Proceso y/o tema auditado	Ciclo de vida y Reingeniería de Sistemas de Información.		
Nombre y Cargo de los Auditados	Dolly Esperanza Ovalle Carranza, Jefe OTIC		
Equipo auditor	Pedro Fabian Acosta Vizcaya, pacostav@minsalud.gov.co Yolanda Maria Gomez Bello, ygomezb@ minsalud.gov.co Hector Bello Gomez, hbello@ minsalud.gov.co		
Objetivo auditoria	Validar el cumplimiento del procedimiento "realización de Cruces y extracción de Datos" con énfasis en los requerimientos referentes a las Base de Datos Única de Afiliados (BDUA) y el Sistema de Afiliación Transaccional (SAT), generados por parte de las dependencias del Ministerio o entidades que por su competencia requieren esta información.		
Alcance auditoria	Inicia con la verificación de los requerimientos entrantes, a través del procedimiento; "realización de Cruces y extracción de Datos"; enfocados en la Base de Datos Única de Afiliados y el Sistema de Afiliación Transaccional, generados durante la vigencia de 2019.		
Periodo de la auditoria	Nov-Dic de 2019	Lugar	Ministerio de Salud y Protección Social.

Introducción y contextualización

- **INTRODUCCIÓN Y ANTECEDENTES**

La Oficina de Control Interno se permite presentar el informe preliminar de Auditoria al proceso "Ciclo de vida y Reingeniería de Sistemas de Información" desde el procedimiento de "Realización de Cruces y Extracción de Datos"; con énfasis tanto en el cumplimiento del procedimiento como lo relacionado en la manera de entregar la información que tiene el MSPS sobre la *Base de Datos Única de Afiliados* ***BDUA.*** Esta auditoria fue realizada desde el día 15 de noviembre de 2019 hasta el 15 de diciembre de 2019, frente a la verificación de los requerimientos entrantes, a través del procedimiento CVSP02, BDUA y el Sistema de Afiliación Transaccional - SAT, generados durante la vigencia de 2019.

El Sistema de Afiliación Transaccional - SAT, iniciado desde el 2015 con la puesta en operación del portal www.miseguridadsocial.gov.co, con un desarrollo gradual y progresivo, hoy tiene en operación funcionalidades como traslados entre EPS, movilidad entre regímenes, inclusión y exclusión de beneficiarios y avanza en el desarrollo de otras funcionalidades en salud, en temas como riesgos laborales y creando capacidad para integrar a las Cajas de Compensación Familiar, bajo el marco de los siete macro proyectos incluidos en el PETI vigente.

Otro de estos macro proyectos se basa en el Sistema de Gestion de Datos o Bodega de Datos del SISPRO, repositorio con más de 37.500 millones de registros provenientes de 45 fuentes, que genera 2.730 indicadores de actualización periódica. El uso de esta información es cada vez mayor, con 740.000 consultas promedio mes a los cubos de información (mayo 2019) https://www.sispro.gov.co/Pages/Home.aspx, Este Sistema de información de datos de salud recibe insumo e información por parte del BDUA, a través de un funcionario de la Oficina de Tecnologías de la Información de Comunicaciones.

Con las anteriores acciones se busca la unificación de la información, centrada en el ciudadano y la disposición oportuna de la misma. Durante esta auditoría, frente a la validación, las entrevistas y la búsqueda de información, se

identificó que los principales logros obtenidos durante los últimos años, se concluyen en:

- Disposición de información al ciudadano sobre sus atenciones de salud.
- Unificación de información a través de articulación de bases de datos.
- Desarrollo de sistemas transaccionales.
- Implementación de la estrategia de Gobierno En Línea – GEL y evolución a Gobierno Digital

Un logro fundamental es que, por primera vez, el ciudadano puede consultar información de sus atenciones de salud. En el 2016 el Ministerio dispuso información de salud de la persona, a la cual sólo puede acceder el ciudadano plenamente identificado en www.miseguridadsocial.gov.co, para garantizar el habeas data y la protección de datos personales. Esto a partir de la disposición de un conjunto de Datos Básicos de la Historia de Salud del Ciudadano, que hacen parte de la Historia Clínica, los cuales facilitarán el acceso, la oportunidad y la disponibilidad de los datos para su atención en salud, a través de mecanismos electrónicos o digitales. La disposición de variables para consulta, que se ha efectuado en forma gradual, permite que a la fecha el ciudadano pueda consultar datos actualizados de 32 variables relacionados con consultas, procedimientos, hospitalizaciones y urgencias de los dos últimos años, datos de residencia, actividad económica, consulta de sus aportes al sistema general de seguridad social, condición de discapacidad, víctima, antecedentes en salud, entre otras.

Dentro de los objetivos más importantes esta la unificación de información a través de la articulación de bases de datos. El Ministerio avanza en la estandarización y el intercambio de datos entre diferentes bases que tienen como unidad de análisis al ciudadano, entre ellas los datos de afiliación con los de atenciones en salud, condición de discapacidad, aportes, subsidios, entre otros, que permiten tener la trazabilidad de la persona en el Sistema y proporcionan información para el seguimiento al goce efectivo del derecho a la salud, en cumplimiento de la Ley Estatutaria de Salud.

Para lo anterior, desde el 2014 se inició la construcción de la tabla de evolución de documento de identificación que correlaciona los distintos documentos de una persona a lo largo de su vida. Esta tabla automatizada, de actualización semanal, permite contar con información de afiliados únicos al Sistema de Salud, a través del serial único de identificación. El uso del serial ha permitido la depuración de la Base de Datos Única de Afiliados a Salud – BDUA, de tal forma que la información del 97% de los afiliados que conforman la BDUA coincide con la información de referencia de identificación reportada por la Registraduría Nacional del Estado Civil - RNEC en el caso de los nacionales y Migración Colombia en el caso de los extranjeros, incluidos los permisos especiales de permanencia – PEP otorgados a los migrantes de la República Bolivariana de Venezuela. Esta información permite un mayor control en el giro de recursos en los regímenes contributivo y subsidiado y el control de fallecidos en los procesos de pensiones, en la solicitud de medicamentos o en la elaboración de prescripciones por profesionales de la salud.

El serial único de identificación constituye la base para la articulación de los diferentes sistemas y la unificación de información de Salud y Protección Social. Los aplicativos que hoy operan con el serial único de identificación son: Base de Datos Única de Afiliados a Salud – BDUA, Sistema de Afiliación Transaccional – SAT, Registro de Prescripción en línea MIPRES NoPBS, Sistema de Gestión de Datos – SGD (bodega de datos), Registro Único de Afiliados a la Protección Social – RUAF, Registro en línea de Nacimientos y Defunciones - ND, Registros Individuales de Prestaciones de Servicios de Salud - RIPS y, Registro para la Localización y Caracterización de Personas con Discapacidad – RLCPD.

De igual manera el Ministerio trabaja desde el 2014 en la estandarización de datos, necesaria para que los datos en salud, de los cuales dispongan los actores del SGSSS, sean homologados en los aplicativos y medios electrónicos que los intercambien. Bajo esta orientación en el 2015 se expidió la Resolución 3166 de 2015, estándar de datos para medicamentos de uso humano, para facilitar el intercambio de información farmacéutica; la Resolución 2048 de

2015, catálogo enfermedades huérfanas; la Circular 24 de 2015, catálogo común de patologías para el Registro Individual de Prestación de Servicios de Salud – RIPS. En el 2016, 17 tablas de referencia de medicamentos fueron publicadas y/o actualizadas con datos estandarizados, dentro del proceso adelantado con diferentes dependencias del Ministerio para la entrada en operación del registro en línea de MiPRES y, entre el 2017 y 2018 se tienen publicadas en el Repositorio Institucional Digital – RID, para consulta por el público, los catálogos consolidados de variables de 83 fuentes de información, de flujos de información correspondientes a 21 fuentes y de siglas (361), en http://url.minsalud.gov.co/catalogos-minsalud.

NORMATIVIDAD APLICABLE

- **Decreto 1151 de 2008** "Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones"
- **Decreto 2693 de 2012**. "Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, Y se dictan otras disposiciones".
- **Decreto 1078 del 26 de mayo de 2015**. "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".
- **Decreto 1008 del 14 de junio de 2018**. "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".
- **Políticas Modelo Integrado de Planeación y Gestión**
- **Ley 1751 de 2015, Estatutaria de Salud**, "Por medio del cual se regula el derecho fundamental a la salud y se dictan otras disposiciones".
- **Ley 1438 de 2011**, "Por medio del cual se reforma el Sistema General de Seguridad Social en Salud y se dictan otras disposiciones".
- **Ley 1581 de 2012**, "Por la cual se dictan disposiciones generales para la protección de datos personales".
- **Decreto 4107 de 2011**, "Por el cual se determinan los objetivos y la estructura del Ministerio de Salud y Protección Social y se integra el Sector Administrativo de Salud y Protección Social".
- **Decreto 2573 de 2014**, "Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones".
- **MIPG**, "Política de fortalecimiento organizacional y simplificación de procesos Política de Gobierno Digital TIC para la Gestión Política Seguridad Digital".

- **Resolución 1726 de 2019**, "Por la cual se crea el Comité Técnico para el Funcionamiento, Administración y Operación Integral del Sistema de Afiliación Transaccional - SAT en materia de salud y Base de Datos Única de Afiliados - BDUA del Ministerio de Salud y Protección Social

- **1091 de 2015,** "Por la cual se crea el Comité Técnico de la Base de Única de Afiliados - -BDUA del Ministerio de Salud y Protección Social"

- **Resolución 3166 de 2015.** "Por medio de la cual se define y se implementa el estándar de datos para medicamentos de uso humano en Colombia"

- **Ley 1712 de 2014.** "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones"

- **DESARROLLO Y GESTIÓN DE AUDITORIA**

En desarrollo de la auditoría, la técnica inicial implementada fue la revisión de la información documental, posteriormente, se procedió a verificar en campo las evidencias físicas, así como el cumplimiento de los procesos y los procedimientos que se llevan a cabo en cada de las temáticas involucradas dentro del objeto auditado y finalmente se realizó el análisis y evaluación por parte de la Oficina de Control Interno.

En virtud de lo anterior, el proceso implementado en terreno para desarrollar la auditoria, se basó en la siguiente estructura:

- **PROCESO CICLO DE VIDA Y REINGENIERÍA DE SISTEMAS DE INFORMACIÓN**

Este proceso incluye tres necesidades estructuradas para realizar el desarrollo o mantenimiento, para realizar cruces o extracción y para implementar el servicio de mesa de ayuda

Dentro del proceso de auditoria se abarco el procedimiento CVSP02 Realización de Cruces y Extracción de Datos, que busca atender los requerimientos de cruces y extracción, a través de la generación de información, con el propósito de facilitar el análisis y consultas puntuales por parte de las dependencias del Ministerio o entidades que por su competencia requieren esta información.

- **PROCEDIMIENTO: REALIZACIÓN DE CRUCES Y EXTRACCIÓN DE DATOS**

Con el objetivo de evaluar la gestión que se realiza por parte de la OTIC, respecto al procedimiento, se aplicaron entrevistas, mesas de trabajo e inspecciones de soportes, evidenciándose:

Políticas de operación.

En primera medida, la que tiene que ver con: *"El desarrollo de las actividades por parte de Oficina de TIC debe*

atender lo dispuesto en el documento ***GVTS01*** *Lineamientos Generales de Operación para la OTIC.*", es necesario tener en cuenta las siguientes observaciones dentro del documento de los lineamientos:

- En el **Alcance** es conveniente indicar las demás resoluciones que se deben tener en cuenta dentro del decreto 4107 de 2011, teniendo en cuenta que se indica que todos, de manera directa e indirecta, deben ceñirse a las funciones de la OTIC, pero a ellas van relacionas, por ejemplo, políticas, procedimientos, mapa de procesos, entre otros documentos.
- En la política número 2 se hace necesario actualizar el nombre de Ftps por SFTP, ya que los auditados manifestaron que a diferencia del FTP se utiliza una conexión encriptada tanto en la información como en los datos de archivo, como se muestra en la siguiente imagen:

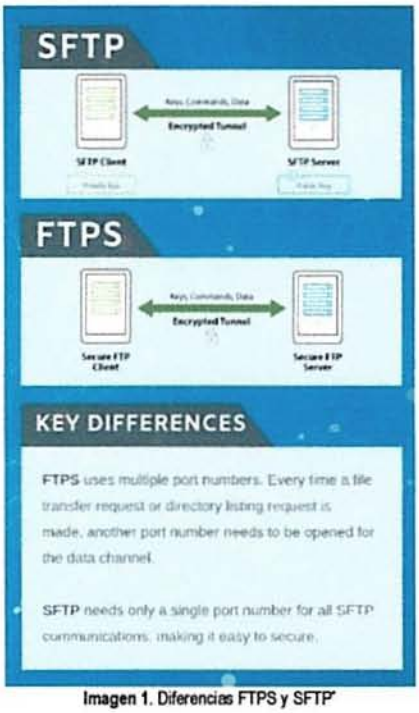

Imagen 1. Diferencias FTPS y SFTP[*]

- Al revisar los lineamientos, de manera específica en lo que tiene que ver en forma expresa en el procedimiento, se observó que se encuentra desactualizado, teniendo en cuenta, por ejemplo en el lineamiento No. 26 convenios para cruces de información y No. 27 Informe de los convenios, en la nota i) menciona que "*El supervisor de un convenio debe tener presente las funciones dispuestas en la Resolución 02133 del 3 de Junio de 2014 del Ministerio de Salud y Protección Social o la que la modifique*" y la resolución en mención ya fue derogada por la resolución 3243 del 5 de septiembre de 2017, con lo cual es conveniente realizar la actualización respectiva, aunque la nota exprese "*o la que la modifique*". También mencionan la resolución en el lineamiento No. 32.
- Así mismo, consultando el link que hace referencia el listado de los convenios dentro del documento, en el lineamiento No. 26, se observó que la página no se encuentra activa, razón por la cual no se pudo evidenciar los convenios que tiene el Ministerio con otras entidades, como lo muestra la imagen 2 a continuación. Sin embargo, estos fueron evidenciados en el enlace

[*] **Ubicado en:** https://www.goanywhere.com/blog/2016/11/23/sftp-vs-ftps-the-key-differences

https://enlinea.minsalud.gov.co/Convenios/, pero al igual la información allí registrada no se encuentra actualizada, debido a solo hay 17 convenios. Imagen 3.

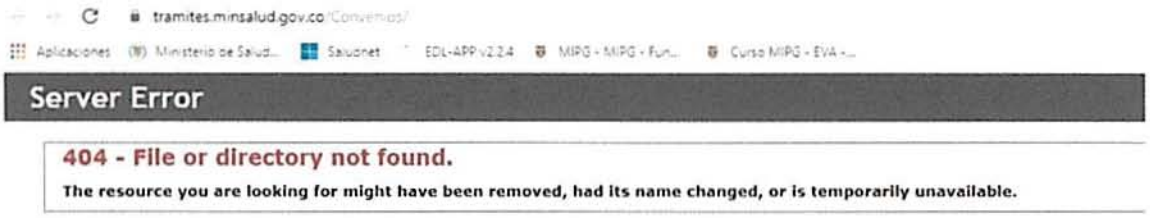

Imagen 2. Error de acceso lineamiento N° 26, tomada en 12/11/2019

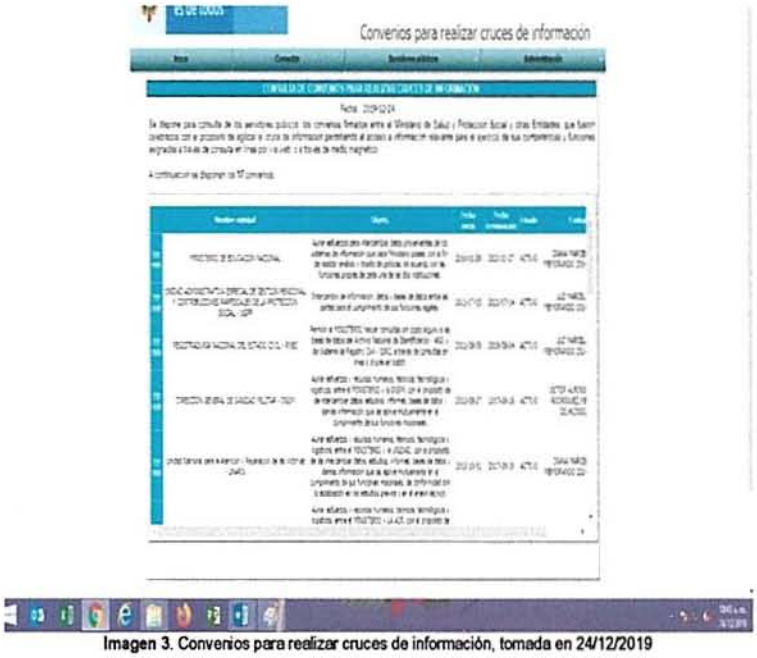

Imagen 3. Convenios para realizar cruces de información, tomada en 24/12/2019

- En el lineamiento No. 11 **Cruces y Entrega de información**. Debe operar conforme a lo establecido en el procedimiento **CVSP02 Realización de Cruces y Extracción de Datos**. Para los cruces de información que van a ser de frecuencia periódica se debe operar según lo descrito en la CVSG03 - Guía para el Cruce o Extracción de Datos, pero al verificar la Guía, ésta tiene expresiones incompletas para la correcta aplicación de los principios a que hace referencia la ley 1581 de 2012. Con lo cual se sugiere actualización.

- Lineamiento No. 23 expresa el cumplimiento de la resolución 2624 de 2013 y esta resolución fue derogada mediante la resolución 2363 de 2018, con lo cual es necesario actualizar.

Finalmente, cuando se realice la actualización, es necesario mirar todo el contexto de los lineamientos para que se ajusten a la actualidad, en cuanto a actos administrativos o documentos que se referencien, para que cualquier funcionario los pueda consultar de manera precisa.

Dentro de la normatividad mencionada en el procedimiento y en la operación de cruces y extracción de datos se menciona la Resolución 1726 de 2019, pero dentro del portal del Ministerio de Salud y Protección Social se identifica que esta resolución tiene error de año de emisión véase imagen 4, es necesario corregir dicho error.

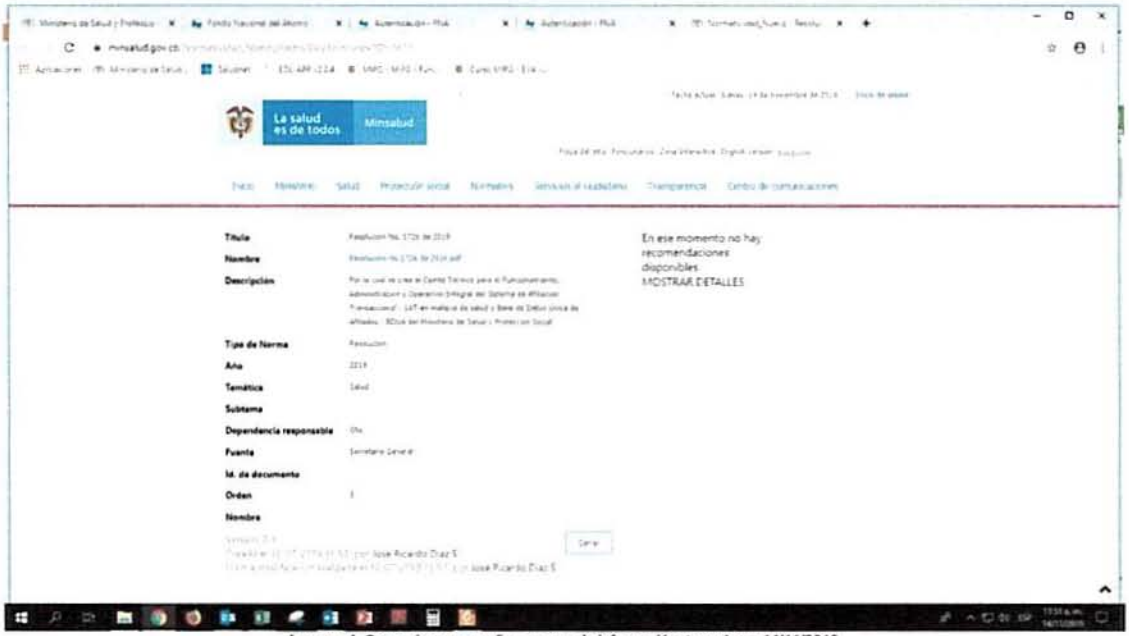

Imagen 4. Convenios para realizar cruces de información, tomada en 14/11/2019

Descripción del procedimiento.

Actividad No. 1. Solicitar la realización de cruces o extracción de los datos.

Esta actividad inicia con la solicitud de los cruces o extracción de datos luego de que, con antelación, las solicitudes asignadas a la OTIC que llegaron por ORFEO hayan sido, distribuidas por temáticas, que son manejadas al interior de la oficina como son:

- Pila
- Registro único de afiliados
- Pisis
- Infraestructura (Contratación relacionada con el tema, seguridad de la información, data center)
- Mipres (prestación servicio de salud)
- SAT
- Gobierno en línea
- BDUA – afiliación
- Consultas uno a uno, DBUA, juzgados
- Mesa de ayuda, servicios de soporte técnico a los aplicativos
- Planeación
- Bodega de datos

Para la solicitud de cruces o extracción de datos, el equipo auditor se enfocó en las temáticas de BDUA y SAT.

De acuerdo con las entrevistas, se informó que todos los requerimientos ingresan por ORFEO, inclusive los que se hacen mediante correo, con lo cual se tiene un control de la información que es necesario generar en los cruces en cuento a BDUA y SAT. De acuerdo a lo anterior se hace necesario actualizar el procedimiento y documentar el medio por el cual se realiza la trazabilidad de dichos requerimientos, específicamente mencionar al gestor de documentación del Ministerio de Salud y Protección Social "ORFEO"

Actividad No. 2. Revisar la solicitud

Esta actividad es realizada por el jefe de la Oficina de Tecnología de la Información y las Comunicaciones - OTIC, el funcionario a cargo de la temática y conjuntamente con la abogada a cargo en la dependencia, determinan la pertinencia o no de la información, acorde con la normatividad y la estructura de la información. Dentro de esta actividad hace falta incluir como responsable el cargo que se tiene para el abogado, debido a que éste hace parte de la definición de la pertinencia de la respuesta al requerimiento de manera positiva o negativa. Lo anterior determina de manera positiva el control que se hace respecto a la entrega de la información que se solicita, sin embargo, este control no se refleja dentro de la actividad.

Se hace necesario generar punto de finalización o control, donde se evidencia la comunicación como respuesta de la solicitud de cruce de información, específicamente cuando la respuesta es "No pertinente".

Actividad No. 3. Generar el archivo de cruce o extracción de datos.

En esta actividad se referencia la "Guía para el cruce o extracción de datos" – CVSG03, cuyo objetivo es "orientar el desarrollo de las actividades para realizar el cruce o extracción de datos básicos de personas de carácter periódico contra bases de datos de sistemas de información misionales o con la bodega de datos de SISPRO".

Dentro de este documento (Guía), hacen referencia a la Ley 1581 de 2012 en cuanto al cumplimiento de los principios de que trata el artículo 4°, los cuales son sintetizados o resumidos de una manera que no se expresa en forma precisa los principios como tal. Un ejemplo de ello es: "Adoptar las medidas técnicas, humanas y administrativas necesarias para asegurar la reserva y confidencialidad de la información", es diferente a expresar: "Adoptar las medidas técnicas, humanas y administrativas para otorgar seguridad a los registros evitando adulteración, pérdida, consulta, uso o acceso no autorizado y fraudulento ...", se hace necesario fortalecer la precisión de los principios de acuerdo a lo establecido en la ley 1581 de 2012, artículo 4°

En cuanto al tema del esquema SFTP para el envío de información, se expresa que deben enviarse los archivos usando el separador pipeline y estar protegidos con una clave de seguridad. Al respecto de esta última, de acuerdo con la entrevista realizada en cuanto a los cruces con información de BDUA, no se genera clave de seguridad, debido a que el envío se hace de manera directa al usuario específico por medio del SFTP, en el cual se maneja usuario y clave, y solo el usuario autorizado tiene acceso, tanto el que envía como el que recibe.
De otra parte, bajo el esquema SFTP, en la guía se mencionan los campos básicos que debe contener el archivo a cruzar, y en la descripción se muestra que hay información no anonimizada y como si esto fuera para todos los archivos que se envían por este esquema.

En la misma guía se contempla el tema de las solicitudes de acceso al FTPS del Ministerio, el cual se maneja de la

siguiente manera:

- Generación de convenios entre entidades externas que requieran el cruce de información y los resultados de la misma. Estos convenios se hacen por escrito y tienen dentro de ellos las consideraciones y características, compromisos que se requieren para poder llevarlos a cabo. Tema mencionado con antelación.
- Por el tamaño de los archivos de información generados se requiere la solicitud oficial de usuarios FTPS por parte de las entidades externas (convenios) o inclusive de dependencias del Ministerio. En la guía, en el numeral "6.1 Solicitud de acceso a FTPS del Ministerio", Nota 3, se expresa "La solicitud deberá realizarse una única ves por cada entidad.", lo cual se considera debe ser evaluado, debido a que los "usuarios" autorizados pueden cambiar, y se requeriría una nueva solicitud.
- Para la creación de usuarios se requiere de la creación de contenedores y al respecto se evidenció que la creación de los contenedores donde están los archivos de información que son compartidos con las entidades o dependencias, son creados por el rol de experto senior, de acuerdo a la verificación del contrato Senior de la compañía **UNE EPM Telecomunicaciones S. A.** firmado mediante Orden de Compra No. 19530 de 2017, en el ámbito del **Acuerdo Marco de Precios para la prestación de Servicios de Nube Privada No. -430- 1 AMP-2016,** con la compañía **UNE EPM Telecomunicaciones S. A.**, cuyo objeto se define como la **ADQUSICIÓN DE LOS SERVICIOS TECNOLOGICOS PARA EL AMBIENTE DE PRODUCCION DE LAS APLICACIONES MISIONALES DEL MINISTERIO DE SALUD Y PROTECCION SOCIAL,** compañía que destina a uno de sus funcionarios (Experto Senior) para que permanezca en la entidad ejerciendo funciones en el ambiente de infraestructura.
- En entrevista se solicitó ver el compromiso de confidencialidad que el Experto Senior de **UNE EPM Telecomunicaciones S. A.** suscribió con dicha empresa, pero se argumentó que este documento es de carácter reservado al cual no se tiene acceso, situación que llama la atención puesto que es este ministerio quien contrata con dicha empresa y debería por lo menos tener una copia digital de este documento en el entendido de que al verse materializado el riesgo este compromiso presta merito probatorio y es una herramienta para un eventual necesidad.
- Otra forma de generar información es la que se hace para las estadísticas en salud, la cual es para consulta de la ciudadanía, pero para ello, cuando se requiere este tipo de información, es necesario crear igual un usuario y capacitar a peticionario en la manera de manejar los cubos de información para obtener la información que requiere.
- Dentro de lo observado de usuarios y los contenedores de almacenamiento de información entregada o recibida, respecto a los cruces o extracción de información relacionada con BDUA, se cuenta a la fecha de la auditoria con los siguientes convenios: Supersalud, Migración Colombia, Colpensiones, Inpec, Policía Nacional Instituto nacional de salud, cuenta de alto costo y ADRES.
- Aun cuando todos los funcionarios o contratistas deben firmar un documento denominado COMPROMISO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE INFORMACIÓN; que exige reserva en el manejo de la información que le es confiada; no deja de ser un potencial riesgo que sea un empleado de la empresa contratista quien tenga una responsabilidad tan delicada como es la asignación de usuarios y contraseñas además de manejar la información que se produce en la OTIC relacionada con herramientas misionales tan sensibles como la contenida en la BDUA o SAT, por mencionar tan solo dos de los Aplicativos Misionales de la entidad.

De igual manera se evidencia la falta de conocimiento frente al procedimiento y uso de formatos del MSPS, por parte de las personas contratadas por la empresa UNE EPM Telecomunicaciones S.A., generando ausencia de calidad, formalismo y control frente a las tareas diarias, referente al marco del mapa de procesos.

Actividad No. 4. Disponer al solicitante el archivo generado

En esta actividad, cada uno de los responsables de las temáticas que tienen que ver con respuesta de envío de información, son quienes disponen de los archivos en los contenedores creados para ese fin. La disposición es de manera inmediata luego de contar con el VoBo tanto del servidor que tiene el cargo el tema jurídico (dentro de la OTIC), como de la Jefe de OTIC, con la respectiva respuesta escrita y enviada por ORFEO.

Por otra parte, dentro de esta actividad se indica que el responsable es el profesional de OTIC asignado a la temática de desarrollo o de bodega de datos, pero no es siempre este profesional, teniendo en cuenta que, para la extracción de datos y cruces de la BDUA, el responsable es el de la temática de BDUA, con lo cual es necesario dejar abierto el responsable a la temática que lo genero.

Actividad No. 5 Verificar el archivo generado.

De acuerdo a lo expresado en esta actividad y a lo aclarado por los funcionarios entrevistados, esta actividad solo aplica para los requerimientos internos (Ministerio), con lo cual es confusa al leerla porque se puede interpretar que luego de que se entrega una información, hacen presencia en el Ministerio para verificar que sí era la correcta, cuando lo que se quiso expresar era que, luego de entregada la información a una dependencia del Ministerio, ésta manifestara si era correcta o no, para realizar los ajustes. Esto conllevaría a que, si se presenta esta situación, con antelación a generar la información, no se realizó una reunión en donde se defina de manera precisa lo que se requiere.

- **BASE DE DATOS ÚNICA DE AFILIADOS (BDUA)**

Acorde con lo encontrado dentro de la realización de la auditoria, de manera expresa, la entidad cuenta con dos funcionarios que se encargan del manejo de cruces o extracción de datos de la BDUA, ellos son de contrato y cuentan con usuarios y perfiles otorgados por la empresa (UNE), que tiene la administración tanto del data center donde se encuentra la base de datos, como de la creación de los usuarios y perfiles de acceso a la información. Aunque esta información es una copia (o fotografía) de la base, es información sensible y de cuidado hacia el manejo y consulta de quienes tienen acceso a ella.

Pero no solamente los funcionarios contratistas bajo el ministerio tienen acceso a la Base de datos, sino contratistas asignados por UNE para la administración del data center, lo cual conlleva a un riesgo de acceso indebido a información, que es necesario que el ministerio valore.

- **SISTEMA DE AFILIACIÓN TRANSACCIONAL (SAT)**

Dispone de información diaria y hay sincronización de la información entre BDUA y SAT, teniendo en cuenta que BDUA recibe información de los entes territoriales, las EPS, entre otros y SAT recibe la información de novedades y seguridad social y afiliaciones, por lo que deben estar sincronizadas para que SAT finalmente maneje toda la información.

Este sistema está en proceso de ser único, lo cual de alguna manera reemplazaría a BDUA, sin embargo, aunque ya está en funcionamiento y en ambiente de producción, se realiza la verificación de su funcionamiento encontrando el

siguiente error:

Imagen 5. Mensaje SAT, al realizar solicitud de novedad, tomada en 26/12/2019

Se evidencia que, al tratar de generar una novedad por parte de un afiliado, el sistema reporta el mensaje de "*1 - El reporte de la novedad ha sido cancelado dado que usted y/o alguno de los beneficiarios, de su grupo familiar, tiene en trámite una novedad reportada en la EPS. Le invitamos a que intente nuevamente en un término de 10 días calendario...*" El mensaje anterior es presentado para cualquier tipo de novedad y esta prueba fue realizada con varios números de cédula.

- RIESGO: "***USO INDEBIDO DE INFORMACIÓN PRIVILEGIADA DURANTE LA GENERACIÓN DE CRUCES O EXTRACCIÓN DE INFORMACIÓN DE LAS BASES DE DATOS DE LOS SISTEMAS DE INFORMACIÓN MISIONALES***"

Dentro de las causas definidas para este riesgo y los controles que se deben llevar a cabo, no se han realizado los propuestos como son:

- Actualización del procedimiento CVSP02 y sus documentos relacionados (GVTS01 – lineamientos generales de operación para OTIC, CVSF05 – anexo técnico para reporte de información) en donde se contemple, por ejemplo, controles e ejecución de procesos de cruces o extracción de información.
- Acuerdos de confidencialidad actualizados
- Actualización de políticas de seguridad
- Control de usuarios habilitados para acceder a las bases de datos
- Cotejar la aplicación del código de ética (integridad) con relación a la gestión de la OTIC semestralmente, mediante el subcomité integrado de gestión.
- Verificación aleatoria de actividades atípicas de las salidas de información
- Verificación de usuarios y accesos a las bases contra el formato SIMF02, SIMF03, que es donde se encuetan los usuarios autorizados e inhabilitados

Aunque este riesgo no se ha materializado, no se pueden dejar de lado el cumplimiento de lo pactado para disminuir o controlar su ocurrencia.

De otra parte, es importante tener en cuenta cómo es el manejo de tanto de los funcionarios que llevan a cabo la

labor de cruces o extracción de información, como de la entidad que tiene todo el control sobre la seguridad de la información que tienen a su cargo.

Este tema tiene que ver también con el diseño, implementación y mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad a la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de la información minimizando a la vez los riesgos de seguridad de la información.

La aplicación de la ISO 27001 es eficaz para la gestión de la información por encargo de otros, por ejemplo, empresas de subcontratación de TI, como es el caso de UNE.

Hallazgos

1. Se evidencio que los lineamientos No. 26 convenios para cruces de información y No. 27 Informe de los convenios del procedimiento *Realización de Cruces y Extracción de Datos*, se encuentran desactualizados, afectando de manera directa al procedimiento respecto a la información documentada y requerida por el Sistema Integrado de Gestión.

2. Durante esta auditoria se evidencio que la información publicada respecto a los convenios que tiene el Ministerio con otras entidades, no se encuentra actualizada, encontrando únicamente 17 convenios. Lo anterior incumple con la Ley de Transparencia y del derecho de acceso a la información pública y con los objetivos establecidos por el MSPS frente a la determinación de las comunicaciones internas y externas.

3. Dentro del proceso de creación de usuarios FTPS por parte de las entidades externas (convenios) o inclusive de dependencias del Ministerio evidenciado durante esta auditoría, se observó que únicamente existe el trámite de manera presencial. Lo anterior incumple con la política de Fortalecimiento Organizacional y simplificación de procesos, del Modelo Integrado de Planeación y Gestión y el objetivo de calidad "Mejorar la agilidad del acceso a los trámites de la entidad" del Ministerio de Salud y Protección Social. Este hallazgo se mantiene, ya que es evidente la necesidad inmediata de generar el procedimiento no presencial manifestado por la OTIC.

Observaciones y/o Sugerencias

1. Dentro de las políticas de operación específicamente en el Alcance es conveniente indicar las demás resoluciones que se deben tener en cuenta dentro del decreto 4107 de 2011, teniendo en cuenta que se indica que todos, de manera directa e indirecta, deben ceñirse a las funciones de la OTIC, pero a ellas van relacionas, por ejemplo, políticas, procedimientos, mapa de procesos, entre otros documentos.

2. En la política número 2 se hace necesario actualizar el nombre de Ftps por SFTP, ya que los auditados manifestaron que a diferencia del FTP se utiliza una conexión encriptada tanto en la información como en los datos de archivo.

3. Teniendo en cuenta que la Guía para el Cruce o Extracción de Datos - CVSG03, hace parte integral del procedimiento CVSP02 Realización de Cruces y Extracción de Datos y que se presenta de manera resumida y para tener en cuenta la correcta aplicación de los principios a que hace referencia la ley 1581 de 2012, es necesario mantener de manera precisa estos principios para que no se desvirtúe su correcta aplicación. (Lo anterior expresado en el lineamiento 11 del documento GVTS01 – Lineamientos Generales de operación para la OTIC.

4. Lineamiento No. 23 expresa el cumplimiento de la resolución 2624 de 2013 y esta resolución fue derogada mediante la resolución 2363 de 2018, con lo cual es necesario actualizar.

5. Es pertinente corregir, en el portal del Ministerio, que la Resolución 1726 de 2019, por la cual se crea el comité técnico para el funcionamiento, administración y operación integral del sistema de afiliación transaccional – SAT, la fecha del documento que lo vincula (imagen 4, parte superior del documento).

6. Acorde con lo informado, el procedimiento inicia con los requerimientos radicados en la herramienta ORFEO, la cual permite tener una trazabilidad de dichos requerimientos, esquema o tema que no aparece referenciado dentro del inicio del procedimiento.

7. Frente a la Actividad de revisar la solicitud, ésta es realizada por la jefe de la Oficina de Tecnología de la Información y las Comunicaciones - OTIC, conjuntamente con el funcionario a cargo de la temática y la abogada a cargo en la dependencia, pero este control y responsabilidad no se encuentran registrados dentro de la actividad y se considera pertinente y positivo respecto a la entrega de la información que se solicita.

8. Así mismo, y como resultado de la anterior observación, se hace necesario generar punto de finalización o control, donde se evidencia la comunicación como respuesta de la solicitud de cruce de información, específicamente cuando la respuesta es "No pertinente".

9. En la actividad de "Generar el archivo de cruce o extracción de datos" se referencia la "Guía para el cruce o extracción de datos" – CVSG03, cuyo objetivo es "orientar el desarrollo de las actividades para realizar el cruce o extracción de datos básicos de personas de carácter periódico contra bases de datos de sistemas de información misionales o con la bodega de datos de SISPRO". Dentro de este documento (Guía), hacen referencia a la Ley 1581 de 2012 en cuanto al cumplimiento de los principios de que trata el artículo 4°, los cuales son sintetizados o resumidos de una manera que no se expresa en forma precisa los principios como tal. Un ejemplo de ello es: "Adoptar las medidas técnicas, humanas y administrativas necesarias para asegurar la reserva y confidencialidad de la información", es diferente a expresar: "Adoptar las medidas técnicas, humanas y administrativas para otorgar seguridad a los registros evitando adulteración, pérdida, consulta, uso o acceso no autorizado y fraudulento...", se hace necesario fortalecer la precisión de los principios de acuerdo a lo establecido en la ley 1581 de 2012, artículo 4°.

10. Para la creación de usuarios se requiere de la creación de contenedores y al respecto se evidenció que la creación de los contenedores donde están los archivos de información que son compartidos con las entidades o dependencias, son creados por el rol de experto senior, de acuerdo a la verificación del contrato Senior de la compañía UNE EPM Telecomunicaciones S. A. firmado mediante Orden de Compra No. 33212 de 2018, en el ámbito del Acuerdo Marco de Precios para la prestación de Servicios de Nube Privada No. -430- 1 AMP-2016, con la compañía UNE EPM Telecomunicaciones S. A., cuyo objeto se define como la ADQUSICIÓN DE LOS SERVICIOS TECNOLOGICOS PARA EL AMBIENTE DE PRODUCCION DE LAS APLICACIONES MISIONALES DEL MINISTERIO DE SALUD Y PROTECCION SOCIAL, compañía que destina a uno de sus funcionarios (Experto Senior) para que permanezca en la entidad ejerciendo funciones en el ambiente de infraestructura. De acuerdo a lo anterior se sugiere que esta operación en infraestructura sea transmitida y se genere conocimiento por parte del funcionario de carrera administrativa del Ministerio, con el fin de minimizar la curva de aprendizaje y no se dependen en su totalidad de un tercero.

11. Respecto al compromiso de confidencialidad que el Experto Senior de UNE EPM Telecomunicaciones S.A. suscribió con dicha empresa se sugiere revisar por qué no se tiene copia digital, almacenada con restricción

reservada. Lo anterior con el fin de conocer el contexto y el alcance frente a la Seguridad de la información de aquel contratante que presenta un servicio para con el Ministerio de Salud y Protección Social de información confidencial y de potencial riesgo.

12. Es de vital importancia para el Ministerio, desde el punto de vista de contratistas y las funciones que ellos tienen, contar con funcionarios de planta o carrera que sean "backup" de las funciones que realizan en casos extremos de no poder contar con ellos. Para el caso específico, nos referimos a quienes manejan el procedimiento auditado desde la información de BDUA. Por lo anterior, en conveniente generar "Gestión del conocimiento" con las actividades que desarrollan. Tema referenciado a dimensión de MIPG.

13. Mediante pruebas de validación del funcionamiento del Sistema de Afiliación Transaccional (SAT), se evidencio que, al tratar de generar una novedad por parte de un afiliado, el sistema reporta el mensaje de "*1 - El reporte de la novedad ha sido cancelado dado que usted y/o alguno de los beneficiarios, de su grupo familiar, tiene en trámite una novedad reportada en la EPS. Le invitamos a que intente nuevamente en un término de 10 días calendario.*" por lo que dicha situación va en contra del objetivo de calidad "Fortalecer los mecanismos de atención al usuario" y mejorar la agilidad del acceso a los trámites de la entidad. Lo anterior dejo de ser hallazgo, ya que la revisión de las funcionalidades de SAT, no estaban definidas dentro del alcance. Sin embargo se recomienda revisar y solucionar dichas inconsistencias de la plataforma.

Fecha de informe de auditoria	28 de Enero de 2020

Nombre y firma del equipo auditor:

Pedro Fabian Acosta Vizcaya

Yolanda María Gómez Bello

Hector Bello Gómez