn:consultaCUNDataServiceFault" />
  </wsdl:operation>
</wsdl:portType>
<wsdl:binding name="WSConsultaSICSoap11Binding" type="tns:WSConsultaSICPortType">
  <soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
  <wsdl:operation name="consultaCUN">
    <soap:operation soapAction="urn:consultaCUN" style="document"/>
    <wsdl:input>
      <soap:body use="literal"/>
    </wsdl:input>
    <wsdl:output>
      <soap:body use="literal"/>
    </wsdl:output>
    <wsdl:fault name="DataServiceFault">
      <soap:fault name="DataServiceFault" use="literal"/>
    </wsdl:fault>
  </wsdl:operation>

```

```

</wsdl:binding>
<wsdl:service name="WSConsultaSIC">
  <wsdl:port binding="tns:WSConsultaSICSoap11Binding" name="WSConsultaSICHttpSoap11Endpoint">
    <soap:address location="http://wscun.sic.gov.co/consultaCUNSIC_1.0.0/WSConsultaSIC/WSConsultaSIC"/>
  </wsdl:port>
</wsdl:service>

</wsdl:definitions>

```

Imagen 2. Servicio SIC

Petición: Teniendo en cuenta que existen tres maneras de obtener información a partir del servicio expuesto por la SIC, a continuación se indican las diferentes formas de envío de parámetros desde los cuales un cliente de consumo puede obtener información, dependiendo del tipo de filtro que quiera aplicar:

Petición para el uso del filtro por número de CUN

```

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:dat="http://ws.wso2.org/dataservice">
  <soapenv:Header/>
  <soapenv:Body>
    <dat:consultaCUN>
      <dat:identificadorOperador>1</dat:identificadorOperador>
      <dat:anoRadicacionCun>1</dat:anoRadicacionCun>
      <dat:ConsecutivoRadCun>000000001</dat:ConsecutivoRadCun>
      <dat:numeroRadicacion>0</dat:numeroRadicacion>
      <dat:anoRadicacion>0</dat:anoRadicacion>
      <dat:nombreOperador>%</dat:nombreOperador>
      <dat:tipoidentificacion>%</dat:tipoidentificacion>
      <dat:numeroIdentificacion>0</dat:numeroIdentificacion>
    </dat:consultaCUN>
  </soapenv:Body>
</soapenv:Envelope>

```

Petición para el uso del filtro por número de radicación

```

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:dat="http://ws.wso2.org/dataservice">
  <soapenv:Header/>
  <soapenv:Body>
    <dat:consultaCUN>
      <dat:identificadorOperador>0</dat:identificadorOperador>
      <dat:anoRadicacionCun>0</dat:anoRadicacionCun>
      <dat:ConsecutivoRadCun>0</dat:ConsecutivoRadCun>
      <dat:numeroRadicacion>123456</dat:numeroRadicacion>
      <dat:anoRadicacion>21</dat:anoRadicacion>
      <dat:nombreOperador>0</dat:nombreOperador>
      <dat:tipoidentificacion>0</dat:tipoidentificacion>
      <dat:numeroIdentificacion>0</dat:numeroIdentificacion>
    </dat:consultaCUN>
  </soapenv:Body>
</soapenv:Envelope>

```

Petición para el uso del filtro por tipo y número de identificación

```

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:dat="http://ws.wso2.org/dataservice">
  <soapenv:Header/>
  <soapenv:Body>
    <dat:consultaCUN>

```

```

<dat:identificadorOperador>0</dat:identificadorOperador>
<dat:anoRadicacionCun>0</dat:anoRadicacionCun>
<dat:ConsecutivoRadCun>0</dat:ConsecutivoRadCun>
<dat:numeroRadicacion>0</dat:numeroRadicacion>
<dat:anoRadicacion>0</dat:anoRadicacion>
<dat:nombreOperador>NOMBRE DEL OPERADOR REGISTRADO EN LA SIC</dat:nombreOperador>
<dat:tipoidentificacion>CC</dat:tipoidentificacion>
<dat:numeroIdentificacion>12345678</dat:numeroIdentificacion>
</dat:consultaCUN>
</soapenv:Envelope>
</soapenv:Body>

```

5.2.6.4 Servicio Operador

Corresponde al servicio que debe exponer el operador para que la SIC lo consuma. Incluye el método para la consulta del CUN. A continuación, se describe el XSD del servicio:

```

<definitions xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
xmlns:tns="urn:WSConsultaOperador" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns="http://schemas.xmlsoap.org/wsdl/" targetNamespace="urn:WSConsultaOperador">
  <types>
    <xsd:schema xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
xmlns:tns="urn:WSConsultaOperador" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns="http://schemas.xmlsoap.org/wsdl/" targetNamespace="urn:WSConsultaOperador">
      <xsd:import namespace="http://schemas.xmlsoap.org/soap/encoding/" />
      <xsd:import namespace="http://schemas.xmlsoap.org/wsdl/" />
    </xsd:schema>
  </types>
  <message name="consultaCUN_Request">
    <part name="wsdl" type="xsd:string"> </part>
    <part name="identificadorOperador" type="xsd:int"> </part>
    <part name="anoRadicacionCun" type="xsd:int"> </part>
    <part name="ConsecutivoRadCun" type="xsd:int"> </part>
    <part name="tipoidentificacion" type="xsd:string"> </part>
    <part name="numeroIdentificacion" type="xsd:int"> </part>
  </message>
  <message name="consultaCUN_pruebasResponse">
    <part name="respuesta" type="xsd:string"> </part>
  </message>
  <message name="consultaCUN_Response">
    <part name="respuesta" type="xsd:string"> </part>
  </message>
  <message name="consultaCUNResponse">
    <part name="respuesta" type="xsd:string"> </part>
  </message>
  <message name="consultaCUNRequest">
    <part name="wsdl" type="xsd:string"> </part>
    <part name="identificadorOperador" type="xsd:int"> </part>
    <part name="anoRadicacionCun" type="xsd:int"> </part>
    <part name="ConsecutivoRadCun" type="xsd:int"> </part>
    <part name="tipoidentificacion" type="xsd:string"> </part>
    <part name="numeroIdentificacion" type="xsd:int"> </part>
  </message>
  <message name="consultaCUN_pruebasRequest">
    <part name="wsdl" type="xsd:string"> </part>
    <part name="identificadorOperador" type="xsd:int"> </part>
    <part name="anoRadicacionCun" type="xsd:int"> </part>
    <part name="ConsecutivoRadCun" type="xsd:int"> </part>
    <part name="tipoidentificacion" type="xsd:string"> </part>
    <part name="numeroIdentificacion" type="xsd:int"> </part>
  </message>

```

```

</message>
<portType name="consultaCUNPortType">
  <operation name="consultaCUN">
    <input message="tns:consultaCUNRequest"> </input>
    <output message="tns:consultaCUNResponse"> </output>
  </operation>
  <operation name="consultaCUN_pruebas">
    <input message="tns:consultaCUN_pruebasRequest"> </input>
    <output message="tns:consultaCUN_pruebasResponse"> </output>
  </operation>
  <operation name="consultaCUN_">
    <input message="tns:consultaCUN_Request"> </input>
    <output message="tns:consultaCUN_Response"> </output>
  </operation>
</portType>
<binding name="consultaCUNSoap11Binding" type="tns:consultaCUNPortType">
  <soap:binding style="rpc" transport="http://schemas.xmlsoap.org/soap/http"/>
  <operation name="consultaCUN">
    <soap:operation soapAction="urn:WSConsultaOperador#consultaCUN" style="rpc"/>
    <input>
      <soap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
namespace="urn:WSConsultaOperador" use="encoded"/>
    </input>
    <output>
      <soap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
namespace="urn:WSConsultaOperador" use="encoded"/>
    </output>
  </operation>
  <operation name="consultaCUN_pruebas">
    <soap:operation soapAction="urn:WSConsultaOperador#consultaCUN_pruebas" style="rpc"/>
    <input>
      <soap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
namespace="urn:WSConsultaOperador" use="encoded"/>
    </input>
    <output>
      <soap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
namespace="urn:WSConsultaOperador" use="encoded"/>
    </output>
  </operation>
  <operation name="consultaCUN_">
    <soap:operation soapAction="urn:WSConsultaOperador#consultaCUN_" style="rpc"/>
    <input>
      <soap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
namespace="urn:WSConsultaOperador" use="encoded"/>
    </input>
    <output>
      <soap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
namespace="urn:WSConsultaOperador" use="encoded"/>
    </output>
  </operation>
</binding>
<service name="consultaCUN">
  <port binding="tns:consultaCUNSoap11Binding" name="consultaCUNHttpSoap11Endpoint">
    <soap:address location="http://wscun.sic.gov.co/consultaCUNSIC_1.0.0/consultaCUN/WSConsultaOperador"/>
  </port>
</service>
</definitions>

```

Imagen 3. Servicio Operador

Petición: A modo de ejemplo, a continuación se cita la estructura del mensaje SOAP generado desde el cliente de consumo de la SIC para los dos tipos de consulta de PQRs que expone el servicio del operador:

Mensaje SOAP para la consulta de PQRs por número de CUN

```

<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
<ns:consultaCUN xmlns:ns="http://tempuri.org/">
  <ns:identificadorOperador>1111</ns:identificadorOperador>
  <ns:anoRadicacionCun>21</ns:anoRadicacionCun>
  <ns:ConsecutivoRadCun>1</ns:ConsecutivoRadCun>
  <ns:tipoidentificacion>%%</ns:tipoidentificacion>
  <ns:numeroIdentificacion>0</ns:numeroIdentificacion>
</ns:consultaCUN>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>

```

Mensaje SOAP para la consulta de PQRs por tipo y número de identificación

```

<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
<ns:consultaCUN xmlns:ns="http://tempuri.org/">
  <ns:identificadorOperador>0</ns:identificadorOperador>
  <ns:anoRadicacionCun>0</ns:anoRadicacionCun>
  <ns:ConsecutivoRadCun>0</ns:ConsecutivoRadCun>
  <ns:tipoidentificacion>CC</ns:tipoidentificacion>
  <ns:numeroIdentificacion>12345678</ns:numeroIdentificacion>
</ns:consultaCUN>
</SOAP-ENV:Body></SOAP-ENV:Envelope>

```

Respuesta: Teniendo en cuenta que la etiqueta <respuesta> es de tipo String-XML, a continuación se relacionan dos ejemplos de respuesta dependiendo el usuario que consulta la información y uno para aquella consulta que no contenga resultados:

Usuario persona natural

```

<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:tns="https://WSConsultaOperador/">
<soap:Body>
<ns1:consultaCUNResponse xmlns:ns1="http://WSConsultaOperador/">
<parameters xsi:type="tns:consultaCUNResponse">
<respuesta xsi:type="xsd:string">
  <![CDATA[
    <tns:ArrayOfIntegracionCUN xmlns:tns="http://ws.wso2.org/dataservice">
      <tns:IntegracionCUN>
        <tns:nombreOperador>OPERADOR</tns:nombreOperador>
        <tns:codigoUnicoNumerico>
          <tns:identificadorOperador>1234</tns:identificadorOperador>
          <tns:anoRadicacionCun>14</tns:anoRadicacionCun>
          <tns:ConsecutivoRadCun>0000000002</tns:ConsecutivoRadCun>
        </tns:codigoUnicoNumerico>
        <tns:nomPersona>
          <tns:primerNombre>NOMBRE_1</tns:primerNombre>
          <tns:segundoNombre>NOMBRE_2</tns:segundoNombre>
          <tns:primerApellido>APELLIDO_1</tns:primerApellido>
          <tns:segundoApellido>APELLIDO_2</tns:segundoApellido>
        </tns:nomPersona>
        <tns:tipoldNacionalPersona>
          <tns:codTipoldNacionalPersona>CC</tns:codTipoldNacionalPersona>
          <tns:nomTipoidentificacionNacionalPersona>
            CEDULA DE CIUDADANIA
          </tns:nomTipoidentificacionNacionalPersona>

```

```

</tns:tipoldNacionalPersona>
<tns:grupoNumeroidentificacion>1044999999
</tns:grupoNumeroidentificacion>
<tns:descripcionEstado>
  ANALISIS POR PARTE DEL OPERADOR
</tns:descripcionEstado>
<tns:fechaAsignacion>2013-04-11T00:00:00</tns:fechaAsignacion>
<tns:fechaEstRespuesta>2013-04-11</tns:fechaEstRespuesta>
<tns:razonSocial></tns:razonSocial>
<tns:tipoQuejaSic>
  <tns:nomTipoQuejaSic>
    ACTIVACION DE LINEAS ACTIVACION DE LINEAS
  </tns:nomTipoQuejaSic>
  <tns:codTipoQuejaSic>1</tns:codTipoQuejaSic>
</tns:tipoQuejaSic>
</tns:IntegracionCUN>
</tns:ArrayOfIntegracionCUN>
]]>
</respuesta>
</parameters>
</ns1:consultaCUNResponse>
</soap:Body>
</soap:Envelope>

```

Usuario persona jurídica

```

<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:tns="https://WSConsultaOperador/">
<soap:Body>
<ns1:consultaCUNResponse xmlns:ns1="http://WSConsultaOperador/">
<parameters xsi:type="tns:consultaCUNResponse">
<respuesta xsi:type="xsd:string">
  <![CDATA[
    <tns:ArrayOfIntegracionCUN xmlns:tns="http://ws.wso2.org/dataservice">
      <tns:IntegracionCUN>
        <tns:nombreOperador>OPERADOR</tns:nombreOperador>
        <tns:codigoUnicoNumerico>
          <tns:identificadorOperador>1234</tns:identificadorOperador>
          <tns:anoRadicacionCun>14</tns:anoRadicacionCun>
          <tns:ConsecutivoRadCun>0000000002</tns:ConsecutivoRadCun>
        </tns:codigoUnicoNumerico>
        <tns:nomPersona>
          <tns:primerNombre></tns:primerNombre>
          <tns:segundoNombre></tns:segundoNombre>
          <tns:primerApellido></tns:primerApellido>
          <tns:segundoApellido></tns:segundoApellido>
        </tns:nomPersona>
        <tns:tipoldNacionalPersona>
          <tns:codTipoldNacionalPersona>NI</tns:codTipoldNacionalPersona>
          <tns:nomTipoidentificacionNacionalPersona>
            NUMERO DE IDENTIFICACION TRIBUTARIA
          </tns:nomTipoidentificacionNacionalPersona>
        </tns:tipoldNacionalPersona>
        <tns:grupoNumeroidentificacion>10006000911</tns:grupoNumeroidentificacion>
        <tns:descripcionEstado>
          ANALISIS POR PARTE DEL OPERADOR
        </tns:descripcionEstado>
        <tns:fechaAsignacion>2013-04-11T00:00:00</tns:fechaAsignacion>
        <tns:fechaEstRespuesta>2013-04-11</tns:fechaEstRespuesta>
        <tns:razonSocial>MI RAZON SOCIAL</tns:razonSocial>
        <tns:tipoQuejaSic>
          <tns:nomTipoQuejaSic>
            ACTIVACION DE LINEAS ACTIVACION DE LINEAS
          </tns:nomTipoQuejaSic>
          <tns:codTipoQuejaSic>1</tns:codTipoQuejaSic>
        </tns:tipoQuejaSic>

```

```

    </tns:IntegracionCUN>
  </tns:ArrayOfIntegracionCUN>
  ]>
</respuesta>
</parameters>
</ns1:consultaCUNResponse>
</soap:Body>
</soap:Envelope>

```

Respuesta sin resultados

```

<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:tns="https://WSConsultaOperador/">
<soap:Body>
<ns1:consultaCUNResponse xmlns:ns1="http://WSConsultaOperador/">
<parameters xsi:type="tns:consultaCUNResponse">
<respuesta xsi:type="xsd:string">
<![CDATA[
<tns:ArrayOfIntegracionCUN xmlns:tns="http://ws.ws2.org/dataservice />
]]>
</respuesta>
</parameters>
</ns1:consultaCUNResponse>
</soap:Body>
</soap:Envelope>

```

Como salvedad, es importante tener en cuenta que, para garantizar el consumo del servicio, se debe contar previamente con la debida configuración de accesos de seguridad e infraestructura del lado del operador a la petición saliente originada desde los servidores de la SIC, que permitan garantizar la visibilidad entre servidores y como consecuencia de esto, el consumo del servicio.

6 ETAPA III – ENVÍO DE EXPEDIENTES DE APELACIÓN A LA SIC POR MEDIOS ELECTRÓNICOS

6.1 DEFINICIONES DE CRITERIOS DE SEGURIDAD Y CALIDAD

6.1.1 CRITERIOS DE SEGURIDAD

6.1.1.1 Confidencialidad

En relación con la confidencialidad de la información, los operadores deben implementar el protocolo TLS (**Transport Layer Security**) v 1.2 o superior.

Adicionalmente, a nivel de los mensajes que son intercambiados a través del Web Service Expuesto por la SIC, se implementará el estándar WS-Security aplicando criptografía asimétrica o de clave pública¹, mecanismo que permite el cifrado de mensajes para asegurarse de que ninguna parte ni proceso puede acceder a la información del mensaje o divulgarla, ya que, sólo puede descifrar y leer el mensaje, un servicio que conozca la clave correspondiente. Este mecanismo requiere un intercambio de llaves, donde la SIC entregará su llave pública a los operadores, quienes, a su vez, deberán entregar su llave pública a la SIC, de tal modo que se pueda realizar la encriptación del mensaje. Las llaves intercambiadas para este fin, serán las mismas utilizadas para realizar la firma del mensaje.

¹ https://es.wikipedia.org/wiki/Criptograf%C3%ADa_asim%C3%A9trica

Para asegurar la confidencialidad mientras se transmiten a la SIC los archivos correspondientes a los expedientes de apelaciones, se recomienda utilizar una conexión SSH.

6.1.1.2 Integridad

Se garantizará la integridad de los mensajes intercambiados entre la SIC y los operadores a través del Web Service, implementando el estándar WS-Security haciendo uso del mecanismo de criptografía asimétrica descrito en el punto anterior. Éste utiliza la firma de mensajes para asegurarse que la información no sea modificada, o eliminada durante su transmisión. Cuando se implementa este esquema, se genera una firma digital XML en el contenido del mensaje SOAP, garantizando que, si se realizan cambios no autorizados en los datos del mensaje, la validación de la firma realizada por la otra parte no será satisfactoria. Este mecanismo requiere un intercambio de llaves, donde la SIC entregará su llave pública a los operadores, quienes, a su vez, deberán entregar su llave pública a la SIC, de tal modo que se pueda realizar la validación de la firma en el mensaje. Las llaves intercambiadas para este fin, serán las mismas utilizadas para realizar la encriptación del mensaje.

Los operadores deberán garantizar la integridad de información de los paquetes mediante la utilización de XML Signature. Para asegurar que los datos transmitidos sean íntegros, deben generarse archivos comprimidos con su respectivo hash calculado, nombrado de la misma forma que el archivo que contiene los documentos anexos de la PQR o solicitud de indemnización.

El hash debe ser calculado sobre el archivo comprimido que contenga la información completa necesaria para el estudio de la reclamación. Debe ser usada la función SHA-2 la cual genera una salida de hash de 256 bits.

La Superintendencia de Industria y Comercio debe realizar la comprobación del hash después de la transmisión para asegurar la integridad de la información enviada, igualmente se debe garantizar la información almacenada realizando el cálculo del hash cada vez que vaya a ser usado, realizando un cálculo del mismo sobre el archivo almacenado.

6.1.1.3 Auditoría

En relación con la transmisión de archivos a la SIC, se deben habilitar los logs de auditoría del servidor SSH, con el fin de determinar posibles intentos de autenticación fallidas. También se debe realizar la auditoría de transmisión de archivos por medio del protocolo SCP entre los servidores de los operadores y los servidores de la Superintendencia de Industria y Comercio. Se debe asegurar que se generen logs a nivel de SSH y SCP en los servidores, con el fin de realizar seguimiento a cualquier actividad de autenticación y transmisión de archivos.

En el log se debe registrar como mínimo, lo siguiente:

- Fecha y hora de la transmisión
- Operador que realiza la transmisión
- Resultado de la transacción (Éxito o Fallo)

6.1.1.4 No repudio

El no repudio, se mitigará a nivel de autenticación contra el servicio SSH, por medio de un certificado, asegurando que el único usuario permitido para acceder a los archivos que contienen información sensible con información relacionada a las PQRs sea la SIC.

A nivel de mensajes intercambiados a través del Web Service expuesto por la SIC, se garantizará el no repudio a través de la implementación de WS-Security para firma y encriptación de mensajes como se describió en los puntos anteriores.

6.1.1.5 Control de acceso

El servicio solo podrá ser consumido desde la IP indicada por cada uno de los operadores/proveedores. El mismo servicio está expuesto con protocolo seguro (https).

Para la transferencia de archivos, la SIC entregará una llave pública para certificación de ssh.

6.2 ESPECIFICACIONES TÉCNICAS

Para los efectos del presente anexo son mecanismos de reporte de apelaciones ante la Superintendencia de Industria y Comercio, los que se describen a continuación:

- a) Formulario web.
- b) Servicio Web.

6.2.1 FORMULARIO WEB

El formulario web es un mecanismo a través del cual los operadores pueden remitir los recursos de apelación a la Superintendencia de Industria y Comercio. Dicho mecanismo puede ser accedido utilizando los datos de registro (usuario y contraseña) que fueron remitidos en las comunicaciones de notificación de CUN, haciendo uso de la dirección web <http://serviciolinea.sic.gov.co/cun/>, opción que está disponible en la página web de la Superintendencia de Industria y Comercio, en la sección dedicada a Protección al consumidor.

En caso de no contar con la precitada información, se debe remitir una comunicación formal por escrito a la Dirección de Investigaciones de Protección de Usuarios de Servicios de Comunicaciones de la Superintendencia de Industria y Comercio, suscrita por el representante legal de la respectiva sociedad.

Las especificaciones técnicas del formulario web están basadas en las reglas de validación que se desarrollaron en cada campo del formulario, las cuales hacen referencia a la interacción del operador frente al formulario.

A continuación, se muestra el diseño del formulario web para realizar el proceso de reporte de apelaciones por parte de los operadores.

El primer paso, es el acceso al sistema, en el cual es necesario digitar los datos que fueron remitidos con anterioridad por la SIC. Esta sección adicionalmente tiene la funcionalidad de realizar el proceso de recuperación de contraseña la cual será remitida a la cuenta de correo electrónico asociada a cada operador que haya registrado ante la SIC.

Acceso de Usuarios Registrados

Usuario *

Contraseña *

[Recuperar mi contraseña](#)

Use un usuario y contraseña válido para poder tener acceso a la plataforma.

El CUN (Código Único Numérico) tiene como objetivo ser un número único a nivel nacional para procesar la apelación del usuario y realizar el correspondiente seguimiento de su queja, petición o recurso de reposición del servicio proveído por el proveedor de servicios de telecomunicaciones y operador de servicios postales.

Los siguientes documentos reglamentan y vigilan el Código Único Numérico:

- Resolución 3066 de la CRC de 2011
- Resolución 3038 de la CRC de 2011
- Circular Única Título III
- Anexo Técnico 2013

Links de Interés:

- Consulta de Datos Abiertos
- Manual de usuario
- Consulta de PQRs y Apelaciones

En caso de tener inconvenientes con el ingreso al programa, repórtelo al correo soportecun@sic.gov.co

Imagen 4. Acceso al Sistema CUN Web

La siguiente imagen, corresponde al formulario web desarrollado para que los operadores, realicen el proceso de reporte de apelaciones ante la SIC.

Este formulario está compuesto por dos pasos (ver numeral 6.2.1.1 formulario de reporte), que deben ser diligenciados en su totalidad. La confirmación de la remisión de la información debe ser presentada en una ventana emergente, para lo cual es necesario que en cada computador se habiliten las ventanas emergentes con el fin de poder visualizar la confirmación que constituyen constancia de radicación ante la Superintendencia de Industria y Comercio.

6.2.1.1 Formulario de reporte

CUN - CÓDIGO ÚNICO NUMÉRICO > Reporte Apelaciones > Datos Ciudadano

Cerrar Sesión

1 Datos del Ciudadano
2 Descripción de la Queja
3 Resultado

DATOS DE IDENTIFICACIÓN

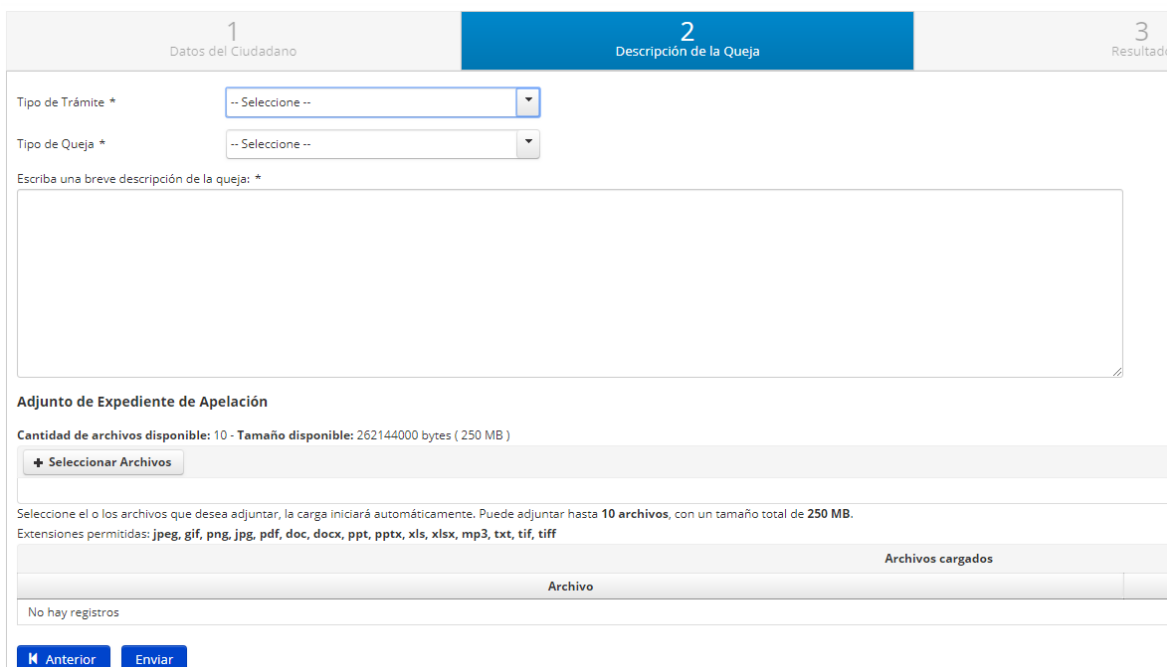
CUN Fecha de Asignación *

Operador *

DATOS DEL USUARIO QUE REALIZÓ EL TRÁMITE ANTE EL OPERADOR
Si cambia algún dato del usuario, será actualizado al finalizar el registro de la Queja.

Tipo de Documento * <input type="text" value="Cédula de Ciudadanía"/>	Número de Documento * <input type="text" value="123456"/> <input type="button" value="Nueva Búsqueda"/>	
Primer Nombre * <input type="text" value="LUIS"/>	Segundo Nombre <input type="text" value="EDGAR"/>	
Primer Apellido * <input type="text" value="RODRIGUEZ"/>	Segundo Apellido <input type="text" value="MARTINEZ"/>	
Dirección * <input type="text" value="AVENIDA CARRACAS NO. 1 - 1"/>		
Teléfono Fijo <input type="text"/>	Teléfono Celular <input type="text"/>	Fax <input type="text"/>
País * <input type="text" value="COLOMBIA"/>	Departamento * <input type="text" value="BOGOTÁ, D.C."/>	Ciudad * <input type="text" value="BOGOTÁ, D.C."/>
Correo electrónico * <input type="text" value="c.smontes@sic.gov.co"/>	<input type="checkbox"/> Persona sin correo electrónico	

IMPORTANTE: La dirección de correo electrónico permite que la SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO tenga un medio de comunicación más directo con usted, por este motivo ingrese un correo válido para recibir comunicaciones de la SIC

Imagen 5. Formulario de Reporte de Expediente de Apelaciones paso 1

Imagen 6. Formulario de Reporte de Expediente de Apelaciones paso 2

A continuación, se especifican las reglas implementadas en el formulario.

6.2.1.2 Validaciones de los campos del reporte de apelaciones

Tabla 7. Validaciones de los Campos de Reporte de Apelaciones

Nombre del campo	Descripción del campo	Tipo	Longitud	Validaciones	Observaciones
IO	Corresponde a los 4 primeros dígitos que identifican al operador.	Entero	4	<ul style="list-style-type: none"> Campo de texto. Campo requerido. Campo protegido contra escritura. 	<ul style="list-style-type: none"> El campo se auto diligencia con los datos del operador en sesión.
AA	Corresponde a los 2 últimos dígitos del año en el que se registra en el sistema de pqr del operador, la primera radicación de la solicitud.	Entero	2	<ul style="list-style-type: none"> Campo de texto. Campo requerido. El campo debe permitir digitar solo números. 	<ul style="list-style-type: none"> La longitud debe ser de 2 caracteres el máximo de escritura. Debe de auto diligenciar y sugerir el año actual de la apelación que se desea ingresar. No debe de permitir un año mayor al actual
CR	Es un número secuencial ascendente de diez dígitos dado	Entero	10	<ul style="list-style-type: none"> Campo de texto. Campo requerido. 	<ul style="list-style-type: none"> La longitud debe ser máximo de 10 dígitos Al momento de digitar el número correspondiente

Nombre del campo	Descripción del campo	Tipo	Longitud	Validaciones	Observaciones
	por el sistema de pqr de cada operador a cada asunto nuevo originado en el año en que se radicó la primera comunicación. Se inicia en 0000000001 el primer día hábil de cada año.			<ul style="list-style-type: none"> El campo debe permitir digitar solo números. 	a este campo se debe generar una alertar al usuario o consumidor en el caso de que existe una apelación con ese número CUN (IO-AA-CR) ya registrado en la SIC, no tiene que dejarlo pasar al siguiente paso del formulario.
Fecha de asignación	Es la fecha de asignación del CUN, esta fecha nace en el momento que nace la PQR.	DateTime		<ul style="list-style-type: none"> Campo requerido 	<ul style="list-style-type: none"> La fecha debe ser la misma fecha de creación del CUN con horas, minutos y segundo que genero el sistema.
Tipo de Documento	Corresponde tipo de documento asociado al usuario que presentó la PQR.	String	2	<ul style="list-style-type: none"> Lista de selección única. Campo requerido. 	<ul style="list-style-type: none"> Las opciones que debe contener son las siguientes: <ul style="list-style-type: none"> NIT => NI CEDULA DE CIUDADANIA => CC CEDULA DE EXTRANJERIA => CE Al momento de seleccionar cualquiera de las diferentes opciones se debe habilitar el campo Número de documento para escritura, de lo contrario todo el campo debe de permanecer de solo lectura.
Número de documento	Corresponde al número de documento asociado al usuario que presentó la PQR.	Entero	11	<ul style="list-style-type: none"> Campo de texto. Campo numérico Campo requerido. 	<ul style="list-style-type: none"> Una vez que se digite la información de este campo, buscará si existe información en la base de datos de la SIC. Si encuentra datos, se deben mostrar la información en los respectivos campos "nombre, dirección, teléfono, email, etc." los cuales quedarán protegidos contra escritura, no obstante, se activará un botón que permitirá al operador tener un formulario alternativo que le permitirá actualizar datos del ciudadano como dirección, teléfono, email.

Nombre del campo	Descripción del campo	Tipo	Longitud	Validaciones	Observaciones
					<ul style="list-style-type: none"> En caso de no encontrar información, se debe habilitar los campos para su respectivo registro.
Primer Nombre	Corresponde al primer nombre asociado al usuario que presentó la PQR.	String	20	<ul style="list-style-type: none"> Campo de texto Campo requerido. Campo alfabético 	<ul style="list-style-type: none"> No se debe permitir escribir espacios al inicio del campo ni al final
Segundo Nombre	Corresponde al segundo nombre asociado al usuario que presentó la PQR.	String	20	<ul style="list-style-type: none"> Campo de texto Campo requerido. Campo alfabético 	<ul style="list-style-type: none"> No se debe permitir escribir espacios al inicio del campo ni al final
Primer Apellido	Corresponde al primer apellido asociado al usuario que presentó la PQR.	String	20	<ul style="list-style-type: none"> Campo de texto Campo requerido. Campo alfabético 	<ul style="list-style-type: none"> No se debe permitir escribir espacios al inicio del campo ni al final
Segundo Apellido	Corresponde al segundo apellido asociado al usuario que presentó la PQR.	String	20	<ul style="list-style-type: none"> Campo de texto Campo requerido. Campo alfabético 	<ul style="list-style-type: none"> No se debe permitir escribir espacios al inicio del campo ni al final
Dirección	Corresponde a la dirección física de notificación asociado al usuario que presentó la PQR.	String	60	<ul style="list-style-type: none"> Campo de texto Campo requerido. Campo alfabético 	<ul style="list-style-type: none"> No se debe permitir escribir espacios al inicio del campo ni al final
Teléfono Fijo	Corresponde número de teléfono fijo asociado al usuario que presentó la PQR.	Entero	12	<ul style="list-style-type: none"> Campo de texto Campo requerido. Campo numérico 	<ul style="list-style-type: none"> No se debe permitir escribir espacios al inicio del campo ni al final
Teléfono Celular	Corresponde al número telefónico celular asociado al usuario que presentó la PQR.	Entero	10	<ul style="list-style-type: none"> Campo de texto Campo requerido. Campo numérico 	<ul style="list-style-type: none"> No se debe permitir escribir espacios al inicio del campo ni al final
Fax	Corresponde al número de fax asociado al usuario que presentó la PQR.	Entero	10	<ul style="list-style-type: none"> Campo de texto Campo requerido. Campo numérico 	<ul style="list-style-type: none"> No se debe permitir escribir espacios al inicio del campo ni al final
País	Corresponde al país asociado al usuario que presentó la PQR.	String	2	<ul style="list-style-type: none"> Campo lista de selección única. 	<ul style="list-style-type: none"> Este campo debe de estar pre diligenciado en la opción Colombia.

Nombre del campo	Descripción del campo	Tipo	Longitud	Validaciones	Observaciones
				<ul style="list-style-type: none"> Campo requerido. 	
Departamento	Corresponde al departamento asociado al usuario que presentó la PQR.	Entero	10	<ul style="list-style-type: none"> Campo lista de selección única. Campo requerido. Campo deshabilitado. 	<ul style="list-style-type: none"> Este campo traerá la lista de departamentos pertenecientes a cada país
Ciudad	Corresponde a la ciudad asociado al usuario que presentó la PQR.	Entero	10	<ul style="list-style-type: none"> Campo lista de selección única. Campo requerido. Campo deshabilitado. 	<ul style="list-style-type: none"> Este campo traerá la lista de ciudades pertenecientes a la llave país y departamento.
Correo electrónico	Corresponde a la dirección de correo electrónico asociado al usuario que presentó la PQR.	String	40	<ul style="list-style-type: none"> Campo texto. Campo requerido. Campo de escritura de correo electrónico. Campo alfanumérico. 	<ul style="list-style-type: none"> Este campo no debe escribir caracteres especiales, solo el carácter del @ debe estar permitido. El campo permitirá cuentas de correo electrónico
Trámite	Corresponde al tipo de servicio que hace referencia a la PQR (TELEFONÍA MÓVIL, INTERNET / OTROS SERVICIOS NO DOMICILIARIOS, TELEFONIA FIJA)	Entero	10	<ul style="list-style-type: none"> Campo lista de selección única. Campo requerido. 	<ul style="list-style-type: none"> Es campo obligatorio
Tipo de PQR y Solicitud de Indemnización	Corresponde al tipo de queja relacionada para los servicios del CUN y asociada a cada PQR o solicitud de indemnización.	Entero	10	<ul style="list-style-type: none"> Campo lista de selección única. Campo requerido. 	La tipología que debe tenerse en cuenta es la prevista en el RPU y en el Título III de la Circular Única, en el caso de Postales.
Descripción de la queja	Descripción de la queja asociada a la PQR.	String	500	<ul style="list-style-type: none"> Campo de texto. Campo requerido. Campo mínimo de 20 caracteres. 	<ul style="list-style-type: none"> Es campo obligatorio
Respuesta Operador	Respuesta que da el operador a la	String	500	<ul style="list-style-type: none"> Campo de texto 	<ul style="list-style-type: none"> Es campo obligatorio

Nombre del campo	Descripción del campo	Tipo	Longitud	Validaciones	Observaciones
	queja asociada en la PQR			<ul style="list-style-type: none"> • Campo requerido • Campo mínimo de 20 caracteres. 	
Observaciones	Campo donde se detalla explícitamente si es requerido o no, actualizar la información del cliente	String	500	<ul style="list-style-type: none"> • Campo de texto • Campo mínimo de 20 caracteres. 	No se debe permitir escribir espacios al inicio del campo ni al final, Se debe detallar que datos del usuario deben actualizarse, ya que el servicio no hará ninguna actualización asociada al usuario de forma automática.
Adjunto	Son cada uno de los archivos que contiene el expediente de apelaciones.	Archivo		<ul style="list-style-type: none"> • Campo requerido. 	<ul style="list-style-type: none"> • Archivos que contiene que conforma el expediente de apelaciones en forma digital, este expediente es cargado por web uno a uno para complementar el trámite. • Es campo obligatorio. • La cantidad máxima de archivos que se pueden adjuntar es de 5 • El tamaño máximo por archivo es de 30mb • La extensión de los diferentes tipos de archivos que se pueden adjuntar son los siguientes: <i>jpeg, gif, png, jpg, pdf, doc, docx, ppt, pptx, xls, xlsx, mp3, txt, tif y tiff.</i>

6.2.2 WEB SERVICE

Este servicio permite realizar a un operador o vigilado la solicitud de radicación de una apelación de una PQR ante la SIC. El servicio recibe los datos del operador, del quejoso y de la apelación y retorna un mensaje de éxito o error con el radicado de la solicitud. Si la solicitud fue recibida exitosamente, se retorna el número de radicado asignado por el sistema de trámites de esta autoridad administrativa. Se aclara que el número recibido como respuesta del WS, corresponde al número de radicación de la solicitud.

Luego de ser registrada la radicación, esta solicitud queda en una lista para ser procesada. Como parte de este proceso el sistema de la SIC descargará desde el operador el archivo de soporte del expediente, para lo cual el operador debe haber configurado su servidor SSH.

Por último, el sistema de la SIC enviará al operador un correo electrónico de notificación del éxito de la radicación, con un PDF adjunto en el que se informan todos los datos de la radicación. Si el proceso de radicación fallase por cualquier motivo, el operador recibirá un correo de notificación del fallo de la radicación.

En los únicos casos en los que el operador no recibirá notificación por correo electrónico serán en aquellos en los que no se encuentre adecuadamente configurada la dirección de correo del operador en la SIC, o en el caso en que el buzón de correo presente fallas.

El Web Service para solicitud de radicación de apelación implementa el estándar de seguridad WS-Security, debe ser consumido mediante un mensaje encriptado y firmado digitalmente, y dará un resultado encriptado y firmado de igual forma. Dado lo anterior, para que se pueda enviar y recibir estos mensajes adecuadamente, se deberá realizar un intercambio de llaves entre la SIC y el operador de la siguiente forma:

- El operador deberá Generar un Certificado de Persona Jurídica Entidad o Empresa, a través de una entidad certificadora de confianza.
- Una vez generado el certificado, se deberá enviar la llave pública correspondiente a la Superintendencia de Industria y Comercio al correo soportecun@sic.gov.co.
- Tan pronto se reciba la llave pública por parte del operador, la SIC enviará su llave pública al correo electrónico desde el que se recibió la llave pública por parte del mismo.

Nota: Si ya se dispone de un certificado de este tipo por parte del operador, no es necesario generar uno nuevo, y se debe enviar la llave pública correspondiente a la SIC.

En las próximas secciones, se describe con más detalle el proceso de interacción entre la SIC y el operador al momento de realizar el consumo del Web Service.

6.2.2.1 Diagrama de Interacción entre Operadores y SIC

La integración por medio de servicios entre sistemas de información requiere la definición del modelo de datos o estructura de datos a ser usada como paquete de transmisión tanto desde la SIC como del operador. Para tal efecto, se ha definido un único esquema de transmisión, de tal manera que la integración de servicios sea transparente.

La solución seleccionada fue por medio de una lógica asíncrona segura de transferencia de archivos. En la siguiente imagen se muestran los pasos relevantes del proceso y los artefactos involucrados.

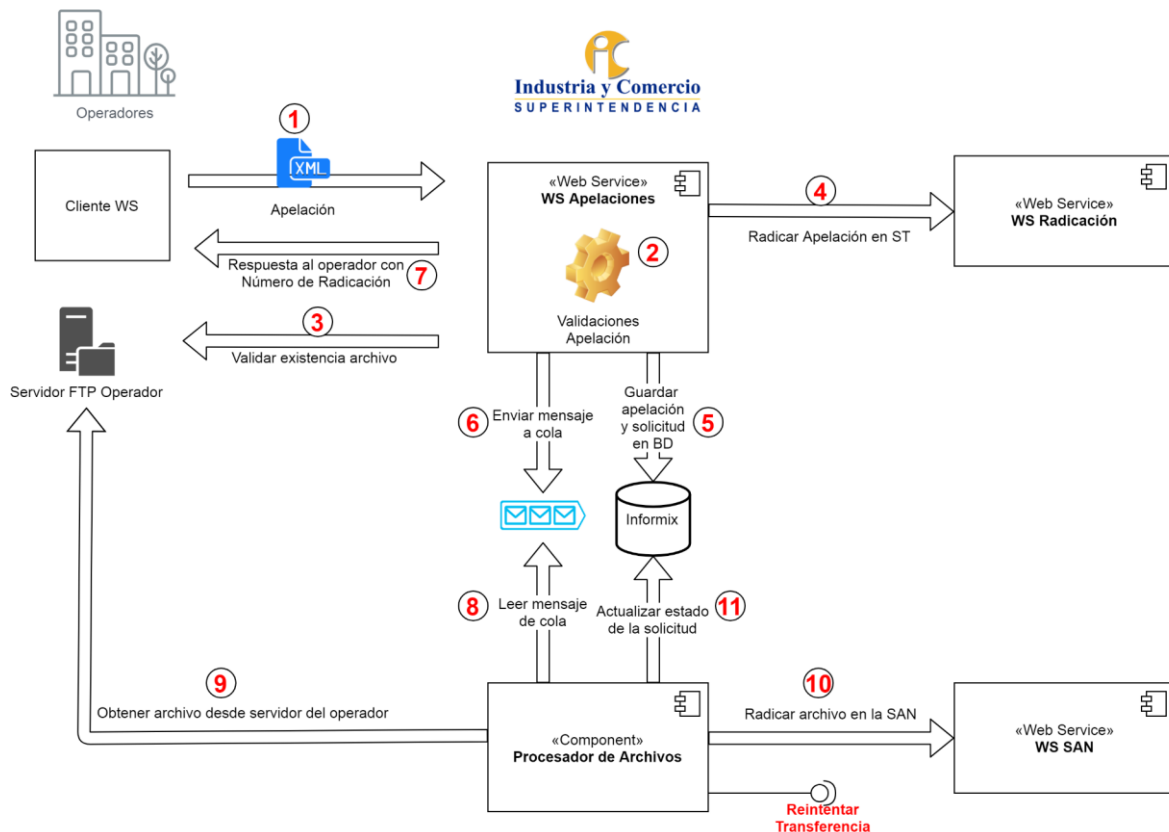


Imagen 7. Proceso diseñado para recepción de documentación de soporte.

A continuación se hace una descripción de los pasos evidenciados en la imagen anterior:

Por parte del operador:

1. El operador genera un paquete de datos que representa las características de estado de la PQR/Apelación y lo envía a la SIC por medio del servicio tecnológico dispuesto para esto. El mensaje generado desde el operador debe estar firmado y encriptado de acuerdo a las políticas de WS-Security, para firma y encriptación definidas por el contrato. Si es decisión del operador no implementar este mecanismo, se ofrece por parte de la SIC una URL para consumo del servicio que no requiere de la implementación de WS-Security. Como respuesta a la invocación del servicio, el operador recibirá por parte de la SIC, un número de radicación de la apelación.

Por parte de la SIC:

2. El servidor se encarga de validar la seguridad del mensaje del paso 1 y recibe el paquete de datos o la "Apelación" para darle trámite. Valida la "Apelación" a nivel de tipos de dato esperados para cada parámetro de entrada.
3. El servicio "WS Apelaciones" verifica que existan los archivos indicados por la apelación. Para esto, se establece una conexión vía SSH hacia el servidor FTP del operador

- mediante autenticación por llave pública y acceso único al servidor remoto a través de reglas de firewall configuradas desde ambos puntos de la conexión.
4. Una vez validados los datos y los archivos de la apelación, se procede a radicar la apelación mediante el servicio “WS Radicación”. El número de radicación obtenido será la respuesta al operador posteriormente.
 5. Los datos de la apelación son registrados en base de datos para fines estadísticos o de reportes internos de la entidad.
 6. Si hay archivos asociados a la apelación, es encolada una tarea para su posterior descarga desde el servidor FTP del operador, conexión y transferencia, que se logra mediante autenticación al servidor SSH por llave pública y acceso al servidor remoto, a través de reglas de firewall configuradas desde ambos puntos de la conexión.
 7. El “WS Apelaciones” responde al operador con el número de radicación mientras de forma asíncrona se ejecutan las operaciones de transferencia del expediente, el cual puede contener uno o más archivos comprimidos en un .zip.
 8. El componente “Procesador de archivos” se encarga de ir tomando tareas de la cola en segundo plano para permitir que se sigan atendiendo apelaciones por el “WS Apelaciones”.
 9. El componente “Procesador de archivos” se encarga de generar una conexión segura hacia el servidor FTP del operador con el fin de lograr la descarga de los archivos de la apelación. La conexión al servidor SSH se logra mediante autenticación por llave pública y acceso al servidor remoto, a través de reglas de firewall configuradas desde ambos puntos de la conexión.
 10. Una vez descargados los archivos, estos son almacenados en las áreas de almacenamiento en red (SAN) de la SIC y son asociados al expediente mediante el número de radicación.
 11. Una vez el proceso de almacenamiento ha sido finalizado, el sistema actualiza en base de datos el estado de la solicitud.
 12. Finalmente, el sistema de la SIC enviará al operador un correo electrónico de notificación del éxito de la radicación, con un PDF adjunto en el que se informa todos los datos de la radicación. Si el proceso de radicación fallase por cualquier motivo el operador recibirá un correo de notificación del fallo de la radicación.

Este proceso se repite continuamente, dado que la tarea de recibir apelaciones puede realizarse en cualquier momento y debido a que obtener los archivos es un proceso que requiere de un tiempo considerable, dependiendo del tamaño de los archivos que se transmiten, es necesario hacer uso de una estrategia de colas que permita manejar una funcionalidad asíncrona, es decir, que mientras se realiza la radicación de solicitudes, también se pueda adelantar la transferencia de archivos, evitando que el operador se quede en espera de una respuesta síncrona.

6.2.2.2 Estructura de Datos de Transmisión

El siguiente esquema define la estructura implementada por la SIC expuesta en internet para que el operador realice el reporte de apelaciones.

Como se mencionó previamente, la SIC ofrece la posibilidad de consumir el servicio implementando el estándar WS-Security para firma y encriptación de los mensajes, o sin implementarlo. La decisión del esquema de consumo se deja al operador.

A continuación, la definición del contrato para consumir el servicio sin implementar WS-Security:

```

<wsdl:definitions xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" xmlns:wsp="http://www.w3.org/ns/ws-policy"
xmlns:wSDL="http://schemas.xmlsoap.org/wsdl/" xmlns:wSaws="http://www.w3.org/2005/08/addressing"
xmlns:tNS="http://solicitudradicacion.ws.cs.mintic.gov.co/"
xmlns:SP="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy"
xmlns:SOAP="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:ns1="http://schemas.xmlsoap.org/soap/http"
name="RadicarSolicitudApelacion" targetNamespace="http://solicitudradicacion.ws.cs.mintic.gov.co/">
  <wsdl:types>
    <xs:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-wssecurity-utility-1.0.xsd" xmlns:wsp="http://www.w3.org/ns/ws-policy"
xmlns:wSDL="http://schemas.xmlsoap.org/wsdl/" xmlns:wSaws="http://www.w3.org/2005/08/addressing"
xmlns:tNS="http://solicitudradicacion.ws.cs.mintic.gov.co/"
xmlns:SP="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy"
xmlns:SOAP="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:ns1="http://schemas.xmlsoap.org/soap/http"
elementFormDefault="unqualified" targetNamespace="http://solicitudradicacion.ws.cs.mintic.gov.co/" version="1.0">
      <xs:element name="radicarSolicitudApelacion" type="tNS:radicarSolicitudApelacion"/>
      <xs:element name="radicarSolicitudApelacionResponse"
type="tNS:radicarSolicitudApelacionResponse"/>
      <xs:complexType name="radicarSolicitudApelacion">
        <xs:sequence>
          <xs:element minOccurs="0" name="integracionCUN"
type="xs:string"/>
        </xs:sequence>
      </xs:complexType>
      <xs:complexType name="radicarSolicitudApelacionResponse">
        <xs:sequence>
          <xs:element minOccurs="0" name="return" type="xs:string"/>
        </xs:sequence>
      </xs:complexType>
    </xs:schema>
  </wsdl:types>
  <wsdl:message name="radicarSolicitudApelacionResponse">
    <wsdl:part element="tNS:radicarSolicitudApelacionResponse" name="parameters"> </wsdl:part>
  </wsdl:message>
  <wsdl:message name="radicarSolicitudApelacion">
    <wsdl:part element="tNS:radicarSolicitudApelacion" name="parameters"> </wsdl:part>
  </wsdl:message>
  <wsdl:portType name="RadicacionSolicitudApelacion">
    <wsdl:operation name="radicarSolicitudApelacion">
      <wsdl:input message="tNS:radicarSolicitudApelacion"
name="radicarSolicitudApelacion"> </wsdl:input>
      <wsdl:output message="tNS:radicarSolicitudApelacionResponse"
name="radicarSolicitudApelacionResponse"> </wsdl:output>
    </wsdl:operation>
  </wsdl:portType>
  <wsdl:binding name="RadicarSolicitudApelacionSoapBinding" type="tNS:RadicacionSolicitudApelacion">
    <soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="radicarSolicitudApelacion">
      <soap:operation soapAction="" style="document"/>
      <wsdl:input name="radicarSolicitudApelacion">
        <soap:body use="literal"/>
      </wsdl:input>
      <wsdl:output name="radicarSolicitudApelacionResponse">
        <soap:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:service name="RadicarSolicitudApelacionNoSec">
    <wsdl:port binding="tNS:RadicarSolicitudApelacionSoapBinding"
name="RadicacionSolicitudApelacionPort">

```

```

      <soap:address
location="http://wscun.sic.gov.co/RadicarCunApelacionWS/RadicarSolicitudApelacionNoSec/RadicarSolicitudApelacionNoSec"/>
      </wsdl:port>
    </wsdl:service>
  </wsdl:definitions>

```

Imagen 8. Estructura de datos para el intercambio de información del CUN – Sin WS-Security

A continuación, la definición del contrato para consumir el servicio implementando WS-Security:

```

<wsdl:definitions xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" xmlns:wsp="http://www.w3.org/ns/ws-policy"
xmlns:wSDL="http://schemas.xmlsoap.org/wsdl/" xmlns:wSaws="http://www.w3.org/2005/08/addressing"
xmlns:tNS="http://solicitudradicacion.ws.cs.mintic.gov.co/"
xmlns:sP="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy"
xmlns:SOAP="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:ns1="http://schemas.xmlsoap.org/soap/http"
name="RadicarSolicitudApelacion" targetNamespace="http://solicitudradicacion.ws.cs.mintic.gov.co/">
  <wsdl:types>
    <xs:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" xmlns:wsp="http://www.w3.org/ns/ws-policy"
xmlns:wSDL="http://schemas.xmlsoap.org/wsdl/" xmlns:wSaws="http://www.w3.org/2005/08/addressing"
xmlns:tNS="http://solicitudradicacion.ws.cs.mintic.gov.co/"
xmlns:sP="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy"
xmlns:SOAP="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:ns1="http://schemas.xmlsoap.org/soap/http"
elementFormDefault="unqualified" targetNamespace="http://solicitudradicacion.ws.cs.mintic.gov.co/" version="1.0">
      <xs:element name="radicarSolicitudApelacion" type="tNS:radicarSolicitudApelacion"/>
      <xs:element name="radicarSolicitudApelacionResponse"
type="tNS:radicarSolicitudApelacionResponse"/>
      <xs:complexType name="radicarSolicitudApelacion">
        <xs:sequence>
          <xs:element minOccurs="0" name="integracionCUN"
type="xs:string"/>
        </xs:sequence>
      </xs:complexType>
      <xs:complexType name="radicarSolicitudApelacionResponse">
        <xs:sequence>
          <xs:element minOccurs="0" name="return" type="xs:string"/>
        </xs:sequence>
      </xs:complexType>
    </xs:schema>
  </wsdl:types>
  <wsdl:message name="radicarSolicitudApelacionResponse">
    <wsdl:part element="tNS:radicarSolicitudApelacionResponse" name="parameters"/>
  </wsdl:message>
  <wsdl:message name="radicarSolicitudApelacion">
    <wsdl:part element="tNS:radicarSolicitudApelacion" name="parameters"/>
  </wsdl:message>
  <wsdl:portType name="RadicacionSolicitudApelacion">
    <wsdl:operation name="radicarSolicitudApelacion">
      <wsdl:input message="tNS:radicarSolicitudApelacion"
name="radicarSolicitudApelacion"/>
      <wsdl:output message="tNS:radicarSolicitudApelacionResponse"
name="radicarSolicitudApelacionResponse"/>
    </wsdl:operation>
  </wsdl:portType>
  <wsdl:binding name="RadicarSolicitudApelacionSoapBinding" type="tNS:RadicacionSolicitudApelacion">
    <wsp:PolicyReference URI="#SecurityServiceSignThenEncryptPolicy"/>
    <soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="radicarSolicitudApelacion">
      <soap:operation soapAction="" style="document"/>
      <wsdl:input name="radicarSolicitudApelacion">
        <soap:body use="literal"/>
      </wsdl:input>

```

```

        <wsdl:output name="radicarSolicitudApelacionResponse">
            <soap:body use="literal"/>
        </wsdl:output>
    </wsdl:operation>
</wsdl:binding>
<wsdl:service name="RadicarSolicitudApelacion">
    <wsdl:port binding="tns:RadicarSolicitudApelacionSoapBinding"
name="RadicacionSolicitudApelacionPort">
        <soap:address
location="http://wscun.sic.gov.co/RadicarCunApelacionWS/RadicarSolicitudApelacion/RadicarSolicitudApelacion"/>
    </wsdl:port>
</wsdl:service>
<wsp:Policy xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy"
wsu:Id="SecurityServiceSignThenEncryptPolicy">
    <wsp:ExactlyOne>
        <wsp:All>
            <sp:AsymmetricBinding
xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
                <wsp:Policy>
                    <sp:AlgorithmSuite>
                        <wsp:Policy>
                            <sp:TripleDes/>
                        </wsp:Policy>
                    </sp:AlgorithmSuite>
                    <sp:Layout>
                        <wsp:Policy>
                            <sp:Lax/>
                        </wsp:Policy>
                    </sp:Layout>
                    <sp:OnlySignEntireHeadersAndBody/>
                </wsp:Policy>
            </sp:AsymmetricBinding>
            <sp:SignedParts
xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
                <sp:Body/>
            </sp:SignedParts>
            <sp:EncryptedParts
xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
                <sp:Body/>
            </sp:EncryptedParts>
            <sp:Wss10 xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
                <wsp:Policy>
                    <sp:MustSupportRefIssuerSerial/>
                </wsp:Policy>
            </sp:Wss10>
        </wsp:All>
    </wsp:ExactlyOne>
</wsp:Policy>
</wsdl:definitions>

```

Estructura de datos para el intercambio de información del CUN – Con WS-Security

Por último, se detalla la estructura interna del elemento 'IntegracionCUN' resaltado en la imagen anterior del contrato de servicio.

Elemento XML	Tipo XML	Descripción
<IntegracionCUN />	IntegracionCUN	Elemento que encapsula el objeto único de transporte utilizado por el servicio.
<tipoTramiteSic />	TipoTramiteSIC	Contiene información que identifica el tipo de trámite que se está realizando. Los posibles valores para este campo son definidos por la SIC y establecidos en el Anexo Técnico provisto para tal fin. <ul style="list-style-type: none"> • codTipoTramiteSIC • nomTipoTramiteSIC
<codTipoTramiteSic />	String	Código que identifica el trámite que se está realizando, de acuerdo al Anexo Técnico. Obligatorio Longitud: 2 caracteres
<nomTipoTramiteSic />	String	Nombre del trámite que se está realizando de acuerdo al Anexo Técnico. Opcional Longitud: 50 caracteres
<tipoQueja />	TipoQueja	Contiene información que identifica el tipo de queja del PQR que se apeló. Los posibles valores para este campo son definidos por la SIC y establecidos en el Anexo Técnico provisto para tal fin.
<codtipoQuejaSic />	String	Código que clasifica la queja del PQR, de acuerdo al Anexo Técnico. Obligatorio Longitud: 10 dígitos
<nomtipoQuejaSic />	String	Corresponde al Nombre del tipo de queja del PQR de acuerdo al Anexo Técnico. Opcional Longitud: 255 dígitos
<numRadicadoCun />	NumRadicadoCun	Corresponde al número de radicación de la apelación ante la SIC <ul style="list-style-type: none"> • anoRadicacionCun • numRadicacionCun • controlRadicadoCun • consecutivoRadicacion • fechaRadicacion
<anoRadicacionCun />	Entero	Corresponde al Año de Radicación del CUN ante la SIC Obligatorio Longitud: 2 dígitos
<numRadicacionCun />	Entero	Corresponde al número de Radicación del CUN ante la SIC Longitud: 10 dígitos En todas las respuestas debe recibirse este parámetro de forma obligatoria.
<controlRadicadoCun />	Entero	Corresponde al control de Radicación del CUN ante la SIC Longitud: 2 dígitos

		En todas las respuestas debe recibirse este parámetro de forma obligatoria.
<consecutivoRadicacion />	Entero	Corresponde al consecutivo de Radicación del CUN ante la SIC Longitud: 10 dígitos En todas las respuestas debe recibirse este parámetro de forma obligatoria.
<fechaRadicacion />	Fecha	Corresponde a la fecha de radicación de la apelación ante la SIC y debe tener el siguiente Formato AAAA-MM-DDTHH:MM:SS donde T es cualquier carácter de separación. Obligatorio Longitud: 19 dígitos
<numRadicadoCunStr />	String	Corresponde al formado del radicado producto de la unión del año y número de radicado de la apelación ante la SIC; ejemplo: 19-2439 Obligatorio
<codigoUnicoNumerico />	CodigoUnicoNumerico	El código único numérico CUN que identifica la PQR está conformado por tres partes: <ul style="list-style-type: none"> • Identificador del Vigilado • Año de Radicación • Consecutivo de Radicación CUN
<identificadorOperador />	Entero	Identificador único del vigilado del CUN: Longitud: 4 dígitos Obligatorio
<anoRadicacionCun />	Entero	Año de Radicación del CUN Obligatorio Longitud: 2 dígitos
<ConsecutivoRadCun />	Entero	Consecutivo de Radicación CUN Obligatorio Longitud: 10 dígitos
<codEstadoCUN />	String	Código que indica el estado en que se encuentra el PQR de acuerdo a la tabla de valores posibles indicada por la SIC en el Anexo Técnico. Obligatorio Longitud: 10 caracteres
<descripcionQueja />	String	Texto con la descripción de la queja presentada por el usuario. Obligatorio Longitud: 255 caracteres
<fechaAsignacion />	Fecha	Corresponde a la fecha de radicación de la PQR y debe tener el siguiente Formato AAAA-MM-DDTHH:MM:SS donde T es cualquier carácter de separación. Obligatorio
<operador />	Operador	Contiene la información de identificación y validación del operador o vigilado: <ul style="list-style-type: none"> • tipoDocumento • numeroDocumento

		<ul style="list-style-type: none"> • nombreOperador • usuario • password
<tipoDocumento />	String	<p>Hace referencia al tipo de documento asociado al número de identificación de la razón social del operador. Los posibles valores son los determinados por la SIC en el Anexo, sin embargo, todos los operadores manejan como valor por defecto el NIT, por lo que este campo debe ir diligenciado como "NI".</p> <p>Obligatorio Longitud: 2 caracteres</p>
<numeroDocumento />	String	<p>Corresponde al valor del NIT sin dígito de chequeo.</p> <p>Obligatorio Longitud: 10 caracteres</p>
<nombreOperador />	String	<p>Corresponde al nombre de la empresa que provee el servicio (vigilada por la Superintendencia de Industria y Comercio) y ante la cual se presentó la PQR y la apelación.</p> <p>Obligatorio Longitud 200 caracteres.</p>
<usuario />	String	<p>Usuario asignado por la SIC al vigilado para el sistema CUN-SIC</p> <p>Obligatorio Longitud: 8 caracteres</p>
<password />	String	<p>Clave asignada por la SIC al vigilado para el sistema CUN-SIC para autenticarse ante el servicio</p> <p>Obligatorio Longitud: 50 caracteres</p>
<nomPersona />	NomPersona	<p>Corresponde a la información de los nombres y apellidos del usuario, cuando la respuesta de la consulta es para una persona natural.</p>
<primerNombre />	String	<p>Corresponde al Primer nombre del usuario</p> <p>Obligatorio Longitud: 50 caracteres</p>
<segundoNombre />	String	<p>Corresponde al Segundo nombre del usuario,</p> <p>Opcional Longitud: 50 caracteres</p>
<primerApellido />	String	<p>Corresponde al Primer apellido del usuario</p> <p>Obligatorio Longitud: 50 caracteres</p>
<segundoApellido />	String	<p>Corresponde al Segundo apellido del usuario,</p> <p>Obligatorio Longitud: 50 caracteres</p>
<razonSocial />	String	<p>Nombre de la entidad o empresa quejosa Si es una persona jurídica este campo es obligatorio.</p> <p>Longitud: 200 caracteres</p>
<tipoldNacionalPersona />		<p>Corresponde a la información del código y nombre del tipo de documento del usuario, según sea el caso, persona natural o persona jurídica.</p>

<codTipoldNacionalPersona />	String	<p>Contiene el tipo de identificación del usuario que presentó la PQR, teniendo en cuenta las siguientes convenciones:</p> <table border="1" data-bbox="786 317 1393 554"> <thead> <tr> <th>Código</th> <th>Nombre</th> </tr> </thead> <tbody> <tr> <td>CC</td> <td>Cedula de ciudadanía</td> </tr> <tr> <td>CE</td> <td>Cedula de extranjería</td> </tr> <tr> <td>NI</td> <td>Número de Identificación Tributaria (NIT)</td> </tr> <tr> <td>PP</td> <td>Pasaporte</td> </tr> <tr> <td>TI</td> <td>Tarjeta de identidad</td> </tr> <tr> <td>TM1</td> <td>Tarjeta Militar</td> </tr> </tbody> </table> <p>Obligatorio Longitud: 2 caracteres</p> <p>Los valores posibles para este campo se toman del Anexo Técnico suministrado por la SIC.</p>	Código	Nombre	CC	Cedula de ciudadanía	CE	Cedula de extranjería	NI	Número de Identificación Tributaria (NIT)	PP	Pasaporte	TI	Tarjeta de identidad	TM1	Tarjeta Militar
Código	Nombre															
CC	Cedula de ciudadanía															
CE	Cedula de extranjería															
NI	Número de Identificación Tributaria (NIT)															
PP	Pasaporte															
TI	Tarjeta de identidad															
TM1	Tarjeta Militar															
<nomTipoidentificacionNacionalPersona />	String	<p>Corresponde al nombre del tipo de documento asociado al código de tipo de documento</p> <table border="1" data-bbox="786 858 1382 1129"> <thead> <tr> <th>Código</th> <th>Nombre</th> </tr> </thead> <tbody> <tr> <td>CC</td> <td>Cedula de ciudadanía</td> </tr> <tr> <td>CE</td> <td>Cedula de extranjería</td> </tr> <tr> <td>NI</td> <td>Número de Identificación Tributaria (NIT)</td> </tr> <tr> <td>PP</td> <td>Pasaporte</td> </tr> <tr> <td>TI</td> <td>Tarjeta de identidad</td> </tr> <tr> <td>TM1</td> <td>Tarjeta Militar</td> </tr> </tbody> </table> <p>Opcional Longitud: 50 caracteres</p> <p>Los valores posibles para este campo se toman del Anexo Técnico suministrado por la SIC.</p>	Código	Nombre	CC	Cedula de ciudadanía	CE	Cedula de extranjería	NI	Número de Identificación Tributaria (NIT)	PP	Pasaporte	TI	Tarjeta de identidad	TM1	Tarjeta Militar
Código	Nombre															
CC	Cedula de ciudadanía															
CE	Cedula de extranjería															
NI	Número de Identificación Tributaria (NIT)															
PP	Pasaporte															
TI	Tarjeta de identidad															
TM1	Tarjeta Militar															
<numeroidentificacion><numero></numero></numeroidentificacion>	String	<p>Número de documento del usuario. Alfanumérico Obligatorio Longitud: 20 caracteres</p>														
<nomenclaturaDireccion />	String	<p>Dirección de notificación o domicilio del usuario Obligatorio Longitud: 200 caracteres</p>														
<codIdentificacionPaisAlf2 />	String	<p>Código del país del domicilio o dirección de notificación del usuario. En el caso de Colombia es CO. Obligatorio Longitud: 4 caracteres</p>														
<nomDepartamento />	String	<p>Corresponde al nombre del departamento del domicilio o dirección de notificación del usuario. Obligatorio Longitud: 50 caracteres</p>														

<codDepartamentoAlf2 />	String	Código del departamento del domicilio o dirección de notificación del usuario. Este código corresponde al definido por Divipola del DANE. Obligatorio Longitud: 4 caracteres
<nomMunicipio />	String	Nombre del municipio del domicilio o dirección de notificación del usuario. Obligatorio Longitud: 200 caracteres
<codMunicipioAlf5 />	String	Código del municipio del domicilio o dirección de notificación del usuario. Este código corresponde al definido por Divipola del DANE. Obligatorio Longitud: 2 caracteres
<numTelefonoUbicacion />	String	Número de teléfono fijo de contacto del usuario. Opcional Longitud: 15 caracteres
<fax />	String	Número de fax del usuario. Opcional Longitud: 15 caracteres
<numeroCelularPersona />	String	Número de teléfono celular del usuario. Obligatorio (según el tipo de queja asociado) Longitud: 15 caracteres
<direccionCorreoElectronico />	String	Dirección de correo electrónico valido del usuario, ya que, a partir de este valor, llegara una notificación indicando el éxito del proceso de radicación. Obligatorio Longitud: 100 caracteres
<archivoAdjunto />		Elemento que contiene la información asociada al expediente asociado a la radicación de la apelación. <ul style="list-style-type: none"> • urlArchivoAdjunto • nomArchivoAdjunto
<urlArchivoAdjunto />	String	Dirección (URI) de la ubicación del archivo en el servidor remoto del Operador. Obligatorio Longitud: 300 caracteres
<nomArchivoAdjunto />	String	Nombre del archivo en formato ZIP que contiene todos los archivos soporte del expediente. Obligatorio Longitud: 100 caracteres
<mensajeServicio />	MensajeServicio	Corresponde al elemento que encapsula el mensaje retornado por el servicio, se compone de los siguientes elementos: <ul style="list-style-type: none"> • CodigoError • Descripcion

<CodigoError />	String	Código de error del servicio. Para ver el listado completo de códigos de error, por favor remitirse al apartado puntual dentro de este mismo documento. Obligatorio Longitud: 4
<Descripcion />	String	Descripción del error por parte del servicio. Para ver el listado completo de códigos de error y sus descripciones, por favor remitirse al apartado puntual dentro de este mismo documento. Obligatorio Longitud: 2048
<respuestaOperador />	String	Corresponde a la respuesta del operador frente a la pqr presentada por el usuario Obligatorio Longitud: 1000 caracteres
<observaciones />	String	Corresponde a las observaciones adicionales del operador frente al recurso de apelación presentado. Por ejemplo, la solicitud explícita de la actualización de datos del usuario. Obligatorio Longitud: 500 caracteres
<timestamp />	Marca de tiempo	Marca de tiempo en formato AAAA-MM-DDTHH:MM:SS donde T es cualquier carácter de separación. Esta fecha y hora corresponden a la fecha en que el vigilado envía la solicitud de registro de radicación ante la SIC, a través del servicio WEB. Esta hora debe estar sincronizada con la hora legal colombiana. Obligatorio

A continuación, un ejemplo de una trama XML de respuesta completa, resaltando el **número de radicación**:

```

<integracionCUN xmlns="http://schemas.datacontract.org/2004/07/Sic">
  <tipoTramiteSic>
    <codTipoTramiteSic>383</codTipoTramiteSic>
    <nomTipoTramiteSic>TELEFONIA_FIJA</nomTipoTramiteSic>
  </tipoTramiteSic>
  <tipoQueja>
    <codtipoQuejaSic>57</codtipoQuejaSic>
    <nomtipoQuejaSic>EQUIPOS TERMINALES</nomtipoQuejaSic>
  </tipoQueja>
  <numRadicadoCun>
    <anoRadicacionCun>18</anoRadicacionCun>
    <numRadicacionCun>194279</numRadicacionCun>
    <controlRadicadoCun> </controlRadicadoCun>
    <consecutivoRadicacion>0</consecutivoRadicacion>
    <fechaRadicacion>2019-08-09T16:33:28.000-05:00</fechaRadicacion>
  </numRadicadoCun>
  <numRadicadoCunStr>18-194279</numRadicadoCunStr>
  <codigoUnicoNumerico>
    <identificadorOperador>7231</identificadorOperador>
    <anoRadicacionCun>17</anoRadicacionCun>
    <ConsecutivoRadCun>112176</ConsecutivoRadCun>
  </codigoUnicoNumerico>

```

```

<codEstadoCUN>2</codEstadoCUN>
<descripcionQueja>Descripción: Esta es una solicitud de prueba, por favor ignorarla.</descripcionQueja>
<fechaAsignacion>2018-02-21T19:46:00Z</fechaAsignacion>
<operador>
  <tipoDocumento>NI</tipoDocumento>
  <numeroDocumento>1070587102</numeroDocumento>
  <nombreOperador>Operador Prueba SIC</nombreOperador>
  <usuario>OPER7102</usuario>
  <password>12345678</password>
</operador>
<nomPersona>
  <primerApellido>AP1 TEST</primerApellido>
  <segundoApellido xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:nil="true"/>
  <primerNombre>NOM1 TEST</primerNombre>
  <segundoNombre xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:nil="true"/>
</nomPersona>
<razonSocial>Empresa prueba migracion WS</razonSocial>
<tipoldNacionalPersona>
  <codTipoldNacionalPersona>NI</codTipoldNacionalPersona>
  <nomTipoldNacionalPersona>NIT</nomTipoldNacionalPersona>
</tipoldNacionalPersona>
<numeroIdentificacion>
  <numero>11112222</numero>
</numeroIdentificacion>
<nomenclaturaDireccion>CL 9 SUR 13 13 PI 2</nomenclaturaDireccion>
<codIdentificacionPaisAlf2>CO</codIdentificacionPaisAlf2>
<nomDepartamento>CUNDINAMARCA</nomDepartamento>
<codDepartamentoAlf2>25</codDepartamentoAlf2>
<nomMunicipio>SOACHA</nomMunicipio>
<codMunicipioAlf5>25754</codMunicipioAlf5>
<numTelefonoUbicacion>123654</numTelefonoUbicacion>
<fax></fax>
<numeroCelularPersona></numeroCelularPersona>
<direccionCorreoElectronico>abc@sic.gov.co</direccionCorreoElectronico>
<archivoAdjunto>
  <urlArchivoAdjunto>C:\Users\BvSsh_VirtualUsers\pruebas.zip</urlArchivoAdjunto>
  <nomArchivoAdjunto>pruebas.zip</nomArchivoAdjunto>
</archivoAdjunto>
<mensajeServicio>
  <CodigoError>210</CodigoError>
  <Descripcion>OK-Éxito</Descripcion>
</mensajeServicio>
<secuenciaEvento>0</secuenciaEvento>
<solicitud>454</solicitud>
<respuestaOperador>Esta es la respuesta del operador</respuestaOperador>
<observaciones>Estas son mis observaciones</observaciones>
<timestamp>2019-08-09T16:30:13.685443-05:00</timestamp>
</integracionCUN>

```

Estructura de datos para el intercambio de información del CUN – Response

6.2.2.3 Tipología de Mensajes y Errores

Con el fin de que el sistema pueda cumplir con los requerimientos no funcionales de seguridad, registro y bitácora de sucesos para diagnóstico y calidad, se hace necesario implementar un manejo estructurado de errores que sea informado, registrable y permita a las partes integradas (SIC, Operador, Usuario) poder evidenciar los datos ante las posibles incidencias.

Teniendo en cuenta esto, se ha dispuesto de un espacio dentro del objeto de intercambio de información entre el operador y la SIC.

El tipo de dato “MensajeServicio” representa un conjunto de datos de control de flujo de información que permitirá identificar si existió algún problema con la ejecución de los métodos, si hubo algún error y, adicionalmente, establecer una marca de tiempo para identificar la historia de los datos transmitidos.

Los detalles de este dato son los siguientes:

- **CodigoError:** Código de identificación del error del operador o de la SIC según sea el caso.
- **Descripción:** Descripción textual del error.
- **Opcional:** Cadena con datos adicionales que describan el error.
- **TimeStamp:** Marca de tiempo en formato de fecha larga que incluye la hora, minutos y segundos.

La tipología de código de errores es la siguiente:

Tabla 8. Tipología de Código Errores

ERROR/MENSAJE	CAPA	NÚMERO
1 Error	1 Acceso a Datos	0 - 9
	2 Aplicación	0 - 9
2 Mensaje	1 OK	0
	2 Diagnóstico	0 - 9

Las anteriores tipologías incluyen manejo de errores y mensajes, que permitirán que la parte que recibe una respuesta pueda tener la información necesaria para tomar medidas pertinentes en caso de un error.

A continuación, se muestra el listado del uso de la codificación de errores:

Tabla 9. Listado del uso de la codificación de errores

CODIGO DE ERROR	DESCRIPCIÓN
210	OK – Éxito
1001	Mensaje de error con la comunicación del WEB Service interno del sistema
1002	Error Autenticación por credenciales inválidas
1003	Error número CUN se encuentra en otra solicitud
1004	Error interno del sistema
1005	Error Validar datos de entrada
1006	Error Actualizar datos del quejoso
1007	Error Transferencia de archivo
1008	Error Validar archivo.ZIP
1009	Error SMTP
1010	Error Enviar notificación

1011	Error Ejecución de la aplicación
1012	Error Escribir en la SAN
1013	Error Convertir el PDF
1014	Error Desempaquetar archivo.ZIP
1015	Error Al renombrar el archivo
1016	Mensaje para informar error en la radicación

Todo objeto de intercambio debe estar acompañado por el elemento “MensajeServicio” como se ha visto en el esquema de transmisión. Un ejemplo de éste sería:

```

<MensajeServicio>
<CodigoError>121</CodigoError>
<Descripción>Error de procesamiento de datos en la lógica de negocios</Descripción>
<Opcional>Exception: ArithmeticException Handler: System.DivideByZeroException: Attempted to divide by zero.
  at ExceptionTestClass.Main()</Opcional>
<TimeStamp>2011-06-09 23:53:40</TimeStamp>
</MensajeServicio>

```

Imagen 9. Ejemplo Esquema de Transmisión

Nótese que los dos últimos dígitos del mensaje de error se han dejado abiertos para manejo interno de los sistemas, esto, debido a que no se conocen los detalles internos de implementación de las partes y las tecnologías usadas en los desarrollos particulares para la construcción de los componentes de servicio e integración.

6.2.2.4. Eventuales Fallas del Sistema: Pueden presentarse fallas en la solicitud y/o inicio del consumo del servicio o en el proceso de transferencia de datos. Sin embargo, la plataforma web service está diseñada para detectar en cuál de los extremos se presenta la falla y, en caso que la falla sea atribuible al sistema de la SIC, al operador le corresponde: (i) **reportar el suceso de inmediato** al correo electrónico soportecun@sic.gov.co, en el que indique en qué consistió de la falla y; (ii) deberá guardar constancia de ello, a fin de evaluar la procedencia o no de la suspensión del término de radicación del(los) recurso(s) de apelación.

7 CONFIGURACIÓN SERVIDOR DE ARCHIVOS EN LINUX

En esta sección se detallan los aspectos requeridos para la instalación del servidor de archivos en ambiente Linux.

7.1 REQUERIMIENTOS DE HARDWARE Y SOFTWARE

A continuación, se detallan los requisitos de hardware y de software del servidor de archivos.

7.1.1 HARDWARE

Tabla 10. Hardware recomendado servidor de archivos

Servidor	Hardware
Sistema de Archivos	<p><i>Características físicas</i></p> <p>Plataforma de 64 Bits Procesador a 2.0 GHz o más, dual core o superior 4 GB memoria 1TB de almacenamiento (esto es dependiente de la cantidad de archivos almacenados)</p> <p><i>Características de red</i> Requiere de IP pública</p>

7.1.2 SOFTWARE

Tabla 11. Software base requerido ambiente Linux

Servidor	Software Base Requerido
Sistema de Archivos	<p><i>Sistema operativo basado en distribuciones:</i> Red Hat Enterprise Linux 5 o superior² CentOS 5 o superior³ Debian 6 o superior⁴</p> <p><i>La instalación base del sistema operativo debe tener como mínimo:</i> Glibc⁵, es una librería base para C en Linux. Libpcap⁶, es una librería utilizada para la captura de paquetes. Normalmente esta librería se encuentra instalada por defecto. IPtables, es un firewall que permite definir políticas de filtrado del tráfico que circula por la red⁷ SSH (Secure Shell), es un programa que permite acceder a la aplicación de forma remota utilizando un protocolo seguro de comunicación.⁸</p>

7.1.3 COSTOS APROXIMADOS

Tabla 12. Costos aproximados componente de Hardware	Características	Valor
Servidor de Aplicaciones	Plataforma de 64 Bits Procesador: Intel Xeon E-2224 3.5G, 8M cache,	\$3.050.000 COP (Precio de referencia ⁹)

² <http://co.redhat.com/>

³ <http://www.centos.org>

⁴ <http://www.debian.org/index.es.html>

⁵ <http://es.wikipedia.org/wiki/Glibc>

⁶ <http://sourceforge.net/projects/libpcap/>

⁷ <http://es.wikipedia.org/wiki/Netfilter/iptables>

⁸ <http://es.wikipedia.org/wiki/Ssh>

⁹ <https://www.dell.com/co/empresas/p/poweredge-t40/pd>

<i>Tabla 12. Costos aproximados</i> Componente de Hardware	Características	Valor
	Memoria RAM: 8GB 2666MT/s DDR4 ECC UDIMM Discos Duro: 1TB 7.2K RPM SATA	
Componente de Software	Características	Valor
Sistema Operativo Red Hat	Licencia Red Hat Enterprise Linux (rhel) 8	Desde \$179 USD Menos de \$700.000 COP (Precio de referencia ¹⁰)
Glibc:	Software Libre Librería base para C en Linux.	\$0
Libpcap:	Software Libre Librería utilizada para la captura de paquetes. (Normalmente esta librería se encuentra instalada por defecto).	\$0
IPtables:	Software Libre Firewall que permite definir políticas de filtrado del tráfico que circula por la red	\$0
SSH (Secure Shell):	Software Libre Programa que permite acceder a la aplicación de forma remota utilizando un protocolo seguro de comunicación	\$0
Total inversión (valor aproximado)		\$3.700.000

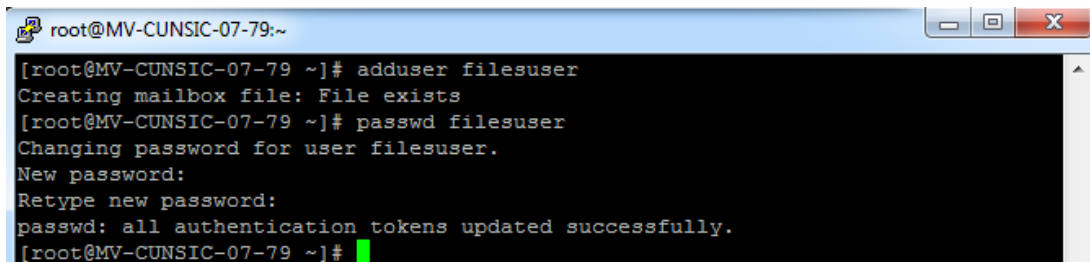
7.2 INSTALACIÓN Y CONFIGURACIÓN DE SSH

Mediante ssh y particularmente con scp se realizará la transferencia de los archivos soporte de las PQR al servidor de la SIC, de tal manera que se utilicen certificados digitales para la autenticación con el sistema, para permitir esto debe realizar los siguientes pasos:

1. Debe crear un usuario específico para la transferencia de archivos hacia la SIC y colocar una contraseña. Para ello debe ejecutar los siguientes comandos en el servidor, indicando que para el ejemplo se está creando el usuario filesuser:

```
adduser filesuser
passwd filesuser
```

¹⁰ <https://www.redhat.com/en/store/linux-platforms>



```

root@MV-CUNSI-07-79:~# adduser filesuser
Creating mailbox file: File exists
[root@MV-CUNSI-07-79 ~]# passwd filesuser
Changing password for user filesuser.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@MV-CUNSI-07-79 ~]#
  
```

Imagen 10. Creación de usuario para transferencia en Linux

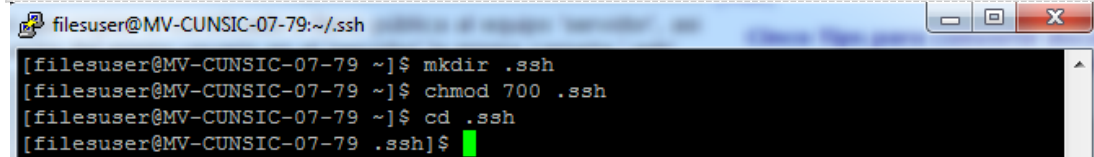
Nota: No se recomienda que la transferencia se haga con el usuario root ya que tendría acceso al sistema operativo
 Tenga en cuenta que todos los archivos deben ser publicados en una ruta vinculada con éste usuario.

- Posteriormente debe ingresar con el usuario creado en el paso anterior, ubicarse en la carpeta home y crear la carpeta `.ssh` con los permisos adecuados, es indispensable que los permisos de ésta carpeta sean únicamente para el usuario creado, ya que de otra manera no funcionará adecuadamente la conexión ssh.

Para realizar la actividad indicada debe ejecutar los siguientes comandos:

```

mkdir .ssh
chmod 700 .ssh
cd .ssh
  
```



```

filesuser@MV-CUNSI-07-79:~/ssh
[filesuser@MV-CUNSI-07-79 ~]$ mkdir .ssh
[filesuser@MV-CUNSI-07-79 ~]$ chmod 700 .ssh
[filesuser@MV-CUNSI-07-79 ~]$ cd .ssh
[filesuser@MV-CUNSI-07-79 .ssh]$
  
```

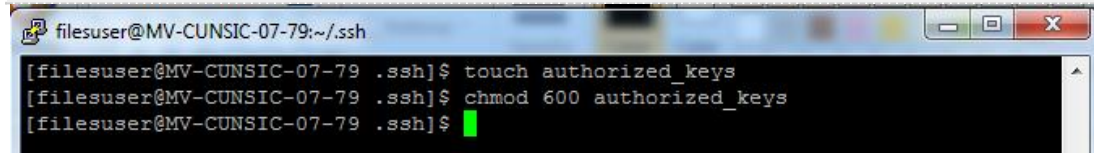
Imagen 11. Creación de directorio `.ssh` en Linux

- Adicionalmente debe crear el archivo `authorized_keys`, el cual contiene las llaves públicas permitidas para el acceso desde un cliente externo hacia el servidor, es indispensable que los permisos del archivo sean únicamente para el usuario creado, ya que de otra manera no funcionará adecuadamente la conexión ssh.

Para realizar la actividad indicada debe ejecutar los siguientes comandos:

```

touch authorized_keys
chmod 600 authorized_keys
  
```



```

filesuser@MV-CUNSI-07-79:~/ssh
[filesuser@MV-CUNSI-07-79 .ssh]$ touch authorized_keys
[filesuser@MV-CUNSI-07-79 .ssh]$ chmod 600 authorized_keys
[filesuser@MV-CUNSI-07-79 .ssh]$
  
```

Imagen 12. Creación de archivo de llaves públicas en Linux

4. Debe agregar la llave pública entregada por la SIC al archivo creado en el paso anterior, para el ejemplo la llave entregada por la SIC corresponde a id_rsa.pub. El archivo debe ser descargado al servidor en la cuenta del usuario creado en el paso 1.

Para realizar la actividad indicada debe ejecutar el siguiente comando:

```
cat ../id_rsa.pub >> authorized_keys
```



Imagen 13. Adición de llave pública de SIC en Linux

5. Para verificar la adecuada adición de la llave, observe el contenido del archivo authorized_keys y deberá encontrar el contenido del archivo de la llave pública entregada por la SIC.

Para realizar la actividad indicada debe ejecutar el siguiente comando:

```
cat authorized_keys
```

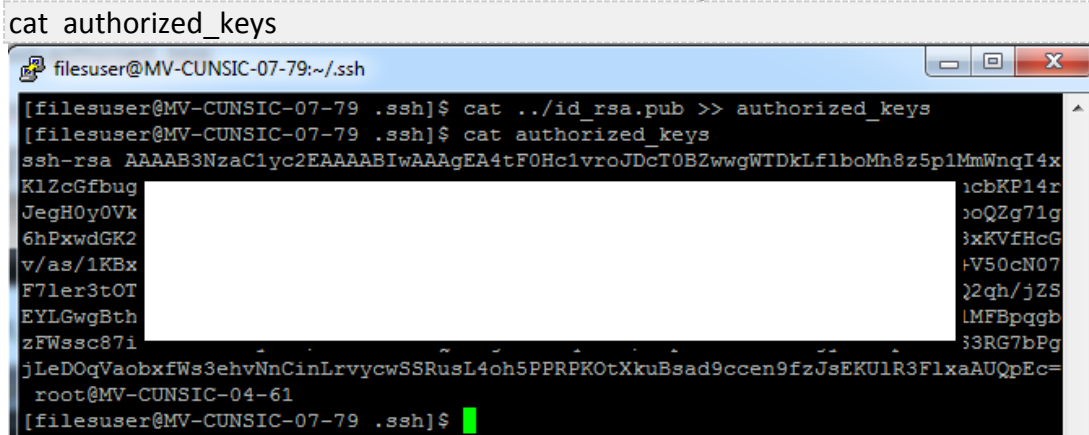


Imagen 14. Verificar llave pública de SIC en Linux

6. Para verificar la adecuada configuración de la llave pública debe comunicarse con la SIC, solicitando realizar una prueba en la cual se debe asegurar que tenga acceso a la cuenta utilizando certificados digitales y no una contraseña específica. Para ello debe informar a la SIC el usuario creado en el paso 1 únicamente, no debe informar la contraseña asignada.

8 CONFIGURACIÓN SERVIDOR DE ARCHIVOS EN WINDOWS

En esta sección se detallan los aspectos requeridos para la instalación del servidor de archivos en ambiente Windows.

8.1 REQUERIMIENTOS DE HARDWARE Y SOFTWARE

A continuación, se detallan los requisitos de hardware y de software del servidor de archivos.

8.1.1 HARDWARE

Tabla 13. Hardware recomendado servidor de archivos

Servidor	Hardware
Sistema de Archivos	<p><i>Características físicas mínimas</i></p> <p>Plataforma de 64 Bits Procesador a 2.0 GHz o más, dual core o superior 4 GB memoria 500GB de almacenamiento (esto es dependiente de la cantidad de archivos almacenados)</p> <p><i>Características de red</i> Requiere de IP pública</p>

8.1.2 SOFTWARE

Tabla 14. Software base requerido ambiente Windows

Servidor	Software Base Requerido
Sistema de Archivos	Sistema Operativo Windows Server 2003, 2008 R2 Standard o superior

8.1.3 COSTOS APROXIMADOS

Tabla 15. Costos aproximados

Componente de Hardware	Características	Valor
Servidor de Aplicaciones	Plataforma de 64 Bits Procesador: Intel Xeon E3-1225 v5 3.3G, 8M cache, Memoria RAM: 8GB 2666MT/s DDR4 ECC UDIMM Discos Duro: 1TB 7.2K RPM SATA 6Gbps	Menos de \$3.000.000 COP (Precio de referencia ¹¹)
Componente de Software	Características	Valor
Sistema Operativo Windows Server 2012	Licencia Windows Server 2012	Desde \$1.000.000 COP (Precio de referencia ¹²)
Bitvise SSH Server	Programa bajo Licencia Estándar tipo Site License. Permite acceder a la aplicación de forma remota utilizando un protocolo seguro de comunicación. Para más información consulte: https://www.bitvise.com/large-scale#site	US\$10

¹¹ <https://www.dell.com/co/empresas/p/poweredge-t30/pd>

¹² <https://lasus.com.co/sistemas-operativos/1982-windows-server-2012-r2-foundation-rok-1cpu-multilang.html>

Componente de Hardware	Características	Valor
Sha256sum	Software Libre Permite generar el hash SHA256 de cualquier archivo por línea de comandos	\$0
Winpcap	Software Libre Librerías base para el acceso de los paquetes en la tarjeta de red	\$0
Python	Software Libre Librería del lenguaje de programación interpretado Python	\$0
Msvcr	Software Libre Librerías de ejecución de C de Microsoft	\$0
Pcap	Software Libre Es un módulo que extiende Python para hacer uso de la librería winpcap	\$0
Total Inversión (valor aproximado)		\$4.000.000

8.2 INSTALACIÓN Y CONFIGURACIÓN DE SSH

Como preámbulo, es importante tener en cuenta que, para garantizar el consumo del servicio, se debe contar previamente con la debida configuración de accesos de seguridad e infraestructura del lado del operador a la petición saliente originada desde los servidores de la SIC al momento de realizar la conexión SSH, esto último con el fin garantizar la visibilidad entre servidores y consecuencia de esto, la transferencia electrónica de expedientes.

Tabla 16. Software requerido SSH

Software Requerido	Descripción
Bitvise SSH Server	Programa que permite acceder a la aplicación de forma remota utilizando un protocolo seguro de comunicación
Sha256sum	Permite generar el hash SHA256 de cualquier archivo por línea de comandos.

Mediante ssh y particularmente con scp se realizará la transferencia de los archivos soporte de las PQRS al servidor de la SIC, de tal manera que se utilicen certificados digitales para la autenticación con el servicio de radicación de apelaciones de la SIC, para permitir esto debe realizar los siguientes pasos, teniendo en cuenta que para el caso de Windows es necesario instalar inicialmente el servidor SSH.

1. Descargar el servidor SSH para Windows denominado BitVise, de la URL <http://www.bitvise.com/download-area>, asegúrese de bajar el servidor ssh tal como lo muestra la siguiente imagen:

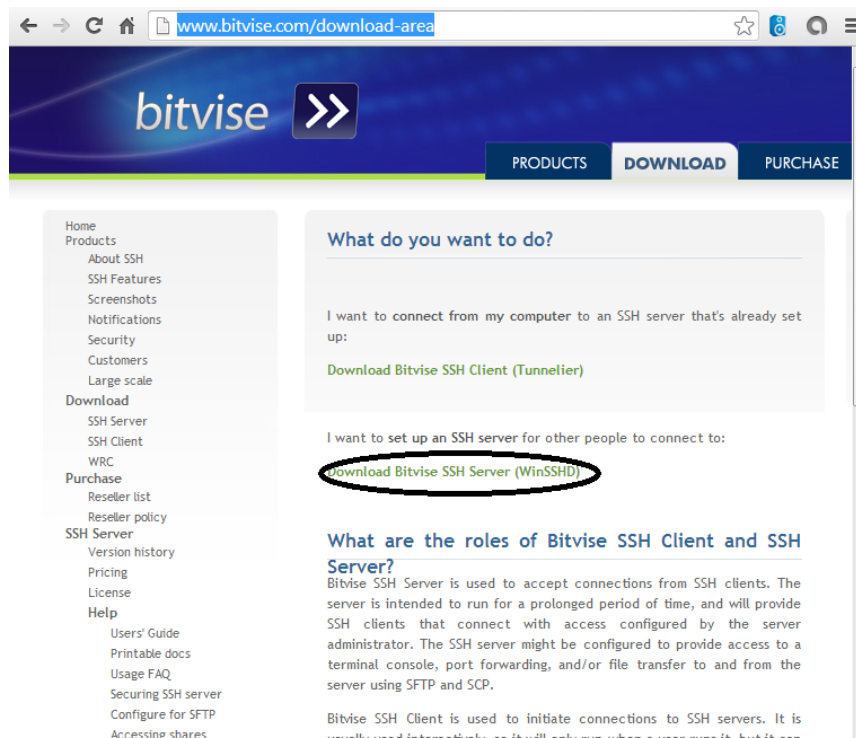


Imagen 15. Página inicial de descarga de bitvise

2. Seleccione el instalador de SSH disponible en la página:

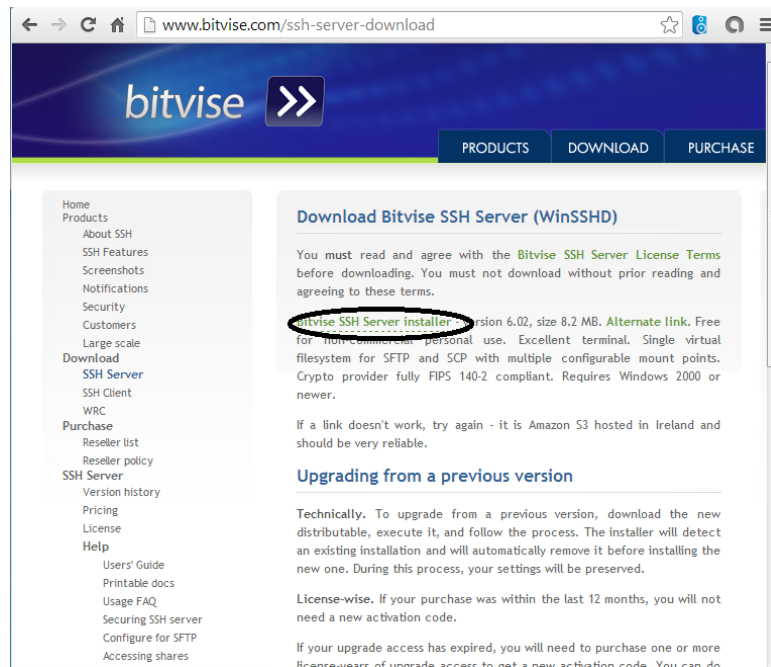


Imagen 16. Seleccionar instalador de Bitvise

3. Ejecute el instalador que se descargó en el paso anterior (**como usuario administrador**), por ejemplo BvSshServer-Inst.exe:

Nombre ^	Fecha de modificación	Tipo	Tamaño
BvSshServer-Inst	30/08/2013 03:21 p...	Aplicación	8.430 KB
msvcr71	30/08/2013 11:18 a...	Archivo WinRAR ZIP	180 KB
pcapy-0.10.8.win32-py2.5	30/08/2013 11:19 a...	Aplicación	80 KB
pypk_v0.2.tar	30/08/2013 11:18 a...	Archivo WinRAR	167 KB
python-2.5.4	30/08/2013 11:20 a...	Paquete de Window...	11.058 KB
WinPcap_4_1_3	30/08/2013 11:19 a...	Aplicación	894 KB

Imagen 17. Instalador de Bitvise

4. Al iniciar el instalador se le solicitará validar la fuente:

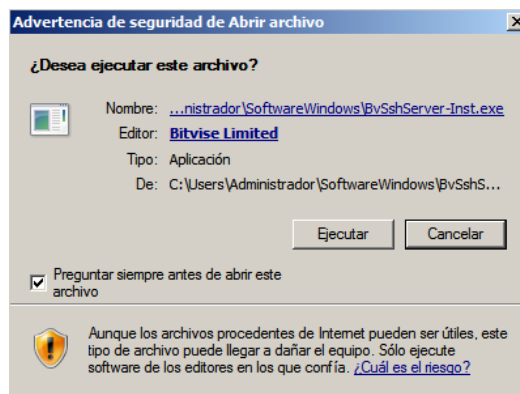


Imagen 18. Validar fuente de Bitvise

5. Se mostrará la pantalla inicial de la instalación. Acepte la licencia de la aplicación, seleccione la opción de instalar un nuevo servidor SSH indicando "Install net Bitvise SSH Server Site" y la subopción "Install new default site (Bitvise SSH Server)", no cambie el directorio de instalación, seleccione la opción de "Run Bitvise SSH Server Control Panel when done" y presione el botón "Install":

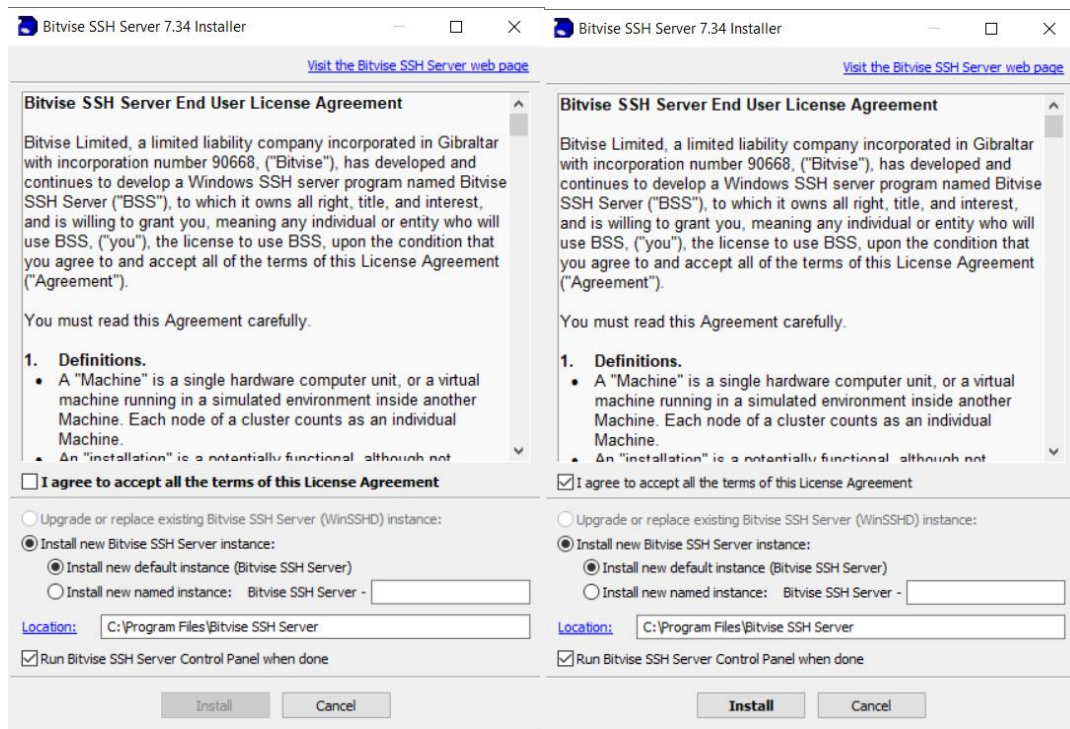


Imagen 19. Opciones de instalación de Bitvise

6. Seleccione el tipo de edición a instalar, tenga en cuenta que para ambiente de pruebas se puede utilizar “Personal Edition” (incluyendo los datos específicos primer nombre, segundo nombre y apellido), **pero para ambiente de producción debe realizar la compra del producto. Es por ello que para ese ambiente debe seleccionar “Standard Edition”:**

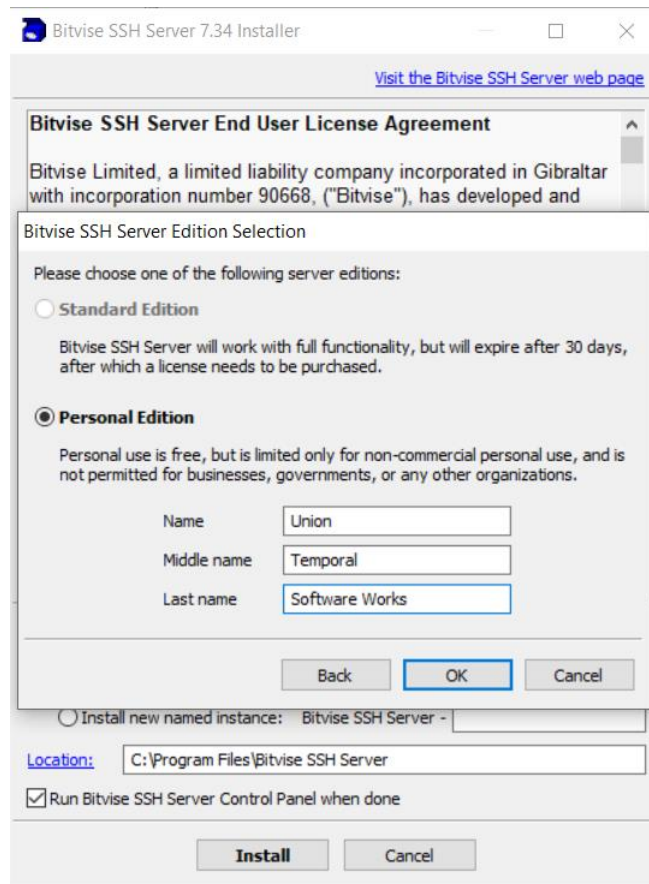


Imagen 20. Tipo de instalación de Bitvise

7. Se iniciará la instalación de Bitvise, al finalizar se mostrará la terminación adecuada, para finalizar simplemente presione el botón “Aceptar”:

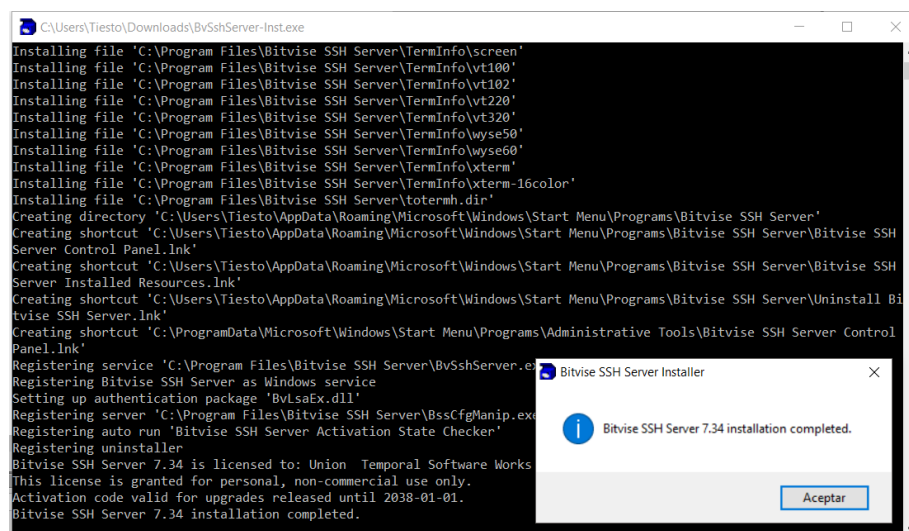
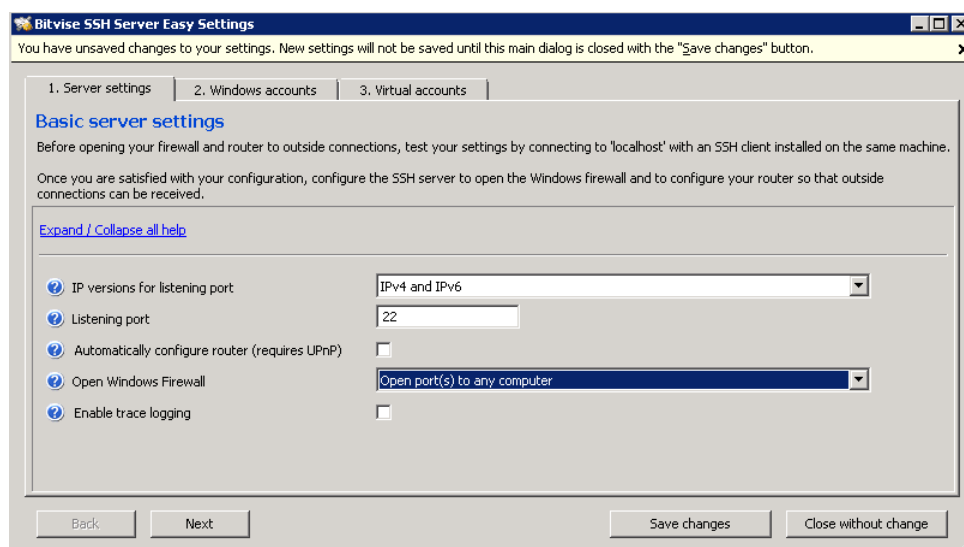
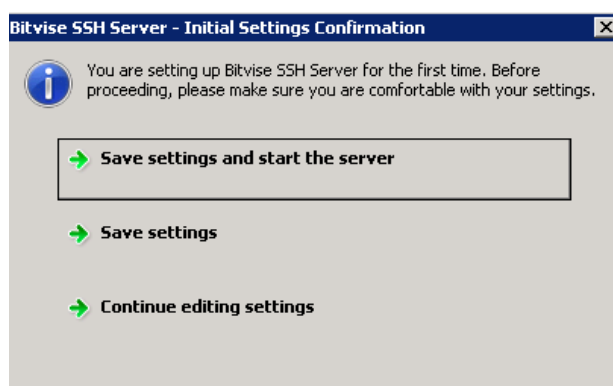


Imagen 21. Fin de instalación de Bitvise

8. Inicialmente abra el puerto 22 para todos los computadores, para poder realizar la prueba inicial, para ello en “Open Windows Firewall” seleccione la opción “Open port(s) to any computer”:

**Imagen 22. Abrir puerto del firewall en Bitvise**

9. Las demás opciones inicialmente debe dejarlas con los valores por defecto, presione el botón “Save changes”.
10. Posteriormente debe indicar almacenar la configuración e iniciar el servidor:

**Imagen 23. Persistir la configuración en Bitvise**

11. El servidor de bitvise debe iniciar adecuadamente y mostrar la siguiente pantalla:

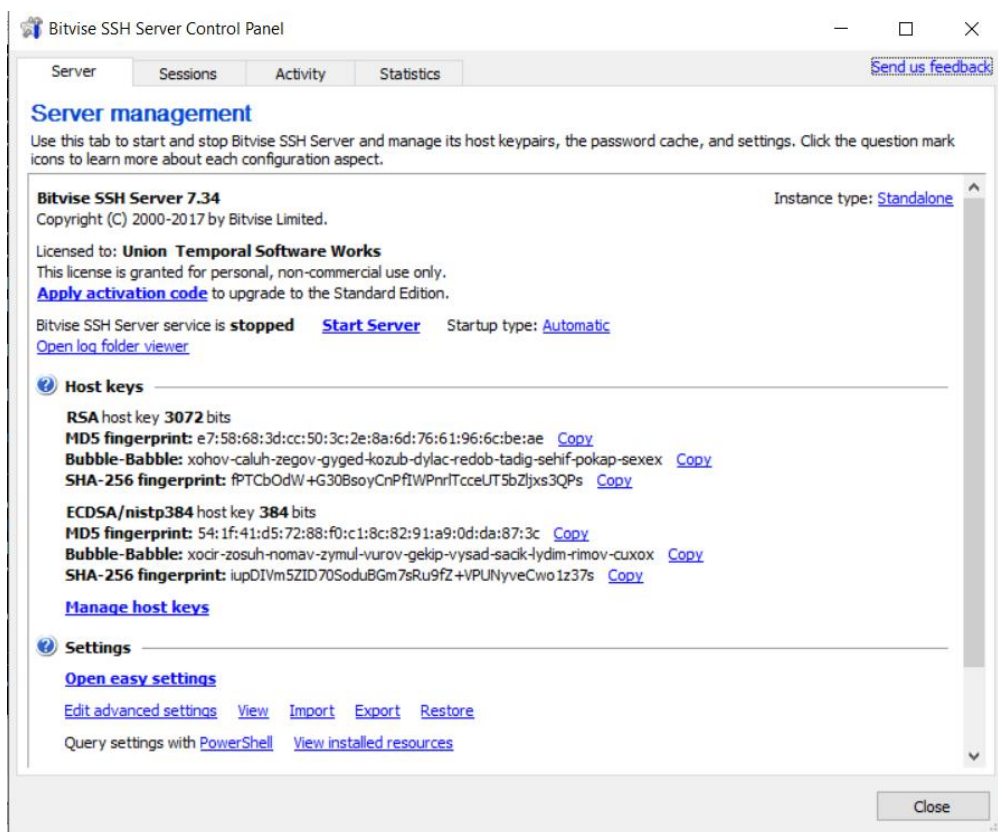


Imagen 24. Inicio del servidor de Bitvise

12. Para realizar la prueba es necesario asegurar la conexión al servidor desde un computador diferente, para ello utilice un cliente ssh en Windows, se sugiere utilizar putty que se encuentra disponible en:

<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>
 Asegurarse de bajar putty<version>-installer.exe

13. Cree una sesión en putty para acceder al servidor: y presione el botón “Open”:

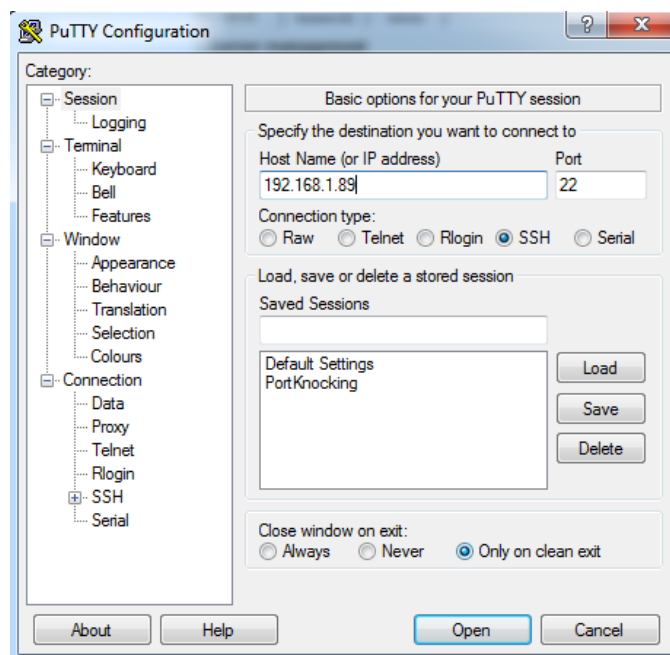


Imagen 25. Creación de sesión en putty

14. Se le solicitará validar la firma que identifica el servidor, simplemente presione el botón "Sí":

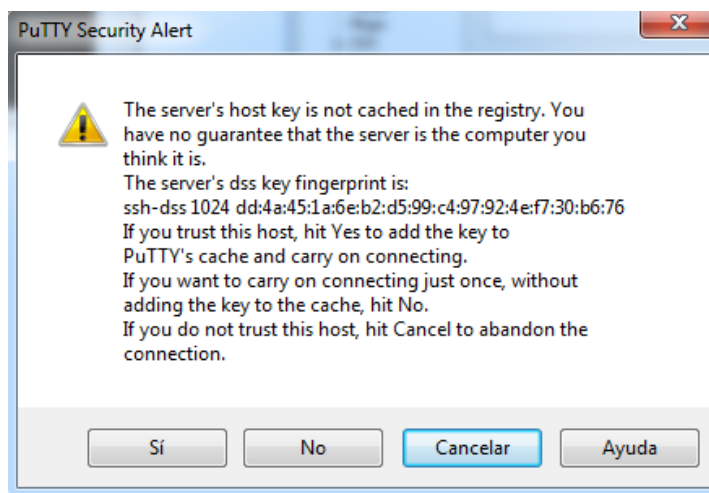


Imagen 26. Validación de llave en putty

15. Se iniciará la sesión SSH en el servidor:



Imagen 27. Inicio de sesión en putty

Con este paso verificará la adecuada conexión al servidor SSH en Windows.

16. Con el fin de permitir la autenticación con llaves, es necesario reiniciar el servidor.
17. Una vez reinicie el servidor abra el Bitvise SSH Server control panel, que fue instalado por el software:

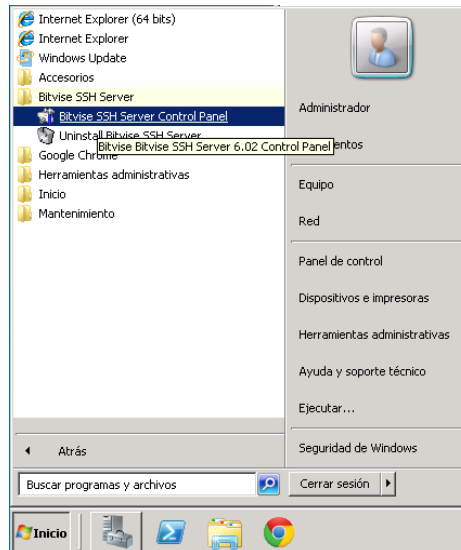


Imagen 28. Abrir control panel de Bitvise

18. A continuación, debe indicar la configuración básica para ello presione el botón “Open easy settings”:

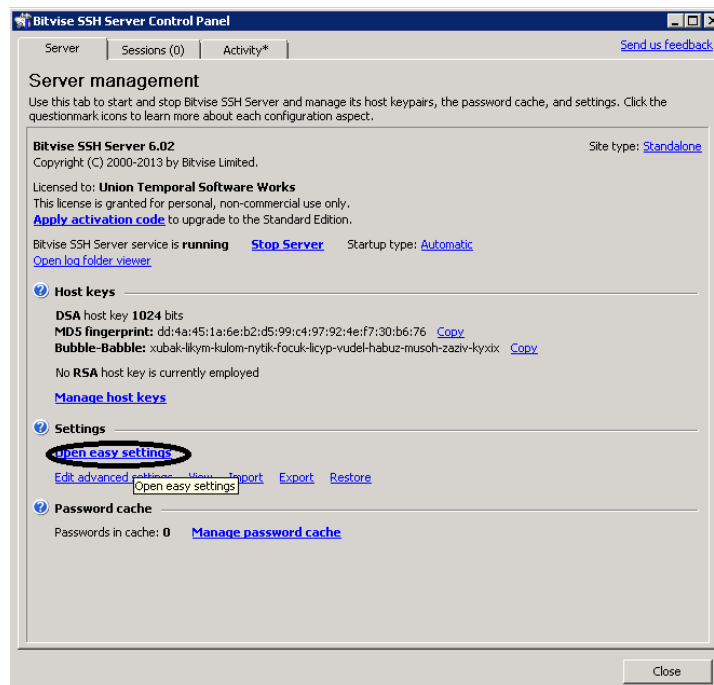


Imagen 29. Control panel de Bitvise

19. Seleccione posteriormente la sección de cuentas virtuales presionando el botón “Virtual accounts”:

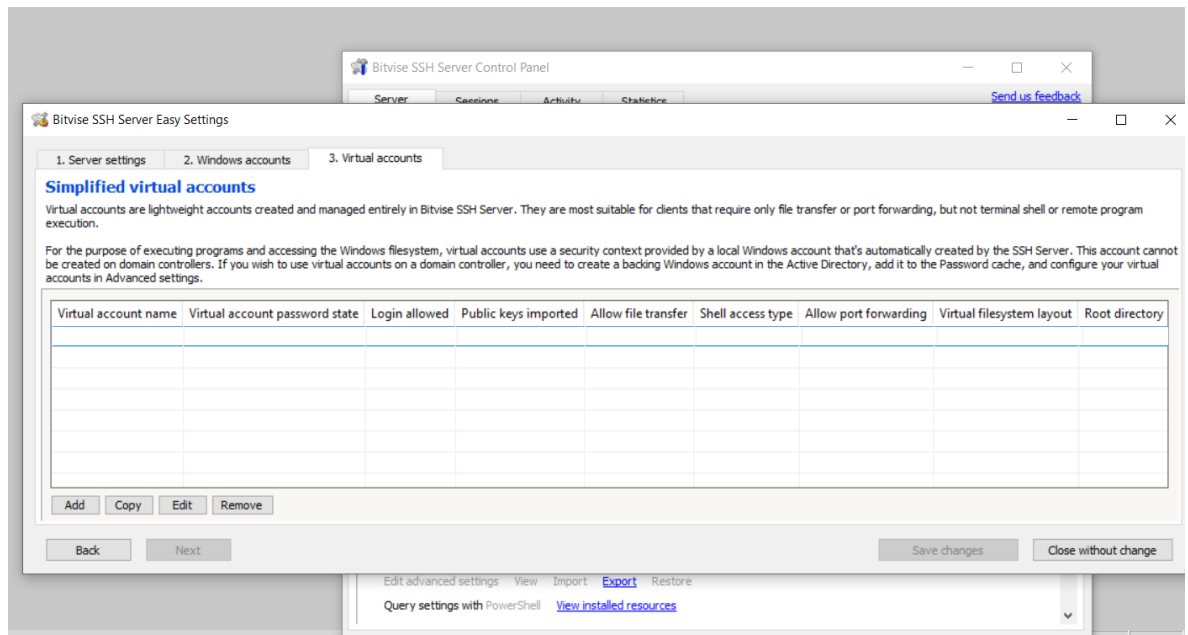


Imagen 30. Cuentas virtuales en Bitvise

20. Adicione una cuenta virtual presionando el botón “Add”:

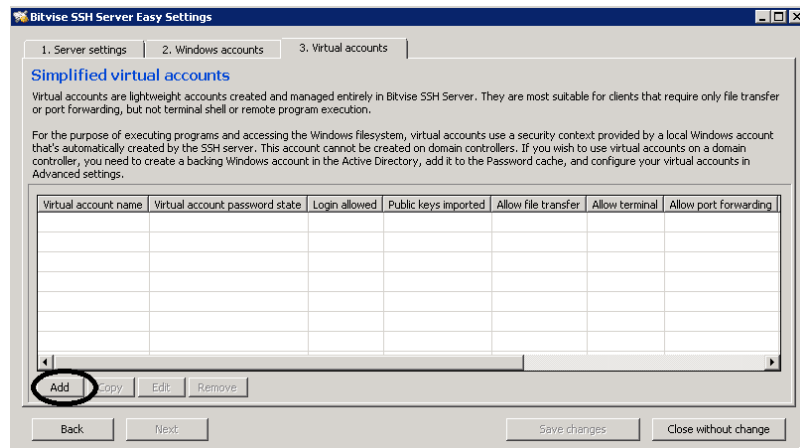


Imagen 31. Adicionar cuenta virtual en Bitvise

21. Agregue un nuevo usuario, para el ejemplo se denominará “pruebaSSH” con el cual se intercambiará la información de los anexos con la SIC, debe informar el nombre del usuario utilizado a la SIC. Igualmente debe darle acceso por terminal seleccionando la opción “Allow file transfer”.
22. Configurar la opción **Command Prompt** para el tipo Shell Access type, al momento de crear el usuario virtual, tal y como se muestra en la siguiente imagen:

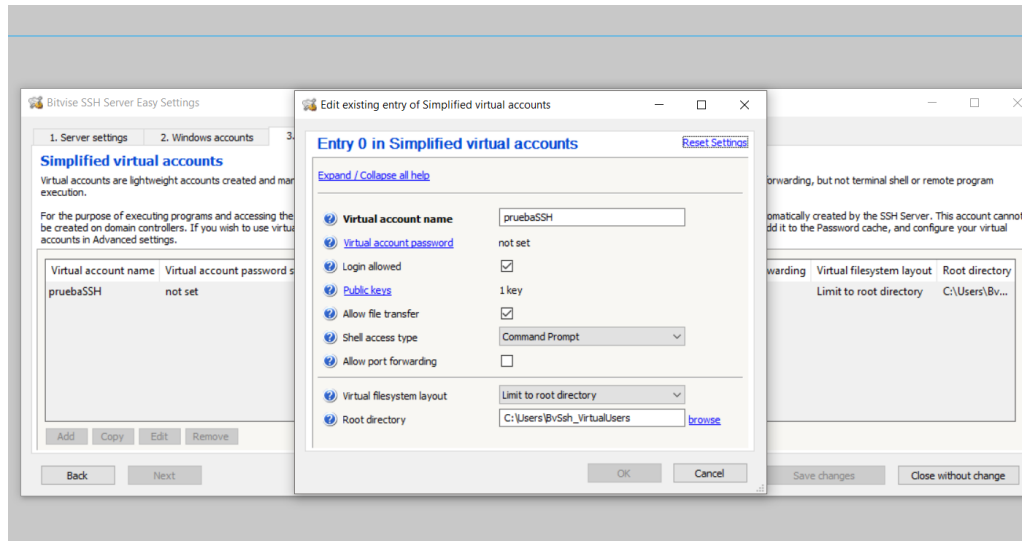


Imagen 32. Datos iniciales de la cuenta virtual en Bitvise

23. Agregue la llave pública enviada por la SIC, para ello haga click en el enlace “Public keys” indicado previamente, posteriormente importe la llave presionando el botón “Import”:

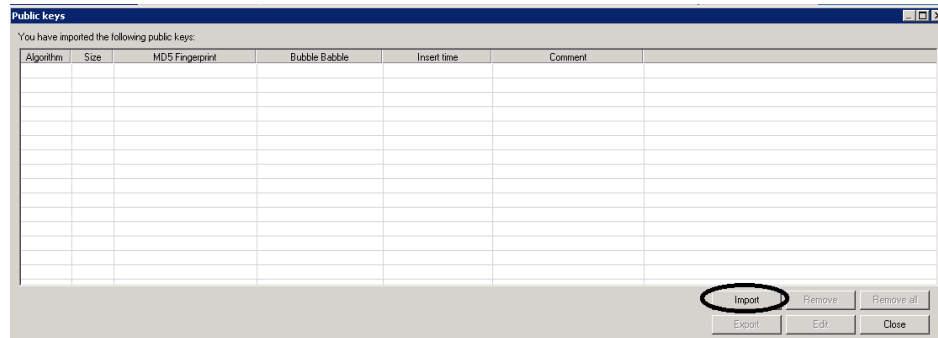


Imagen 33. Importar llave pública en la cuenta virtual en Bitvise

24. Seleccione el archivo que descargo de la llave pública, para el ejemplo se denominará llave publica:

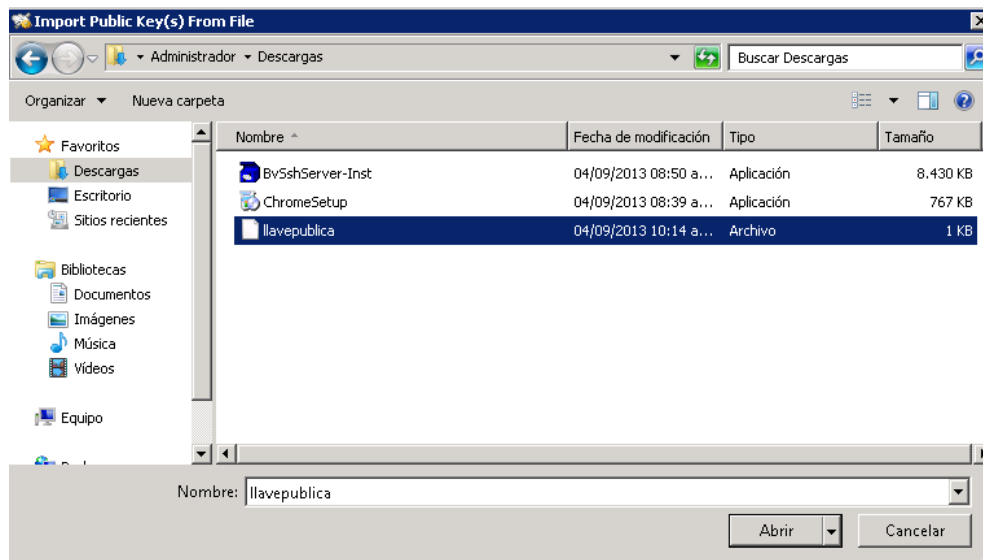


Imagen 34. Seleccionar archivo de llave pública de la cuenta virtual en Bitvise

25. Al abrir el archivo se debe importar la llave y debe observar los datos de ella en la ventana de llaves del servidor:

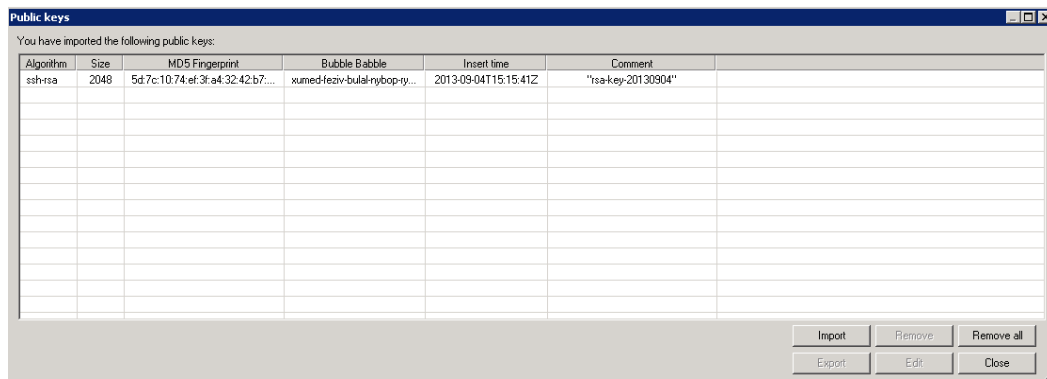


Imagen 35. Resultado de la importación de la llave pública en Bitvise

26. Presione el botón close para continuar con la configuración de la cuenta virtual.

27. En la opción "Virtual filesystem layout" seleccione la opción "Limit to root directory", indique una ruta específica que es donde se alojarán los archivos (allí se colocará el zip) de los archivos anexos, configurar la opción Root directory en la carpeta BvSsh_VirtualUsers ubicada en la ruta **C:\<USERS_WINDOWS>\BvSsh_VirtualUsers** (esta carpeta se crea automáticamente en Windows al momento de instalar el servidor BitVise SSH.). En dicha carpeta se colocarán los archivos a transferir.

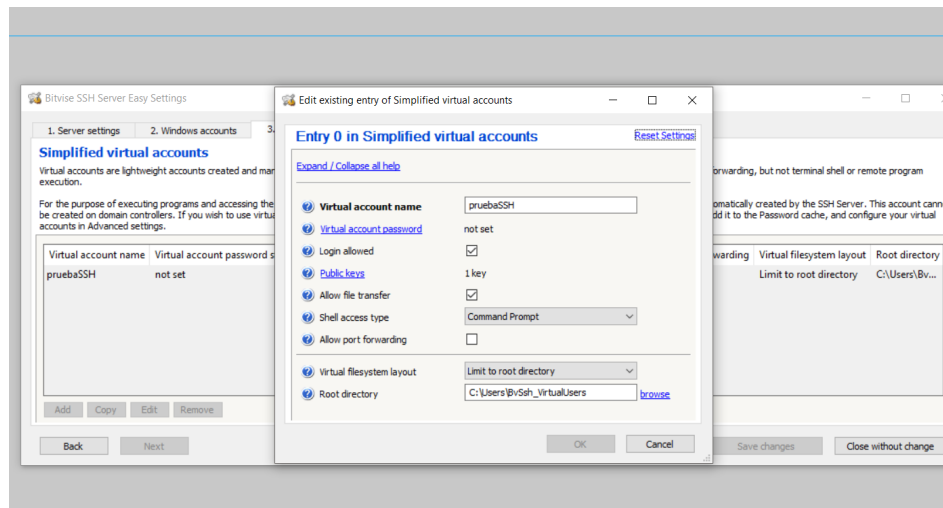


Imagen 36. Datos carpeta archivos de la cuenta virtual en Bitvise

28. Presione el botón “OK” para agregar la cuenta virtual creada.
29. Presione el botón “Save changes” para guardar los cambios sobre las cuentas virtuales.

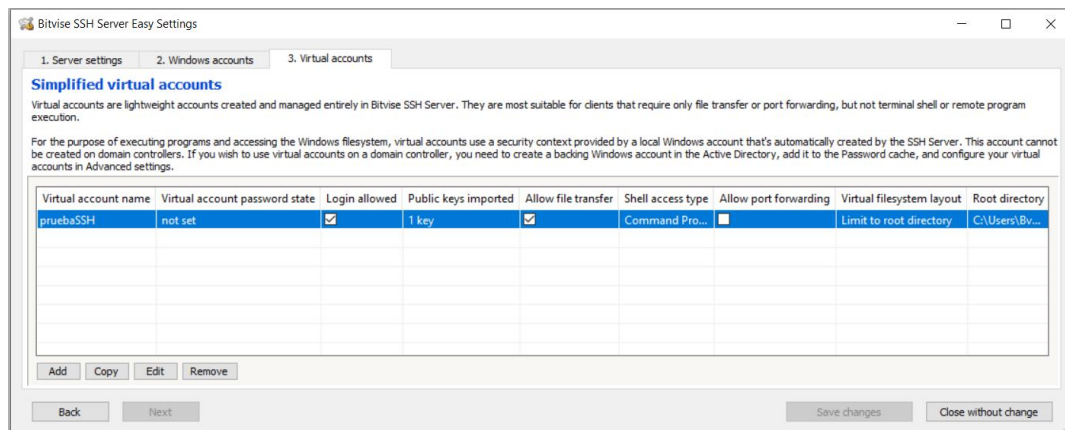
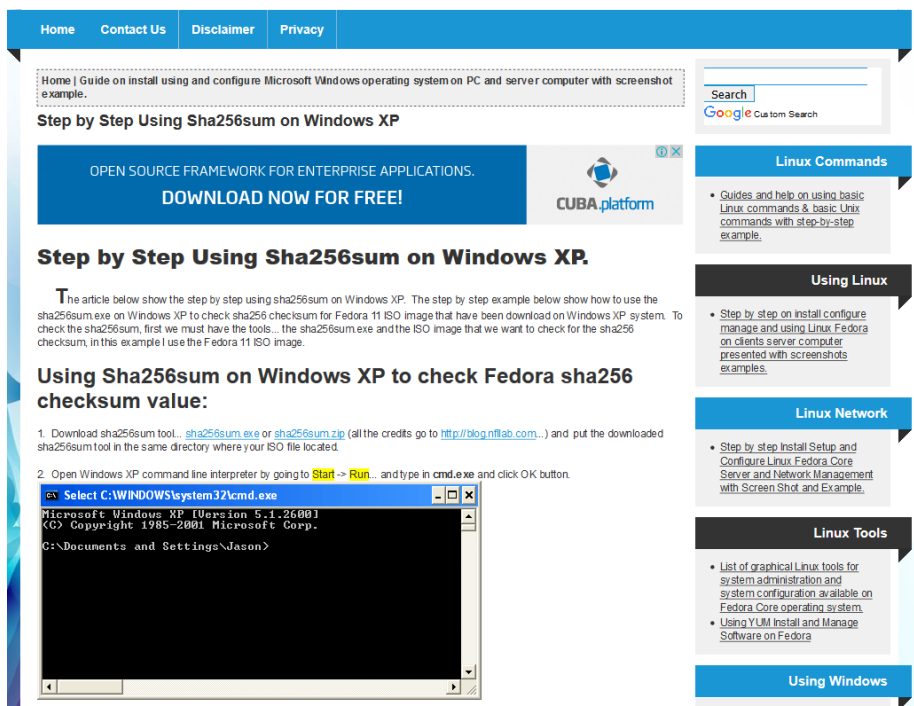


Imagen 37. Guardar la cuenta virtual en Bitvise

30. Descargar la herramienta **sha256sum.exe** de la siguiente url http://www.labtestproject.com/using_windows/step_by_step_using_sha256sum_on_windows_xp.html y colocar dicho archivo en la carpeta **BvSsh_VirtualUsers** ubicada en la ruta **C:\<USERS_WINDOWS>\BvSsh_VirtualUsers**. El propósito de dicha operación es generar el hash asociado al archivo mediante sha256 mediante la herramienta sha256sum.exe independientemente del sistema operativo Windows instalado.



Home | [Contact Us](#) | [Disclaimer](#) | [Privacy](#)

Home | Guide on install using and configure Microsoft Windows operating system on PC and server computer with screenshot example.

Step by Step Using Sha256sum on Windows XP

OPEN SOURCE FRAMEWORK FOR ENTERPRISE APPLICATIONS.
DOWNLOAD NOW FOR FREE!

Step by Step Using Sha256sum on Windows XP.

The article below show the step by step using sha256sum on Windows XP. The step by step example below show how to use the sha256sum.exe on Windows XP to check sha256 checksum for Fedora 11 ISO image that have been download on Windows XP system. To check the sha256sum, first we must have the tools... the sha256sum.exe and the ISO image that we want to check for the sha256 checksum. In this example I use the Fedora 11 ISO image.

Using Sha256sum on Windows XP to check Fedora sha256 checksum value:

- Download sha256sum tool... [sha256sum.exe](#) or [sha256sum.zip](#) (all the credits go to <http://blog.nflab.com...>) and put the downloaded sha256sum tool in the same directory where your ISO file located.
- Open Windows XP command line interpreter by going to **Start -> Run...** and type in `cmd.exe` and click OK button.

```

Select C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Jason>

```

Linux Commands

- Guides and help on using basic Linux commands & basic Linux commands with step-by-step example.

Using Linux

- Step by step on install, configure manage and using Linux Fedora on clients server computer presented with screenshots examples.

Linux Network

- Step by step Install Setup and Configure Linux Fedora Core Server and Network Management with Screen Shot and Example.

Linux Tools

- List of graphical Linux tools for system administration and system configuration available on Fedora Core operating system.
- Using YUM Install and Manage Software on Fedora

Using Windows

Imagen 38. Descarga de la herramienta sha256Sum.exe

Para verificar la adecuada configuración de la llave pública debe comunicarse con la SIC, solicitando realizar una prueba en la cual se debe asegurar que tenga acceso a la cuenta utilizando certificados digitales y no una contraseña específica.

9 INFORMES

Para el total cumplimiento de las normas referentes al CUN, se debe remitir a esta superintendencia una información periódica y otra información al momento de finalizar la implementación de cada etapa. A continuación, se presenta un cuadro con las características de cada informe.

Tabla 17. Software base requerido ambiente Linux

Nombre del informe	Destinatario	Contenido	Periodicidad
informe de resultados de las pruebas piloto de asignación del CUN	Soporte CUN (soportecun@sic.gov.co)	<ul style="list-style-type: none"> Fecha de realización de la Prueba. Casos a probar. Parámetros. (Parámetros de entrada requeridos para realizar la prueba) Persona(s) que realiza(n) la Prueba. Datos del ambiente de Pruebas (motor base de datos, sistema operativo del servidor de aplicación y del servidor de base de datos). Resultado de la Prueba (Exitoso/No exitoso). Nombre y versión del sistema a probar. (Ej. Sistema PQR v.1.0) 	Una vez terminada la implementación.
informes de avance sobre la ejecución de las actividades técnicas por parte de los operadores para implementar los mecanismos de consulta interactiva	Soporte CUN (soportecun@sic.gov.co)	<ul style="list-style-type: none"> Fecha generación del informe. Fecha inicial y final del periodo a reportar. Cronograma de actividades (actividad, descripción, fecha inicial, fecha final, porcentaje avance, resultado de la actividad). 	Mensual durante la implementación.
informe de los resultados de las pruebas piloto de los mecanismos de consulta interactiva	Soporte CUN (soportecun@sic.gov.co)	<ul style="list-style-type: none"> Fecha de realización de la Prueba. Casos a probar. Parámetros.(Parámetros de entrada requeridos para realizar la prueba) Persona(s) que realiza(n) la Prueba. Datos del ambiente de Pruebas. (motor base de datos, sistema operativo del servidor de aplicación y del servidor de base de datos). 	Una vez terminada la implementación.

		<ul style="list-style-type: none"> • Resultado de la Prueba (Exitoso/No exitoso). • Nombre y versión del sistema a probar. (Ej. Consulta PQR v.1.0) 	
informe de los resultados de las pruebas piloto de los mecanismos de reporte de expedientes de apelaciones ante la SIC	Soporte CUN (soportecun@sic.gov.co)	<ul style="list-style-type: none"> • Fecha de realización de la Prueba. • Casos a probar. • Parámetros. (Parámetros de entrada requeridos para realizar la prueba) • Persona(s) que realiza(n) la Prueba. • Datos del ambiente de Pruebas. (motor base de datos, sistema operativo del servidor de aplicación y del servidor de base de datos). • Resultado de la Prueba. (Exitoso/No exitoso). • Nombre y versión del sistema a probar. (Ej. Consulta PQR v.1.0) 	Una vez terminada la implementación.

10 VALORES DE REFERENCIA

A continuación, se describen los valores de referencia que deberán ser empleados por los operadores para los tipos de datos que se enuncian a continuación. Esta información al igual que la documentación de los campos señalados en el numeral anterior, están conforme al estándar definido para el lenguaje de intercambio de información por el Estado Colombiano, para intercambiar información entre organizaciones, facilitando el entendimiento de los involucrados en los procesos de intercambio de información.

Este componente, dentro del proceso de intercambio de información, es de gran importancia debido a que permite unificar el significado y la estructura de los conceptos a intercambiar, evitando que un mismo concepto tenga diferentes interpretaciones.

A continuación, se indicarán los nombres de estos elementos para su búsqueda en el portal del lenguaje de intercambio de información del Mintic:

Tipo identificación Nacional Persona (Aplicación de uso: tipoldNacionalPersona):

Tabla 18. Tipo Identificación Nacional Persona

CODIGO TIPO IDENTIFICACION NACIONAL PERSONA ALFANUMERICO 2	NOMBRE TIPO IDENTIFICACION NACIONAL PERSONA
RE	REGISTRO CIVIL
TI	TARJETA IDENTIDAD
CC	CÉDULA CIUDADANÍA
CE	CÉDULA EXTRANJERÍA
AS	ADULTO SIN IDENTIFICAR
MS	MENOR SIN IDENTIFICAR

RN	RECIÉN NACIDO
PA	PASAPORTE
DE	DOCUMENTO EXTRANJERO
CD	CARNÉ DIPLOMÁTICO
NI	NÚMERO IDENTIFICACIÓN TRIBUTARIA
ND	NO DEFINIDO
TE	TARJETA DE EXTRANJERÍA
OD	OTRO DOCUMENTO

Tipo Tramite de la Superintendencia de Industria y Comercio (Aplicación de uso: tipoTramiteSic):

Tabla 19. Tipo Trámite SIC

CODIGO TRAMITE	NOMBRE TRAMITE
228	TELEFONIA MOVIL CELULAR
328	OTROS SRVCIOS TELECOMUNICACIONES NO DOMICILIRIAS
383	TELEFONIA FIJA
391	SERVICIOS POSTALES

Estado PQR CUN (Aplicación de uso: estadoPqrCun):

Tabla20. Estado PQR CUN

CODIGO ESTADO PQR CUN	ESTADO PQR CUN
1	TRASLADO A OPERADOR COMPETENTE
2	TRASLADO A LA SIC PARA RESOLVER RECURSO DE APELACIÓN
3	RESUELTO
4	ACUMULADO CON EL CUN
5	ANULADO
6	ANALISIS POR PARTE DEL OPERADOR
7	ANALISIS POR PARTE DE LA SIC
8	ETAPA DE PRUEBAS QUE PRACTICA EL OPERADOR
9	ETAPA DE PRUEBAS QUE PRACTICA LA SIC

11 ACUERDO DE NIVEL DE SERVICIO

Para recibir soporte técnico se establecen los siguientes canales de comunicación:

Correo electrónico: soportecun@sic.gov.co

Teleconferencia: Teams de Microsoft¹³, a través de la cuenta de soporte.

MANEJO DE ERRORES

Tabla 21. Manejo de errores

Error presentado	Acción	Tiempo de respuesta
No se puede establecer comunicación con servicio de la SIC	Informar al área de soporte técnico de CUN mediante correo electrónico.	1 día
Error de validación de datos enviados en el servicio	El servicio retorna un mensaje informando el error presentado. No se acepta la solicitud.	Inmediato
Error de autenticación	El servicio retorna un mensaje informando el error presentado. No se acepta la solicitud.	Inmediato
Error en transferencia de archivos	El servicio envía mensaje de correo electrónico a operador/proveedor y a área de soporte técnico de CUN. No se acepta la solicitud.	Inmediato (Después de procesar la petición de transferencia n veces)
Error en radicación en la SIC	El servicio envía mensaje a área de soporte técnico. En este punto ya se han validado los datos y se ha realizado la transferencia de los archivos, por tanto se acepta la radicación con fecha de la solicitud.	0 a 2 días.

¹³ <https://www.microsoft.com/es-co/microsoft-teams/log-in>

12 GLOSARIO DE TERMINOS

- **CUN:** Es el Código Único Numérico que permitirá a los usuarios de los servicios postales y de comunicaciones identificar en todo momento el trámite de su PQR o de su solicitud de indemnización.
- **PQR:** Petición, queja o recurso formulado por el usuario ante el operador, que contribuye al adecuado ejercicio de sus derechos.
- **Quejoso/Usuario:** Persona natural o jurídica, consumidora de servicios de comunicaciones o postales.
- **SIC:** Superintendencia de Industria y Comercio
- **Solicitud de indemnización:** Solicitud que hace el usuario para que el operador del servicio postal le reconozca el pago de las indemnizaciones consagradas en el artículo 25 de la Ley 1369 de 2009.
- **CRC:** Comisión de Regulación de Comunicaciones.
- **Logs:** Equivalente a la palabra bitácora, es un registro oficial de eventos durante un rango de tiempo en particular, usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué.
- **No repudio:** Suministra la prueba de integridad y el origen de los datos en una relación infalsificable, pueden ser identificados por un tercero en cualquier momento.
- **NTC-27001:** Técnicas de seguridad. Sistemas de gestión de seguridad de la información (SGSI). Requisitos Brinda un modelo para el establecimiento, implementación operación, seguimiento, revisión, mantenimiento y mejora de un (SGSI).
- **Transfer Protocol (SMTP),** o protocolo simple de transferencia de correo electrónico. Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras.
- **XML Signature:** Es una recomendación del W3C (World Wide Web Consortium) que define una sintaxis XML para la firma digital. Está orientada hacia la firma de documentos XML. Asegura la integridad de partes de documentos XML transportados. Representa un sistema que a través de una firma digital permite ofrecer autenticidad de los datos. Con la firma digital se confirma la identidad del emisor, la autenticidad del mensaje y su integridad, sin olvidar que los mensajes no serán repudiados.
- **SHA1:** (Secure Hash Algorithm, Algoritmo de Hash Seguro) es un sistema de funciones hash criptográficas para calcular un código resumen de un mensaje o documento electrónico de 160 bits. Este código es el que se usa para proteger los ficheros contra modificaciones no autorizadas (preservar su integridad).
- **RSA-SHA1:** RSA es un sistema criptográfico de clave pública para el cifrado y la autenticación. RSA se combina con la función de hash SHA1 para firmar un mensaje.
- **wsu Timestamp:** Timestamp (estampado cronológico) es una secuencia de caracteres, que denotan la hora y fecha (o alguna de ellas) en la cual ocurrió determinado evento. Este elemento permite marcas de tiempo para aplicar en cualquier parte, incluso como un encabezado SOAP (Simple Object Access Protocol).
- **TLS (Transport Layer Security):** Es un protocolo criptográfico que proporciona comunicaciones seguras por una red. Establece una conexión segura por medio de

un canal cifrado entre el cliente y servidor. Así el intercambio de información se realiza en un entorno seguro y libre de ataques.

- **Contrato de servicio o wsdl:** WSDL (en ocasiones leído como como wisdel) son las siglas de Web Services Description Language, un formato XML que se utiliza para describir servicios Web. La versión 1.0 fue la primera recomendación por parte del W3C y la versión 1.1 no alcanzó nunca tal estatus. La versión 2.0 se convirtió en la recomendación actual por parte de dicha entidad.

WSDL describe la interfaz pública a los servicios Web. Está basado en XML y describe la forma de comunicación, es decir, los requisitos del protocolo y los formatos de los mensajes necesarios para interactuar con los servicios listados en su catálogo. Las operaciones y mensajes que soporta se describen en abstracto y se ligán después al protocolo concreto de red y al formato del mensaje.

Así, WSDL se usa a menudo en combinación con SOAP y XML Schema. Un programa cliente que se conecta a un servicio web puede leer el WSDL para determinar qué funciones están disponibles en el servidor. Los tipos de datos especiales se incluyen en el archivo WSDL en forma de XML Schema. El cliente puede usar SOAP para hacer la llamada a una de las funciones listadas en el WSDL. El WSDL nos permite tener una descripción de un servicio web. Especifica la interfaz abstracta a través de la cual un cliente puede acceder al servicio y los detalles de cómo se debe utilizar.

- **RPU:** Régimen de Protección de Usuarios de Comunicaciones.
- **RPUSP:** Régimen de Protección de Usuarios de Servicios Postales.
- **Administrador:** Representa a cualquier persona que desea administrar los parámetros configurados para la solución
- **Operador:** Representa a cualquier persona que desea radicar una apelación.
- **SOAP:** Es el tipo de servicio que se expone para la comunicación entre capas.
- **GEL-XML:** Establece el estándar para estructurar la información para intercambio de información con otras entidades.
- **SSH:** Representa el tipo de protocolo de transferencia de archivos que se llevara a cabo con el operador cuando el servicio está accesible para realizar el intento de conexión una vez el port knocking fue exitoso.
- **Plataforma Operador:** Es el componente externo desde donde se radican las apelaciones y/o se obtienen los archivos de soporte de la radicación.
- **BITWISE:** Es un servidor SSH para Windows que implementa tanto el uso de ssh como de SCP en Windows.
- **FIREWALL (Cortafuegos):** Un cortafuegos es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.¹⁴
- **IPTABLES:** Son las tablas que provee el cortafuegos/firewall del kernel de Linux¹⁵
- **PUTTY:** PuTTY es un cliente SSH, Telnet, rlogin, y TCP raw con licencia libre.¹⁶
- **SCP:** Secure Copy o SCP es un medio de transferencia segura de archivos informáticos entre un host local y otro remoto o entre dos hosts remotos, usando el protocolo Secure Shell (SSH).¹⁷

¹⁴ Tomado de [http://es.wikipedia.org/wiki/Cortafuegos_\(inform%C3%A1tica\)](http://es.wikipedia.org/wiki/Cortafuegos_(inform%C3%A1tica))

¹⁵ Tomado de <http://en.wikipedia.org/wiki/Iptables>

¹⁶ Tomado de <http://es.wikipedia.org/wiki/Putty>

¹⁷ Tomado de http://es.wikipedia.org/wiki/Secure_Copy

- **SSH:** (Secure SHell) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red.¹⁸
- **URL:** Hace referencia a una dirección virtual que representa la ubicación de un recurso.

Elaboró: Sebastian Montes / Norberto Villegas

Revisó: Jaroslav López

Aprobó: Francisco Andrés Rodríguez Eraso

¹⁸ Tomado de <http://es.wikipedia.org/wiki/Ssh>